Guidebook of Prime Numbers

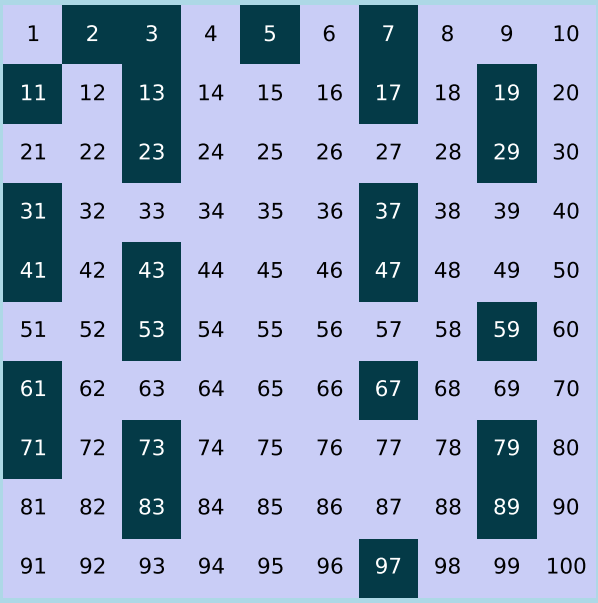
I. Introduction

$$a^{p-1} \overset{p}{=} 1$$

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

$$M_p = 2^p - 1$$

$$2^{136279841} - 1$$



$$(p-1)! + 1 \overset{p}{=} 0$$

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

$$\left(\sum_{p \in \mathbb{P}} \frac{1}{p} \right) \to \infty$$

Taha Sochi

Preface

This book is about prime numbers which is one of the most central subjects of mathematics in general and number theory in particular. The objective of the book is to collect, organize and categorize the most common of our current knowledge about prime numbers in a tidy and concise way. It is important to note the following remarks about this book:

• This is the first volume of this book. Our plan is to expand the book (horizontally and vertically) in each subsequent volume.

• This book (in its first volume) is a concise handbook of prime numbers containing mostly the basic common facts about prime numbers at elementary level, and hence it is mainly useful as a general reference for students and those who are interested in number theory (and prime numbers in particular) at an introductory level. More advanced topics about prime numbers should be sought elsewhere or awaited in the forthcoming volumes.

• The purpose of this book is to fill a gap in the literature of number theory (and prime numbers in particular) which lacks (as far as we know) such a reference.

• The contents of this book (at least in its first volume) are not comprehensive in any way (even at the levels of the volumes of the book) because the topic of prime numbers is huge and extensive. So, we try in this book to collect, categorize and organize the most common knowledge about prime numbers at the intended levels.

• The book (at least in its first volume) does not contain proofs or substantial arguments (let alone exercises or solved problems). Such things may be considered in the forthcoming volumes (depending on the evolving progress and vision as we continue this project).

• There is some repetition of theorems and propositions in some parts and sections of the book due to the involvement of various aspects and considerations in various parts and contexts (such as classifying a given proposition in more than one section depending on its implications). However, we tried to make some variations and distinctions depending on the location and context.

• Some types of the given information in this book are either subject to change (such as the largest known prime number) or they are based on trust and are usually obtained from the Internet (as the only viable source of such information). Therefore, the reader should always double-check these types of information when they are intended for use in serious research or academic work.

• Although the book is about prime numbers, we may occasionally investigate certain aspects of composite numbers (which are the opposite to prime numbers) due to the close relation and interconnection between these two types of numbers. Such casual investigations are generally related to complementary investigations of prime numbers.

• In our view, this book serves as a valuable reference for both lecturers and students of the subject. It is also suitable for general reading by anyone with an interest in mathematics, providing an accessible resource for broadening their understanding and appreciation of the field.

Taha Sochi
London, June 2026

Contents

Preface **1**

Table of Contents **2**

Nomenclature **13**

1 Preliminaries **17**
1.1 Introductory Remarks . . . 17
1.2 The Fascination of Prime Numbers . . . 19
1.3 Basic Facts about Prime Numbers . . . 19
1.4 Generalities about Prime Numbers . . . 21
1.5 Oddities and Exceptions about Prime Numbers . . . 23
1.6 The Infinitude of Prime Numbers . . . 24
1.7 The Fundamental Theorem of Arithmetic . . . 25

2 Types of Primes **27**
2.1 Common Types of Prime Numbers . . . 27
2.1.1 Balanced Primes . . . 27
2.1.2 Bell Primes . . . 28
2.1.3 Carol Primes . . . 28
2.1.4 Catalan Primes . . . 28
2.1.5 Centered Primes . . . 29
2.1.6 Chen Primes . . . 29
2.1.7 Circular Primes . . . 30
2.1.8 Cluster Primes . . . 30
2.1.9 Compositorial Primes . . . 31
2.1.10 Cousin Primes . . . 31
2.1.11 Cuban Primes . . . 31
2.1.12 Cullen Primes . . . 32
2.1.13 Cyclic Primes . . . 32
2.1.14 Cyclotomic Primes . . . 33
2.1.15 Delicate Primes . . . 33
2.1.16 Dihedral Primes . . . 33
2.1.17 Emirp Primes . . . 34
2.1.18 Euler Primes . . . 34
2.1.19 Factorial Primes . . . 35
2.1.20 Fermat Primes . . . 36
2.1.21 Fibonacci Primes . . . 37
2.1.22 Fortunate Primes . . . 37
2.1.23 Full Reptend Primes . . . 38
2.1.24 Generalized Fermat Primes . . . 38
2.1.25 Generalized Mersenne Primes . . . 39
2.1.26 Good Primes . . . 40
2.1.27 Happy Primes . . . 40

2.1.28 Harmonic Primes . . . 41
2.1.29 Higgs Primes . . . 41
2.1.30 Highly Cototient Primes . . . 42
2.1.31 Home Primes . . . 42
2.1.32 Irregular and Regular Primes (Bernoulli) . . . 43
2.1.33 Irregular and Regular Primes (Euler) . . . 44
2.1.34 Irregular and Regular Primes (Genocchi) . . . 44
2.1.35 Isolated Primes . . . 45
2.1.36 Jacobsthal Primes . . . 45
2.1.37 Kynea Primes . . . 46
2.1.38 Leyland Primes . . . 46
2.1.39 Lucas Primes . . . 46
2.1.40 Lucky Primes . . . 47
2.1.41 Mersenne Primes . . . 48
2.1.42 Mersenne Divisors . . . 50
2.1.43 Mersenne Prime Exponents . . . 51
2.1.44 Mills Primes . . . 51
2.1.45 Minimal Primes . . . 51
2.1.46 Mirimanoff Primes . . . 52
2.1.47 $n^2 + 1$ Primes . . . 52
2.1.48 $n^4 + 1$ Primes . . . 52
2.1.49 Near-Square Primes . . . 53
2.1.50 Non-Generous Primes . . . 53
2.1.51 NSW Primes . . . 53
2.1.52 Padovan Primes . . . 54
2.1.53 Palindromic Primes . . . 54
2.1.54 Palindromic Wing Primes . . . 54
2.1.55 Pandigital Primes . . . 55
2.1.56 Partition Primes . . . 55
2.1.57 Pell Primes . . . 56
2.1.58 Permutable Primes . . . 56
2.1.59 Perrin Primes . . . 57
2.1.60 Pierpont Primes . . . 57
2.1.61 Pillai Primes . . . 58
2.1.62 Prime-Indexed Primes . . . 58
2.1.63 Primeval Primes . . . 59
2.1.64 Primorial Primes . . . 60
2.1.65 Proth Primes . . . 61
2.1.66 Pythagorean Primes . . . 62
2.1.67 Quartan Primes . . . 62
2.1.68 Ramanujan Primes . . . 63
2.1.69 Repunit Primes . . . 63
2.1.70 Reversible Primes . . . 64
2.1.71 Riesel Primes . . . 64
2.1.72 Safe Primes . . . 65
2.1.73 Self Primes . . . 66
2.1.74 Sexy Primes . . . 66

2.1.75 Smarandache-Wellin Primes . . . 67
2.1.76 Sophie Germain Primes . . . 67
2.1.77 Stern Primes . . . 67
2.1.78 Strobogrammatic Primes . . . 68
2.1.79 Strong Primes . . . 68
2.1.80 Supersingular Primes . . . 69
2.1.81 Thabit Primes . . . 69
2.1.82 Tribonacci Primes . . . 70
2.1.83 Truncatable Primes . . . 70
2.1.84 Twin Primes . . . 71
2.1.85 Unique Primes . . . 72
2.1.86 Untouchable Primes . . . 73
2.1.87 Wagstaff Primes . . . 73
2.1.88 Wall-Sun-Sun Primes . . . 74
2.1.89 Weak Primes . . . 74
2.1.90 Wieferich Primes . . . 74
2.1.91 Wilson Primes . . . 75
2.1.92 Wolstenholme Primes . . . 75
2.1.93 Woodall Primes . . . 76
2.2 Tentative Types of Prime Numbers . . . 76
2.2.1 Chebyshev Primes . . . 77
2.2.2 Lucas-Wieferich Primes . . . 77
2.2.3 Weak Irregular Primes . . . 77
2.3 Emerging Types of Prime Numbers . . . 78
2.3.1 Bad Primes . . . 78
2.3.2 Complete Primes . . . 78
2.3.3 Composite-Indexed Primes . . . 79
2.3.4 D014689 Primes . . . 79
2.3.5 D2357 Primes . . . 80
2.3.6 D4689 Primes . . . 80
2.3.7 Digit-Increasing and Digit-Decreasing Primes . . . 80
2.3.8 Index-Added Primes I . . . 81
2.3.9 Index-Added Primes II . . . 81
2.3.10 Index-Subtracted Primes I . . . 82
2.3.11 Index-Subtracted Primes II . . . 82
2.3.12 Jump Primes . . . 82
2.3.13 Mixed-Digit Primes . . . 82
2.3.14 Nesting and Non-Nesting Primes . . . 83
2.3.15 Primes with and without Repeated Digits . . . 83
2.3.16 Prime-Sum Primes . . . 84
2.3.17 Product-Digit Primes . . . 84
2.3.18 Residue Primes . . . 84
2.3.19 Sum-Minus Primes . . . 85
2.3.20 Sum-Plus Primes . . . 85
2.3.21 Transformed and Image Primes . . . 85
2.3.22 Type-Indexed Primes I . . . 86
2.3.23 Type-Indexed Primes II . . . 87

2.4 Primes with Infinitely Many Members . . . 87
2.5 Primes with Finitely Many Members . . . 88
2.6 Primes with Few Known Members . . . 88
2.7 Primes with no Known Members . . . 89
2.8 Primes with no Members . . . 89
2.9 General Remarks . . . 89

3 Categorizations of Primes **92**
3.1 Generic Categorizations of Primes . . . 92
3.1.1 Certainty of Primality . . . 92
3.1.2 Modularity . . . 93
3.1.3 Parity . . . 93
3.1.4 Real vs Complex . . . 93
3.1.5 Record . . . 93
3.1.6 Recreation . . . 94
3.1.7 Relation to Other Disciplines . . . 94
3.1.8 Size . . . 94
3.1.9 Theoretical Involvement in Certain Theories . . . 94
3.2 Categorizations and Comparisons of Prime Types . . . 95
3.2.1 Algebraic Form . . . 95
3.2.2 Base Dependency . . . 97
3.2.3 Divisibility and Modularity . . . 98
3.2.4 Expressibility . . . 99
3.2.5 Grouping and Association . . . 99
3.2.6 Indexing . . . 100
3.2.7 Interval Relationship . . . 101
3.2.8 Magnitude Comparison . . . 101
3.2.9 Recreation . . . 102
3.2.10 Sequencing Form . . . 102
3.2.11 Other Considerations . . . 103

4 Relationships of Primes **105**
4.1 Algebraic Form . . . 105
4.1.1 Carol , Kynea and Near-Square Primes . . . 106
4.1.2 Catalan Primes . . . 106
4.1.3 Cullen, Fermat, Pierpont and Proth Primes . . . 106
4.1.4 Centered Primes . . . 108
4.1.5 Mersenne, Riesel and Woodall Primes . . . 108
4.1.6 Mersenne Prime Exponents . . . 109
4.1.7 Mersenne and Pythagorean Primes . . . 109
4.1.8 Pierpont, Proth and Thabit Primes . . . 109
4.1.9 Riesel, Thabit and Woodall Primes . . . 110
4.1.10 $n^2 + 1$ and $n^4 + 1$ Primes . . . 111
4.1.11 Jacobsthal and Wagstaff Primes . . . 111
4.1.12 Factorial, Primorial and Compositorial Primes . . . 112
4.1.13 Fortunate Primes . . . 113
4.1.14 Cuban, Euler and Pythagorean Primes . . . 114
4.1.15 Fermat and Pythagorean Primes . . . 115

4.1.16 Leyland Primes . . . 115
4.1.17 Cyclotomic Primes . . . 115
4.1.18 Accidental Overlaps . . . 116
4.2 Digit Manipulation and Pattern . . . 117
4.2.1 Circular, Permutable, and Repunit Primes . . . 118
4.2.2 Emirp, Palindromic, Repunit, and Reversible Primes . . . 118
4.2.3 Emirp, Permutable, Repunit, and Reversible Primes . . . 118
4.2.4 Palindromic, Permutable, Repunit, and Reversible Primes . . . 119
4.2.5 Minimal and Truncatable Primes . . . 120
4.2.6 Delicate and Minimal Primes . . . 120
4.2.7 Dihedral, Palindromic, Pandigital, Repunit and Strobogrammatic Primes . . . 121
4.2.8 Smarandache-Wellin and Truncatable Primes . . . 121
4.2.9 Fragile and Robust Primality under Digit Operations . . . 122
4.3 Divisibility and Modularity . . . 122
4.3.1 Irregular and Regular Primes . . . 122
4.3.2 Mirimanoff, Wall-Sun-Sun, Wieferich, Wilson and Wolstenholme Primes . . . 124
4.4 Expressibility . . . 124
4.5 Grouping and Association . . . 125
4.6 Indexing . . . 125
4.7 Interval Relationship . . . 125
4.7.1 Cousin, Sexy and Twin Primes . . . 126
4.7.2 Isolated and Twin Primes . . . 126
4.7.3 Chen and Twin Primes . . . 126
4.8 Magnitude Comparison . . . 126
4.8.1 Balanced, Strong and Weak Primes . . . 126
4.8.2 Good Primes . . . 127
4.9 Recreation . . . 127
4.10 Recursive Sequencing . . . 127
4.10.1 Fibonacci, Jacobsthal, Lucas, NSW, Padovan, Pell, Perrin and Tribonacci Primes . . . 128
4.10.2 Bell Primes . . . 128
4.10.3 Partition Primes . . . 128
4.11 Other Considerations . . . 129
4.11.1 Safe and Sophie Germain Primes . . . 129
4.11.2 Ramanujan Primes . . . 129

5 Theorems of Primes **131**
5.1 Common Theorems on Primes . . . 131
5.1.1 Baker-Harman-Pintz Theorem . . . 131
5.1.2 Bertrand's Postulate . . . 131
5.1.3 Binary Quadratic Prime Theorem . . . 132
5.1.4 Bombieri-Vinogradov Theorem . . . 132
5.1.5 Brun's Theorem . . . 132
5.1.6 Brun-Titchmarsh Theorem . . . 133
5.1.7 Chebyshev's Theorem . . . 133
5.1.8 Chen's Theorem I . . . 134
5.1.9 Chen's Theorem II . . . 134
5.1.10 Clement's Theorem . . . 134

5.1.11 Dirichlet's Theorem on Arithmetic Progressions . . . 135
5.1.12 Erdos-Kac Theorem . . . 135
5.1.13 Euler's Criterion . . . 135
5.1.14 Euler's Product Formula . . . 136
5.1.15 Fermat's Little Theorem . . . 136
5.1.16 Goldbach's Ternary Conjecture . . . 137
5.1.17 Green-Tao Theorem . . . 137
5.1.18 Hardy-Ramanujan Theorem . . . 137
5.1.19 Hensel's Theorem . . . 138
5.1.20 Hoheisel's Theorem . . . 138
5.1.21 Iwaniec's Theorem . . . 138
5.1.22 Lagrange's Theorem on Polynomial Congruences . . . 139
5.1.23 Legendre's Formula . . . 139
5.1.24 Linnik's Theorem . . . 140
5.1.25 Littlewood's Theorem . . . 140
5.1.26 Maier's Theorem . . . 140
5.1.27 Mertens' First Theorem . . . 141
5.1.28 Mertens' Second Theorem . . . 141
5.1.29 Mertens' Third Theorem . . . 142
5.1.30 Mills' Theorem . . . 143
5.1.31 Prime Number Theorem . . . 143
5.1.32 Prime Number Theorem for Arithmetic Progressions . . . 144
5.1.33 Primes Modulo 4 Theorem . . . 145
5.1.34 Primes Modulo 6 Theorem . . . 145
5.1.35 Quadratic Reciprocity Law . . . 145
5.1.36 Riemann-von Mangoldt Formula . . . 146
5.1.37 Robin's Theorem . . . 146
5.1.38 Selberg's Formula . . . 147
5.1.39 Siegel-Walfisz Theorem . . . 147
5.1.40 Sylvester-Schur Theorem . . . 148
5.1.41 The Sum of Two Squares Theorem . . . 148
5.1.42 Vinogradov's Theorem . . . 148
5.1.43 Wilson's Theorem . . . 149
5.1.44 Zhang's Theorem . . . 149
5.1.45 Zsigmondy's Theorem . . . 149
5.2 Classification of Theorems . . . 150
5.2.1 Foundations . . . 150
5.2.2 Existence . . . 151
5.2.3 Non-Existence . . . 152
5.2.4 Infinitude . . . 154
5.2.5 Finitude . . . 156
5.2.6 Distribution . . . 157
5.2.7 Algebraic Forms . . . 158
5.2.8 Numeric Forms . . . 160
5.2.9 Role of Primes in the Number System . . . 162
5.2.10 Primality Testing and Sieving . . . 163
5.2.11 Indexing . . . 164

5.2.12 Subsets . . . 164
5.2.13 Divisibility and Modularity . . . 166
5.2.14 Calculation of Primes . . . 169
5.2.15 Estimation of p_n . . . 172
5.3 Relationships between Theorems . . . 173

6 Conjectures of Primes **175**
6.1 Open Problems and Conjectures about Primes . . . 176
6.1.1 *abc* Conjecture . . . 176
6.1.2 Agoh-Giuga Conjecture . . . 176
6.1.3 Agrawal's Conjecture . . . 177
6.1.4 Andrica's Conjecture . . . 177
6.1.5 Artin's Conjecture on Primitive Roots . . . 177
6.1.6 Bateman-Horn Conjecture . . . 177
6.1.7 Bateman-Selfridge-Wagstaff Conjecture . . . 178
6.1.8 Beal's Conjecture . . . 178
6.1.9 Birch-Swinnerton-Dyer Conjecture . . . 178
6.1.10 Brocard's Conjecture . . . 179
6.1.11 Bunyakovsky's Conjecture . . . 179
6.1.12 Cramer's Conjecture . . . 179
6.1.13 Dickson's Conjecture . . . 180
6.1.14 Elliott-Halberstam Conjecture . . . 180
6.1.15 Feit-Thompson Conjecture . . . 181
6.1.16 Firoozbakht's Conjecture . . . 181
6.1.17 First Hardy-Littlewood Conjecture . . . 181
6.1.18 Fortunate Numbers Conjecture . . . 182
6.1.19 Goldbach's Conjecture . . . 182
6.1.20 Hardy-Littlewood Conjecture F . . . 182
6.1.21 Legendre's Conjecture . . . 183
6.1.22 Lehmer's Totient Problem and Conjecture . . . 183
6.1.23 Lemoine's Conjecture . . . 183
6.1.24 Mersenne Conjectures . . . 184
6.1.25 Oppermann's Conjecture . . . 184
6.1.26 Polignac's Conjecture . . . 184
6.1.27 Proth-Gilbreath Conjecture . . . 185
6.1.28 Rassias' Conjecture . . . 185
6.1.29 Riemann's Hypothesis . . . 186
6.1.30 Schinzel's Hypothesis H . . . 186
6.1.31 Schinzel-Sierpinski Conjecture . . . 187
6.1.32 Second Hardy-Littlewood Conjecture . . . 188
6.1.33 Shanks' Conjecture . . . 188
6.1.34 Conjectures on Infinitude of Certain Types of Primes . . . 188
6.1.35 Conjectures on Finitude of Certain Types of Primes . . . 189
6.2 Classification of Open Problems and Conjectures . . . 190
6.2.1 Foundations . . . 190
6.2.2 Existence . . . 190
6.2.3 Non-Existence . . . 190

6.2.4 Infinitude . . . 191
6.2.5 Finitude . . . 193
6.2.6 Distribution . . . 193
6.2.7 Algebraic Forms . . . 194
6.2.8 Numeric Forms . . . 194
6.2.9 Role of Primes in the Number System . . . 195
6.2.10 Primality Testing and Sieving . . . 195
6.2.11 Subsets . . . 196
6.2.12 Divisibility and Modularity . . . 196
6.2.13 Calculation of Primes . . . 196
6.2.14 Estimation of p_n . . . 196
6.3 Relationships between Conjectures . . . 197
6.4 Relationships between Theorems and Conjectures . . . 199
6.5 Falsified Conjectures . . . 200
6.6 Potential Open Problems and Conjectures . . . 202

7 Tests and Sieves of Primes 205
7.1 Introductory Remarks . . . 205
7.2 Simple Tests . . . 207
7.3 Primality Tests . . . 209
7.3.1 AKS Test . . . 209
7.3.2 APR Test . . . 209
7.3.3 Baillie-PSW Test . . . 210
7.3.4 Division Test . . . 210
7.3.5 Elliptic Curve Primality Proving . . . 211
7.3.6 Fermat Test . . . 211
7.3.7 Fibonacci Test . . . 211
7.3.8 Frobenius Test . . . 212
7.3.9 Lucas Test . . . 212
7.3.10 Lucas-Lehmer Test . . . 213
7.3.11 Lucas-Lehmer-Riesel Test . . . 213
7.3.12 Miller-Rabin Test . . . 214
7.3.13 Morrison Test . . . 214
7.3.14 Pell Test . . . 215
7.3.15 Pepin Test . . . 215
7.3.16 Pocklington Test . . . 215
7.3.17 Proth Test . . . 215
7.3.18 Solovay-Strassen Test . . . 216
7.3.19 Wilson Test . . . 216
7.3.20 Tests for Specific Prime Types . . . 216
7.3.21 Hypothetical Tests . . . 218
7.3.22 Primality Testing and Conjectures . . . 219
7.4 Prime Sieves . . . 221
7.4.1 Atkin's Sieve . . . 221
7.4.2 Eratosthenes' Sieve . . . 222
7.4.3 Euler's Sieve . . . 222
7.4.4 Sundaram's Sieve . . . 223

7.4.5 Wheel Sieve . . . 223
7.4.6 Brun's Sieve . . . 224
7.4.7 Harman's Sieve . . . 224
7.4.8 Large Sieve . . . 224
7.4.9 Legendre's Sieve . . . 225
7.4.10 Selberg's Sieve . . . 225
7.4.11 Turan's Sieve . . . 226
7.4.12 Sieves for Specific Prime Types . . . 226
7.5 Classifications of Primality Tests . . . 227
7.5.1 Analytical vs Computational . . . 227
7.5.2 Computational Complexity . . . 228
7.5.3 Deterministic vs Probabilistic . . . 228
7.5.4 Deterministic vs Stochastic . . . 229
7.5.5 General vs Specific . . . 230
7.5.6 Primality vs Compositeness . . . 231
7.5.7 Nature of Tests from Input-Output Perspective . . . 231
7.6 Classifications of Prime Sieves . . . 231
7.6.1 Algorithmic vs Analytic/Combinatorial . . . 231
7.6.2 Analytic vs Combinatorial . . . 232
7.6.3 Computational Complexity . . . 233
7.6.4 General vs Special . . . 233
7.7 Theorems and Conjectures on Testing and Sieving . . . 234
7.8 Relationships between Tests and Sieves . . . 234
7.8.1 Relationships and Comparisons among Tests . . . 234
7.8.2 Relationships and Comparisons among Sieves . . . 237
7.8.3 Relationships and Comparisons between Tests and Sieves . . . 239
7.9 Topics Related to Primality Testing and Sieving . . . 240
7.9.1 Almost-Primes in Testing and Sieving . . . 240
7.9.2 Carmichael Numbers . . . 240
7.9.3 Riesel Problem and Number . . . 241
7.9.4 Sierpinski Problem and Number . . . 241
7.9.5 Pseudoprimes in Testing and Sieving . . . 241
7.9.6 Prime Factorization of Large Numbers . . . 242
7.10 Factorization Algorithms . . . 243
7.10.1 Continued Fraction Factorization . . . 244
7.10.2 Dixon's Factorization Method . . . 245
7.10.3 Elliptic Curve Method . . . 245
7.10.4 Fermat's Factorization Method . . . 246
7.10.5 General Number Field Sieve . . . 247
7.10.6 Multiple Polynomial Quadratic Sieve . . . 248
7.10.7 Pollard's Rho Algorithm . . . 249
7.10.8 Pollard's $p-1$ Algorithm . . . 249
7.10.9 Quadratic Sieve . . . 250
7.10.10 Shanks' Square Forms Factorization . . . 251
7.10.11 Special Number Field Sieve . . . 251
7.10.12 Trial Division Algorithm . . . 252
7.10.13 Williams' $p+1$ Algorithm . . . 253

8 Distribution of Primes **254**
8.1 General Facts about Distribution of Primes . . . 254
8.2 Prime Counting and Distribution Functions . . . 255
8.2.1 The π Function . . . 255
8.2.2 The li and Li Functions . . . 255
8.2.3 Riemann's Prime-Power Counting Function . . . 256
8.2.4 Riemann's R-Function . . . 257
8.2.5 Chebyshev's Functions . . . 257
8.3 Relationships among Prime Counting and Distribution Functions . . . 258
8.4 Theorems about Distribution of Primes . . . 259
8.5 Conjectures about Distribution of Primes . . . 259
8.6 Prime Gaps . . . 263
8.6.1 Size and Distribution of Prime Gaps . . . 263
8.6.2 Patterns of Prime Gaps . . . 264
8.6.3 Known Prime Gaps . . . 265
8.7 Topics Related to the Distribution of Primes . . . 266
8.7.1 Chebyshev's Bias . . . 266
8.7.2 Ulam Spiral . . . 266
8.7.3 Number of Primes vs Number of Their Digits . . . 266
8.7.4 Relations between Prime Distribution and Primality Testing and Sieving . . . 267

9 Miscellaneous Topics **270**
9.1 Sequences Related to Primes . . . 270
9.1.1 Aliquot Sequence . . . 270
9.1.2 Catalan-Mersenne Sequence . . . 270
9.1.3 Cunningham Chains . . . 270
9.1.4 Euclid-Mullin Sequence . . . 271
9.1.5 Pillai Sequence . . . 271
9.1.6 Prime-Counting Sequence . . . 271
9.1.7 Prime Gaps Sequence . . . 272
9.1.8 Sequences of Prime-Generating Constants . . . 272
9.2 Series Related to Primes . . . 272
9.2.1 Harmonic Series of Primes . . . 272
9.2.2 Alternating Harmonic Series of Primes . . . 273
9.2.3 Series of Reciprocal Squares of Primes . . . 273
9.2.4 Twin Prime Series . . . 273
9.3 Constants Related to Primes . . . 273
9.4 Generalization of Primality into Higher Dimensions . . . 275
9.4.1 Gaussian Primes . . . 275
9.4.2 Gaussian Mersenne Primes . . . 276
9.4.3 Eisenstein Primes . . . 276
9.4.4 Hurwitz Primes . . . 276
9.5 Semiprimes . . . 277
9.6 Almost-Primes . . . 278
9.7 Pseudoprimes . . . 279
9.7.1 Absolute Pseudoprimes . . . 279
9.7.2 Catalan Pseudoprimes . . . 279

9.7.3 Elliptic Pseudoprimes . . . 279
9.7.4 Euler-Jacobi Pseudoprimes . . . 279
9.7.5 Euler Pseudoprimes . . . 280
9.7.6 Fermat Pseudoprimes . . . 280
9.7.7 Fibonacci Pseudoprimes . . . 280
9.7.8 Frobenius Pseudoprimes . . . 281
9.7.9 Lucas Pseudoprimes . . . 281
9.7.10 Perrin Pseudoprimes . . . 281
9.7.11 Somer-Lucas Pseudoprimes . . . 281
9.7.12 Strong Pseudoprimes . . . 281
9.7.13 Wieferich Pseudoprimes . . . 282
9.8 Methods and Algorithms . . . 282
9.8.1 Evaluation of $\pi(x)$ . . . 282
9.8.2 Prime Calculation and Generation . . . 283
9.9 Residue Classes of Primes . . . 283
9.10 Integers as Sums of Natural Powers of Primes . . . 284
9.11 Relationships between Primes and Other Types of Numbers . . . 284

10 Applications of Primes **286**
10.1 Cryptography . . . 287
10.2 Number Theory . . . 287
10.3 Computing . . . 287

11 General Resources for Primes **288**
11.1 Books . . . 288
11.2 General Encyclopedias . . . 289
11.3 GIMPS . . . 289
11.4 Journals . . . 290
11.5 Large Language Models . . . 290
11.6 Mathematical Software . . . 291
11.7 OEIS . . . 291
11.8 Online Educational Materials . . . 292
11.9 Online Forums and Chat Rooms . . . 292
11.10 Preprint Repositories . . . 293
11.11 The Prime Pages . . . 293

References **295**

Index **296**

Nomenclature

In the following list, we define the common symbols, notations and abbreviations which are used in the book as a quick reference for the reader.

$\sim$	asymptotic equivalence symbol
$!$	factorial
$\in$	in (or belong to)
$\ni$	(backward) in (or belong to)
$\notin$	not in (or do not belong to)
$\times$, $\cdot$	multiplication sign
$\to$	tends to (or followed by)
$\dot{-}$	the monus operator
$\{\cdots\}$	set
$\lvert a\rvert$	absolute value of a
$\overline{a}$	repeating (periodic) decimal
$\lceil a \rceil$	ceiling function (smallest integer greater than or equal to a)
$\lfloor a \rfloor$, floor(a)	floor function (greatest integer less than or equal to a)
$\lfloor a \rceil$	round of a (nearest integer to a)
$A \Rightarrow B$	A implies B
A	Mills' constant
$\mathcal{B}_2$	Brun's constant (or twin primes constant)
B_n	n^{th} Bernoulli number ($n \in \mathbb{N}_0$)
$\mathscr{B}_n$	n^{th} Bell number ($n \in \mathbb{N}_0$)
C	prime-encoding number in Sierpinski's formula
C_A	Artin's constant (≈ 0.3739558136)
C_{BH}	Bateman-Horn factor
C_{CE}	Copeland-Erdos constant ($0.23571113\ldots$)
CFRAC	Continued Fraction Factorization
C_n	n^{th} Catalan number ($n \in \mathbb{N}_0$)
C_m^n	binomial coefficient
ECM	Elliptic Curve Method
ECPP	Elliptic Curve Primality Proving
E_n	n^{th} Euler number ($n \in \mathbb{N}_0$)
Eq., Eqs.	Equation, Equations
F_k	k^{th} Fermat number ($k \in \mathbb{N}_0$)
$\mathcal{F}_n$	n^{th} Fibonacci number ($n \in \mathbb{N}_0$)
$\mathscr{F}_n$	n^{th} fortunate number ($n \in \mathbb{N}$)
$F_{b,n}$	generalized Fermat number/prime ($b, n \in \mathbb{N}_0$ and $b > 1$)

$F_{a,b,n}$	generalized Fermat number/prime ($a, b \in \mathbb{N}$ and $n \in \mathbb{N}_0$)
g_n	n^{th} prime gap, i.e. the gap between n^{th} and $(n+1)^{th}$ primes
G_n	n^{th} Genocchi number ($n \in \mathbb{N}_0$)
gcd	greatest common divisor
$\gcd(m, n)$	greatest common divisor of m and n
GNFS	General Number Field Sieve
GRH	Generalized (or Grand) Riemann Hypothesis
H_n	n^{th} harmonic number ($n \in \mathbb{N}$)
$\mathrm{HP}(n)$	home prime of n ($1 < n \in \mathbb{N}$)
i	the imaginary unit of the complex numbers (i.e. $\mathrm{i}^2 = -1$)
$\mathrm{i}, \mathrm{j}, \mathrm{k}$	the three imaginary units of the quaternion system
iff	if and only if
$\mathrm{ind}_g a$	discrete index (or logarithm) of a base g
J_n	n^{th} Jacobsthal number ($n \in \mathbb{N}_0$)
$J(x)$	Riemann prime-power counting function
lcm	least common multiple
$\mathrm{lcm}(m, n)$	least common multiple of m and n
$\mathrm{li}(x)$	logarithmic integral function (of $x \in \mathbb{R}$)
$\mathrm{Li}(x)$	offset logarithmic integral function (of $x \in \mathbb{R}$)
$\ln(x)$, $\log(x)$	natural logarithm (of $x \in \mathbb{R}$)
$\log_b(x)$	logarithm of x to base b
L	Linnik's constant (≤ 5)
L_n	n^{th} Lucas number ($n \in \mathbb{N}_0$)
L_n	n^{th} lucky number ($n \in \mathbb{N}$)
$\liminf$	limit inferior
$\limsup$	limit superior
$m \mid n$	m divides n
$m \nmid n$	m does not divide n
$(m)_n$	number m in base n
$m \overset{k}{=} n$	m and n are congruent modulo k
$m \equiv n \pmod{k}$	m and n are congruent modulo k
$m \overset{k}{\neq} n$	m and n are not congruent modulo k
$m \not\equiv n \pmod{k}$	m and n are not congruent modulo k
m^*	modular multiplicative inverse of m
mod	modulo (or modulus)
M	Meissel-Mertens constant (≈ 0.2614972128)
M_n	Mersenne number (where $n \in \mathbb{N}_0$ or $n \in \mathbb{N}$) according to the common convention
M_p	Mersenne number (where $p \in \mathbb{P}$) according to another convention

$\mathscr{M}_p$	Gaussian Mersenne prime
$M_{b,n}$	generalized Mersenne prime
M_{M_p}	double Mersenne prime
$M(n)$	Mertens' function (of $n \in \mathbb{N}$)
MPQS	Multiple Polynomial Quadratic Sieve
$n\#$	n^{th} primorial number of 2^{nd} kind (product of all prime numbers $\leq n$)
$\mathbb{N}$	the set of natural numbers (i.e. $1, 2, 3, \ldots$)
$\mathbb{N}_0$	the set of non-negative integers (i.e. $0, 1, 2, 3, \ldots$)
N_n	n^{th} NSW number ($n \in \mathbb{N}_0$)
$\left(\frac{n}{m}\right)$	Jacobi symbol (m is odd positive integer)
$\left(\frac{n}{p}\right)$	Legendre symbol (p is odd prime)
O	big O notation
$\mathbb{O}$	the set of odd integers
$\mathcal{O}$	the neutral element on an elliptic curve
$O_k n$	order of integer n (modulo k)
OEIS	The On-Line Encyclopedia of Integer Sequences
p	prime number
p_n	n^{th} prime number ($n \in \mathbb{N}$)
$P(n)$	partition function (of $n \in \mathbb{N}_0$)
$p_n\#$	n^{th} primorial number of 1^{st} kind (product of first n prime numbers)
$P_{p_n}^{\pm}$	primorial prime
$\mathbb{P}$	the set of prime numbers
P_e	even perfect number
P_n	n^{th} Padovan number ($n \in \mathbb{N}_0$)
$\mathcal{P}_n$	n^{th} Pell number ($n \in \mathbb{N}_0$)
P_n	n^{th} Perrin number ($n \in \mathbb{N}_0$)
PNT	Prime Number Theorem
PNTAP	Prime Number Theorem for Arithmetic Progressions
$\mathbb{Q}$	the set of rational numbers
QS	Quadratic Sieve
$\mathbb{R}$	the set of real numbers
R_n	n^{th} Ramanujan prime ($n \in \mathbb{N}$)
$R(x)$	Riemann R-function (of $x \in \mathbb{R}$)
RH	Riemann Hypothesis
RSA	a family of public-key cryptosystems
$\Re(s)$	real part of complex variable s
S_p	safe prime (i.e. $S_p = 2p + 1$ where $p \in \mathbb{P}$)
$s(n)$	restricted divisor function (of $n \in \mathbb{N}$)
$S(k)$	sum of digits of k ($k \in \mathbb{N}$)

SNFS	Special Number Field Sieve
SQUFOF	Shanks' Square Forms Factorization
T_n	n^{th} Tribonacci number ($n \in \mathbb{N}_0$)
U_n	repunit integer with n 1's (usually in base 10)
vs	versus
W_p	Wagstaff prime (corresponding to $p \in \mathbb{P}$)
$\mathbb{Z}$	the set of integers
$\mathbb{Z}/n\mathbb{Z}$	ring of integers modulo n
α	Wright's constant (≈ 1.9287800)
γ	Euler-Mascheroni constant (≈ 0.57721566)
$\zeta(s)$	zeta function (of complex variable s)
$\theta(x)$	first Chebyshev prime-counting function (of $x \in \mathbb{R}$)
$\Lambda(n)$	von Mangoldt function (of $n \in \mathbb{N}$)
$\mu(n)$	Mobius function (of $n \in \mathbb{N}$)
$\pi(x)$	prime-counting function (of $x \in \mathbb{R}$)
$\pi_2(x)$	counting function of semiprimes (i.e. number of semiprimes $\leq x$ where $x \in \mathbb{R}$)
$\pi(x; q, a)$	prime-counting function in the arithmetic progression a modulo q (of $x \in \mathbb{R}$)
$\Pi(x)$	Riemann prime-power counting function (of $x \in \mathbb{R}$)
$\prod$	product operator
ρ	prime constant ($0.0110101000101\ldots$)
$\sigma(n)$	divisor function (of $n \in \mathbb{N}$)
Σ	summation operator
$\tau(n)$	divisor-counting (or tau) function (of $n \in \mathbb{N}$)
$\phi(n)$	totient (or phi or Euler) function (of $n \in \mathbb{N}$)
$\Phi_n(x)$	n^{th} cyclotomic polynomial (of $x \in \mathbb{R}$)
$\psi(x)$	second Chebyshev prime-counting function (of $x \in \mathbb{R}$)

Chapter 1
Preliminaries

In this chapter we present and briefly discuss a number of subjects and issues in preparation for the forthcoming investigations.

1.1 Introductory Remarks

Before we go through the details of investigation of prime numbers it is useful to be aware of the following remarks:

1. This book is about prime numbers in general and is an attempt to fill a gap in the existing literature of mathematics (as well as number theory and prime numbers in particular). Most studies (historical and current) on prime numbers are largely focused on the fine details of this subject without sufficient attention to the larger picture and comprehensive view which consider, for instance, the classification, categorization, and inter-relationships of prime numbers and among their many types and classes. There is also insufficient attention to the general structure of this discipline. We try in this book to address these issues by collecting and presenting in an organized fashion the main current knowledge about prime numbers to provide a comprehensive and panoramic view to this important subject. As indicated, the current book is supposed to represent the first volume of a series about prime numbers where the content will be elaborated in detail and in depth.
2. This volume is intended to represent the very basic level of this subject and hence it is a "handbook" for everyone interested in prime numbers as it provides a good reference about the most preliminary facts and knowledge on this subject. Our intention is to go higher on the knowledge ladder of prime numbers gradually and step by step in the forthcoming volumes of this book. As noted before, our plan is to expand this book (horizontally and vertically) in each subsequent volume (although alternative plans within this general vision may be adopted if found more appropriate). If we failed to continue this project (for whatever reason) we hope that other authors take the responsibility of continuing this important project.
3. The commonly occurring symbols of global significance are collected and explained in the § Nomenclature. Hence, we may not explain symbols locally except the local ones which need such explanation.
4. Although the book is about prime numbers,[1] we occasionally talk about composite numbers (in general or of particular types) due to the intimate relationship between prime and composite numbers and their complementary status and role in number theory. We may also talk about similar subjects related to prime numbers for the sake of common benefit and completeness, e.g. composite Fermat numbers in the context of Fermat primes (see the Note in § 2.1.20) or perfect numbers in the context of Mersenne primes (see Note 2 in § 2.1.41).
5. Some of the information provided in this book (such as the largest known prime number or the number of known Mersenne primes) are taken from the Internet. This type of information is provided as a curiosity or to give an idea about the kind or size of the concerned issues and hence we do not guarantee the reliability of such information since we may not conduct credible checks on their correctness and accuracy. Accordingly, such information should be taken with caution, i.e. for any serious purposes

[1] Actually, this book is about prime numbers within number theory and hence we will avoid issues related to prime numbers beyond this theory (such as applications of prime numbers within certain fields and subjects like cryptography).

more thorough and rigorous research should be conducted. Moreover, these types of information are usually subject to change and update (as new discoveries occur from time to time) and hence they should be checked for possible updates.[2] In general, most of the information given in this book are updated to the date of publication of this book (and hence we generally do not commit ourselves to mention the date of obtaining the information although we may do occasionally).[3]

6. Numbers (and statements about numbers) in this book are in the decimal system (i.e. base 10 numeric system) unless stated otherwise.
7. We have no commitment to explain the basic concepts (or techniques or methods or terminology) of number theory. For example, if we mention the Jacobi symbol or quadratic residue we may not explain what these terms mean. So, the book is not self-contained from this perspective. Therefore, for maximal benefit from the book the reader should have a reasonable level of education in number theory and must be familiar with the main concepts of number theory. However, we usually provide basic definitions and notes when this is convenient to us. Nevertheless, the reader can always consult number theory textbooks (or the Internet) to fill the gap in his knowledge. We should also note that most of the contents of the book (in its first volume) require rather limited mathematical education and knowledge and hence the book is generally useful for general reading in mathematics for those with a college level education (as well as higher levels let alone the experts in this field).
8. As indicated in the Preface, there is some repetition where certain statements (or propositions or theorems or conjectures or ... etc.) are repeated in different parts and sections in the book because they belong to different topics and categories. Most of these repetitions arise from investigations of different aspects of the same issue and are therefore intentional rather than mere copy-and-paste duplication. Moreover, the nature of the book (as a guidebook or handbook) should justify a certain level of repetition in general.
9. For the convenience of the reader, we use cross referencing extensively, noting that such referrals are hyperlinked in the electronic copies of the book but we did not highlight the hyperlinked objects (e.g. by coloring) to avoid distortion.
10. Prime numbers is a very extensive, complicated and messy subject with many gray areas that confuse even the specialists in this subject. So, certain parts of this book may not get the approval of some individuals (whether professional scholars or amateur readers), and this is understandable. However, we will take into consideration any objections or concerns in the future volumes of this book (and potentially in the future editions of this volume).
11. Assessments of rather subjective nature are common in the literature of science and mathematics. Such assessments usually lead to contradictions, controversies and criticisms (due mostly to differences in opinions or differences in perspectives and considerations). We try in this book to avoid this kind of assessments (or at least keep it to minimum). However, when such assessments are made we generally rely on authoritative references or base our view on reasonably-thorough inspection of the literature.
12. In our view, the most important feature of this book (or rather this volume) is its general structure rather than its contents (noting that the contents of some parts and sections are very simple or even trivial). Another important feature of this book is that it highlights issues that deserve attention (even though the provided content can be basic). These features are important for both novice and expert readers and can be highly beneficial in the study and research of this subject.

[2] It is important to note in this regard that the investigation of prime numbers continues to be one of the most active and vibrant areas of research (in mathematics and in general) which attracts huge numbers of researchers (whether professional mathematicians or novice and "hobbyist" mathematicians), and hence there are always novel results and claims (which are either unverified or controversial) that require inspection and scrutiny.

[3] For convenience, we may provide an internet address (URL) to the source of information or to authoritative websites.

1.2 The Fascination of Prime Numbers

Prime numbers have fascinated mathematicians for more than two millennia. From the time of the ancient Greeks, who recognized primes as the fundamental building blocks of the integers, these numbers have occupied a central place in number theory.[4] Their simple definition (i.e. a positive integer greater than one that has no positive divisors other than one and itself) contrasts sharply with the complexity and apparent unpredictability of their distribution. This combination of simplicity and mystery has made prime numbers one of the most fascinating and enduring subjects of mathematical inquiry and curiosity.

The study of prime numbers has led to some of the deepest results and most challenging open problems in mathematics. Questions about how frequently primes occur, how they are distributed, and how they relate to one another have inspired generations of mathematicians and continue to drive research today. Beyond their theoretical importance, prime numbers have also found some practical applications, most notably in modern cryptography, where they underpin many widely used methods for secure communication (see chapter 10). Thus, prime numbers are valued not only for their intrinsic mathematical beauty and obscurity (and even "mystical" nature) but also for their profound influence on both pure mathematics and contemporary technology.

A legitimate question may be posed: why prime numbers (not composite numbers) attract this exceptional attention and fascination? The unique status of prime numbers originates from their special role which arises from the fact that they are the fundamental building blocks of the positive integers. Every integer greater than one is either a prime or can be expressed as a product of prime numbers, and this factorization is unique apart from the order of the factors (see § 1.7). Consequently, understanding prime numbers means understanding the structure of all integers. Composite numbers do not possess the same fundamental status, since they are constructed from primes and inherit many of their properties through their prime factorizations. For this reason, many questions about integers ultimately reduce to questions about prime numbers, making the study of primes (rather than composites) central to number theory and to mathematics as a whole.

1.3 Basic Facts about Prime Numbers

The following are some basic facts that everyone interested in prime numbers must know:[5]

1. *Prime number* (or *prime* for short) is a natural number greater than 1 that is divisible only by 1 and itself (considering only the positive divisors). The first few primes are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$. Non-prime natural numbers (excluding 1) are described as *composite*. Accordingly, all non-negative integers are either prime or composite except 0 and 1 which are neither.[6]
2. Prime numbers are the basic building blocks of the structure of numbers (i.e. integers) which are the subject of number theory (see § 1.7).
3. Primality (as well as compositeness) is an *absolute* property, and hence it is independent of any relation to other mathematical entities and attributes (such as other numbers in the number system) apart from

[4] Substantial historical and archaeological evidence indicate that even the ancient civilizations of Mesopotamia and Egypt (and possibly other civilizations) were aware of the prime numbers and their basic characteristics (although mostly at the practical level).

[5] Some of these facts and statements may seem trivial, but they are included for the sake of completeness and to support readers who are new to the subject.

[6] Regrading 0, it is not prime because it is divisible by any other number while prime must be divisible only by 1 and itself (considering positive divisors). It is also not composite because it cannot be expressed as a product of primes.
Regrading 1, it is not composite because it cannot be expressed as a product of primes. However, it is like a prime (since it is divisible only by 1 and itself) and hence it seems reasonable to classify it as prime. So, the reason for not considering it prime seems to be the desire to preserve the property of uniqueness of prime factorization (according to the fundamental theorem of arithmetic; see § 1.7). For example, if 1 is prime then 4 can be prime-factorized in infinitely many ways, e.g. 1×2^2, $1^2 \times 2^2$, $1^3 \times 2^2$, etc. It may also be argued that 1 is not prime because it is divisible only by 1 (or only by itself), i.e. not by 1 and itself since the two are the same.

what is given in its definition. For example, primality is independent of the base of the number system, e.g. a prime number is prime in base 2 and base 8 and base 10 (and any other base) simultaneously. However, certain types of primality are relative as they (for example) depend on the base of the employed number system and the representation of primes (see for instance § 2.1.7, § 2.1.69 and § 2.1.83).

4. Primality is an *intrinsic* property and hence it is independent of any casual contexts and attributes such as being in a certain mathematical relation or equation. Yes, this applies to our commonly used number system (i.e. integers within the real numbers) which are the subject of number theory in its traditional domain. Beyond this (such as other number systems like complex numbers or quaternions, or within certain mathematical structures like rings) primality may become relative or relational property (i.e. a property linked to the number system or structure). In simple words, we must distinguish between the intrinsic nature of primality in standard arithmetic and everyday mathematics, and its extrinsic (or acquired or relational) nature in higher algebra and exotic mathematical structures (see for instance § 9.4).
5. Primality is a *deterministic* (or definitive) property, and hence any probabilistic aspect of primality itself is related to our (lack of) knowledge. As we will see, some integers may satisfy certain (necessary but not sufficient) primality conditions or pass certain probabilistic primality tests and hence they are labeled as "probable primes". Similarly, there are certain aspects related to primality (such as the distribution of prime numbers among integers and their patterns) which are subject to certain probabilistic factors and statistical considerations.
6. Prime numbers are historically (and continue to be) one of the most active fields of investigation and research in mathematics (and even beyond). Despite this, many mysteries and open questions still exist (and continue to emerge) despite the massive efforts to solve these mysteries and subtleties. In fact, prime numbers can be considered as one of the most challenging and subtle subjects of human knowledge.
7. There are infinitely many prime numbers (Euclid's theorem).[7]
8. Every prime number can generate infinitely many composite numbers through multiplication. However, no finite set of prime numbers can generate all composite numbers. Likewise, no finite set of composite numbers can generate all prime numbers through any definitive mathematical operation.
9. Prime numbers become sparser (i.e. less frequent) as we move up the number line. More generally, prime numbers and specific infinite subsets and types of them become increasingly rare as integers grow in size.
10. Generally, the gap between successive prime numbers varies unpredictably. However, the average size of the gap between successive primes increases as we go up on the number line.
11. There are arbitrarily large gaps between consecutive primes.
12. As of March 2026, the largest known prime number is $2^{136279841}-1$ (which consists of 41024320 decimal digits noting that it is a Mersenne prime; see § 2.1.41).[8]
13. Every prime number (other than 2) is odd, i.e. 2 is the only even prime number.
14. The last digit of any multi-digit prime number must be 1, 3, 7, or 9.
15. Every odd prime must be either of the form $(4k+1)$ or of the form $(4k-1)$ where $k \in \mathbb{N}$. Equivalently, for any prime $p > 2$ we have $p \overset{4}{=} 1$ or $p \overset{4}{=} 3$.
16. Every prime $p > 3$ must be either of the form $(6k+1)$ or of the form $(6k-1)$ where $k \in \mathbb{N}$. Equivalently, for any prime $p > 3$ we have $p \overset{6}{=} 1$ or $p \overset{6}{=} 5$.
17. Any two (or more) distinct primes are pairwise coprime. More generally, the natural powers of distinct primes are coprime.

[7] There are also infinitely many composite numbers, but this statement is trivial since we can create an infinite set of composite numbers from a finite set of prime numbers (let alone from an infinite set of prime numbers).

[8] See `https://t5k.org/largest.html` and `https://www.mersenne.org/primes/`.

18. Any prime number p is coprime to all positive integers which are less than p.
19. $p|(n_1 n_2 \dots n_k)$ *iff* $p|n_i$ for some $1 \leq i \leq k$ where p is prime (generalized Euclid's lemma).
20. Non-negative integers are partitioned (comprehensively and mutually exclusively) as primes, composites, and neither (i.e. 0 and 1).[9]
21. If $n \in \mathbb{N}$ is composite then n has a prime divisor $\leq \sqrt{n}$. As a result (i.e. by contraposition), if $n \in \mathbb{N}$ does not have a prime divisor $\leq \sqrt{n}$ then n is prime. This fact is important for the search for primes and test for primality, i.e. to verify that a given number is prime we need only to establish that it has no prime divisor $\leq \sqrt{n}$ with no need to test for potential prime divisors $> \sqrt{n}$.
22. The square root of any prime number p is irrational. More generally, the n^{th} root ($\mathbb{N} \ni n > 1$) of any prime number is irrational.
23. No three consecutive natural numbers (> 1) can be all prime (i.e. at least one of them must be composite).[10]
24. The least positive divisor greater than 1 of any integer $n > 1$ is a prime number.
25. There are primes with no repeated digits (like 149), and primes with some repeated digits (like 199). Also, there are primes whose digits are all identical (i.e. repunit primes; see § 2.1.69).[11]
26. No polynomial (other than constant) with integer coefficients outputs only prime numbers for all integer inputs.
27. Primes do not form a group under addition or multiplication because they do not satisfy the group properties of closure, identity, and inverse.
28. There are many methods for finding primes; most of which are computational sieves (i.e. methods for searching for and identifying primes collectively within a given range by filtering primes or composites within that range, e.g. all primes less than 1000). There are also many methods for primality (or compositeness) testing to verify if a given integer is prime or not. These methods vary in many aspects and perspective such as being analytical or numerical or being deterministic or probabilistic.

1.4 Generalities about Prime Numbers

The following are some of the common facts of universal significance (like all, any, each, every, none, etc.) about prime numbers or related to prime numbers:

1. Any prime number has exactly two positive divisors (i.e. 1 and itself).
2. Any prime number p can be factorized as a product of only two or three distinct integer factors, i.e. $p = (1)(p)$ or $p = (-1)(-p)$ or $p = (1)(-1)(-p)$.
3. No prime number is a perfect power a^b (where $a, b \in \mathbb{N}$ and $b > 1$). Moreover, every prime number is square-free.[12]
4. No prime number can be perfect or abundant; every prime is a deficient number.[13]
5. For any prime number p and positive integer k, p^k has exactly $k + 1$ positive divisors.
6. All prime numbers greater than 2 are odd.
7. All prime numbers are coprime to each other. This also applies to their positive powers.
8. All n^{th} roots of any prime number are irrational (where n is an integer > 1).
9. All prime numbers greater than 5 end in 1, 3, 7, or 9 (in base 10).

[9] This statement means (partly) that a positive integer > 1 must be either prime or composite in the sense that it cannot be neither or both.

[10] The condition "> 1" is about "at least one of them must be composite".

[11] It is obvious that such statements are base-dependent (where the conventional base is 10). It is worth noting that there are infinitely many primes with repeated digits and only finitely many with no repeated digits, while the infinitude of repunit primes is an open problem.

[12] A square-free integer is an integer that is not divisible by any perfect square greater than 1.

[13] A positive integer is deficient/perfect/abundant *iff* the sum of its proper divisors is less than/equal/greater than the number.

10. For all primes p, $\sigma(p) = p+1$ (where σ is the divisor function of p). In fact, n is prime *iff* $\sigma(n) = 1+n$.[14]
11. For all primes p, $s(p) = 1$ (where s is the restricted divisor function of p). In fact, n is prime *iff* $s(n) = 1$.[15]
12. For all primes p, $\tau(p) = 2$ (where τ is the divisor-counting function of p). In fact, n is prime *iff* $\tau(n) = 2$.[16]
13. For all primes p, $\phi(p) = p-1$ (where ϕ is the totient function of p). In fact, n is prime *iff* $\phi(n) = n-1$.[17]
14. For all primes p, $\mu(p) = -1$ (where μ is the Mobius function of p).[18]
15. All prime factors of $n! + 1$ are greater than n.[19]
16. Every odd prime satisfies $p^2 \overset{4}{=} 1$.[20]
17. Every odd prime satisfies $p^2 \overset{8}{=} 1$.
18. Every prime > 3 satisfies $p^2 \overset{24}{=} 1$.
19. Every prime number is a divisor of some binomial coefficient.
20. Every natural number greater than 1 has at least one prime divisor.
21. Every prime divides infinitely many Catalan numbers (see the Note in § 2.1.4).
22. Every odd prime divides at least one Mersenne number (see Note 1 in § 2.1.41).
23. Every integer greater than 1 is either a prime or can be expressed uniquely as a product of primes (the fundamental theorem of arithmetic; see § 1.7).
24. Every prime number satisfies Fermat's little theorem (see § 5.1.15).
25. Every prime number satisfies Wilson's theorem (see § 5.1.43).
26. All prime numbers except 2 and 5 have decimal expansions of their reciprocals that eventually repeat.[21] Also see § 2.1.23.
27. All odd primes are of the form $4n + 1$ or $4n - 1$ (where $n \in \mathbb{N}$).
28. All primes greater than 3 are of the form $6n + 1$ or $6n - 1$ (where $n \in \mathbb{N}$).
29. Every prime of the form $4n + 1$ (where $n \in \mathbb{N}$) can be uniquely[22] expressed as a sum of two perfect squares. The converse is also true (excluding 2), i.e. no prime of the form $4n - 1$ can be expressed as the sum of two perfect squares. See § 5.1.41.
30. Every odd prime can be uniquely expressed as the difference of two perfect squares:[23]

$$p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2 \tag{2}$$

31. No prime can be written as the difference of two squares of positive integers (i.e. $m^2 - n^2$) unless the

[14] The divisor function of a positive integer n gives the sum of all positive divisors of n (including 1 and n).
[15] The restricted divisor function of a positive integer n gives the sum of the proper divisors of n.
[16] The divisor-counting function of a positive integer n counts the number of positive divisors of n (including 1 and n).
[17] The totient function of a positive integer n counts the number of positive integers $\leq n$ that are relatively prime to n.
[18] The Mobius function $\mu(n)$ of a positive integer n is defined as $\mu(1) = 1$, and for $n > 1$:

$$\mu(n) = \begin{cases} (-1)^k & (n \text{ is square-free}) \\ 0 & (n \text{ is not square-free}) \end{cases} \tag{1}$$

where $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the standard prime factorization of n, with k distinct prime factors (noting that square-free means no a_i is greater than 1; see § 1.7).
[19] This implies that there are infinitely many prime numbers since there are infinitely many numbers of the form $n! + 1$. See § 1.6.
[20] This (and the next) is a property of all odd integers (not just prime numbers).
[21] The reason for being repeating is because the reciprocals are rational numbers. The exception of 2 and 5 (which the decimal representation of their reciprocals terminates) is because 2 and 5 are the factors of 10 which is the base of the decimal system of representation.
[22] Up to sign changes or order of terms.
[23] The exception of 2 (i.e. by "odd") is because any difference of perfect squares is either odd or a multiple of 4 (and 2 is neither).

integers are consecutive.[24]

32. For every prime p, the set $\{0, 1, 2, \ldots, p-1\}$ forms a complete residue system (modulo p).
33. Every prime number p has at least one primitive root (modulo p).[25]
34. For every odd prime p, there are exactly $(p-1)/2$ quadratic residues (modulo p), and $(p-1)/2$ quadratic non-residues (modulo p).[26]
35. For every prime $p \geq 7$ there is at least one pair of consecutive quadratic residues (modulo p) and one pair of consecutive quadratic non-residues (modulo p).
36. For any prime p of the form $4k+1$, -1 is a quadratic residue (modulo p).
37. For any prime p of the form $4k-1$, -1 is a quadratic non-residue (modulo p).
38. For any odd prime p:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \tag{3}$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \tag{4}$$

$$\left(\frac{n^2}{p}\right) = \left(\frac{n}{p}\right)^2 \tag{5}$$

where the left hand sides (and the right hand side of the last) represent the Legendre symbol.

39. For any prime p, the set $\{1, 2, \ldots, p-1\}$ forms a group under multiplication modulo p.[27]
40. For every prime p, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field.
41. For every prime p, every non-zero element of the ring $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse.
42. For every prime p, the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots, p-1\}$ is cyclic of order $p-1$.

1.5 Oddities and Exceptions about Prime Numbers

The following are some examples of common oddities and exceptions about prime numbers or related to prime numbers:[28]

1. The only even prime is 2.
2. The only prime whose digits are all even is 2.
3. The only factorial number that is prime is 2 (i.e. $2 = 2!$).
4. The only prime that divides none of Mersenne numbers is 2 (see § 2.1.41).
5. The only prime that is neither balanced nor strong nor weak is 2 (see § 2.1.1, § 2.1.79 and § 2.1.89).[29]
6. For $n \in \mathbb{N}_0$, the only prime of either form $3^n \pm 1$ is 2, i.e. $2 = 3^0 + 1 = 3^1 - 1$.
7. The only prime of the form $n^3 + 1$ is 2 ($n \in \mathbb{N}$).
8. The only prime that cannot be expressed as a difference of perfect squares is 2.
9. The only prime p where both p and $p+2$ can be expressed as sums of two perfect squares is 2.

[24] From this point and its predecessor we conclude:
- Every odd prime can be written as a difference of two squares of integers in exactly one way (i.e. the integers must be consecutive).
- The prime 2 is the only exception (as it cannot be written in this way).

[25] An integer r is called a *primitive root* (modulo k) if every integer n coprime to k is congruent (modulo k) to a natural power of r. In mathematical terms, this means $n \stackrel{k}{=} r^s$ for some $s \in \mathbb{N}$ with both n and r being coprime to k. Primitive root (modulo k) may also be defined (more simply) as an element in a reduced residue system (modulo k) whose natural powers generate all the elements in the system.

[26] An integer n coprime to k is a *quadratic residue* (modulo k) if the congruence $x^2 \stackrel{k}{=} n$ has a solution. If n is coprime to k and no such solution exists, then n is a *quadratic non-residue* (modulo k).

[27] We may also say: for any prime p, the multiplicative group of integers (modulo p) has order $p-1$. It is noteworthy that the primality of p is a necessary and sufficient condition for this set to be a group under multiplication (modulo p).

[28] Also refer to `https://t5k.org/curios/home.php` and see Point 3 of § 11.11.

[29] This is because 2 has no predecessor prime and hence this classification does not apply to it.

10. The only prime of the form $n^2 - 1$ is 3 (when $n = 2$; $n \in \mathbb{N}$).
11. The only prime of the form $n^n - 1$ is 3 (when $n = 2$; $n \in \mathbb{N}$).
12. The only prime p for which $p^2 + 2$ is also prime is $p = 3$.
13. The only prime that is both a Fermat prime and a Mersenne prime is 3 (see § 2.1.20 and § 2.1.41).
14. The only Fibonacci prime with composite index is 3 (see § 2.1.21).
15. The only triangular number that is prime is 3.[30]
16. The only prime of the form $2n^2 + 3n + 1$ (where $n \in \mathbb{Z}$) is 3 (corresponding to $n = -2$).
17. The only prime of the form $n^2 - 4$ is 5 (when $n = 3$; $n \in \mathbb{N}$).
18. The only prime number which is the sum and the difference (simultaneously) of pairs of (distinct) primes is 5, i.e. $5 = 2 + 3$ and $5 = 7 - 2$.
19. The only prime with a prime gap of 2 with its nearest prime neighbors is 5.
20. The only Jacobsthal prime with composite index is 5 (see § 2.1.36).
21. The only prime of the form $2^p + 1$ (where $p \in \mathbb{P}$) is 5.
22. The only prime of the form $n^3 - 1$ is 7 (when $n = 2$; $n \in \mathbb{N}$).
23. The only palindromic prime (in base 10) of even number of digits is 11 (see § 2.1.53).
24. The only consecutive primes are 2 and 3.[31]
25. The only consecutive pairs of twin primes are $(3, 5)$ and $(5, 7)$, i.e. they share a number which is 5.[32]
26. The only balanced prime with a prime gap of 2 with its nearest prime neighbors is 5 (see § 2.1.1).
27. The only prime pair whose (non-trivial) perfect powers differ by 1 is (2, 3), i.e. $3^2 - 2^3 = 1$.[33]
28. The only non-negative integers which are neither prime nor composite are 0 and 1.
29. The only multi-digit prime numbers with identical digits are repunits (see § 2.1.69).
30. 2 and 5 are the only primes whose reciprocals have a terminating decimal representation (i.e. not repeating like the reciprocals of all other primes). Also see § 2.1.23.
31. (5, 11, 17, 23, 29) is the only sexy prime quintuplet (see § 2.1.74).
32. The only odd prime gap g_n $(= p_{n+1} - p_n)$ is $g_1 = 1$ which occurs only between 2 and 3.
33. The only binomial coefficients that are prime are those of the form C_1^p (or C_{p-1}^p) where $p \in \mathbb{P}$.
34. The only prime that is both a Mersenne prime and a Wagstaff prime is 3 (see § 2.1.41 and § 2.1.87).

1.6 The Infinitude of Prime Numbers

The infinitude of prime numbers has many proofs (where it is reported that there are at least 200 proofs). Some of these proofs are direct while others are indirect (i.e. the infinitude of primes is implied by certain theorems whose content and subject is not the infinitude of primes). The following are a few examples of the proofs of the infinitude of primes:

1. Euclid's proof: this is the most ancient and the most direct (and possibly the most simple) proof of infinitude which starts by assuming the finitude of primes where this assumption leads to a contradiction.[34]
2. Euler's proof: this is based on the divergence of the harmonic series of prime numbers (i.e. $\sum_{p \in \mathbb{P}} 1/p$; see § 9.2.1) which should be true only if there are infinitely many prime numbers.[35] Also see § 5.1.28.
3. Erdos' proof: this is based on the unique factorization of any positive integer into two factors: squared

[30] Triangular numbers are integers of the form $(n^2 + n)/2$ where $n \in \mathbb{N}$.
[31] "Consecutive" here means there is no integer between them.
[32] Equivalently, the only cousin prime pair (see § 2.1.10) with a prime in-between is (3, 7). Similarly, (3, 5, 7) are the only triplet of consecutive odd integers that are all prime.
[33] Actually, this is Mihailescu's theorem (or Catalan's conjecture) applied to prime numbers.
[34] Euclid's proof may be formulated in different forms and flavors; some of which follow logic other than contradiction (e.g. proof by cases) and hence its nature (as a proof by contradiction or otherwise) should depend on these details.
[35] In fact, the divergence of the harmonic series of prime numbers has several proofs (and so is the infinitude of primes which is based on this fact).

and square-free (which leads, assuming the finitude of primes, to a contradiction and hence this is a proof by contradiction).
4. The proof of the statement: "Fermat numbers are pairwise relatively prime" can be used as an indirect proof of the infinitude of primes (see § 2.1.20).[36]
5. Furstenberg's topological proof of the infinitude of prime numbers which is a proof by contradiction (i.e. assuming the finitude of primes leads to the conclusion that a certain set is both open and closed).
6. The proof of the statement: "any prime divisor of a Mersenne number $M_p = 2^p - 1$ is of the form $2kp+1$ (where p is an odd prime and $k \in \mathbb{N}$)" can be used as an indirect proof of the infinitude of primes.
7. The proof of the statement: "any prime factor of $n! + 1$ is $> n$" can be used as an indirect proof of the infinitude of primes.
8. Bertrand's postulate (see § 5.1.2) can be used as a proof for the infinitude of prime numbers (noting that this is related to Ramanujan primes; see Point 3 of § 2.1.68).
9. Some proofs of theorems on the infinitude of primes of certain forms and types may also be included provided that these proofs do not rely on the infinitude of primes in general.[37]

1.7 The Fundamental Theorem of Arithmetic

This theorem states that every natural number greater than 1 is either a prime or can be factored as a product of two or more prime numbers in a unique way, except for the order of the factors. Accordingly, if n is an integer greater than 1 then it can be written uniquely as:

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \tag{6}$$

where $p_1, p_2, \dots, p_k$ are distinct prime numbers and $a_1, a_2, \dots, a_k$ are positive integers. This way of expressing an integer $n > 1$ as a product of powers of distinct prime numbers $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ is called *prime factorization* (or *prime decomposition*) of n.

We note the following:
1. An integer $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ is *square-free iff* none of $a_1, a_2, \dots, a_k$ is greater than 1.
2. Every integer greater than 1 is divisible by some prime. This follows directly from the fundamental theorem of arithmetic.
3. In the above statement of the fundamental theorem of arithmetic, "two or more" does not require being distinct, i.e. they can be distinct or non-distinct (totally or in part). Yes, in Eq. 6 we assume $p_1, p_2, \dots, p_k$ to be distinct to have a unique form.
4. The above form of prime factorization (as given by Eq. 6 and within the stated conditions) may be called "standard prime factorization" to distinguish it from non-standard prime factorization when some of $a_1, a_2, \dots, a_k$ are allowed to be zero for certain purposes.
5. Prime factorization (as defined above) is restricted to integers greater than 1 (even though trivially for prime numbers). However, in many contexts and arguments it may be required to extend and broaden the concept of prime factorization to include 0, 1, and negative integers. So, sometimes it is useful to adopt the convention that the "prime factorization" of 0 is 0, of 1 is 1, and of $\mathbb{Z} \ni n < 0$ is the same as the prime factorization of $|n|$ (or with the inclusion of -1).
6. If $n \in \mathbb{N}$ is given in its prime decomposition as $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ ($a_i \in \mathbb{N}$, $1 \le i \le k$) then all the positive divisors of n (including 1 and n) are precisely the integers of the form:

$$p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \qquad (b_i \in \mathbb{N}_0,\ b_i \le a_i,\ 1 \le i \le k) \tag{7}$$

[36] This proof is attributed to Goldbach and hence it is often called Goldbach's proof.
[37] See for instance § 5.2.4. Also, some proofs of Dirichlet's theorem on arithmetic progressions (see § 5.1.11) may be valid as examples of such proofs.

where we consider all the possible combinations of b_i.

7. If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ then:

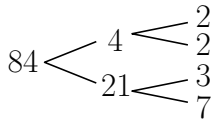
$$\tau(n) = \prod_{i=1}^{k} (a_i + 1) \tag{8}$$

where $\tau(n)$ is the divisor-counting function of n (see footnote [16]).

8. There are two main methods for prime factorization (i.e. how to obtain the prime factorization of a given composite number):[38]

• The *direct method* (or *upside-down division method*) where we repeatedly divide the given number by the smallest prime that divides it, recording the prime divisors as we proceed, until the remaining quotient is prime. Thus, we test the primes in increasing order (i.e. $2, 3, 5, 7, \ldots$) and repeat a prime as many times as necessary. For example, if we want to prime-factorize 84 by this method then we divide 84 by 2 (since it is even) to get 42, then we divide 42 by 2 (since it is even) to get 21, then we divide 21 by 3 (since it is divisible by 3) to get 7, and we stop here because 7 is prime and hence it cannot be divided further. Accordingly, $84 = 2^2 \times 3 \times 7$.

• The *factor tree method* where the given number is placed at the root of a tree and repeatedly factored into smaller factors until all the terminal branches of the tree are prime. For example, if we want to prime-factorize 84 by this method, we produce a factor tree such as the one below. The prime factors of 84 occur at the terminal branches of the tree (namely 2, 2, 3, 7), and hence $84 = 2^2 \times 3 \times 7$.



[38] The focus of this note is on "generic methods" (outlining the factorization process) rather than "algorithms". We also note that these methods are similar and can be regarded as essentially identical.

Chapter 2
Types of Primes

In this chapter, we briefly investigate various types of prime numbers. This investigation is by no means comprehensive, as numerous other types are not listed here, because (for instance) they are restricted to certain academic circles or research groups, or because they have little theoretical and practical (and possibly even recreational) significance, or because their status as specific or conventional prime types is ambiguous (see for example § 2.2). Indeed, there are infinitely many possible ways of defining new types of prime numbers by imposing different conditions or criteria. Our investigation in this chapter also extends to certain categories of prime numbers (where the meaning of "categories" will become clearer as we proceed with our investigation; see § 2.4 through § 2.9).

2.1 Common Types of Prime Numbers

This section is largely about the most commonly studied types of prime numbers (where we order the investigated types alphabetically for easy access).

2.1.1 Balanced Primes

A balanced prime is a prime number which is the average of the nearest primes before and after it (and hence it has equal prime gap on both sides), that is:

$$p_n = \frac{p_{n-1} + p_{n+1}}{2} \tag{9}$$

where p_n is the n^{th} prime number which is supposedly a balanced prime. For example, 5 is a balanced prime because $5 = (3 + 7)/2$. We note:

1. The first 15 balanced primes (i.e. those < 1000) are: 5, 53, 157, 173, 211, 257, 263, 373, 563, 593, 607, 653, 733, 947, 977.[39]
2. The largest known[40] balanced prime is a 15004-digit number discovered in 2022[41] (beating the previous record which is the 7532-digit number $197418203 \times 2^{25000} - 1$).
3. The gap between a balanced prime and its nearest prime neighbors is either 2 (for number 5) or a multiple of 6 (for balanced primes greater than 5).[42]
4. It is conjectured that there are infinitely many balanced primes.
5. The concept of "balanced prime" is generalized to higher orders where the "balanced prime of order n" means the prime number which is the average of the nearest n primes before and after it (and hence the *ordinary* balanced prime is a balanced prime of order 1).[43]

[39] See `https://oeis.org/A006562`.

[40] "The largest known" here and in the upcoming occurrences mostly require checking and updating. We provide such information mainly for curiosity and to have a general idea about the order of size of such items.

[41] The number is reportedly $2494779036241 \times 2^{49800} + 7$. Apparently this is a proven prime (noting that there is seemingly a larger probable known balanced prime). However, we strongly recommend further checks to all these details.

[42] This is related to the fact that all primes greater than 3 are of the form $6n \pm 1$ ($n \in \mathbb{N}$).

[43] See for example `https://oeis.org/A082077` and `https://oeis.org/A082078`. It is worth noting that this generalization is based on the concept of "average" (i.e. mathematical mean) rather than on the concept of "prime gap".

6. Balanced primes, strong primes (see § 2.1.79) and weak primes (see § 2.1.89) partition[44] the set of odd prime numbers (i.e. all primes excluding 2 and hence 2 is the only prime number which is neither balanced nor strong nor weak). Also see § 2.1.26.

2.1.2 Bell Primes

A Bell prime is a Bell number that is prime (see the upcoming Note). We note:
1. The first 4 Bell primes (i.e. those $< 10^{37}$) are: 2, 5, 877, 27644437 (corresponding to $\mathscr{B}_2, \mathscr{B}_3, \mathscr{B}_7, \mathscr{B}_{13}$).[45]
2. The largest known Bell prime (by index) is apparently $\mathscr{B}_{2841}$.
3. It is conjectured that there are infinitely many Bell primes.

Note: The *Bell numbers* ($\mathscr{B}_n$ where $n = 0, 1, 2, \ldots$) are integers that count the different ways of partitioning a set which has precisely n elements. We note:
A. The Bell numbers may be defined by the following recurrence relation:

$$\mathscr{B}_{n+1} = \sum_{k=0}^{n} C_k^n \mathscr{B}_k \tag{10}$$

where $\mathscr{B}_0 = 1$ and C_k^n is the binomial coefficient.
B. The first 12 Bell numbers (i.e. those $< 10^6$) are: 1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570 (corresponding to $n = 0, 1, 2, \ldots, 11$).[46]
C. According to Touchard's congruence (where $p \in \mathbb{P}$):

$$\mathscr{B}_{n+p} \equiv \mathscr{B}_n + \mathscr{B}_{n+1} \pmod{p} \tag{11}$$

2.1.3 Carol Primes

Carol primes are prime numbers of the form $(2^n - 1)^2 - 2 = 4^n - 2^{n+1} - 1$ where $n \in \mathbb{N}$. We note:
1. The first 8 Carol primes (i.e. those $< 10^{10}$) are: 7, 47, 223, 3967, 16127, 1046527, 16769023, 1073676287 (corresponding to $n = 2$, 3, 4, 6, 7, 10, 12, 15).[47]
2. The largest known Carol prime is apparently $(2^{695631} - 1)^2 - 2$ (with about 419 thousand decimal digits).
3. Carol primes are a special case of the primes of the form $m^2 - 2$ (which are a kind of near-square primes; see § 2.1.49).
4. It is conjectured that there are infinitely many Carol primes.
5. Carol primes may also be defined more generally as the primes of the form $(b^n - 1)^2 - 2$ where b is an even positive integer and $n \in \mathbb{N}$.
6. Carol primes are usually associated with Kynea primes due to their similarity in form (see § 2.1.37).

2.1.4 Catalan Primes

These are Catalan numbers which are prime (see the upcoming Note). It is proven that there are no Catalan primes other than $C_2 = 2$ and $C_3 = 5$.

Note: The *Catalan numbers* are defined by the formula:

$$C_n = \frac{C_n^{2n}}{n+1} = \frac{(2n)!}{n!(n+1)!} \qquad (n = 0, 1, 2, \ldots) \tag{12}$$

[44] "Partition" means exhaustiveness and mutual exclusiveness.
[45] See `https://oeis.org/A051131` and `https://oeis.org/A051130`.
[46] See `https://oeis.org/A000110`.
[47] See `https://oeis.org/A091516` and `https://oeis.org/A091515`. Seemingly, there are only 44 known Carol primes.

where C_n is the n^{th} Catalan number and C_n^{2n} is the binomial coefficient. We note:
A. The first 10 Catalan numbers (i.e. those $< 10^4$) are: 1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862.[48]
B. Every prime number divides infinitely many Catalan numbers.

2.1.5 Centered Primes

Centered primes (which may also be called *centered polygonal primes* or *centered k-gonal primes*) are prime numbers that appear in sequences of centered polygonal numbers (see the upcoming Note). For example:
• 19, 31, 109, 199, 409, 571, 631, 829 are centered triangular primes because they are prime numbers appearing in the sequence of centered triangular numbers.[49]
• 5, 13, 41, 61, 113, 181, 313, 421, 613, 761 are centered square primes because they are prime numbers appearing in the sequence of centered square numbers.[50]
• 31, 181, 331, 601, 1051, 1381, 3331, 4951, 5641, 5881, 9151 are centered pentagonal primes because they are prime numbers appearing in the sequence of centered pentagonal numbers.[51]
The finitude of centered k-gonal primes for $k = 8$ and $k = 9$ is proven (i.e. there are no centered k-gonal primes for $k = 8$ and $k = 9$), while the infinitude of centered k-gonal primes for all other $k \geq 3$ is conjectured.

Note: The *centered polygonal numbers* are positive integers representing the number of dots forming regular polygons by a central dot surrounded by successive regular polygonal layers (e.g. equilateral triangle, square, regular pentagon, etc.). Examples are:
A. *Centered triangular numbers* which are given by the formula $[(3n^2 - 3n)/2] + 1$ $(n = 1, 2, 3, \ldots)$. The first 12 entries of this sequence are: 1, 4, 10, 19, 31, 46, 64, 85, 109, 136, 166, 199.[52]
B. *Centered square numbers* which are given by the formula $2n^2 + 2n + 1$ $(n = 0, 1, 2, \ldots)$. The first 12 entries of this sequence are: 1, 5, 13, 25, 41, 61, 85, 113, 145, 181, 221, 265.[53]
C. *Centered pentagonal numbers* which are given by the formula $(5n^2 + 5n + 2)/2$ $(n = 0, 1, 2, \ldots)$. The first 12 entries of this sequence are: 1, 6, 16, 31, 51, 76, 106, 141, 181, 226, 276, 331.[54]

2.1.6 Chen Primes

A Chen prime is a prime number p such that $p + 2$ is either a prime or a semiprime (i.e. a product of two primes; see § 9.5). For example, 5 and 19 are Chen primes because $5 + 2 = 7$ which is a prime, while $19 + 2 = 21$ which is a semiprime (i.e. $21 = 3 \times 7$). We note:
1. The first 20 Chen primes (i.e. those < 100) are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47, 53, 59, 67, 71, 83, 89.[55]
2. The largest known Chen prime is apparently $2996863034895 \times 2^{1290000} - 1$ (with about 388 thousand decimal digits). Also see Point 7 of § 2.1.84.
3. All lower members of twin prime pairs are necessarily Chen primes, but only some upper members of twin prime pairs are Chen primes. Also see § 4.7.3.

---

[48] See `https://oeis.org/A000108`.
[49] See `https://oeis.org/A125602`. These primes are of the form $[(3n^2 - 3n)/2] + 1$ where $n \in \mathbb{N}$, and hence the given 8 entries correspond to $n = 4, 5, 9, 12, 17, 20, 21, 24$ (see `https://oeis.org/A125603`).
[50] See `https://oeis.org/A027862`. These primes are of the form $n^2 + (n+1)^2$ where $n \in \mathbb{N}$, and hence the given 10 entries correspond to $n = 1, 2, 4, 5, 7, 9, 12, 14, 17, 19$ (see `https://oeis.org/A027861`).
[51] See `https://oeis.org/A145838`. These primes are of the form $(5n^2 + 5n + 2)/2$ where $n \in \mathbb{N}$, and hence the given 11 entries correspond to $n = 3, 8, 11, 15, 20, 23, 36, 44, 47, 48, 60$ (see `https://oeis.org/A145837`).
[52] See `https://oeis.org/A005448`.
[53] See `https://oeis.org/A001844`.
[54] See `https://oeis.org/A005891`.
[55] See `https://oeis.org/A109611`.

4. Chen primes contain arithmetic progressions of arbitrary length.
5. There are infinitely many Chen primes (see § 5.1.9). However, the infinitude of Chen primes with composite $p + 2$ (let alone prime $p + 2$ which is the twin prime problem) is an open problem. This infinitude (like the infinitude of twin primes) is conjectured.

Also refer to Chen's theorem II (see § 5.1.9) which is closely related to Chen primes.

2.1.7 Circular Primes

A circular prime is a prime number that remains prime under all cyclic permutations of its digits. An example of circular primes is 113 because 113, 131 and 311 are all primes. We note:

1. Being circular is base-dependent (where 10 is the conventional base).
2. The first 25 circular primes in base 10 (i.e. those < 1000) are:. 2, 3, 5, 7, 11, 13, 17, 31, 37, 71, 73, 79, 97, 113, 131, 197, 199, 311, 337, 373, 719, 733, 919, 971, 991.[56]
3. The largest known circular prime is apparently the repunit $U_{8177207} = (10^{8177207} - 1)/9$.[57]
4. All circular primes (except 2 and 5) contain only the digits 1, 3, 7, 9 (because otherwise some of their cyclic permutations will be even and/or divisible by 5).
5. All repunit primes (see § 2.1.69) are circular, and hence repunit primes are a (proper) subset of circular primes.
6. All permutable primes (see § 2.1.58) are circular, and hence permutable primes are a (proper) subset of circular primes (e.g. 197 is circular but not permutable).
7. It is conjectured that there are only finitely many circular primes (excluding repunit primes; see Point 6 of § 2.1.69).[58]

2.1.8 Cluster Primes

A cluster prime is an odd prime p where every even integer m ($2 \leq m \leq p - 3$) can be written as the difference between two primes which are less than or equal to p. For example, 13 is a cluster prime because all even positive integers which are less than or equal to $13 - 3$ (i.e. 2, 4, 6, 8, 10) can be written as differences between two primes which are less than or equal to p, that is: $2 = 5 - 3$ (or $7 - 5$ or $13 - 11$), $4 = 7 - 3$ (or $11 - 7$), $6 = 11 - 5$ (or $13 - 7$), $8 = 11 - 3$ (or $13 - 5$), and $10 = 13 - 3$. We note:

1. The first 23 cluster primes (i.e. those < 100) are: 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89.[59]
2. All prime numbers under 100 (excluding 2 and 97) are cluster primes.
3. The prime gap preceding a cluster prime is always less than or equal to 6 (i.e. 2 or 4 or 6).
4. It is unknown if there are infinitely many cluster primes. In fact, the infinitude of cluster primes should imply the existence of infinitely many prime pairs (p_{n-1}, p_n) with a gap of 6 or less between them which is an open (and very difficult problem) related to the twin prime conjecture and the bound on the gaps between prime numbers in general (see § 5.1.44).[60]

---

[56] See `https://oeis.org/A068652`.

[57] Apparently the repunit $U_{8177207}$ is a probable prime. The largest proven circular prime is apparently the repunit U_{109297}. The largest known non-repunit circular prime is seemingly 999331. Also see § 2.1.69.

[58] Noting that permutable primes are a proper subset of circular primes (see Point 6), it seems that this conjecture contradicts the conjecture of infinitude of permutable primes (see Point 11 of § 2.1.58) unless the permutable primes conjecture includes repunit primes while the circular primes conjecture excludes them. Alternatively, there may be contradicting conjectures about the infinitude of (at least) one of these types of primes.

[59] See `https://oeis.org/A038134`.

[60] It is worth noting that there may not be a specific conjecture about the infinitude of cluster primes, but this issue (as indicated above) is related to other issues (connected to the bounded gaps theorems) with specific conjectures such as twin prime conjecture (see Point 1 of § 6.1.34), and Polignac's conjecture (see § 6.1.26). In fact, this seems to apply to many other claimed conjectures about the infinitude of certain types of prime numbers (as listed and stated mostly in the subsections of this section).

2.1.9 Compositorial Primes

A compositorial prime is a prime number of the form $(n!/n\#) \pm 1$, where $n!$ is the factorial of n and $n\#$ is the n^{th} primorial number (i.e. of the second kind; see the Note in § 2.1.64) which is the product of all primes $\leq n$ (and hence $n!/n\#$ represents the product of all non-prime positive integers less than or equal to n). We note:

1. Referring to the Note in 2.1.64, in the above definition of compositorial prime we are using the n^{th} primorial number of the second kind (i.e. $n\#$ not $p_n\#$).
2. The first 6 compositorial primes (i.e. those < 1000) are: 2, 3, 5, 23, 191, 193.[61]
3. The largest known compositorial prime is apparently $751882!/751882\# + 1$ (with about 3.76 million decimal digits).
4. There are a number of compositorial twin prime pairs (i.e. both $n!/n\# - 1$ and $n!/n\# + 1$ are primes) such as (3, 5), (191, 193) and $(280!/280\# - 1, 280!/280\# + 1)$.
5. Compositorial primes may be seen as the "composite analog" of primorial primes (see § 2.1.64) noting that $n!/n\#$ represents the product of all non-prime positive integers $\leq n$.
6. It is conjectured that there are infinitely many compositorial primes.

Also see § 2.1.19 and § 2.1.64.

2.1.10 Cousin Primes

Cousin primes are a pair of prime numbers which are 4 apart (such as 3 and 7). We note:

1. According to the above definition, 4 is not necessarily a prime gap, and hence another prime may exist between cousin primes. However, the only prime triplet of the form $(p, p+2, p+4)$ is (3, 5, 7) and hence (3, 7) is the only cousin prime pair with a prime in-between. So, if we exclude (3, 7) we can say that 4 is a prime gap.
2. The first 14 cousin prime pairs (i.e. those < 200) are: (3, 7), (7, 11), (13, 17), (19, 23), (37, 41), (43, 47), (67, 71), (79, 83), (97, 101), (103, 107), (109, 113), (127, 131), (163, 167), (193, 197).[62]
3. The largest known cousin prime pair is apparently $(p, p+4)$ where $p = 954589277 \times (2^{332267} - 2^{110758}) + 2^{221511} - 3$ (with about 100 thousand digits each).[63]
4. It is conjectured that there are infinitely many cousin primes (apparently as an instance or part of Polignac's conjecture; see § 6.1.26).

2.1.11 Cuban Primes

A cuban prime p is a prime of the form:

$$p = \frac{x^3 - y^3}{x - y} \qquad (x, y \in \mathbb{N}) \tag{13}$$

where $x = y + 1$ or $x = y + 2$. The name "cuban" is because of the involvement of cubes in this definition. We note:

1. The above equation simplifies to $p = 3y^2 + 3y + 1$ for the first kind (i.e. $x = y + 1$), and simplifies to $p = 3y^2 + 6y + 4$ for the second kind (i.e. $x = y + 2$).[64] So, a cuban prime is specifically a prime value

[61] We have:
$2 = (n!/n\#) + 1$ for $n = 0, 1, 2, 3$ $3 = (n!/n\#) - 1$ for $n = 4, 5$ $5 = (n!/n\#) + 1$ for $n = 4, 5$
$23 = (n!/n\#) - 1$ for $n = 6, 7$ $191 = (n!/n\#) - 1$ for $n = 8$ $193 = (n!/n\#) + 1$ for $n = 8$
Also see `https://oeis.org/A140293` and `https://oeis.org/A140294`.

[62] See `https://oeis.org/A023200` and `https://oeis.org/A046132`.

[63] See `https://www.pzktupel.de/CPAP/CPAP02`.

[64] Considering the parity of these expressions we can say: cuban primes of the second kind must always have an odd y, while the cuban primes of the first kind can have an even (as well as odd) y.

produced by these polynomials for some $y \in \mathbb{N}$.
2. The first 11 cuban primes (i.e. those < 1000) of the first kind are: 7, 19, 37, 61, 127, 271, 331, 397, 547, 631, 919.[65] For example, $7 = 3y^2 + 3y + 1$ for $y = 1$ (and hence $x = 2$), and $19 = 3y^2 + 3y + 1$ for $y = 2$ (and hence $x = 3$).
3. The first 11 cuban primes (i.e. those < 10000) of the second kind are: 13, 109, 193, 433, 769, 1201, 1453, 2029, 3469, 3889, 4801.[66] For example, $13 = 3y^2 + 6y + 4$ for $y = 1$ (and hence $x = 3$), and $109 = 3y^2 + 6y + 4$ for $y = 5$ (and hence $x = 7$).
4. The largest known cuban prime is a 3153105-digit number discovered in 2023 (noting that this is seemingly a probable rather than a proven prime).
5. Every cuban prime of the first kind is a centered hexagonal number.[67]
6. The infinitude of cuban primes seems to be conjectured by some mathematicians, although this could be as an implication or instance of other general conjectures (e.g. Bunyakovsky's conjecture; see § 6.1.11) rather than an independent conjecture which is specific to the cuban primes.
7. The two variables (i.e. x and y) of the cuban primes are correlated (i.e. by the conditions $x = y + 1$ and $x = y + 2$) and this enables the reduction of the algebraic formula of this type of primes to the two single-variable formulae, i.e. $3y^2 + 3y + 1$ and $3y^2 + 6y + 4$ as seen in Point 1 above. However, this correlation may be relaxed (by letting $x = y + k$ for a variable $k \in \mathbb{N}$) and hence we get *generalized cuban primes* which are a type of prime numbers defined by genuine (i.e. non-correlated) two variables (like, for instance, Leyland primes; see § 2.1.38).

2.1.12 Cullen Primes

A Cullen prime is a Cullen number that is prime (see the upcoming Note). We note:
1. The number of known Cullen primes is 16 (i.e. those corresponding to n equal to: 1, 141, 4713, 5795, 6611, 18496, 32292, 32469, 59656, 90825, 262419, 361275, 481899, 1354828, 6328548, 6679881).[68]
2. It is unknown if there are infinitely many Cullen primes (noting that the infinitude of Cullen primes is conjectured).
3. Cullen primes are of particular interest in computational number theory, both as targets for large-scale searches and as a setting for specialized primality testing and primality proving algorithms.

Also see § 2.1.93.

Note: A *Cullen number* is a positive integer of the form $2^n n + 1$ where $n \in \mathbb{N}_0$. The first 13 Cullen numbers (i.e. those $< 10^5$) are: 1, 3, 9, 25, 65, 161, 385, 897, 2049, 4609, 10241, 22529, 49153.[69]

2.1.13 Cyclic Primes

Apparently, "cyclic primes" is used by some authors to label circular primes (see § 2.1.7), while used by others to label full reptend primes (see § 2.1.23). In fact, we cannot rule out the possibility of other conventions. Hence, the interested readers should investigate this issue thoroughly to avoid confusion and mistakes.

---

[65] See `https://oeis.org/A002407`.
[66] See `https://oeis.org/A002648`.
[67] The n^{th} centered hexagonal number is given by the formula $H(n) = 3n^2 + 3n + 1$ where $n \in \mathbb{N}_0$. See `https://oeis.org/A003215`.
[68] See `https://oeis.org/A005849` and `https://oeis.org/A050920`. But also see `https://primegrid.fandom.com/wiki/Cullen_Prime_Search` and `https://t5k.org/top20/page.php?id=42`.
[69] See `https://oeis.org/A002064`.

2.1.14 Cyclotomic Primes

A cyclotomic prime is a prime number of the form $\Phi_n(2)$ where $\Phi_n(x)$ is the n^{th} cyclotomic polynomial.[70] These primes are usually investigated in algebraic number theory. We note:

1. The $x = 2$ value in the definition of cyclotomic primes is the most common (but not the only) integer argument considered in the investigation of this type of primes. The importance of the $x = 2$ value (which makes it the default or the conventional value for cyclotomic primes) comes from the fact that it is related to important prime types such as Fermat and Mersenne primes (which are cyclotomic at $x = 2$; see § 2.1.20 and § 2.1.41), that is:
   - Fermat primes satisfy $F_k \equiv 2^{2^k} + 1 = \Phi_{2^{k+1}}(2)$ where $k \in \mathbb{N}_0$.
   - Mersenne primes satisfy $M_p \equiv 2^p - 1 = \Phi_p(2)$ where $p \in \mathbb{P}$.
2. Examples of cyclotomic primes are: 3, 5, 7, 31 (corresponding to $n = 2, 4, 3, 5$).
3. It is conjectured that there are infinitely many cyclotomic primes.[71] This conjecture is obviously related to other conjectures, e.g. if the infinitude of Fermat or Mersenne or Wagstaff primes (see § 2.1.20, § 2.1.41 and § 2.1.87) is proved then this conjecture will be confirmed (but the converse is untrue).[72]

2.1.15 Delicate Primes

A delicate prime (also known as *digitally delicate prime* or *weakly prime*) is a prime number that becomes composite if any one of its digits is replaced (i.e. individually) by any other digit.[73] We note:

1. Being delicate is base-dependent (where 10 is the conventional base).
2. The first 5 delicate primes in base 10 (i.e. those $< 10^6$) are: 294001, 505447, 584141, 604171, 971767.[74]
3. Delicate primes (which are "weakly primes") should not be confused with "weak primes" (see § 2.1.89).
4. There are infinitely many delicate primes in any base.[75] In fact, there is a positive proportion of delicate primes among all prime numbers.
5. The concept of delicate primes is extended to the concept of "widely digitally delicate primes" which means primes that become composite even if we change any one of the (infinitely many) leading zeros to another digit.[76]

2.1.16 Dihedral Primes

A dihedral prime (also known as *dihedral calculator prime*) is a prime number that remains prime (whether itself or another prime) under certain reflectional and rotational *visual* symmetries (see the upcoming Point 1) when displayed in a seven-segment display. We note:

1. The aforementioned symmetries are up-down (or vertical) mirror reflection, left-right (or horizontal) mirror reflection, surface mirror reflection, 180° rotation, as well as any combination of these symmetries. It is important to note "visual" in the above definition to distinguish the symmetries here from non-visual

[70] The n^{th} cyclotomic polynomial $\Phi_n(x)$ in $\mathbb{Z}[x]$ is the unique monic irreducible polynomial with integer coefficients which is a divisor of $x^n - 1$ and whose roots are the primitive n^{th} roots of unity.

[71] It is proved that there are infinitely many composite numbers of the form $\Phi_n(2)$.

[72] For Wagstaff primes we have $W_p = \Phi_{2p}(2)$.

[73] It is not clear if the convention excludes a leading zero which changes the order of the number, i.e. from being a number with n digits to a number with less than n digits.

[74] See `https://oeis.org/A050249`. We did not find reliable information or official record about the largest known delicate prime.

[75] More precisely, there are infinitely many prime numbers p such that, in a fixed base $b \geq 2$ (e.g. base 10), every integer obtained by changing exactly one digit of p to a different digit in $0, \ldots, b-1$ (while avoiding leading zero) is composite (Erdos' theorem).

[76] An explicit example of such a prime was found recently. Moreover, it is proven that there are infinitely many of these primes.

symmetries used in the definition of other types of prime numbers (see § 2.1.17 and § 2.1.53).[77]
2. To be qualified as a dihedral prime it must satisfy all these symmetries. For instance, the prime number 3 satisfies the vertical reflection symmetry (i.e. by a horizontal mirror) but it does not satisfy the horizontal reflection symmetry (i.e. by a vertical mirror) and hence it is not a dihedral prime.
3. Being dihedral prime is a decimal (i.e. base 10) attribute, although the concept can be generalized to other bases.
4. Dihedral prime must contain only digits that remain valid digits under all the aforementioned symmetries, and hence dihedral primes can contain only the following digits: 0, 1, 2, 5, and 8.[78]
5. Repunit primes (see § 2.1.69) are a proper subset of dihedral primes.
6. The first 8 dihedral primes (i.e. those $< 10^5$) are: 2, 5, 11, 101, 181, 1181, 1811, 18181.[79]
7. The largest known (non-repunit) dihedral prime is apparently the palindrome $10^{180054} + 8 \times \frac{10^{58567}-1}{9} \times 10^{60744} + 1$ (with about 180 thousand decimal digits).
8. It is seemingly conjectured that there are infinitely many dihedral primes (noting that this is also related to the conjectured infinitude of repunit primes because the infinitude of repunit primes should imply the infinitude of dihedral primes).
9. A distinction must be made between the mirror reflection in dihedral primes and that in emirp primes and palindromic primes (see § 2.1.17 and § 2.1.53), i.e. the mirror-reflection is visual in the former but non-visual (i.e. textual) in the latter. However, every dihedral prime is either an emirp or a palindrome (but the reverse is untrue). In other words, dihedral primes are a proper subset of reversible primes (see § 2.1.70).

2.1.17 Emirp Primes

An emirp prime (or just *emirp*) is a prime number that results in a different prime when its digits are reversed[80] (e.g. 17 and 73 which become 71 and 37 when their digits are reversed). We note:
1. Being emirp is base-dependent (where 10 is the conventional base).
2. The first 36 emirp primes in base 10 (i.e. those < 1000) are: 13, 17, 31, 37, 71, 73, 79, 97, 107, 113, 149, 157, 167, 179, 199, 311, 337, 347, 359, 389, 701, 709, 733, 739, 743, 751, 761, 769, 907, 937, 941, 953, 967, 971, 983, 991.[81]
3. The largest known emirp prime is seemingly $10^{47253} - 22 \times 10^{21607} - 1$ (with about 47 thousand decimal digits).[82]
4. It is conjectured that there are infinitely many emirp primes.

Also see § 2.1.53 and § 2.1.70.

2.1.18 Euler Primes

An Euler prime is a prime number of the form $n^2 + n + 41$ for some $n \in \mathbb{N}_0$. We note:
1. The first 13 Euler primes (i.e. those < 200) are: 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197 (corresponding to $n = 0, 1, \ldots 12$).[83]
2. The largest known Euler prime is seemingly a 398204-digit number discovered in 2013.

---

[77] Some of these symmetries are redundant because they can be achieved by combination of other symmetries. However, we included them for clarity.
[78] We note that some restrict the allowed digits to the self-reflecting ones (i.e. 0, 1, and 8) and this should eliminate the dihedral primes that contain 2 and 5.
[79] See `https://oeis.org/A134996`.
[80] Reversion may be seen as "horizontal mirror-reflection" but not in a visual sense.
[81] See `https://oeis.org/A006567`.
[82] See `https://t5k.org/curios/page.php?number_id=6053382`. But also see `https://oeis.org/A006567`.
[83] See `https://oeis.org/A005846` and `https://oeis.org/A056561`.

3. All the integers of the form $n^2 + n + 41$ for $n = 0, 1, \ldots 39$ are primes.[84]
4. Some authors may impose the condition "for some $n \in \mathbb{Z}$ (instead of "for some $n \in \mathbb{N}_0$"). However, since:
$$(-n-1)^2 + (-n-1) + 41 = n^2 + n + 41$$
this extension is redundant because it produces the numbers repetitively (i.e. twice).
5. Some authors may use the form $n^2 - n + 41$ or use both forms (i.e. $n^2 + n + 41$ and $n^2 - n + 41$). However:
$$(n+1)^2 - (n+1) + 41 = n^2 + n + 41$$
and hence using the form $n^2 - n + 41$ is equally valid, while using both forms is repetitive (i.e. it produces the numbers twice), and thus any one of these forms is sufficient.
6. Euler primes are different from the primes of the so-called "Euler numbers" (or their absolute value) such as 5 and $|-61|$ (although 61 is also an Euler prime).[85]
7. Euler primes are different from the prime(s) of the so-called "Eulerian numbers" such as 11.[86]
8. It is conjectured that there are infinitely many Euler primes (and this could be an instance of more general conjectures like Bunyakovsky's conjecture or the Hardy-Littlewood conjecture F; see § 6.1.11 and § 6.1.20).[87]

2.1.19 Factorial Primes

A factorial prime is a prime number of the form $n! \pm 1$ where $n \in \mathbb{N}$. We note:

1. There are not many known factorial primes because they grow at an extremely rapid rate (where the count is reported to be 53).
2. The first 7 factorial primes (i.e. those $< 10^4$) are: 2, 3, 5, 7, 23, 719, 5039 (corresponding to $n = 1, 2, 3, 3, 4, 6, 7$).[88]
3. The largest known factorial prime is seemingly $632760! - 1$ (with 3395992 digits).[89]
4. 2 is the only number which is a "factorial prime" in two senses, i.e. being of the form $n! + 1$ and being a factorial (i.e. $2 = 2!$) and a prime number at the same time.
5. If we replace $n \in \mathbb{N}$ in the above definition with $n \in \mathbb{N}_0$ then 2 becomes the only number which is a factorial prime for two values of n, i.e. $2 = 0! + 1$ and $2 = 1! + 1$.
6. 3 is the only known value of n for which both $n! - 1$ and $n! + 1$ are prime (corresponding to 5 and 7). In fact, it is conjectured that 3 is the only value of n for which both $n! - 1$ and $n! + 1$ are prime.[90]
7. Because the number $n! \pm 1$ is coprime to every positive integer $\leq n$, the divisibility primality test of $n! \pm 1$ requires inspection of only the primes p's where $n < p \leq (n! \pm 1)^{1/2}$. This facilitates the search for factorial primes (although the efficiency gain is usually trivial since this excludes only the very small primes).
8. "Factorial prime" may be generalized to include factorials of higher orders and hence becomes "multi-factorial prime", i.e. primes of the forms: $n! \pm 1$, $n!! \pm 1$, $n!!! \pm 1$, etc. For example, 79 is a triple factorial

---

[84] In fact, "Euler primes" may be restricted to these 40 primes.

[85] *Euler numbers* (or *secant numbers*) are integers (denoted E_n) appearing as coefficients in the Taylor series expansion of some trigonometric functions. We note that $E_4 = 5$ and $E_6 = -61$.

[86] *Eulerian number* is a concept in combinatorics that represents the number of permutations of certain numbers.

[87] There may also be similar conjectures about the primes of "Euler numbers" and/or "Eulerian numbers" (which we mentioned in Points 6 and 7). The interested readers should refer to the literature.

[88] See `https://oeis.org/A088054`.

[89] See `https://googology.fandom.com/wiki/Largest_known_factorial_prime` and `https://t5k.org/largest.html`.

[90] In other words, the only known twin factorial prime pair with the same n is $(3! - 1, 3! + 1)$, i.e. (5, 7). It is commonly suspected (and apparently conjectured) that there is no other twin factorial prime pair (i.e. with the same n).

(i.e. multi-factorial of order 3) prime because:[91]

$$79 = (8 \times 5 \times 2) - 1 = 8!!! - 1 \tag{14}$$

9. Wilson's theorem imposes certain limitations on the numbers that can be factorial primes. For example, for $n \geq 3$ if $n+1$ is prime then $n!+1$ cannot be prime, because (according to Wilson's theorem; see § 5.1.43) if $n+1$ is prime then:

$$([n+1]-1)!+1 \overset{n+1}{=} 0 \qquad \text{i.e.} \qquad n!+1 \overset{n+1}{=} 0 \tag{15}$$

and hence $n!+1$ is composite (because it is divisible by $n+1$).
10. It is conjectured that there are infinitely many factorial primes.[92]
11. There is some similarity between factorial primes and primorial primes (see § 2.1.64). This also applies to compositorial primes (see § 2.1.9).

2.1.20 Fermat Primes

A Fermat prime is a prime number of the form (2^n+1) where $n \in \mathbb{N}$. It can be shown that if (2^n+1) is prime then n is a power of 2, i.e. $n = 2^k$ where $k \in \mathbb{N}_0$. This means that Fermat primes are of the form $(2^{2^k}+1)$, noting that this form is a necessary but not sufficient condition for primality (e.g. $2^{2^5}+1$ is composite). Accordingly, we may define Fermat prime as a Fermat number that is prime (see the upcoming Note). We note:

1. Currently (March 2026), the number of known Fermat primes is only five (which are the first five Fermat numbers 3, 5, 17, 257, 65537 corresponding to $n = 1, 2, 4, 8, 16$ or $k = 0, 1, 2, 3, 4$).[93]
2. It is conjectured that there are only finitely many Fermat primes. It is also conjectured that the known five Fermat primes are the only ones.
3. No Fermat prime F_k can be expressed as $F_k = s^p - t^p$ where $s, t \in \mathbb{N}$ $(s > t)$ and p is an odd prime.
4. Fermat primes are cyclotomic and hence Fermat primes are a (proper) subset of cyclotomic primes (see § 2.1.14), i.e. $F_k \equiv 2^{2^k}+1 = \Phi_{2^{k+1}}(2)$ where $k \in \mathbb{N}_0$. Also, Fermat primes (except 3) are Pythagorean primes (see § 2.1.66) because they are of the form $4k+1$.
5. $n = 2$ is the only natural number for which both (2^n-1) and (2^n+1) are prime numbers.
6. Also see § 7.3.15.

Note: A *Fermat number* is a natural number of the form $2^{2^k}+1$ (where $k \in \mathbb{N}_0$) regardless of being prime or not. Accordingly, Fermat primes is a proper subset of Fermat numbers. We note:

A. The first 7 Fermat numbers (i.e. those $< 10^{38}$) are:[94]

$$3, 5, 17, 257, 65537, 4294967297, 18446744073709551617$$

B. Fermat numbers are generally symbolized as F_k where k is the second exponent (e.g. $F_3 = 2^{2^3}+1$).
C. All Fermat numbers are odd (as can be seen from their form).
D. Fermat numbers can be generated by the recursive formula $F_k = 2 + (F_0 F_1 \dots F_{k-1})$.
E. Fermat numbers are pairwise relatively prime, i.e. F_s and F_t are coprime where $s \neq t$ $(s, t \in \mathbb{N}_0)$.[95]
F. No Fermat number F_k $(k \neq 1)$ can be the sum of two primes.
G. $F_k = (F_{k-1}-1)^2 + 1$ where $k \in \mathbb{N}$.

---

[91] See for instance `https://oeis.org/A084438` and `https://oeis.org/A007661`.
[92] Actually, there is a stronger version of this conjecture, that is: there are infinitely many factorial primes of each form.
[93] See `https://oeis.org/A019434`. Also see the upcoming Note.
[94] See `https://oeis.org/A000215`.
[95] This is used to prove the infinitude of prime numbers (see Point 4 in § 1.6).

H. $F_k = F_{k-1}^2 - 2(F_{k-2} - 1)^2$ where $k > 1$.
I. $F_k + 1 = 6n$ where $k, n \in \mathbb{N}$.
J. The last digit of F_k is 7 where $k > 1$.

2.1.21 Fibonacci Primes

A Fibonacci prime is a Fibonacci number that is prime (see the upcoming Note). We note:
1. The first 9 Fibonacci primes (i.e. those $< 10^6$) are: 2, 3, 5, 13, 89, 233, 1597, 28657, 514229 (corresponding to $n = 3$, 4, 5, 7, 11, 13, 17, 23, 29 in the sequence of Fibonacci numbers).[96]
2. Apparently, the largest proven Fibonacci prime is $\mathcal{F}_{201107}$, while the largest probable Fibonacci prime is $\mathcal{F}_{11964299}$.
3. All Fibonacci primes have a prime index (i.e. n in $\mathcal{F}_n$) except $n = 4$, i.e. 3 is the only Fibonacci prime with a composite index. However, having a prime index (excluding $\mathcal{F}_4$) is a necessary but not sufficient condition for the primality of Fibonacci numbers.
4. The only Fibonacci primes which are also twin primes are 3, 5, and 13.
5. Based on the known data, the distribution of Fibonacci primes among Fibonacci numbers is rather irregular and sparse and this trend generally intensifies as the Fibonacci sequence progresses.
6. It is conjectured that there are infinitely many Fibonacci primes.

Note: The *Fibonacci numbers* are the numbers of the *Fibonacci sequence* which is defined recursively by the formula:

$$\mathcal{F}_0 = 0,\ \mathcal{F}_1 = 1 \qquad \text{and} \qquad \mathcal{F}_n = \mathcal{F}_{n-2} + \mathcal{F}_{n-1} \text{ (for } 1 < n \in \mathbb{N})$$

We note:
A. The first 17 Fibonacci numbers (i.e. those < 1000) are: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987 (corresponding to $n = 0, 1, 2, \ldots, 16$).[97]
B. The Fibonacci sequence is periodic modulo any integer $m > 1$ (and this period is called the Pisano period).
C. The only consecutive Fibonacci numbers that are both prime are (2, 3) and (3, 5). Beyond that, no consecutive pair is both prime.
D. If $\mathcal{F}_m$ and $\mathcal{F}_n$ are Fibonacci numbers then $\gcd(\mathcal{F}_m, \mathcal{F}_n) = \mathcal{F}_{\gcd(m,n)}$.
E. If $\mathcal{F}_m$ and $\mathcal{F}_n$ are Fibonacci numbers greater than 1 and $\mathcal{F}_m | \mathcal{F}_n$ then $m|n$.

2.1.22 Fortunate Primes

A fortunate prime is a fortunate number that is prime (see the upcoming Note). We note:
1. All known fortunate numbers are prime. We did not find specific information about the largest known fortunate prime (which is the largest calculated fortunate number) noting that the sequence of fortunate numbers is not monotonically increasing (i.e. values in the sequence can decrease and repeat).
2. It is conjectured that there are infinitely many fortunate primes. It is also conjectured that all fortunate numbers are prime (see § 6.1.18).

Note: The n^{th} *fortunate number* $\mathscr{F}_n$ is defined as:

$$\mathscr{F}_n = q - p_n\# \tag{16}$$

[96] See `https://oeis.org/A005478` and `https://oeis.org/A001605`. Seemingly, there are only 57 known Fibonacci primes (37 proven and 20 probable).
[97] See `https://oeis.org/A000045`.

where $p_n\#$ is the n^{th} primorial of the first kind (which is the product of the first n prime numbers; see the Note in § 2.1.64), q is the smallest prime number strictly greater than $p_n\# + 1$, and $n \in \mathbb{N}$. For example:

$$\mathscr{F}_1 = q - p_1\# = 5 - 2 = 3 \qquad \mathscr{F}_2 = q - p_2\# = 11 - 6 = 5 \qquad \mathscr{F}_3 = q - p_3\# = 37 - 30 = 7 \quad (17)$$

We note:

A. The first 15 fortunate numbers are: 3, 5, 7, 13, 23, 17, 19, 23, 37, 61, 67, 61, 71, 47, 107 (corresponding to $n = 1, 2, \ldots, 15$).[98] The first 15 fortunate numbers (i.e. those < 100) in numerical order and without duplicates are: 3, 5, 7, 13, 17, 19, 23, 37, 47, 59, 61, 67, 71, 79, 89.[99]

B. As seen in the previous point, the fortunate numbers are not monotonic, i.e. they do not strictly increase (e.g. $\mathscr{F}_5 = 23$ and $\mathscr{F}_6 = 17$). Moreover, they contain repetition (e.g. $\mathscr{F}_5 = \mathscr{F}_8 = 23$ and $\mathscr{F}_{10} = \mathscr{F}_{12} = 61$).

C. If a fortunate number $\mathscr{F}_n$ is to be composite, its prime factors must be greater than p_n (because q is prime and $p_n\#$ is divisible by every prim $\leq p_n$). Accordingly, we must have $\mathscr{F}_n > p_n$.

D. All known fortunate numbers are prime. It is conjectured that all fortunate numbers are prime.

2.1.23 Full Reptend Primes

A full reptend prime is a prime number p ($\neq 2, 5$) which the decimal expansion of its reciprocal $1/p$ has a repeating period of length $(p-1)$ digits, i.e. $1/p = 0.\overline{d_1 d_2 \ldots d_{p-1}}$.[100] For example, 7 is a full reptend prime because $1/7 = 0.\overline{142857}$ whose period length is $7 - 1 = 6$. We note:

1. Full reptend prime may also be called: *full repetend prime*, *long prime*, *proper prime*, and *maximal period prime*.
2. The first 35 full reptend primes (i.e. those < 500) are: 7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, 223, 229, 233, 257, 263, 269, 313, 337, 367, 379, 383, 389, 419, 433, 461, 487, 491, 499.[101]
3. A prime number p ($\neq 2, 5$) is a full reptend prime *iff* 10 is a primitive root (modulo p), that is:[102]

$$O_p 10 = p - 1 \quad (18)$$

   In fact, this may be used as a definition for full reptend prime.
4. The concept of "full reptend prime" may be generalized to bases other than 10 (and hence it becomes base-dependent).
5. It is conjectured that there are infinitely many full reptend primes (seemingly as an instance of Artin's conjecture on primitive roots; see § 6.1.5).

2.1.24 Generalized Fermat Primes

These are primes of the form $b^{2^n} + 1$ for $b, n \in \mathbb{N}_0$ and $b > 1$.[103] As seen earlier (refer to § 2.1.20), Fermat primes are primes of the form $2^{2^k} + 1$ and this should explain the "generalized Fermat primes" name (as well as the fact that Fermat primes are a subset of generalized Fermat primes). We note:

---

[98] See `https://oeis.org/A005235`.

[99] See `https://oeis.org/A046066`.

[100] We note that 2 and 5 are excluded because the decimal expansions of their reciprocals are terminating, i.e. $1/2 = 0.5$ and $1/5 = 0.2$. See Point 26 of § 1.4 and Point 30 of § 1.5.

[101] See `https://oeis.org/A001913`. We did not find information about the largest known full reptend prime.

[102] As indicated, 2 and 5 are excluded because they are the prime factors of 10.

[103] The condition $n \in \mathbb{N}$ may be imposed instead (which is sensible because otherwise every odd prime p will be trivially a generalized Fermat prime, i.e. $F_{p-1,0} = p$). Also, some authors may impose the condition $b > 2$ instead (seemingly to exclude Fermat primes and hence they are two distinct types).

1. Generalized Fermat primes may also be defined as the primes of *generalized Fermat numbers* ($F_{b,n}$) which are defined as $F_{b,n} = b^{2^n} + 1$ with $b, n \in \mathbb{N}_0$ and $b > 1$.[104] This definition is equivalent to the above definition.
2. Generalized Fermat primes may also be defined (differently) as the primes of the form $F_{a,b,n} = a^{2^n} + b^{2^n}$ for $a, b \in \mathbb{N}$ and $n \in \mathbb{N}_0$.[105] This definition is more general than the above definition, i.e. the above definition is a special case of this definition corresponding to $b = 1$. However, in this book we do not use this definition (except if we refer to it specifically).
3. Some of the common generalized Fermat primes are:

$F_{2,0} = 3$	$F_{2,1} = 5$	$F_{2,2} = 17$	$F_{2,3} = 257$	$F_{2,4} = 65537$
$F_{4,0} = 5$	$F_{4,1} = 17$	$F_{4,2} = 257$	$F_{4,3} = 65537$	
$F_{6,0} = 7$	$F_{6,1} = 37$	$F_{6,2} = 1297$		
$F_{10,0} = 11$	$F_{10,1} = 101$			

4. As of December 2025, the largest known generalized Fermat prime is apparently $2524190^{2^{21}} + 1$ (with about 13.4 million decimal digits).
5. The base b of any generalized Fermat prime must be even because otherwise $F_{b,n}$ will be even and > 2 (and hence composite).
6. All generalized Fermat primes with $n > 0$ are congruent to 1 (modulo 4).
7. It is conjectured that there are infinitely many generalized Fermat primes (excluding the trivial case $F_{p-1,0} = p$ which we mentioned earlier).

2.1.25 Generalized Mersenne Primes

There are different definitions for this type of primes (and hence there is no standard or conventional generalized Mersenne primes). For example, it may be defined as:
• A prime number of the form $b^k - a^k$ with proper conditions on $a, b, k \in \mathbb{N}$ to be prime (e.g. $3^2 - 2^2 = 5$ and $4^3 - 3^3 = 37$).
• A prime number of the form $a^n - (a-1)^n$ with proper conditions on $a, n \in \mathbb{N}$ to be prime [e.g. $2^2 - (2-1)^2 = 3$ and $2^3 - (2-1)^3 = 7$].
• A prime number of the form $(p^k - 1)/(p-1)$ where p and k are primes[106] [e.g. $(2^2 - 1)/(2-1) = 3$ and $(3^3 - 1)/(3-1) = 13$].
• A prime number of the form $p^q - p + 1$ where p and q are positive integers (e.g. $2^2 - 2 + 1 = 3$ and $3^4 - 3 + 1 = 79$).
• A prime number of the form $f(2^n)$, where $f(x)$ is a low-degree polynomial with small integer coefficients (e.g. $2^3 - 1 = 7$ and $2^4 - 3 = 13$).[107]

However, it may seem that the most natural definition of generalized Mersenne prime (as a generalization to the standard Mersenne primes; see § 2.1.41) is that it is a prime number of the form $M_{b,n} = b^n - 1$ where $1 < b \in \mathbb{N}$ and $n \in \mathbb{N}$. However, this definition is useless (as an extension to standard Mersenne primes) because the numbers of the form $b^n - 1$ with $b > 2$ and $n > 1$ are composite [i.e. they have a factor of $(b-1) > 1$] while the primes with $b > 2$ and $n = 1$ are not Mersenne-like (as they have no exponentiation) and hence they are not really *generalized* Mersenne primes. We note that generalized

[104] It is worth noting that generalized Fermat numbers share some properties with Fermat numbers (see the Note in § 2.1.20). For example, generalized Fermat numbers (for a given even base b) are pairwise relatively prime (and this may also be used as a proof for the infinitude of prime numbers; see Point 4 of § 1.6).
[105] Some use the condition $a > b \geq 1$ and this should provide a clearer and non-repetitive definition. We note that the literature about generalized Fermat primes (and numbers) is not entirely consistent, with non-universal conventions concerning notation, terminology, and definitions; therefore care should be taken to identify which convention is being used.
[106] The conditions on p and k may be relaxed, e.g. $p \in \mathbb{Z}$ and hence other types like repunits may be included such as $(10^2 - 1)/(10 - 1) = 11$.
[107] This may be called *Solinas prime*.

Mersenne primes may also be called *Solinas primes* although this seemingly applies to only a specific definition of generalized Mersenne primes (as indicated already in footnote [107]).

2.1.26 Good Primes

A good prime is a prime number p_n whose square is greater than the product of any other two primes equidistant from it in the sequence of prime numbers, that is:

$$p_n^2 > p_{n-i}\, p_{n+i} \tag{19}$$

for all $1 \leq i \leq (n-1)$ where p_n is the n^{th} prime number. For example, 11 is a good prime because:

$$11^2 > 7 \times 13 \qquad 11^2 > 5 \times 17 \qquad 11^2 > 3 \times 19 \qquad 11^2 > 2 \times 23 \tag{20}$$

We note:
1. The first 16 good primes (i.e. those < 200) are: 5, 11, 17, 29, 37, 41, 53, 59, 67, 71, 97, 101, 127, 149, 179, 191.[108]
2. Good primes may also be defined as above but with the condition $i = 1$, i.e. $p_n^2 > p_{n-1}p_{n+1}$. This definition includes more primes, i.e. the good primes of the previous definition are a proper subset of those of this definition. According to this definition, the first 23 good primes (i.e. those < 200) are: 5, 11, 17, 29, 37, 41, 53, 59, 67, 71, 79, 97, 101, 107, 127, 137, 149, 157, 163, 173, 179, 191, 197.[109]
3. There are infinitely many good primes (considering each version).[110]
4. Prime numbers that do not satisfy the definition of good primes may be classified as "bad primes" or "non-good primes". However, inspection of the literature indicates that this category of prime numbers is not recognized as a standard prime type. The reason is apparently that the opposite of a good prime lacks significant mathematical utility within current number theory. Nonetheless, it may deserve some attention for potential utilization in prime number research. Also see § 2.3.1.

Also see § 2.1.1, § 2.1.79 and § 2.1.89.

2.1.27 Happy Primes

A happy prime is a happy number that is prime (see the upcoming Note). We note:
1. The first 23 happy primes (i.e. those < 500) are: 7, 13, 19, 23, 31, 79, 97, 103, 109, 139, 167, 193, 239, 263, 293, 313, 331, 367, 379, 383, 397, 409, 487.[111]
2. The largest known happy prime (in base 10) is reportedly $2^{136279841} - 1$ (which is currently the largest known prime number with about 41 million decimal digits).[112]
3. It is conjectured that there are infinitely many happy primes.

Note: The *happy numbers* are positive integers which the iterative sum of the squares of their digits eventually reaches 1. For example, 7 is a happy number because:

$$7 \;\rightarrow\; 7^2 = 49 \;\rightarrow\; 4^2 + 9^2 = 97 \;\rightarrow\; 9^2 + 7^2 = 130 \;\rightarrow\; 1^2 + 3^2 + 0^2 = 10 \;\rightarrow\; 1^2 + 0^2 = 1 \tag{21}$$

[108] See `https://oeis.org/A028388`. There is no record of the largest known good prime.

[109] See `https://oeis.org/A046869`.

[110] Any proof(s) of the infinitude of good primes should be proof(s) for the infinitude of prime numbers (see § 1.6) if such proof(s) do not assume the infinitude of primes.

[111] See `https://oeis.org/A035497`.

[112] See `https://t5k.org/curios/page.php?number_id=25786` and `https://www.primepuzzles.net/puzzles/puzz_021.htm`. The previous record was $2^{42643801} - 1$ (with about 12.8 million decimal digits) noting that both are Mersenne primes.

We note:
A. Being happy is base-dependent (where 10 is the conventional base).
B. The first 20 happy numbers (i.e. those ≤ 100) are: 1, 7, 10, 13, 19, 23, 28, 31, 32, 44, 49, 68, 70, 79, 82, 86, 91, 94, 97, 100.[113]
C. A happy number remains happy under any permutation of its digits.
D. Happy numbers are zero-invariant, i.e. adding or removing zeros from a happy number does not change its state of happiness.
E. Numbers which are not happy may be called "unhappy" or "sad".

2.1.28 Harmonic Primes

A harmonic prime is a prime number that divides the numerators of exactly three harmonic numbers (see the upcoming Note). We note:
1. Some authors seem to define harmonic prime as a prime number that divides the numerator of at least one harmonic number. However, this makes harmonic primes include all odd primes. In fact, for every prime $p > 3$, p is guaranteed to divide the numerators of at least three harmonic numbers, and hence the "*exactly* three harmonic numbers" condition is to avoid triviality (by excluding those primes that divide the numerators of more than three harmonic numbers). It is worth noting that for any prime $p > 3$, p is guaranteed to divide the numerators of H_{p-1}, H_{p^2-p}, and H_{p^2-1}; a prime is therefore a harmonic prime if it divides the numerators of only these three specific harmonic numbers and no others.
2. The first 16 harmonic primes (i.e. those < 200) are: 5, 13, 17, 23, 41, 67, 73, 79, 107, 113, 139, 149, 157, 179, 191, 193.[114]
3. It is conjectured that there are infinitely many harmonic primes.

Note: The n^{th} *harmonic number* H_n is defined as the sum of the reciprocals of the first n natural numbers, that is:

$$H_n = \sum_{k=1}^{n} \frac{1}{k} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \tag{22}$$

We note:
A. The first 10 harmonic numbers are: $1, \frac{3}{2}, \frac{11}{6}, \frac{25}{12}, \frac{137}{60}, \frac{49}{20}, \frac{363}{140}, \frac{761}{280}, \frac{7129}{2520}, \frac{7381}{2520}$.[115]
B. The numerator of every harmonic number (in its reduced fractional form) is odd. The denominator of every harmonic number (in its reduced fractional form) except H_1 is even.
C. No harmonic number is an integer except H_1 (i.e. 1).
D. The harmonic series is divergent.

2.1.29 Higgs Primes

A Higgs prime is a prime number p with a totient $\big[\text{i.e. } \phi(p) = p - 1\big]$ that evenly divides the square of the product of the smaller Higgs primes. For example, 7 is a Higgs prime because:

$$\phi(7) = 6 \quad \text{divides} \quad (2 \times 3 \times 5)^2 = 900$$

but 17 is not a Higgs prime because:

$$\phi(17) = 16 \quad \text{does not divide} \quad (2 \times 3 \times 5 \times 7 \times 11 \times 13)^2 = 901800900$$

[113] See `https://oeis.org/A007770`.
[114] See `https://oeis.org/A092101`. We did not find reliable information or official record about the largest known harmonic prime.
[115] See `https://oeis.org/A001008` and `https://oeis.org/A002805`.

We note:
1. The first 19 Higgs primes (i.e. those < 100) are: 2, 3, 5, 7, 11, 13, 19, 23, 29, 31, 37, 43, 47, 53, 59, 61, 67, 71, 79.[116]
2. Number 2 is a Higgs prime in a rather trivial (or vacuous) sense because it is not preceded by any smaller prime (let alone "smaller Higgs primes"). Also, number 3 is preceded by a single Higgs prime (i.e. 2) and hence "product" applies to it loosely (not strictly).
3. It is conjectured that there are infinitely many Higgs primes. In fact, Higgs primes are abundant (at least within the primes below one million) and hence this conjecture seems to be generally accepted.
4. "Higgs prime" may be generalized to natural powers other than 2 (i.e. referring to "square" in the above definition), and hence we get Higgs primes of first or third orders (or higher orders). The conjecture in the previous point seems to apply even to Higgs primes of orders greater than 2 (noting that there are only four Higgs primes of the first order which are 2, 3, 7 and 43).[117]

2.1.30 Highly Cototient Primes

A highly cototient prime is a highly cototient number that is prime (see the upcoming Note). We note:
1. The first 14 highly cototient primes (i.e. those < 1000) are: 2, 23, 47, 59, 83, 89, 113, 167, 269, 389, 419, 509, 659, 839.[118]
2. It is conjectured that there are infinitely many highly cototient primes.

Note: A natural number $K > 1$ is described as *highly cototient* if the equation $x - \phi(x) = K$ has more solutions than the equation $x - \phi(x) = k$ for any integer k (where $1 < k < K$ and ϕ is the totient function). We note:

A. The first 19 highly cototient numbers (i.e. those < 500) are: 2, 4, 8, 23, 35, 47, 59, 63, 83, 89, 113, 119, 167, 209, 269, 299, 329, 389, 419.[119]
B. All known highly cototient numbers except 2, 4, 8 are odd. In fact, after 167 all known highly cototient numbers end in the digit 9. Numerical and theoretical evidence suggests that highly cototient numbers are predominantly odd.

2.1.31 Home Primes

A home prime $\mathrm{HP}(n)$ of a natural number $n > 1$ is the prime number that results from repeatedly applying prime factorization to the successive concatenation of the prime factors of n (in non-decreasing order, with multiplicity) and the numbers obtained by concatenating those factors. For example, $\mathrm{HP}(4) = 211$, $\mathrm{HP}(6) = 23$ and $\mathrm{HP}(9) = 311$ because:

$4 = 2 \times 2$	$\rightarrow$	$22 = 2 \times 11$	$\rightarrow$	211 is prime
$6 = 2 \times 3$	$\rightarrow$			23 is prime
$9 = 3 \times 3$	$\rightarrow$	$33 = 3 \times 11$	$\rightarrow$	311 is prime

We note:
1. Being home prime is base-dependent (where 10 is the conventional base).
2. The first 10 home primes are: 2, 3, 211, 5, 23, 7, 3331113965338635107, 311, 773, 11 (corresponding to $n = 2, 3, \ldots, 11$).[120]

[116] See `https://oeis.org/A007459`. We did not find reliable information or official record about the largest known Higgs prime.
[117] In fact, as the order increases, Higgs primes should become even more abundant as the divisibility condition becomes easier to satisfy.
[118] See `https://oeis.org/A105440`. We did not find reliable information or official record about the largest known highly cototient prime.
[119] See `https://oeis.org/A100827`.
[120] See `https://oeis.org/A037274`.

3. The home prime of a prime number p is p itself. By convention, $\mathrm{HP}(n) = -1$ if (hypothetically) no prime is reached by the above-described process of successive prime factorization and concatenation.
4. It is conjectured that every natural number $n > 1$ has a home prime. While the existence of infinitely many primes guarantees that the set of distinct home primes is infinite (see Point 3), it remains unknown whether composite numbers map onto a finite or infinite subset of these primes (including, potentially, the entire set of prime numbers).

2.1.32 Irregular and Regular Primes (Bernoulli)

An odd prime p is irregular if it divides the numerator (in lowest terms) of at least one of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$; otherwise, it is regular (see the upcoming Note).[121] "Regular prime" may also be defined as an odd prime p that does not divide the class number of the p^{th} cyclotomic field. We note:

1. The first 8 irregular primes (i.e. those < 200) are: 37, 59, 67, 101, 103, 131, 149, 157.[122]
2. The first 37 regular primes (i.e. those < 200) are: 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 43, 47, 53, 61, 71, 73, 79, 83, 89, 97, 107, 109, 113, 127, 137, 139, 151, 163, 167, 173, 179, 181, 191, 193, 197, 199.[123]
3. Historically, the classification of primes to irregular/regular appeared during the search for a proof for Fermat's last theorem (where it was shown that $x^p + y^p = z^p$ has no solution in positive integers when p is a regular prime).
4. The infinitude of irregular primes is proven.
5. It is conjectured that there are infinitely many regular primes.
6. As we will see (refer to § 2.1.33 and § 2.1.34), there are other types of "irregular" and "regular" primes similar to the "Bernoulli irregular and regular primes" (as defined above). Hence, "Bernoulli" is commonly indicated for the primes of this subsection (by saying, for instance, "Bernoulli irregular primes" or "B-irregular primes") for distinction and clarity. However, unconditional "irregular" and "regular" are understood to be of Bernoulli-type by default, unless indicated otherwise.

Note: The *Bernoulli numbers* (B_n where $n = 0, 1, 2, \ldots$) are a sequence of rational numbers that appear in the Taylor series expansions of the trigonometric and hyperbolic tangent functions. We note:

A. The first 11 Bernoulli numbers (i.e. B_0 to B_{10}) are:[124]

$$\frac{1}{1}, \frac{\pm 1}{2}, \frac{1}{6}, \frac{0}{1}, \frac{-1}{30}, \frac{0}{1}, \frac{1}{42}, \frac{0}{1}, \frac{-1}{30}, \frac{0}{1}, \frac{5}{66}$$

   The $\pm$ signs of B_1 indicate the two sign conventions of the Bernoulli numbers (which actually affect only B_1).[125]

B. For all odd $n > 1$, $B_n = 0$. Moreover, B_n for even $n > 0$ alternate in sign.

C. The magnitude of the even Bernoulli numbers (excluding the first few terms) grows very quickly as n increases (and eventually diverges to infinity).

D. There is an intimate relationship between the Bernoulli numbers and the Riemann zeta function (see Eq. 48). More specifically, the Bernoulli numbers actually generate the values of the Riemann zeta function at specific integer points.

---

[121] Whether "2" is a regular prime (or "regularity" is inapplicable to the only-even prime) seems to be a controversial issue (where contradicting views can be found in the literature and Internet sources). This seems to be the result of different conventions.

[122] See `https://oeis.org/A090798`. We did not find sufficiently reliable information about the largest known irregular prime (but also see `https://mathworld.wolfram.com/IrregularPrime.html`).

[123] See `https://oeis.org/A007703`. We did not find sufficiently reliable information about the largest known regular prime.

[124] See `https://oeis.org/A027641`, `https://oeis.org/A164555` and `https://oeis.org/A027642`.

[125] Compare `https://oeis.org/A027641` and `https://oeis.org/A164555`.

2.1.33 Irregular and Regular Primes (Euler)

An Euler irregular prime (also known as an *E-irregular prime*) is an odd prime p that divides at least one of the Euler numbers $E_2, E_4, \ldots, E_{p-3}$; otherwise, it is *E-regular* (see the upcoming Note).[126] We note:
1. The first 13 Euler irregular primes (i.e. those < 200) are: 19, 31, 43, 47, 61, 67, 71, 79, 101, 137, 139, 149, 193.[127]
2. There are infinitely many Euler irregular primes.
3. It is conjectured that there are infinitely many Euler regular primes.

Note: The *Euler numbers* E_n $(n = 0, 1, 2, \ldots)$ are a sequence of integers that appear as coefficients in the Taylor series expansion of certain hyperbolic and trigonometric functions (notably sech and sec). We note:
A. The first 6 non-zero Euler numbers are: $1, -1, 5, -61, 1385, -50521$ (corresponding to $n = 0$, 2, 4, 6, 8, 10).[128]
B. For all odd n, $E_n = 0$. Moreover, E_n for even n alternate in sign.
C. Euler numbers arise (and are used) in a number of pure and applied mathematical disciplines such as number theory, topology, analysis, and combinatorics.

2.1.34 Irregular and Regular Primes (Genocchi)

A Genocchi irregular prime (also known as a *G-irregular prime*) is an odd prime p that divides at least one of the Genocchi numbers $G_2, G_4, \ldots, G_{p-3}$; otherwise, it is *G-regular* (see the upcoming Note). We note:
1. The similarity of the Genocchi (ir)regular prime with the Bernoulli (ir)regular and Euler (ir)regular primes (see § 2.1.32 and § 2.1.33) is obvious.
2. Because Genocchi numbers are defined by the relation $G_n = 2(1 - 2^n)B_n$ (see the upcoming Note), every B-irregular prime is also G-irregular (but the reverse is not true; e.g. the prime 1093 is G-irregular but B-regular).
3. The first 21 Genocchi irregular primes (i.e. those < 200) are: 17, 31, 37, 41, 43, 59, 67, 73, 89, 97, 101, 103, 109, 113, 127, 131, 137, 149, 151, 157, 193.[129]
4. The infinitude of the Genocchi irregular primes seems to be proved recently.[130]
5. It is conjectured that there are infinitely many Genocchi regular primes.

Note: The *Genocchi numbers* are the coefficients G_n $(n \in \mathbb{N}_0)$ in the following relation:

$$\frac{2x}{1 + e^x} = \sum_{n=0}^{\infty} G_n \frac{x^n}{n!} \tag{23}$$

We note:
A. The first 12 Genocchi numbers are: 0, 1, -1, 0, 1, 0, -3, 0, 17, 0, -155, 0 (corresponding to $n = 0, 1, 2, \ldots, 11$).[131]
B. The n^{th} Genocchi number is related to (and may be defined by) the n^{th} Bernoulli number through the

[126] Note the similarity with the Bernoulli irregular prime (see § 2.1.32). We note that Euler regular primes attract less research interest than E-irregular primes (and this is generally true for other types of regular and irregular primes).
[127] See `https://oeis.org/A120337`.
[128] See `https://oeis.org/A028296`. Also see `https://oeis.org/A000364`.
[129] See `https://oeis.org/A321217`.
[130] The fact that B-irregular primes (whose infinitude is supposedly proven already; see § 2.1.32) are a proper subset of G-irregular primes should make an independent proof of the infinitude of G-irregular primes redundant. However, it seems that the recent proof is more than about the infinitude of G-irregular primes.
[131] See `https://oeis.org/A036968` noting the absence of the first entry (i.e. 0) in this list.

relation: $G_n = 2(1-2^n)B_n$. Now, if we adopt the $B_1 = -1/2$ convention then this definition (and the resulted list of Genocchi numbers) are the same as before. However, if we adopt the $B_1 = +1/2$ convention then this differs with the previous definition and list in the sign of G_1 only, i.e. $G_1 = -1$.[132]

C. For all odd $n > 1$, $G_n = 0$. Moreover, G_n for even $n > 0$ alternate in sign. See Point B in the Note of § 2.1.32.

2.1.35 Isolated Primes

An isolated prime (also known as *single prime* and *non-twin prime*) is a prime p where $p-2$ and $p+2$ are both non-prime. We note:

1. The first 17 isolated primes (i.e. those < 200) are: 2, 23, 37, 47, 53, 67, 79, 83, 89, 97, 113, 127, 131, 157, 163, 167, 173.[133]
2. There are infinitely many isolated primes.[134]

2.1.36 Jacobsthal Primes

A Jacobsthal prime is a Jacobsthal number that is prime (see the upcoming Note). Jacobsthal prime may also be defined as a prime number of the form $\left[2^n - (-1)^n\right]/3$ where $n \in \mathbb{N}$. We note:

1. The first 10 Jacobsthal primes (i.e. those $< 10^{12}$) are: 3, 5, 11, 43, 683, 2731, 43691, 174763, 2796203, 715827883 (corresponding to $n = 3$, 4, 5, 7, 11, 13, 17, 19, 23, 31 in the Jacobsthal sequence).[135]
2. The largest known Jacobsthal prime is apparently $(2^{141079}+1)/3$ (with about 42.5 thousand decimal digits).[136]
3. Every Jacobsthal prime is a Wagstaff prime (see § 2.1.87) and vice versa (excluding $J_4 = 5$ which is a Jacobsthal prime but not a Wagstaff prime). In fact, the indices n of Jacobsthal primes (excluding $J_4 = 5$) are the same indices that produce Wagstaff primes. This means that the indices of the Jacobsthal primes (excluding $J_4 = 5$) are all prime numbers, and hence $J_4 = 5$ is the only Jacobsthal prime with a composite index.
4. All Jacobsthal primes (excluding $J_4 = 5$) are of the form $4k-1$ for some $k \in \mathbb{N}$.
5. It is conjectured that there are infinitely many Jacobsthal primes.

Note: The *Jacobsthal numbers* are the numbers of the *Jacobsthal sequence* which is defined recursively by each of the following formulae:

- $J_0 = 0$, $J_1 = 1$ and $J_n = 2J_{n-2} + J_{n-1}$ (for $1 < n \in \mathbb{N}$).
- $J_0 = 0$ and $J_{n+1} = 2J_n + (-1)^n$ (for $0 \leq n \in \mathbb{N}_0$).
- $J_0 = 0$ and $J_{n+1} = 2^n - J_n$ (for $0 \leq n \in \mathbb{N}_0$).

Jacobsthal numbers may also be defined non-recursively by each of the following formulae:

- $J_n = \lfloor 2^n/3 \rceil$ (i.e. the nearest integer to $2^n/3$) where $n \in \mathbb{N}_0$.
- $J_n = \left[2^n - (-1)^n\right]/3$ (where $n \in \mathbb{N}_0$).

The first 12 Jacobsthal numbers (i.e. those < 1000) are: 0, 1, 1, 3, 5, 11, 21, 43, 85, 171, 341, 683.[137]

[132] See `https://oeis.org/A226158`.

[133] See `https://oeis.org/A007510`.

[134] The infinitude of isolated primes can be easily proved by Dirichlet's theorem (see § 5.1.11). Also, by Brun's theorem (see § 5.1.5) the sum of the reciprocals of all twin primes converges to a finite constant, demonstrating that twin primes are a highly sparse subset of the prime numbers. Now, because the sum of the reciprocals of all primes diverges to infinity (see § 9.2.1), it is a direct consequence that the remaining subset (i.e. the isolated primes) must be infinite. In fact, a density analysis suggests that asymptotically almost all prime numbers are isolated primes.

[135] See `https://oeis.org/A049883` and `https://oeis.org/A107036`.

[136] There are apparently larger, but probable, known Jacobsthal primes; the largest of these is seemingly $(2^{15135397}+1)/3$ (with about 4.6 million decimal digits). Also, some sources report that the largest proven is $(2^{138937}+1)/3$ not $(2^{141079}+1)/3$. So, the readers should be cautious about such information.

[137] See `https://oeis.org/A001045`.

2.1.37 Kynea Primes

Kynea primes are primes of the form $(2^n + 1)^2 - 2 = 4^n + 2^{n+1} - 1$ where $n \in \mathbb{N}_0$. We note:

1. The first 9 Kynea primes (i.e. those $< 10^{10}$) are: 2, 7, 23, 79, 1087, 66047, 263167, 16785407, 1073807359 (corresponding to $n = 0$, 1, 2, 3, 5, 8, 9, 12, 15).[138]
2. The largest known Kynea prime is reportedly $(2^{8527770} + 1)^2 - 2$ (with about 513 thousand decimal digits).
3. Kynea primes are a special case of the primes of the form $m^2 - 2$ (which are a kind of near-square primes; see § 2.1.49).
4. It is conjectured that there are infinitely many Kynea primes.
5. Kynea primes may also be defined more generally as the primes of the form $(b^n + 1)^2 - 2$ where b is an even positive integer and $n \in \mathbb{N}$.
6. Kynea primes are usually associated with Carol primes due to their similarity in form (see § 2.1.3). Consequently, "Carol-Kynea primes" may be used by some to refer to the primes of the form $(2^n \pm 1)^2 - 2$ or $(b^n \pm 1)^2 - 2$, i.e. primes of Carol or Kynea types.

2.1.38 Leyland Primes

These are prime numbers of the form $x^y + y^x$ for integers $x, y > 1$ (and possibly $x \geq y$ to avoid repetition).[139] For example, 17 is a Leyland prime because $17 = 3^2 + 2^3$. We note:

1. The first 5 Leyland primes (i.e. those $< 10^{16}$) are: 17, 593, 32993, 2097593, 8589935681.[140]
2. The largest known proven Leyland prime is apparently $104824^5 + +5^{104824}$ (with about 73 thousand decimal digits) noting that there are larger known probable Leyland primes.
3. A number of the form $x^y - y^x$ (for integers $x, y > 1$) may be called Leyland number of the second kind, and hence we get *Leyland primes of the second kind* which are the primes of these Leyland numbers. For example, 17 is a Leyland prime of the second kind because $17 = 3^4 - 4^3$. The first 5 Leyland primes of the second kind (i.e. those $< 10^5$) are: 7, 17, 79, 431, 58049.[141]
4. It is reported that there are currently 416 known proven primes and 2437 known probable Leyland primes of the first kind, and 635 proven and 3040 probable Leyland primes of the second kind.
5. It is conjectured that there are infinitely many Leyland primes (of each kind).

2.1.39 Lucas Primes

A Lucas prime is a Lucas number that is prime (see the upcoming Note). We note:

1. The first 11 Lucas primes (i.e. those $< 10^6$) are: 2, 3, 7, 11, 29, 47, 199, 521, 2207, 3571, 9349 (corresponding to $n = 0$, 2, 4, 5, 7, 8, 11, 13, 16, 17, 19 in the sequence of Lucas numbers).[142]
2. The largest known proven Lucas prime is apparently L_{202667} (with over 42 thousand decimal digits) noting that there are larger known probable Lucas primes.[143]
3. There are relationships between Fibonacci primes (see § 2.1.21) and Lucas primes[144] due to the

[138] See `https://oeis.org/A091514` and `https://oeis.org/A091513`. We note that some exclude 2 (corresponding to $n = 0$) from Kynea primes.

[139] We note that *Leyland number* is a number of the form $x^y + y^x$ for integers $x, y > 1$ and hence Leyland primes are the primes of Leyland numbers.

[140] See `https://oeis.org/A094133`. It is worth noting that if we relax the condition $x, y > 1$ then 3 can be considered a Leyland prime since $3 = 2^1 + 1^2$.

[141] See `https://oeis.org/A123206`.

[142] See `https://oeis.org/A005479` and `https://oeis.org/A001606`. Seemingly, there are 52 confirmed and 17 probable Lucas primes.

[143] According to some sources, the largest known probable Lucas prime is $L_{5466311}$ which consists of about 1.14 million decimal digits.

[144] See for instance: `https://oeis.org/A121534` and `https://oeis.org/A121533`.

intimate relationship between Fibonacci and Lucas numbers (which is due to the similarity of the generating formulae of the Fibonacci and Lucas sequences).[145]

4. The indices (i.e. n) of Lucas primes are either 0 or power of 2 or prime number (noting that being a power of 2 or prime number is not sufficient for the primality of Lucas number, e.g. $L_{32} = 4870847$ and $L_3 = 4$ are both composite).[146]
5. The distribution of Lucas primes among Lucas numbers is rather irregular and sparse and this trend generally intensifies as the Lucas sequence progresses.
6. It is conjectured that there are infinitely many Lucas primes.

Note: The *Lucas numbers* are the numbers of the *Lucas sequence* which is defined recursively by the formula:

$$L_0 = 2,\ L_1 = 1 \qquad \text{and} \qquad L_n = L_{n-2} + L_{n-1} \text{ (for } 1 < n \in \mathbb{N})$$

We note:

A. As we see, Lucas sequence is similar to Fibonacci sequence (see the Note in § 2.1.21).
B. The first 15 Lucas numbers (i.e. those < 1000) are: 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843.[147]

2.1.40 Lucky Primes

A lucky prime is a lucky number that is prime (see the upcoming Note). We note:

1. The first 13 lucky primes (i.e. those < 200) are: 3, 7, 13, 31, 37, 43, 67, 73, 79, 127, 151, 163, 193.[148]
2. It is conjectured that there are infinitely many lucky primes.

Note: The *lucky numbers* are numbers generated through a sieving process similar to the sieve of Eratosthenes used to find prime numbers, but with different rules. The process starts with the list of natural numbers and continues as follows:

• Remove every even number and hence we get: 1, , 3, , 5, , 7, , 9, , 11, , 13, , 15, , 17, , 19, , 21, etc.
• Considering the 2^{nd} number in the remaining list (i.e. 3), remove every 3^{rd} number in the remaining list and hence we get: 1, , 3, , , , 7, , 9, , , , 13, , 15, , , , 19, , 21, etc.
• Considering the 3^{rd} number in the remaining list (i.e. 7), remove every 7^{th} number in the remaining list and hence we get: 1, , 3, , , , 7, , 9, , , , 13, , 15, , , , , , 21, etc.
• Considering the n^{th} (where $n = 4, 5, \ldots$) number in the remaining list (i.e. m), remove every m^{th} number in the remaining list.
• Continue this process of elimination.

The remaining numbers are the "lucky numbers" (because they are lucky to survive this elimination process). We note:

A. The first 23 lucky numbers (i.e. those < 100) are: 1, 3, 7, 9, 13, 15, 21, 25, 31, 33, 37, 43, 49, 51, 63, 67, 69, 73, 75, 79, 87, 93, 99.[149]
B. There are infinitely many lucky numbers.
C. Apart from the sieving process of lucky numbers (which is similar to the sieving process of prime numbers), there are other similarities between prime and lucky numbers; for instance:
   • Twin lucky numbers (such as 7 and 9) are similar to twin prime numbers[150] (and hence the infinitude

[145] For example, we have the following identities which link the Fibonacci and Lucas numbers:

$$L_n = \mathcal{F}_{n-1} + \mathcal{F}_{n+1} \qquad L_n = \mathcal{F}_n + 2\mathcal{F}_{n-1} \qquad \mathcal{F}_{2n} = \mathcal{F}_n L_n$$

[146] Also see `https://oeis.org/A001606`.
[147] See `https://oeis.org/A000032`.
[148] See `https://oeis.org/A031157`. We did not find reliable information or official record about the largest known lucky prime.
[149] See `https://oeis.org/A000959`.
[150] We may also have cousin lucky numbers (like 3 and 7) and sexy lucky numbers (like 3 and 9).

of twin lucky numbers is conjectured).
• A Goldbach-like conjecture is also proposed for lucky numbers.
• Prime and lucky numbers are also similar in their logarithmic asymptotic gap.
However, lucky numbers are spread out more sparsely than prime numbers as we go higher up the number line. More technically, $\mathsf{L}_n > p_n$ for all sufficiently large $n \in \mathbb{N}$ (where L_n is the n^{th} lucky number, and p_n is the n^{th} prime number).

2.1.41 Mersenne Primes

A Mersenne prime is a prime number that is one less than a power of 2, i.e. $2^n - 1$ (for some $1 < n \in \mathbb{N}$). However, because $2^n - 1$ is composite if n is composite, the Mersenne primes are defined more specifically as primes of the form $2^p - 1$ (for some $p \in \mathbb{P}$). We note:

1. As indicated, Mersenne primes are defined as primes of the form $2^p - 1$ (for some $p \in \mathbb{P}$). However, it should be noted that the condition $p \in \mathbb{P}$ in this definition is necessary but not sufficient for being a Mersenne prime. For instance, $2^{11} - 1 = 2047 = 23 \times 89$ which is composite.
2. The numbers that have the form $2^n - 1$ regardless of being prime or not are described as *Mersenne numbers* (see the upcoming Note 1). Accordingly, "Mersenne prime" may be defined as a Mersenne number that is prime.
3. Mersenne primes are closely related to perfect numbers (see Note 2 below).
4. The first 7 Mersenne primes (i.e. those $< 10^9$) are: 3, 7, 31, 127, 8191, 131071, 524287 (corresponding to $p = 2, 3, 5, 7, 13, 17, 19$).[151] As of March 2026, the number of known Mersenne primes is 52.[152]
5. The largest known prime number (which is $2^{136279841} - 1$ with 41024320 decimal digits) is a Mersenne prime (and hence this is the largest known Mersenne prime).[153] In fact, the largest known prime numbers are mostly Mersenne primes. This is because their form allows for high-speed primality testing (see § 7.3.10 and § 7.3.11).
6. Mersenne primes are cyclotomic and hence Mersenne primes are a (proper) subset of cyclotomic primes (see § 2.1.14), i.e. $2^p - 1 = \Phi_p(2)$ where $p \in \mathbb{P}$.
7. Noting that $2^n - 1$ in binary is made of n "1" digits $\big[$e.g. $2^3 - 1 = (111)_2$ and $2^4 - 1 = (1111)_2\big]$, Mersenne primes (and numbers) can be represented most easily in this simple binary form, and this simple representation may be exploited in certain computational algorithms for the search and manipulation of Mersenne primes.
8. It is unknown if there are infinitely many Mersenne primes. According to the LPW conjecture (which stands for Lenstra-Pomerance-Wagstaff), there are infinitely many Mersenne primes.[154]
9. It is unknown if $2^p - 1$ is composite for infinitely many primes p (see Point 1 above). However, it is conjectured that there are infinitely many composite numbers of the form $2^p - 1$ where p is prime (noting that this is conditionally proved based on the prime k-tuples hypothesis; see § 6.1.17).
10. Any prime divisor of a Mersenne number (see the upcoming Note 1) $M_p = 2^p - 1$ (where p is an odd prime) is of the form $2kp + 1$ (where $k \in \mathbb{N}$).[155]
11. Every odd prime number divides at least one Mersenne number $M_n = 2^n - 1$ (see § 5.1.15).
12. There are no primes of the form $a^n - 1$ $(1 < n \in \mathbb{N})$ for any $2 < a \in \mathbb{N}$ because such numbers are divisible by $a - 1$. Accordingly, Mersenne primes are unique from this perspective.
13. In the binary numeral system (base 2), Mersenne primes and repunit primes are identical sets (see §

[151] See `https://oeis.org/A000043`.
[152] See `https://www.mersenne.org/primes/`. Because of the relationship between Mersenne primes and (even) perfect numbers (as indicated already) this is also the number of known perfect numbers (see the upcoming Note 2).
[153] See `https://oeis.org/A000043`, `https://www.mersenne.org/primes/` and `https://t5k.org/largest.html`.
[154] In fact, the LPW conjecture is more than just the assertion of infinitude; it gives an asymptotic formula for the number of Mersenne primes up to a given bound. The infinitude follows as a corollary from that formula.
[155] In fact, this applies even to composite divisors.

2.1.69).

14. *Double Mersenne primes* are prime numbers of the form $2^{2^p-1}-1$ (and hence they are a proper subset of Mersenne primes). It should be obvious that for $2^{2^p-1}-1$ to be prime, 2^p-1 must be prime (i.e. Mersenne prime) and hence it is symbolized as M_{M_p} (which justifies its name as *double* Mersenne prime). Apparently, there are only four known double Mersenne primes which are: 7 (i.e. $M_{M_2}=2^{2^2-1}-1$), 127 (i.e. $M_{M_3}=2^{2^3-1}-1$), 2147483647 (i.e. $M_{M_5}=2^{2^5-1}-1$), and 170141183460469231731687303715884105727 (i.e. $M_{M_7}=2^{2^7-1}-1$).[156] Accordingly, the largest known double Mersenne prime is apparently $M_{M_7}\equiv M_{127}=2^{2^7-1}-1=2^{127}-1$. The infinitude of double Mersenne primes is an open problem with conflicting conjectures in this regard.[157] It is worth noting that the double Mersenne numbers M_{M_p} for all the prime exponents p in the range $11\leq p\leq 59$ are proven to be composite.

Note 1: The *Mersenne numbers* are commonly defined as the numbers of the sequence $M_n=2^n-1$ for all $n\in\mathbb{N}_0$ (or $n\in\mathbb{N}$). However, *Mersenne numbers* may be reserved for the numbers of the form $M_p=2^p-1$ where p is a prime number (regardless of M_p being prime or not). The M_n convention seems to be dominant in the general literature of number theory, while the M_p convention seems to be dominant in the literature of prime number theory (particularly within the Mersenne prime research community). This requires attention when reading the literature about Mersenne numbers. For example, the validity or generality of some theorems and propositions related to Mersenne numbers may be restricted to a specific convention. In our book, we try to be specific and explicit in our statements about Mersenne numbers to avoid ambiguity, but the readers are recommended to check our statements for clarity and accuracy. We should also note that M_p may be used specifically for Mersenne primes (depending on contextual indications) due to the fact that Mersenne primes are a proper subset of the M_p Mersenne numbers.
We note:

1. The first 14 Mersenne numbers of the M_n form where $n\in\mathbb{N}_0$ (i.e. those $<10^4$) are: 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191.[158]
2. The first 14 Mersenne numbers of the M_p form where $p\in\mathbb{P}$ (i.e. those $<10^{14}$) are: 3, 7, 31, 127, 2047, 8191, 131071, 524287, 8388607, 536870911, 2147483647, 137438953471, 2199023255551, 8796093022207 (corresponding to the first 14 prime exponents).[159]
3. If a divides b then 2^a-1 divides 2^b-1 (where $a,b\in\mathbb{N}$).[160]
4. In base 2 (i.e. binary) number system, Mersenne numbers are composed of 1's only.
5. If a Mersenne number M_n is prime then its exponent n must be a prime number p.
6. Two Mersenne numbers $M_m=2^m-1$ and $M_n=2^n-1$ are coprime *iff* their exponents m and n are coprime.
7. We may classify Mersenne numbers into 3 main categories:
   - Mersenne number which is prime and hence its exponent is prime.
   - Mersenne number whose exponent is composite and hence it is also composite.
   - Mersenne number which is composite but its exponent is prime.

   So, the only category that does not exist is "Mersenne number which is prime but its exponent is composite".

Note 2: A *perfect number* is a positive integer that is equal to the sum of its proper divisors. We note:

---

[156] See `https://oeis.org/A077586`.
[157] In fact, some seem to conjecture that the four known double Mersenne primes are the only existing primes of this type.
[158] See `https://oeis.org/A000225`.
[159] See `https://oeis.org/A001348`.
[160] This is obviously related to the Mersenne numbers of the M_n form where $n\in\mathbb{N}$. In fact, this theorem may be one of the reasons why the M_n convention is dominant in general number theory because it allows mathematicians to translate divisibility questions about the exponents directly into divisibility questions about the Mersenne numbers themselves.

1. A number $m \in \mathbb{N}$ is an even perfect number *iff* $m = 2^{n-1}(2^n - 1)$ where $(2^n - 1)$ is prime. Now, the primality of $(2^n - 1)$ entails the primality of n and hence we can write $m = 2^{p-1}(2^p - 1)$. Accordingly, even perfect numbers and Mersenne primes are connected by the formula $P_e = 2^{p-1}M_p$ where P_e is an even perfect number and M_p is the corresponding Mersenne prime.
2. There is a one-to-one correspondence between Mersenne primes and even perfect numbers (by the Euclid-Euler theorem).[161]
3. If M_p is a Mersenne prime then $M_p(M_p + 1)/2$ is an even perfect number. In fact, this may be stated more strongly as: an integer is an even perfect number *iff* it is of the form $M_p(M_p + 1)/2$ where M_p is a Mersenne prime.
4. If M_p is a Mersenne prime then $\sum_{k=1}^{M_p} k$ is an even perfect number (noting that this formula also represents the relationship between Mersenne primes and triangular numbers).
5. The first 8 perfect numbers (i.e. those $< 10^{36}$) are: 6, 28, 496, 8128, 33550336, 8589869056, 137438691328, 2305843008139952128.[162]
6. Currently (March 2026), there are only 52 known perfect numbers (corresponding to the 52 known Mersenne primes).
7. A natural number n is perfect *iff* $\sigma(n) = 2n$ (where σ is the divisor function).
8. A natural number n is perfect *iff* $s(n) = n$ (where s is the restricted divisor function).
9. All known perfect numbers are even. In fact, it is widely believed (and conjectured) that there is no odd perfect number.
10. All even perfect numbers end in 6 or 8. All even perfect numbers (excluding 6) end in 16, 28, 36, 56, 76, or 96. Any even perfect number (except 6) is the sum of consecutive odd cubes.
11. An integer is an even perfect number *iff* it is a triangular number whose index is a Mersenne prime.
12. By definition, no perfect number can be an untouchable number (see the Note in § 2.1.86).
13. It is unknown if there are infinitely many perfect numbers (noting that their infinitude is conjectured). However, it should be noted that the infinitude of perfect numbers is related to the infinitude of Mersenne primes (due to the one-to-one correspondence between Mersenne primes and even perfect numbers).[163]

2.1.42 Mersenne Divisors

The Mersenne divisors are the prime factors of Mersenne numbers with prime exponents (see Note 1 in § 2.1.41). In other words, they are prime numbers p that divide $2^q - 1$ where $q \in \mathbb{P}$. We note:

1. All Mersenne primes are Mersenne divisors. Hence, the set of Mersenne primes is a proper subset of the set of Mersenne divisors.[164]
2. The first 22 Mersenne divisors (i.e. those < 1000) are: 3, 7, 23, 31, 47, 89, 127, 167, 223, 233, 263, 359, 383, 431, 439, 479, 503, 719, 839, 863, 887, 983.[165]
3. The largest known Mersenne divisor is the largest known Mersenne prime (and actually the largest known prime number) i.e. $2^{136279841} - 1$ (see Point 5 of § 2.1.41).

---

[161] The Euclid-Euler theorem states: a number $m \in \mathbb{N}$ is an even perfect number *iff* $m = 2^{p-1}(2^p - 1)$ where $(2^p - 1)$ is prime.

[162] See `https://oeis.org/A000396`.

[163] If there is no odd perfect number then the infinitude of perfect numbers and the infinitude of Mersenne primes are equivalent. However, if odd perfect numbers do exist then the infinitude of Mersenne primes implies the infinitude of perfect numbers but the reverse is not (i.e. there could be infinitely many perfect numbers while only finitely many Mersenne primes).

[164] This is because every Mersenne prime divides a Mersenne number (namely, itself), whereas composite Mersenne numbers have prime divisors that are not Mersenne primes. For example, $2^{11} - 1 = 2047 = 23 \times 89$, so 23 and 89 are Mersenne divisors but not Mersenne primes (see Point 1 of § 2.1.41).

[165] See `https://oeis.org/A122094`.

4. There are infinitely many Mersenne divisors.[166]

2.1.43 Mersenne Prime Exponents

As its name suggests, a Mersenne prime exponent is a prime p such that $2^p - 1$ is prime (i.e. Mersenne prime). We note:
1. The first 14 Mersenne prime exponents (i.e. those < 1000) are: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607.[167]
2. As of March 2026, the number of known Mersenne prime exponents is 52 (which is the same as the number of known Mersenne primes).
3. The largest known Mersenne prime exponent is 136279841 (see Point 5 of § 2.1.41).
4. It is conjectured that there are infinitely many Mersenne prime exponents (noting that this is implied by the Mersenne primes conjecture).

2.1.44 Mills Primes

A Mills prime is a prime obtained from the Mills constant (i.e. through applying the floor function to the Mills constant powers).[168] We note:
1. The first 4 Mills primes (i.e. those $< 10^{28}$) are: 2, 11, 1361, 2521008887.[169]
2. The largest known Mills prime is apparently the 15^{th} number in the sequence (which is a massive number consisting of about 1.67 million decimal digits).[170]
3. The infinitude of Mills primes follows from Mills' theorem (see § 5.1.30). Because the theorem yields an infinite sequence of distinct primes, it directly implies the infinitude of Mills primes (and consequently the infinitude of primes; see § 1.6).

2.1.45 Minimal Primes

A minimal prime is a prime number that does not contain any other prime number as a sub-sequence of its digits.[171] For example, 449 is a minimal prime because none of the sub-sequences of its digits (which are 4, 9, 44, 49) is prime. On the other hand, 13 is not a minimal prime because one of its sub-sequences (i.e. 3) is a prime number. We note:
1. Being minimal (in this sense) is base-dependent (where 10 is the conventional base).
2. There are only 26 minimal primes in the decimal system (i.e. base 10) which are: 2, 3, 5, 7, 11, 19, 41, 61, 89, 409, 449, 499, 881, 991, 6469, 6949, 9001, 9049, 9649, 9949, 60649, 666649, 946669, 60000049, 66000049, 66600049.[172]
3. No multi-digit minimal prime can contain any of the digits 2, 3, 5, and 7 (as each of these digits represents a one-digit prime sub-sequence).

---

[166] This is because the sequence of Mersenne numbers indexed by primes yields an infinite set of pairwise coprime integers (see Point 6 of § 2.1.41), forcing the existence of infinitely many distinct prime divisors.

[167] See `https://oeis.org/A000043`.

[168] Mills' constant is the smallest real number $A > 1$ such that floor $\left(A^{3^n}\right)$ is a prime for all $n \in \mathbb{N}$. The approximate value of Mills' constant is $A \approx 1.306377883863080690468 6$ (assuming the Riemann hypothesis). See § 5.1.30 for more details.

[169] See `https://oeis.org/A051254`.

[170] See `https://oeis.org/A224845`. We note that the 15^{th} number in the sequence is apparently a probable prime.

[171] A sub-sequence is formed by deleting digits while maintaining order. We note that sub-types of "minimal primes" by considering the conditions of digits-order and digits-proximity in their sub-sequences (i.e. with and without these conditions, individually and collectively) may be defined (where the above definition represents only one sub-type of four possible sub-types). Also see § 2.3.2.

[172] See `https://oeis.org/A071062`.

4. Every prime number in base 10 is either a minimal prime or it contains at least one minimal prime as a sub-sequence of its digits. So, the aforementioned 26 minimal primes (as strings) are like building blocks for all prime numbers in base 10.

Also see § 2.3.2.

2.1.46 Mirimanoff Primes

A Mirimanoff prime is a prime number p where p^2 divides $(3^{p-1} - 1)$. We note:

1. There are only two known Mirimanoff primes: 11 and 1006003 (despite extensive search up to about 10^{15} according to some sources).[173]
2. There is obvious similarity between Mirimanoff primes and Wieferich primes (see § 2.1.90). In fact, Mirimanoff primes may be seen as base-3 generalized Wieferich primes.
3. Historically, Mirimanoff primes emerged in the context of research on Fermat's last theorem and remain closely associated with it.
4. It is conjectured that there are infinitely many Mirimanoff primes.

2.1.47 $n^2 + 1$ Primes

These are prime numbers of the form $n^2 + 1$ where $n \in \mathbb{N}$. We note:

1. The first 19 $n^2 + 1$ primes (i.e. those $< 10^4$) are: 2, 5, 17, 37, 101, 197, 257, 401, 577, 677, 1297, 1601, 2917, 3137, 4357, 5477, 7057, 8101, 8837 (corresponding to $n = 1$, 2, 4, 6, 10, 14, 16, 20, 24, 26, 36, 40, 54, 56, 66, 74, 84, 90, 94).[174]
2. The largest known $n^2 + 1$ prime is apparently $(2524190^{1048576})^2 + 1 = 2524190^{2097152} + 1$ (with about 13.4 million decimal digits), which is currently the largest known non-Mersenne prime and the sixth largest known prime.[175]
3. The only $n^2 + 1$ prime with odd n is 2.
4. All $n^2 + 1$ primes with $n > 1$ are Pythagorean (see § 2.1.66).
5. Primes of the form $n^2 + 1$ may be called *near-square primes* although this term may be used in a broader sense (and hence $n^2 + 1$ primes are a proper subset of near-square primes; see § 2.1.49).
6. It is conjectured that there are infinitely many $n^2 + 1$ primes (which is famously known as Landau's fourth problem).[176]

2.1.48 $n^4 + 1$ Primes

These are prime numbers of the form $n^4 + 1$ where $n \in \mathbb{N}$. We note:

1. The first 13 $n^4 + 1$ primes (i.e. those $< 10^7$) are: 2, 17, 257, 1297, 65537, 160001, 331777, 614657, 1336337, 4477457, 5308417, 8503057, 9834497 (corresponding to $n = 1$, 2, 4, 6, 16, 20, 24, 28, 34, 46, 48, 54, 56).[177]
2. The largest known $n^4 + 1$ prime is apparently $(2524190^{524288})^4 + 1 = 2524190^{2097152} + 1$ (with about 13.4 million decimal digits), which is currently the largest known non-Mersenne prime and the sixth largest known prime.[178]
3. The only $n^4 + 1$ prime with odd n is 2.

---

[173] See `https://oeis.org/A014127`.
[174] See `https://oeis.org/A002496` and `https://oeis.org/A005574`.
[175] See `https://t5k.org/top20/page.php?id=3`.
[176] We note that this is an instance of more general conjectures such as the Bunyakovsky conjecture or the Hardy-Littlewood conjecture F (see § 6.1.11 and § 6.1.20).
[177] See `https://oeis.org/A037896` and `https://oeis.org/A000068`.
[178] See `https://t5k.org/top20/page.php?id=3`.

4. The primes of the form $n^4 + 1$ are a proper subset of the quartan primes (see § 2.1.67). They are also a proper subset of the primes of the form $n^2 + 1$ (see § 2.1.47) and of the near-square primes (see § 2.1.49).
5. It is conjectured that there are infinitely many $n^4 + 1$ primes (noting that this is an instance of more general conjectures such as the Bunyakovsky conjecture; see § 6.1.11).

2.1.49 Near-Square Primes

The near-square primes are primes of the form $n^2 + k$ where n is a natural number (or non-zero integer) and k is an integer of small magnitude. We note:
1. The main examples of near-square primes are $n^2 + k$ for $k = -5, -3, -2, +1, +2, +3, +4, +5$.[179]
2. The form of a near-square prime may not be unique, i.e. it can be of the form $n^2 + k$ with different values of n and k. For example, $5 = 3^2 - 4 = 2^2 + 1 = 1^2 + 4$. Similarly, $13 = 4^2 - 3 = 3^2 + 4$.
3. It is conjectured that there are infinitely many near-square primes (for any fixed k that is not zero or the negative of a perfect square).

2.1.50 Non-Generous Primes

A non-generous prime is a prime number p whose least positive primitive root is not a primitive root of p^2. We note:
1. There are only three known non-generous primes which are: 2, 40487, 6692367337.[180] It is reported that there are no other non-generous primes below 10^{12}, and hence non-generous primes are very rare.
2. It is seemingly conjectured that there are infinitely many non-generous primes (although the situation is not very clear).[181]

2.1.51 NSW Primes

An NSW prime is an NSW number that is prime (see the upcoming Note). We note:
1. The first 5 NSW primes (i.e. those $< 10^{17}$) are: 7, 41, 239, 9369319, 63018038201 (corresponding to $n = 1, 2, 3, 9, 14$).[182]
2. The largest known NSW prime is apparently the NSW number with index 139160, i.e. N_{139160}.[183]
3. Regarding the closed-form definition of NSW numbers (see Eq. 24), the exponent (i.e. $2n + 1$ in Eq. 24) of each of the 26 currently known NSW primes is a prime number (and this may be conjectured to hold for all NSW primes, noting that the converse is obviously false).
4. It is conjectured that there are infinitely many NSW primes.

Note: The *NSW numbers* are the numbers of the *NSW sequence* (where NSW stands for Newman-Shanks-Williams) which is defined recursively by the following formula:

$$N_0 = 1, N_1 = 7 \qquad \text{and} \qquad N_n = 6N_{n-1} - N_{n-2} \text{ (for } 1 < n \in \mathbb{N})$$

NSW numbers may also be defined non-recursively by the following formula:

$$N_n = \frac{(1 + \sqrt{2})^{2n+1} + (1 - \sqrt{2})^{2n+1}}{2} \qquad (n \in \mathbb{N}_0) \tag{24}$$

[179] See for instance the following OEIS sequences: A028877, A028874, A028871, A002496, A056899, A049423, A005473, and A056905. We note that 3 is the only prime of the form $n^2 - 1$, and 5 is the only prime of the form $n^2 - 4$, whereas $k = 0$ is impossible because a prime cannot be a perfect square.

[180] See `https://oeis.org/A055578`.

[181] Apparently, some conjectured that there are only finitely many non-generous primes. In fact, it may even be conjectured that the three known non-generous primes are the only such primes in existence.

[182] See `https://oeis.org/A088165` and `https://oeis.org/A113501`. Apparently, there are only 26 known NSW primes.

[183] See `https://oeis.org/A113501`.

The first 10 NSW numbers (i.e. those $< 10^7$) are: 1, 7, 41, 239, 1393, 8119, 47321, 275807, 1607521, 9369319.[184]

2.1.52 Padovan Primes

A Padovan prime is a Padovan number that is prime (see the upcoming Note). We note:
1. The first 8 Padovan primes (i.e. those $< 10^{10}$) are: 2, 3, 5, 7, 37, 151, 3329, 23833 (corresponding to $n = 3$ (or 4), 5, 7, 8, 14, 19, 30, 37 in the sequence of Padovan numbers).[185]
2. The largest known Padovan prime is apparently P_{727734} (with about 89 thousand decimal digits) though it is seemingly probable rather than proven.
3. It is unknown if there are infinitely many Padovan primes (where both infinitude and finitude are seemingly conjectured).

Note: The *Padovan numbers* are the numbers of the *Padovan sequence* which is defined recursively by the formula:

$$P_0 = P_1 = P_2 = 1 \qquad \text{and} \qquad P_n = P_{n-3} + P_{n-2} \text{ (for } 2 < n \in \mathbb{N})$$

The first 21 Padovan numbers (i.e. those ≤ 200) are: 1, 1, 1, 2, 2, 3, 4, 5, 7, 9, 12, 16, 21, 28, 37, 49, 65, 86, 114, 151, 200.[186]

2.1.53 Palindromic Primes

A palindromic number (or palindrome) is a number[187] that remains the same when its digits are reversed, i.e. it is symmetric under mirror-reflection across its center (e.g. 131 and 2552). So, a palindromic prime is a prime number that remains the same when its digits are reversed (e.g. 131 and 151). We note:
1. Being palindromic is base-dependent (where 10 is the conventional base).
2. The only palindromic prime (in base 10) with an even number of digits is 11 (because all even-length palindromes are divisible by 11 with only 11 being prime).
3. All repunit primes (see § 2.1.69) are palindromic (in a "trivial" sense), and hence repunit primes are a proper subset of palindromic primes.
4. The first 20 palindromic primes in base 10 (i.e. those < 1000) are: 2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929.[188]
5. The largest known (non-repunit) palindromic prime is seemingly $10^{2718281} - 5 \times 10^{1631138} - 5 \times 10^{1087142} - 1$ (with about 2.72 million decimal digits).
6. The infinitude of palindromic primes is conjectured (but check whether this conjecture considers the inclusion or exclusion of repunit primes whose infinitude is independently conjectured; see § 2.1.69).
7. A distinction must be made between the mirror-reflection in palindromic primes and dihedral primes (see § 2.1.16), i.e. the mirror-reflection in the dihedral is visual but it is non-visual (i.e. numeric) in the palindromic.

Also see § 2.1.17 and § 2.1.70.

2.1.54 Palindromic Wing Primes

These are palindromic primes whose digits are all identical except for the middle digit, which is different (and hence palindromic wing primes do not include repunit primes as well as non-repunit palindromic

[184] See `https://oeis.org/A002315`.
[185] See `https://oeis.org/A100891` and `https://oeis.org/A112882`.
[186] See `https://oeis.org/A000931` ignoring the first 5 entries.
[187] Actually, it is more general than number (as it includes, for instance, words and sentences) but in this book we are interested in numbers only.
[188] See `https://oeis.org/A002385`.

primes that do not meet this condition).[189] We note:
1. Being palindromic wing is base-dependent (where 10 is the conventional base).
2. Palindromic wing primes are a proper subset of palindromic primes.
3. A palindromic wing prime must have an odd number of digits ≥ 3.
4. The first 21 palindromic wing primes in base 10 (i.e. those $< 10^6$) are: 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929, 11311, 11411, 33533, 77377, 77477, 77977.[190]
5. The largest known palindromic wing prime is apparently $10^{1888529} - 10^{944264} - 1$ (with about 1.9 million decimal digits).[191]
6. The infinitude of palindromic wing primes seems to be conjectured by some mathematicians.

2.1.55 Pandigital Primes

A pandigital prime is a pandigital number that is prime (see the upcoming Note). We note:
1. Referring to the definition of pandigital prime (and perhaps even pandigital number), some authors seem to impose the condition "exactly once" instead of "at least once", and hence we may have different conventions.[192] However, it should be noted that a 10-digit pandigital number in base 10 (i.e. it contains each digit exactly once) cannot be prime because the sum of its digits is 45 which is always divisible by 3 and 9 (as well as the possibility of being divisible by 2 and/or 5). So, any pandigital prime in base 10 must contain more than 10 digits.
2. The following are 5 examples of pandigital primes (in base 10): 10123457689, 10123465789, 10123465897, 10123485679, 10123485769.[193]
3. We did not find an explicit statement in the literature regarding the infinitude of non-strict pandigital primes. However, we think this infinitude can be proven (at least in base 10) by a number of rather elementary arguments. So, please investigate this issue.

Note: A *pandigital number* is an integer that, in a given base, includes in its significant digits every digit used in that base at least once. For example, 12340 is a pandigital number in base 5, while 1234567890 is a pandigital number in base 10. We note:
A. Being pandigital is base-dependent (where 10 is the most conventional base).
B. Examples of strict (i.e. non-repetitive) base 10 pandigital numbers are: 1023456789, 1023456798, 1023456879, 1023456897, 1023456978.[194]
C. A pandigital number may be defined as an integer that contains all digits from 1 to "length" (where "length" is the number of its digits). For instance, the numbers 12345 and 1234567 are pandigital according to this definition. In fact, it is more appropriate to call such numbers "n-digit pandigital numbers" (rather than just "pandigital numbers" which should be reserved to the earlier definition).

2.1.56 Partition Primes

The partition primes are partition numbers that are prime (see the upcoming Note). We note:
1. The first 7 partition primes (i.e. those $< 10^7$) are: 2, 3, 5, 7, 11, 101, 17977 (corresponding to $n = 2$, 3, 4, 5, 6, 13, 36).[195]
2. The largest known partition prime is seemingly $P(1289844341)$ (with 40 thousand decimal digits).[196]

[189] Palindromic wing primes may also be called *near-repdigit palindromic primes* (or similar names).
[190] See `https://oeis.org/A077798`.
[191] See `https://www.worldofnumbers.com/wing.htm`.
[192] Alternatively, pandigital primes with the "exactly once" condition may be labeled as *strict pandigital primes*, and hence they are a subset of pandigital primes.
[193] See `https://oeis.org/A050288`.
[194] See `https://oeis.org/A050278`.
[195] See `https://oeis.org/A049575` and `https://oeis.org/A046063`.
[196] See `https://t5k.org/curios/page.php/1289844341.html`.

3. It is conjectured that there are infinitely many partition primes.

Note: The *partition numbers* are the values of the partition function which is defined as follows: the partition function $P(n)$ of $n \in \mathbb{N}_0$ is the number of possible partitions of n, i.e. the partition function $P(n)$ counts the number of ways to write a non-negative integer n as a sum of positive integers, where the order of the summands does not matter.[197] For example, $P(5) = 7$ because:

$$5 = 1+1+1+1+1, \quad 5 = 1+1+1+2, \quad 5 = 1+1+3, \quad 5 = 1+4, \quad 5 = 1+2+2, \quad 5 = 2+3, \quad 5$$

We note:
A. The partition numbers may be defined by the following recurrence relation:

$$P(n) = \sum_{k=1}^{\infty} (-1)^{k-1} \left[P\left(n - \frac{k(3k-1)}{2}\right) + P\left(n - \frac{k(3k+1)}{2}\right) \right] \qquad (n \geq 1) \qquad (25)$$

where $P(a)$ is the value of the partition function of $a \in \mathbb{Z}$, $P(a) = 0$ for all $a < 0$, and $P(0) = 1$.[198]
B. The first 22 partition numbers (i.e. those < 1000) are: 1, 1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77, 101, 135, 176, 231, 297, 385, 490, 627, 792 (corresponding to $n = 0, 1, 2, \ldots, 21$).[199]

2.1.57 Pell Primes

A Pell prime is a Pell number that is prime (see the upcoming Note). We note:
1. The first 5 Pell primes (i.e. those $< 10^{10}$) are: 2, 5, 29, 5741, 33461 (corresponding to $n = 2$, 3, 5, 11, 13 in the sequence of Pell numbers).[200]
2. The largest known Pell prime is seemingly $\mathcal{P}_{90197}$ (with about 35 thousand decimal digits).[201]
3. All Pell primes have a prime index (i.e. n in $\mathcal{P}_n$), but not all prime-indexed Pell numbers are primes (e.g. $\mathcal{P}_7 = 169$ which is composite).
4. It is conjectured that there are infinitely many Pell primes.

Note: The *Pell numbers* are the numbers of the *Pell sequence* which is defined recursively by the formula:

$$\mathcal{P}_0 = 0, \mathcal{P}_1 = 1 \qquad \text{and} \qquad \mathcal{P}_n = \mathcal{P}_{n-2} + 2\mathcal{P}_{n-1} \text{ (for } 1 < n \in \mathbb{N})$$

The first 12 Pell numbers (i.e. those $< 10^4$) are: 0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741.[202]

2.1.58 Permutable Primes

A permutable prime (also known as *absolute prime* and *anagrammatic prime*) is a prime number that remains prime under any permutation of its digits. An example of permutable primes is 113. We note:
1. Being permutable is base-dependent (where 10 is the conventional base).[203]
2. The first 22 permutable primes in base 10 (i.e. those < 1000) are: 2, 3, 5, 7, 11, 13, 17, 31, 37, 71, 73, 79, 97, 113, 131, 199, 311, 337, 373, 733, 919, 991.[204]

[197] For $n = 0$, $P(0) = 1$ by the convention of the empty sum (there is exactly one way to add zero positive integers to get zero).
[198] It is worth noting that the condition "$P(a) = 0$ for all $a < 0$" ensures that the sum is always finite although the upper limit is ∞.
[199] See `https://oeis.org/A000041`.
[200] See `https://oeis.org/A086383` and `https://oeis.org/A096650`.
[201] This seemingly is a probable rather than proven. The largest known proven Pell prime is seemingly $\mathcal{P}_{13339}$ (with about 5.1 thousand decimal digits).
[202] See `https://oeis.org/A000129`.
[203] Although permutable primes are known as *absolute* primes, they are not actually absolute with regard to the base of employed number system (see Point 3 of § 1.3).
[204] See `https://oeis.org/A003459`. It is worth noting that it is proven that there is no n-digit non-repunit permutable prime for $3 < n < (6 \times 10^{175})$.

3. The largest known (non-repunit) permutable prime is 991. Also see § 2.1.69 for the largest known repunit permutable prime.
4. Any permutable prime (except 2 and 5) contains only the digits 1, 3, 7, and 9 (in base 10).
5. Any permutable prime cannot contain more than two distinct digits (in base 10).
6. Any permutable prime cannot contain two different digits each appearing at least twice (in base 10).
7. All repunit primes (see § 2.1.69) are permutable (in a "trivial" sense), and hence repunit primes are a proper subset of permutable primes.
8. Based on the previous points, we can say: in base 10, a multi-digit permutable prime must be either a repunit or a permutation of a number of the form $a \dots ab$ where a and b are distinct digits from the set $\{1, 3, 7, 9\}$.
9. All permutable primes are circular, and hence permutable primes are a proper subset of circular primes (see § 2.1.7).
10. All permutable primes are reversible, and hence permutable primes are a proper subset of reversible primes (see § 2.1.70).
11. The infinitude of permutable primes seems to be conjectured by some mathematicians. However, if we exclude repunit primes then the conjectured infinitude is not clear (in fact some sources claim it is conjectured that there are no non-repunit permutable primes other than the known ones).[205] Also see Point 7 of § 2.1.7.

2.1.59 Perrin Primes

A Perrin prime is a Perrin number that is prime (see the upcoming Note). We note:

1. The first 11 Perrin primes (i.e. those $< 10^9$) are: 2, 3, 5, 7, 17, 29, 277, 367, 853, 14197, 43721 (corresponding to $n = 2$ [4], 0 [3], 5 [6], 7, 10, 12, 20, 21, 24, 34, 38 in the sequence of Perrin numbers).[206]
2. The largest known Perrin prime is apparently $\mathsf{P}_{1430138}$ (which seemingly is probable not proven and consists of about 175 thousand decimal digits).[207]
3. It is conjectured that there are infinitely many Perrin primes.

Note: The *Perrin numbers* are the numbers of the *Perrin sequence* which is defined recursively by the formula:

$$\mathsf{P}_0 = 3,\ \mathsf{P}_1 = 0,\ \mathsf{P}_2 = 2 \qquad \text{and} \qquad \mathsf{P}_n = \mathsf{P}_{n-3} + \mathsf{P}_{n-2} \text{ (for } 2 < n \in \mathbb{N})$$

We note:

A. The first 25 Perrin numbers (i.e. those < 1000) are: 3, 0, 2, 3, 2, 5, 5, 7, 10, 12, 17, 22, 29, 39, 51, 68, 90, 119, 158, 209, 277, 367, 486, 644, 853.[208]
B. One of the properties of Perrin numbers is that n divides P_n when n is prime. This property makes Perrin numbers a useful tool for primality testing (see for instance Point 30 of § 7.2).

2.1.60 Pierpont Primes

These are primes of the form $2^a 3^b + 1$ for $a, b \in \mathbb{N}_0$. For example, 5 and 19 are Pierpont primes because $5 = 2^2 \times 3^0 + 1$ and $19 = 2^1 \times 3^2 + 1$. We note:

---

[205] Noting that in base 10 there are only 21 known non-repunit permutable primes (see Point 2), and only 11 known repunit primes (possibly including some probable; see Point 2 of § 2.1.69), there are only 32 known permutable primes (possibly including some probable).

[206] See `https://oeis.org/A074788`.

[207] See `https://oeis.org/A112881`.

[208] See `https://oeis.org/A001608`.

1. The first 18 Pierpont primes (i.e. those < 1000) are: 2, 3, 5, 7, 13, 17, 19, 37, 73, 97, 109, 163, 193, 257, 433, 487, 577, 769.[209]
2. The largest known Pierpont prime is apparently $2^{20498148} \times 3^4 + 1$ (with about 6.17 million decimal digits).
3. If p is a Pierpont prime then all the prime factors of $(p-1)$ are 2 or 3 (which is a trivial statement noting the form of Pierpont prime).[210]
4. Fermat primes (see § 2.1.20) are Pierpont primes (i.e. with $a = 2^k$ and $b = 0$) and hence Fermat primes are a proper subset of Pierpont primes.
5. All Pierpont primes (excluding 2 and Fermat primes) are of the form $6n + 1$ for some $n \in \mathbb{N}$ (noting that all the primes greater than 3 are of the form $6n \pm 1$, and noting as well that if $b > 0$ then a must also be > 0 to avoid having an even composite number).
6. It is conjectured that there are infinitely many Pierpont primes.
7. A prime of the form $2^a 3^b - 1$ may be called Pierpont prime of the second kind (and hence the above definition of Pierpont primes becomes restricted to Pierpont primes of the first kind). For example, 5 and 17 are Pierpont primes of the second kind because $5 = 2^1 \times 3^1 - 1$ and $17 = 2^1 \times 3^2 - 1$. The first 14 Pierpont primes of the second kind (i.e. those < 300) are: 2, 3, 5, 7, 11, 17, 23, 31, 47, 53, 71, 107, 127, 191.[211]

2.1.61 Pillai Primes

A Pillai prime is a prime number p for which there is an $n \in \mathbb{N}$ such that:

$$p|(n! + 1) \qquad \text{and} \qquad n \not| (p-1) \tag{26}$$

We note:
1. The first 13 Pillai primes (i.e. those < 200) are: 23, 29, 59, 61, 67, 71, 79, 83, 109, 137, 139, 149, 193 (corresponding to smallest $n = 14$, 18, 15, 8, 18, 9, 23, 13, 86, 16, 16, 50, 102).[212]
2. There are infinitely many Pillai primes.

2.1.62 Prime-Indexed Primes

The prime-indexed primes (also known as *super primes*) are simply prime-indexed primes (where the "index" in this definition refers to the subscript of the prime in the sequence of prime numbers which identifies their order in this sequence, i.e. n in p_n). For example, 3 and 5 are prime-indexed primes because their indices are 2 and 3 which are primes. We note:
1. The first 14 prime-indexed primes (i.e. those < 200) are: 3, 5, 11, 17, 31, 41, 59, 67, 83, 109, 127, 157, 179, 191 (corresponding to $n = 2$, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43).[213]
2. As indicated above, the "index" in the definition of super primes refers to their order in the sequence of prime numbers. Therefore, Fibonacci primes (except 3) are not necessarily super primes (see Point 3 of § 2.1.21) because the prime index of the Fibonacci primes refers to their order in the sequence of Fibonacci numbers. Similarly, Pell primes are not necessarily super primes (see Point 3 of § 2.1.57)

[209] See `https://oeis.org/A005109`.

[210] A positive integer whose prime factors are all $\leq p$ (for some $p \in \mathbb{P}$) is called *p-smooth number* or *p-friable number*, and hence a Pierpont prime minus 1 is a 3-smooth or 3-friable number because its only prime factors are 2 and/or 3 and this naming may give some significance to this statement.

[211] See `https://oeis.org/A005105`.

[212] See `https://oeis.org/A063980` and `https://oeis.org/A063828`. We did not find reliable information or official record about the largest known Pillai prime (possibly because they are not typically tracked as record-breaking large primes like Mersenne primes).

[213] See `https://oeis.org/A006450`. We did not find sufficiently reliable information about the largest known super prime.

because the prime index of the Pell primes refers to their order in the sequence of Pell numbers. For example, the Fibonacci number $\mathcal{F}_{13} = 233$ is prime (with a Fibonacci index 13 which is prime) but it is not a super prime because 233 is p_{51} in the sequence of prime numbers (i.e. with a prime-sequence index of 51 which is composite). Similarly, the Pell number $\mathcal{P}_5 = 29$ is prime (with a Pell index 5 which is prime) but it is not a super prime because 29 is p_{10} in the sequence of prime numbers (i.e. with a prime-sequence index of 10 which is composite).

3. The idea of super primes may be extended to higher levels of indexing and hence we get higher-order super primes, e.g. a second order super prime which is a prime-indexed prime-indexed prime such as 5 which is prime indexed (i.e. 3) which is also prime indexed (i.e. 2).[214]
4. The idea of super primes may also be extended to specific types of prime indices, e.g. prime numbers with palindromic prime indices such as 31, 547, 739 whose indices are 11, 101, 131 (which are palindromic primes; see § 2.1.53).[215]
5. Any integer > 96 is a sum of distinct prime-indexed primes.
6. There are infinitely many prime-indexed primes (because there are infinitely many prime numbers and hence for each prime number p there is a prime number at the p^{th} position in the list of primes).

2.1.63 Primeval Primes

A primeval prime is a primeval number that is prime (see the upcoming Note). We note:

1. The first 13 primeval primes in base 10 (i.e. those $< 10^5$) are: 2, 13, 37, 107, 113, 137, 1013, 1237, 1367, 10079, 10139, 12379, 13679.[216]
2. It is conjectured that there are infinitely many primeval primes.

Note: A *primeval number* is a positive integer n for which the number of distinct prime numbers that can be obtained by permuting some or all of its digits is larger than the number of primes that can be obtained in the same way for any smaller positive integer. For example, 13 is a primeval number because three prime numbers (i.e. 3, 13 and 31) can be obtained from its permutations, whereas no positive integer less than 13 can produce three (or more) such prime numbers. We note:

A. Being primeval is base-dependent (where 10 is the conventional base).
B. The first 13 primeval numbers in base 10 (i.e. those $< 10^4$) are: 1, 2, 13, 37, 107, 113, 137, 1013, 1037, 1079, 1237, 1367, 1379.[217] The number of primes that can be obtained from these 13 primeval numbers is (respectively): 0, 1, 3, 4, 5, 7, 11, 14, 19, 21, 26, 29, 31.[218]
C. The maximum number of distinct primes obtainable from a primeval number with n digits is (corresponding respectively to $n = 1, 2, 3, \ldots, 11$): 1, 4, 11, 31, 106, 402, 1953, 10542, 64905, 362451, 2970505.[219] The smallest n-digit number attaining this maximum is: 2, 37, 137, 1379, 13679, 123479, 1234679, 12345679, 102345679, 1123456789, 10123456789.[220]

[214] Accordingly, 31 is a fourth order super prime, i.e. $31 \to 11 \to 5 \to 3 \to 2$.
[215] See `https://oeis.org/A124173`.
[216] See `https://oeis.org/A119535`. We did not find sufficiently reliable information about the largest known primeval prime.
[217] See `https://oeis.org/A072857`.
[218] See `https://oeis.org/A076497`.
[219] See `https://oeis.org/A076730`.
[220] See `https://oeis.org/A134596` noting that we are using the former definition.

2.1.64 Primorial Primes

A primorial prime $P_{p_n}^{\pm}$ is a prime number that is exactly one more or one less than a primorial number $p_n\#$ (i.e. of the first kind; see the upcoming Note), that is:

$$P_{p_n}^{\pm} = p_n\# \pm 1 \tag{27}$$

We note:

1. Primorial primes may also be called Euclid primes or Euclidean primes because they are defined in a manner similar to the construction used in Euclid's proof of the infinitude of prime numbers. However, these terms may be restricted to the $p_n\# + 1$ form, i.e. Euclid primes or Euclidean primes are the primes of the Euclid numbers (where Euclid numbers are defined as integers of the form $p_n\# + 1$). We should also note that Euclidean primes may be defined as the prime divisors of Euclid numbers. So, caution is required when reading mathematical texts because the terminology in the literature is not universal.
2. There are currently only 52 known primorial primes because primorial numbers grow at an extremely rapid rate, making primality testing exceptionally difficult.
3. The first 10 primorial primes (i.e. those $< 10^{11}$) are: 2, 3, 5, 7, 29, 31, 211, 2309, 2311, 30029 (corresponding to $n = 0$, 1, 2, 2, 3, 3, 4, 5, 5, 6).[221]
4. The largest known primorial prime is apparently $9562633\# + 1$ (with about 4.15 million decimal digits).[222]
5. The first 5 primorial primes of the form $p_n\# - 1$ (i.e. those $< 10^{34}$) are: 5, 29, 2309, 30029, 304250263527209 (corresponding to $n = 2$, 3, 5, 6, 13).[223]
6. The first 5 primorial primes of the form $p_n\# + 1$ (i.e. those $< 10^3$) are: 2, 3, 7, 31, 211 (corresponding to $n = 0$, 1, 2, 3, 4).[224]
7. Not every number of the form $p_n\# \pm 1$ (i.e. primorial ± 1) is prime.[225] This means:
   • There are some n for which only $p_n\# - 1$ or only $p_n\# + 1$ is prime (i.e. there are some primorial numbers which have only one associated primorial prime). For example, $p_4\# - 1 = 209$ is composite ($209 = 11 \times 19$), while $p_4\# + 1 = 211$ is prime. On the other hand, $p_6\# - 1 = 30029$ is prime, while $p_6\# + 1 = 30031$ is composite ($30031 = 59 \times 509$).
   • There are some n for which neither $p_n\# - 1$ nor $p_n\# + 1$ is prime (i.e. there are some primorial numbers which have no associated primorial prime). For example, $p_7\# - 1 = 510509$ which is composite ($510509 = 61 \times 8369$), and $p_7\# + 1 = 510511$ which is also composite ($510511 = 19 \times 26869$).
8. Some twin primes are primorial primes, i.e. both numbers of the pair are primorial, e.g. (3, 5), (5, 7) and (29, 31). Moreover, there are twin primorial primes that share the same n, e.g. (5, 7) which corresponds to $n = 2$ and (29, 31) which corresponds to $n = 3$. So, the numbers in the twin primorial primes can be associated with the same primorial number or with two different primorial numbers (noting that some conventions about the naming may exist and this should be checked).
9. To sum up the last two points we say: for any primorial number $p_n\#$, we have four (mutually exclusive and exhaustive) possibilities: both $p_n\# - 1$ and $p_n\# + 1$ are prime, only $p_n\# - 1$ is prime, only $p_n\# + 1$ is prime, neither $p_n\# - 1$ nor $p_n\# + 1$ is prime.
10. It is unknown if there are infinitely many primorial primes. It is also unknown if there are infinitely many composite numbers of the form $p_n\# \pm 1$. However, there are conjectures that predict the infinitude of

[221] See `https://oeis.org/A228486`.
[222] See `https://t5k.org/largest.html`.
[223] See `https://oeis.org/A057705`.
[224] See `https://oeis.org/A018239`.
[225] This point is related to the twin prime primorial which will be discussed in Point 8.

both (i.e. there are infinitely many n where at least one of $p_n\# - 1$ or $p_n\# + 1$ is prime/composite).[226]

11. Primorial primes may be considered the "prime-based analog" of factorial primes (see § 2.1.19), i.e. primorial primes multiply all consecutive primes up to p_n (± 1) while factorial primes multiply all consecutive integers up to n (± 1).[227]
12. Primorial primes may be viewed as the "prime-based counterparts" of compositorial primes (see § 2.1.9), since primorials and compositorials respectively isolate the prime and composite factors within the product defining a factorial.
13. Because the number $p_n\# \pm 1$ is coprime to every prime $\leq p_n$, a trial division primality test of $p_n\# \pm 1$ requires inspection of only the primes p's where $p_n < p \leq (p_n\# \pm 1)^{1/2}$. This facilitates the search for primorial primes (although the efficiency gain is usually trivial since this excludes only the very small primes).

Note: The n^{th} *primorial number of the first kind* (symbolized as $p_n\#$) is the product of the first n primes where $n \in \mathbb{N}_0$, that is:

$$p_n\# = \prod_{k=1}^{n} p_k \tag{28}$$

By convention $p_0\# = 1$. The first 10 primorial numbers of the first kind (i.e. those $< 10^9$) are: 1, 2, 6, 30, 210, 2310, 30030, 510510, 9699690, 223092870.[228]

The n^{th} *primorial number of the second kind* (symbolized as $n\#$) is the product of all prime numbers $\leq n$ where $n \in \mathbb{N}_0$, that is:

$$n\# = \prod_{p \leq n} p \tag{29}$$

By convention $0\# = 1\# = 1$. The first 13 primorial numbers of the second kind (i.e. those $< 10^4$) are: 1, 1, 2, 6, 6, 30, 30, 210, 210, 210, 210, 2310, 2310 (corresponding to $n = 0, 1, 2, \ldots, 12$).[229]

We should finally note that there is apparently no uniquely-named prime type designated strictly for the primes of the form $n\# \pm 1$. One reason is that since $n\#$ evaluates to the product of all primes less than or equal to n, composite integers simply duplicate the values generated by the preceding prime (e.g. $5\# \pm 1 = 6\# \pm 1$) which violates uniqueness. Moreover, all primes generated by $n\# \pm 1$ can be similarly generated by $p_k\# \pm 1$ (e.g. $p_3\# \pm 1 = 5\# \pm 1$).

2.1.65 Proth Primes

A Proth prime is a Proth number that is prime (see the upcoming Note). We note:

1. The first 17 Proth primes (i.e. those < 1000) are: 3, 5, 13, 17, 41, 97, 113, 193, 241, 257, 353, 449, 577, 641, 673, 769, 929.[230]
2. The largest known Proth prime is apparently $2^{31172165} \times 10223 + 1$ (with about 9.38 million decimal digits).[231]
3. Cullen primes are a proper subset of Proth primes (see § 2.1.12).[232]

[226] It seems that there is even a conjecture about the infinitude of twin primorial primes. These conjectures may be linked to the Hardy-Littlewood prime k-tuple conjecture (see § 6.1.17). We should also note that apparently a recent conjecture predicts that there are approximately three primorial twin prime pairs in total, i.e. pairs of the form $(p_n\# - 1, p_n\# + 1)$. The known examples correspond to $n = 2, 3$ and 5 giving the pairs (5, 7), (29, 31) and (2309, 2311).

[227] In fact, even the number of currently known factorial and primorial primes is about the same (i.e. 53 factorial primes and 52 primorial primes) although this seems to be largely coincidental as there is no known reason to expect the two types to contain the same or similar numbers of primes.

[228] See `https://oeis.org/A002110`.

[229] See `https://oeis.org/A034386`.

[230] See `https://oeis.org/A080076`.

[231] See `https://t5k.org/top20/page.php?id=3`.

[232] If n is odd, it is already in Proth form since $n < 2^n$. If n is even, then writing $n = 2^t u$ (where u is odd) gives

4. When n is a power of 2 and $k = 1$ we get Fermat primes (see § 2.1.20), i.e. Fermat primes are a proper subset of Proth primes.
5. Proth's theorem provides a computationally efficient primality test (see § 7.3.17), and this makes finding large Proth primes relatively easy (i.e. compared to large primes of most other common types).
6. The concept of Proth primes may be generalized to primes of the form $a^n k + 1$ (with conditions similar to those defining Proth numbers and $1 < a \in \mathbb{N}$) and hence we get generalized Proth primes.
7. It is conjectured that there are infinitely many Proth primes.

Also see § 2.1.71.

Note: The *Proth numbers* are integers of the form $2^n k + 1$ where $n \in \mathbb{N}$, k is an odd positive integer, and $k < 2^n$. The first 13 Proth numbers (i.e. those < 100) are: 3, 5, 9, 13, 17, 25, 33, 41, 49, 57, 65, 81, 97.[233]

2.1.66 Pythagorean Primes

These are primes of the form $4n + 1$ where $n \in \mathbb{N}$. We note:

1. The first 11 Pythagorean primes (i.e. those < 100) are: 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97.[234]
2. The largest known Pythagorean prime is apparently the generalized Fermat prime $2524190^{2^{21}} + 1$ (with about 13.4 million decimal digits); see § 2.1.24.[235]
3. Referring to § 5.1.41, every Pythagorean prime can be uniquely expressed as a sum of two perfect squares, and vice versa (excluding 2; see Point 7). So, Pythagorean primes are precisely those odd primes which are the sum of two perfect squares (and this may be used as another definition of Pythagorean primes). For example, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$ and $29 = 2^2 + 5^2$.
4. Geometrically (referring to the previous point), the Pythagorean primes represent (by their square root) the length of the hypotenuse of right-angle triangles with integer-size legs.[236] This should explain why they are "Pythagorean".
5. $m^2 + 1$ (where $m \in \mathbb{Z}$) is divisible by a prime $p > 2$ *iff* p is a Pythagorean prime.
6. There are infinitely many Pythagorean primes.[237] Also see § 8.7.1.
7. As indicated above, Pythagorean primes may be defined as:
   - Primes of the form $4n + 1$ where $n \in \mathbb{N}$.
   - Primes that can be uniquely expressed as a sum of two perfect squares.

   However, the first definition excludes 2 while the second definition includes 2, and hence the two definitions are not equivalent. Yes, if we add "odd" to the second definition (i.e. "Odd primes that can be uniquely expressed as a sum of two perfect squares") then the two definitions are equivalent.

2.1.67 Quartan Primes

A quartan prime is a prime number of the form $x^4 + y^4$ where $x, y \in \mathbb{N}$. We note:

1. The first 14 quartan primes (i.e. those $< 10^4$) are: 2, 17, 97, 257, 337, 641, 881, 1297, 2417, 2657, 3697, 4177, 4721, 6577.[238]
2. The largest known quartan prime is apparently $(2524190^{524288})^4 + 1^4 = 2524190^{2097152} + 1$ (with about 13.4 million decimal digits), which is currently the largest known non-Mersenne prime and the sixth

$2^n n + 1 = 2^{n+t} u + 1$ which is Proth form. Hence every Cullen prime is a Proth prime.

[233] See `https://oeis.org/A080075`.

[234] See `https://oeis.org/A002144`.

[235] See `https://t5k.org/top20/page.php?id=3`.

[236] In fact, the Pythagorean primes also represent (by themselves) the length of the hypotenuse of right-angle triangles with integer-size legs.

[237] The proof(s) of the infinitude of Pythagorean primes (e.g. Dirichlet's theorem; see § 5.1.11) should be proof(s) for the infinitude of prime numbers (see § 1.6) if such proof(s) do not assume the infinitude of primes.

[238] See `https://oeis.org/A002645`.

largest known prime.[239]

3. For all quartan primes (except 2), x and y must have opposite parity.
4. All quartan primes (except 2) can be expressed as $16n + 1$ for some $n \in \mathbb{N}$ (and hence all odd quartan primes are Pythagorean primes).
5. Quartan primes are a proper subset of generalized Fermat primes $F_{a,b,n}$ (see Point 2 of § 2.1.24).
6. It is conjectured that there are infinitely many quartan primes.[240] A proven result closely related to the infinitude of quartan primes is the Friedlander-Iwaniec theorem which states that there are infinitely many primes of the form $x^2 + y^4$ where x and y are integers.[241]

2.1.68 Ramanujan Primes

The n^{th} Ramanujan prime R_n $(n = 1, 2, \ldots)$ is the smallest prime such that there are at least n primes between $x/2$ and x for all $x \geq R_n$. This may also be stated formally in terms of the prime-counting function $\pi(x)$ as: $\pi(x) - \pi(x/2) \geq n$ (where $n \in \mathbb{N}$) for all $x \geq R_n$. For example:

• $R_1 = 2$ (i.e. the Ramanujan prime with $n = 1$ is 2) because 2 is the smallest prime such that there is at least 1 prime in the interval $(x/2, x]$ for all $x \geq 2$.

• $R_2 = 11$ because 11 is the smallest prime such that there are at least 2 primes in $(x/2, x]$ for all $x \geq 11$.[242]

We note:

1. The first 18 Ramanujan primes (i.e. those < 200) are: 2, 11, 17, 29, 41, 47, 59, 67, 71, 97, 101, 107, 127, 149, 151, 167, 179, 181.[243]
2. There is a close relationship between Ramanujan primes and Bertrand's postulate (see § 5.1.2). In fact, the above formal statement [i.e. $\pi(x) - \pi(x/2) \geq n$ for all $x \geq R_n$] may be considered a generalization to Bertrand's postulate noting that the existence of such a smallest prime R_n for any $n \in \mathbb{N}$ is proven (and hence $R_1 = 2$ corresponds to Bertrand's postulate).
3. There are infinitely many Ramanujan primes.[244]

2.1.69 Repunit Primes

"Repunit number" means "repeated unit number" (i.e. a multi-digit integer whose digits are all 1) such as 11, 111, 1111 (noting that repunit numbers may be symbolized by U_n where the suffix n indicates the number of their digits, e.g. $U_2 = 11$ and $U_5 = 11111$). So, repunit primes are those repunit numbers

---

[239] See `https://t5k.org/top20/page.php?id=3`.

[240] This does not appear to follow directly from standard conjectures such as those of Bunyakovsky or Bateman-Horn (see § 6.1.11 and § 6.1.6) since these concern prime values of univariate polynomials, whereas $x^4 + y^4$ is a polynomial in two variables. Nevertheless, either conjecture, applied to the univariate polynomial $x^4 + 1$, would imply the infinitude of quartan primes. Thus, the infinitude of quartan primes is not necessarily an independent conjecture, although its natural formulation as a statement about primes represented by $x^4 + y^4$ is not itself a direct instance of the standard univariate conjectures.

[241] Because the theorem allows both variables to vary independently, it does not guarantee the infinitude of primes in any particular slice (such as $1 + y^4$) and thus does not prove the infinitude of quartan primes.

[242] We note that $3, 5, 7$ do not satisfy this condition because:
- In $(4/2, 4]$ there is only 1 prime and hence 3 fails.
- In $(6/2, 6]$ there is only 1 prime and hence 5 fails.
- In $(10/2, 10]$ there is only 1 prime and hence 7 fails.

[243] See `https://oeis.org/A104272`. We did not find sufficiently reliable information about the largest known Ramanujan prime.

[244] The existence of R_n for every $n \in \mathbb{N}$ immediately implies that there are infinitely many Ramanujan primes (since the R_n form a strictly increasing sequence of primes) and hence the infinitude of prime numbers (see § 1.6). In fact, the existence of R_n for every n is a stronger assertion than the mere infinitude of ordinary primes since it asserts that for every prescribed n there is a threshold beyond which every interval $(x/2, x]$ contains at least n primes. Accordingly, any proof of such a generalized Bertrand-type statement for every n also yields, as a consequence, a proof that there are infinitely many ordinary primes.

which are primes. We note:
1. Being repunit is base-dependent (where 10 is the conventional base and this is what we mean here when we use the U_n notation).
2. Apparently, there are only 11 known repunit primes (in base 10), i.e. those with $n = 2$, 19, 23, 317, 1031, 49081, 86453, 109297, 270343, 5794777, 8177207.[245]
3. The only multi-digit prime numbers with identical digits (i.e. all their digits are the same) are repunits (like $U_2 = 11$ and $U_{19} = 1111111111111111111$).[246]
4. The number of digits (i.e. n) of a repunit prime must be a prime number (noting that this is a necessary but not sufficient condition, e.g. U_3 is composite).[247]
5. In the binary numeral system (base 2), Mersenne primes and repunit primes are identical sets (see § 2.1.41).
6. It is conjectured that there are infinitely many repunit primes in every base that is not a perfect power.[248]
7. "Generalized repunit primes" may be used to refer to prime numbers of the form $(n^k - 1)/(n - 1)$ where $n, k \in \mathbb{N}$.[249] In fact, even Mersenne primes are generalized repunit primes in this sense (i.e. with $n = 2$). The "generalized repunit primes" name may be justified by the fact that $(n^k - 1)/(n - 1)$ represents the geometric progression $n^{k-1} + n^{k-2} + \cdots + n + 1$ which in base n is a number consisting of k repetitions of the digit 1.

2.1.70 Reversible Primes

A reversible prime is a prime number that remains prime when its digits are reversed, and hence "reversible prime" includes both emirp primes (see § 2.1.17) and palindromic primes (see § 2.1.53) although there seems to be different conventions in this regard. We note:
1. Being reversible is base-dependent (where 10 is the conventional base).
2. The first 25 reversible primes in base 10 (i.e. those < 300) are: 2, 3, 5, 7, 11, 13, 17, 31, 37, 71, 73, 79, 97, 101, 107, 113, 131, 149, 151, 157, 167, 179, 181, 191, 199.[250]
3. All emirp primes (see § 2.1.17), palindromic primes (see § 2.1.53) and repunit primes (see § 2.1.69) are reversible and hence these types are proper subsets of reversible primes.
4. It is conjectured that there are infinitely many reversible primes. This follows from the individual infinitude conjectures for emirps and palindromic primes. Notably, this would also follow if the independent conjecture that there are infinitely many repunit primes (which form a proper subset of the palindromic primes) were true.

2.1.71 Riesel Primes

This does not seem to be a commonly-recognized (or standard) type of prime numbers. In fact, "Riesel prime" may be used loosely (or defined strictly) in one of the following meanings (and possibly more):
- Prime number of the form $2^n k - 1$ where $n \in \mathbb{N}$ and $0 < k \in \mathbb{O}$.
- Prime number of the form $2^n k - 1$ where $n \in \mathbb{N}$ and $0 < k \in \mathbb{O}$ (with $k < 2^n$).
- Prime number of the form $2^n k - 1$ where $n \in \mathbb{N}$ and $1 < k \in \mathbb{O}$.
- Prime number of the form $2^n k - 1$ where $n \in \mathbb{N}$ and $1 < k \in \mathbb{O}$ (with $k < 2^n$).

[245] See `https://oeis.org/A004023`. We note that some of these (possibly the last three) are apparently probable. If so, then the largest known proven repunit prime is U_{109297} and the largest known probable repunit prime is $U_{8177207}$.
[246] Being repunit is a necessary but not sufficient condition for a repdigit to be prime.
[247] We note that: for any $m, n \in \mathbb{N}$, the repunit U_m divides U_n *iff* m divides n (in any base ≥ 2).
[248] If the base is a perfect power, there can be at most one repunit prime in that base. For example, in the perfect square bases 4, 9 and 16, the only repunit primes are 5 (base 4) and 17 (base 16), while there are none in base 9.
[249] See for example `https://oeis.org/A076481`, `https://oeis.org/A086122` and `https://oeis.org/A165210`.
[250] See `https://oeis.org/A007500`. For the largest known reversible prime refer to § 2.1.17, § 2.1.53 and § 2.1.69.

However, according to the first meaning (or definition), every odd prime is a Riesel prime because if p is an odd prime then $p+1$ must be an even number which can be written as $p+1=2^nk$ with $n\in\mathbb{N}$ and $0<k\in\mathbb{O}$ and hence $p=2^nk-1$ (which is a Riesel prime according to this meaning). This may explain why other conditions in the above list are imposed.

A less-formal and search-based meaning/definition may be attached to "Riesel primes" as: prime numbers found during the search for a prime to eliminate a candidate k from the Riesel problem (see § 7.9.3). Anyway, "Riesel primes" seems to find its proper and specific meaning (whether technical or non-technical) within the context of investigating the Riesel problem and the search for Riesel number (or numbers).[251]

We think it is sensible and useful to define a standard and technically-specific type of "Riesel primes" on the style of Proth primes (see § 2.1.65) by adopting the second definition in the above list, i.e. Riesel prime is a prime number of the form 2^nk-1 where $n\in\mathbb{N}$, $0<k\in\mathbb{O}$ and $k<2^n$. In the following points (as well as in the rest of this book unless stated otherwise) we adopt this definition:

1. The first 7 Riesel primes (i.e. those <100) are: 3, 7, 11, 23, 31, 47, 79.
2. Every Mersenne prime (see § 2.1.41) is a Riesel prime (corresponding to the case $k=1$), and hence Mersenne primes are a proper subset of Riesel primes.[252]
3. The correspondence between Proth and Riesel primes (see § 2.1.65) in form is like the correspondence between Fermat and Mersenne primes (noting that Fermat and Mersenne primes are subsets of Proth and Riesel primes respectively).
4. Some of the largest known primes are Riesel primes because their form allows for computationally-efficient primality testing (see § 7.3.10 and § 7.3.11). Also see Point 5 of § 2.1.65.
5. We did not find a source that explicitly states the infinitude (or finitude) of Riesel primes (whether as a theorem or as a conjecture). While Dirichlet's theorem (see § 5.1.11) guarantees infinitely many primes of the form 2^nk-1 if n is fixed and k varies without bound, it cannot establish the infinitude of our defined Riesel primes because it fails to account for the condition $k<2^n$. When k is fixed or bounded and n varies, the sequence becomes exponential, and hence it is beyond the scope of Dirichlet's theorem. Anyway, it is natural to conjecture that there are infinitely many Riesel primes (where such a conjecture may be supported by heuristic arguments).[253]
6. The concept of Riesel primes may be generalized to primes of the form a^nk-1 (with $1<a\in\mathbb{N}$, $0<k<a^n$, a and k are coprime and of opposite parity) and hence we get "generalized Riesel primes".

2.1.72 Safe Primes

A safe prime S_p is a prime number of the form $S_p=2p+1$ where p is a (Sophie Germain) prime (see § 2.1.76). In other words, $q\in\mathbb{P}$ is a safe prime *iff* $(q-1)/2$ is prime. We note:

1. The first 25 safe primes (i.e. those <1000) are: 5, 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467, 479, 503, 563, 587, 719, 839, 863, 887, 983 (corresponding to the Sophie Germain primes $p=2$, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, 359, 419, 431, 443, 491).[254]
2. The largest known safe prime is apparently $2618163402417\times2^{1290001}-1$ (with about 388 thousand digits; also see Point 2 of § 2.1.76).
3. All safe primes (except 5) are non-Pythagorean primes (see § 2.1.66).[255]

[251] Also see the following websites: `http://www.prothsearch.com/riesel2.html` and `https://web.archive.org/web/20210715115849/http://www.15k.org/riesellist.html`.

[252] Accordingly, the largest known Riesel prime is the largest known prime which is the Mersenne prime $2^{136279841}-1$.

[253] We note that any independent proof establishing the infinitude of Riesel primes without assuming the existence of infinite primes would inherently serve as a proof for the infinitude of prime numbers (see § 1.6). We should also note that the infinitude of Riesel primes is related to the (commonly conjectured) infinitude of Mersenne primes (which are a proper subset of Riesel primes).

[254] See `https://oeis.org/A005385` and `https://oeis.org/A005384`.

[255] This is because if q is a safe prime then $q=2p+1$ where p is an odd prime (to exclude 5) and hence $q=2(2k+1)+1=$

4. It is conjectured that there are infinitely many safe primes (possibly as a result of the conjectured infinitude of Sophie Germain primes; see § 2.1.76).

2.1.73 Self Primes

A self prime is a self number that is prime (see the upcoming Note). We note:
1. The first 21 self primes in base 10 (i.e. those < 1000) are: 3, 5, 7, 31, 53, 97, 211, 233, 277, 367, 389, 457, 479, 547, 569, 613, 659, 727, 839, 883, 929.[256]
2. The largest known self prime is probably the Mersenne prime $2^{82589933} - 1$ (with about 24.9 million digits).[257]
3. It is conjectured that there are infinitely many self primes in every even base. For odd bases, every odd positive integer is a self number, and hence there are infinitely many self primes.

Note: A *self number* (also known as *Colombian number* and *Devlali number*) is a natural number n that cannot be expressed as a sum of an integer $k \in \mathbb{N}$ and its digit sum, that is:

$$n \neq k + S(k) \qquad \text{(for any } k \in \mathbb{N}\text{)} \tag{30}$$

where $S(k)$ is the sum of the digits of k. For example, 3 is a self number because $3 \neq 1+1$ and $3 \neq 2+2$. On the other hand, 19 is not a self number because $19 = 14 + 1 + 4$. We note:
A. Being self number is base-dependent (where 10 is the conventional base).
B. To test whether n is a self number it is sufficient to check the condition $n \neq k + S(k)$ for only $k < n$ because for all $k \geq n$ the condition $n \neq k + S(k)$ is satisfied since $S(k) \geq 1$.
C. The first 23 self numbers in base 10 (i.e. those < 200) are: 1, 3, 5, 7, 9, 20, 31, 42, 53, 64, 75, 86, 97, 108, 110, 121, 132, 143, 154, 165, 176, 187, 198.[258]
D. There are infinitely many self numbers in every base.

2.1.74 Sexy Primes

Sexy primes are a pair of prime numbers which are 6 apart (such as 5 and 11). We note:
1. According to the above definition, 6 is not necessarily a gap, and hence other primes may exist between sexy primes.
2. The first 15 sexy prime pairs (i.e. those with both primes < 100) are: (5, 11), (7, 13), (11, 17), (13, 19), (17, 23), (23, 29), (31, 37), (37, 43), (41, 47), (47, 53), (53, 59), (61, 67), (67, 73), (73, 79), (83, 89).[259]
3. The largest known sexy prime pair is apparently $(p, p+6)$ where $p = 7977227425 \times (2^{368352} - 2^{257849}) + 2^{110505} - 5$ (with about 111 thousand digits each).[260]
4. There are sexy prime triplets [like (7, 13, 19)] and sexy prime quadruplets [like (41, 47, 53, 59)].[261] Moreover, there is exactly one sexy prime quintuplet [i.e. (5, 11, 17, 23, 29)].
5. It is conjectured that there are infinitely many sexy primes (apparently as an instance of Polignac's conjecture; see § 6.1.26).

$4k + 3$ (where $k \in \mathbb{N}$) which is non-Pythagorean.

[256] See `https://oeis.org/A006378`.

[257] See `https://t5k.org/curios/page.php/82589933.html` noting that this number is currently the second largest known prime, and hence the possibility of the largest known prime (i.e. $2^{136279841} - 1$) to be a self prime should be checked.

[258] See `https://oeis.org/A003052`.

[259] See `https://oeis.org/A023201` and `https://oeis.org/A046117`.

[260] See `https://www.pzktupel.de/CPAP/CPAP02`.

[261] In fact, the infinitude of sexy prime triplets and sexy prime quadruplets is predicted by some conjectures like Dickson's conjecture and the first Hardy-Littlewood conjecture (see § 6.1.13 and § 6.1.17). Also see `https://www.pzktupel.de/CPAP/sexyP`.

2.1.75 Smarandache-Wellin Primes

A Smarandache-Wellin prime is a Smarandache-Wellin number that is prime (see the upcoming Note). We note:

1. The first 3 Smarandache-Wellin primes in base 10 are: 2, 23, 2357 (noting that the fourth is the concatenation of the first 128 primes).[262]
2. The largest known Smarandache-Wellin prime (in base 10) is apparently the one formed by concatenating the first 1429 prime numbers (with 5719 decimal digits).[263]
3. It is conjectured that there are infinitely many Smarandache-Wellin primes.

Note: A *Smarandache-Wellin number* is a natural number formed by concatenating the first n ($n \in \mathbb{N}$) prime numbers in their increasing order. We note:

A. Being a Smarandache-Wellin number is base-dependent (where 10 is the conventional base).
B. The first 8 Smarandache-Wellin numbers in base 10 are: 2, 23, 235, 2357, 235711, 23571113, 2357111317, 235711131719.[264]

2.1.76 Sophie Germain Primes

A prime number p is a Sophie Germain prime *iff* $2p + 1$ is also prime. The latter (i.e. $2p + 1$) is called a safe prime (see § 2.1.72). For example, 2 is a Sophie Germain prime (because $2 \times 2 + 1 = 5$ is also prime) while 5 is a safe prime (corresponding to 2). We note:

1. The first 25 Sophie Germain primes (i.e. those < 500) are: 2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293, 359, 419, 431, 443, 491.[265]
2. The largest known Sophie Germain prime is apparently $2618163402417 \times 2^{1290000} - 1$ (with about 388 thousand digits; also see Point 2 of § 2.1.72).[266]
3. It is conjectured that there are infinitely many Sophie Germain primes. This should consequently apply to safe primes.
4. Historically, Sophie Germain primes are linked to (attempts to prove) Fermat's last theorem. They are also linked to Cunningham chains (see § 9.1.3).
5. Sophie Germain and safe primes are important in cryptography (mainly in the creation of safe communication protocols).
6. There are primes which are both Sophie Germain and safe at the same time (but in different relations, i.e. corresponding to different numbers).[267] For example, 11 is a safe prime with respect to the Sophie Germain prime 5 (because $11 = 2 \times 5 + 1$) and it is a Sophie Germain prime with respect to the safe prime 23 (because $23 = 2 \times 11 + 1$). So, in this sense (i.e. for an individual number) Sophie Germain and safe primes are not mutually exclusive (although as pairs they are exclusive).

2.1.77 Stern Primes

A prime number p is a Stern prime if there is no smaller prime q and a positive integer b such that $p = q + 2b^2$. We note:

---

[262] See `https://oeis.org/A069151` and `https://oeis.org/A046035`.
[263] See `https://oeis.org/A046035`, `https://oeis.org/A046284` and `https://oeis.org/A263959`. These records suggest that there are currently only 8 known Smarandache-Wellin primes, i.e. those resulting from the concatenation of the first 1, 2, 4, 128, 174, 342, 435, 1429 primes (alternatively, those ending with the following primes: 2, 3, 7, 719, 1033, 2297, 3037, 11927). Also see `https://t5k.org/curios/page.php/1429.html`.
[264] See `https://oeis.org/A019518`.
[265] See `https://oeis.org/A005384`.
[266] See `https://t5k.org/largest.html`.
[267] Such primes may be called *Sophie Germain safe primes*.

1. There are only 8 known Stern primes which are: 2, 3, 17, 137, 227, 977, 1187, 1493.[268]
2. Stern primes are studied in additive number theory in connection with the representation of integers as sums of primes and related Goldbach-type problems.
3. It is conjectured that there are only finitely many Stern primes. In fact, it is conjectured that the 8 known Stern primes are the only such primes.

2.1.78 Strobogrammatic Primes

A strobogrammatic prime is a prime number whose numeral (in a given base) appears the same when rotated 180 degrees. We note:
1. Being strobogrammatic is base-dependent (where 10 is the conventional base).
2. To be strobogrammatic (in base 10), the number can contain only the following digits: 0, 1, 6, 8, 9.
3. The first 8 strobogrammatic primes (i.e. those $< 10^5$) are: : 11, 101, 181, 619, 16091, 18181, 19861, 61819.[269]
4. The largest known (non-repunit) strobogrammatic prime is apparently the dihedral (and tetradic palindrome) $10^{180054} + 8 \times \frac{10^{58567}-1}{9} \times 10^{60744} + 1$ (with about 180 thousand decimal digits; see § 2.1.16).[270] Refer to Point 2 of § 2.1.69 for the largest repunit strobogrammatic prime.
5. Repunit primes (see § 2.1.69) are a proper subset of strobogrammatic primes.
6. Strobogrammatic primes composed only of the digits 0, 1, and 8 (e.g. 11, 101, and 181) are also dihedral primes and palindromic primes (see § 2.1.16 and § 2.1.53).
7. It is conjectured that there are infinitely many strobogrammatic primes (noting that this is related to the conjectures about the infinitude of dihedral primes, palindromic primes and repunit primes).

2.1.79 Strong Primes

A strong prime (p_n) is a prime number that is greater than the average of the primes immediately before and after it, that is:

$$p_n > \frac{p_{n-1} + p_{n+1}}{2} \tag{31}$$

where n is the prime index in the sequence of prime numbers. For example, 11 and 17 are strong primes because $11 > (7 + 13)/2$ and $17 > (13 + 19)/2$. We note:
1. The first 10 strong primes (i.e. those < 100) are: 11, 17, 29, 37, 41, 59, 67, 71, 79, 97.[271]
2. In terms of prime gap, the gap preceding a strong prime is larger than the gap succeeding it, i.e. $(p_n - p_{n-1}) > (p_{n+1} - p_n)$.[272] Hence, in a twin prime pair (p_n, p_{n+1}) where $p_n > 5$, p_n is always a strong prime because the gap to the previous prime (i.e. $p_n - p_{n-1}$) is greater than 2 (see Point 9 of § 2.1.84).
3. There are infinitely many strong primes.[273]
4. Balanced primes (see § 2.1.1), strong primes, and weak primes (see § 2.1.89) partition the set of odd prime numbers.
5. "Strong prime" has another definition in cryptography (which is beyond the scope of this book), and hence the readers should be cautious. Also see Point 5 of § 2.1.89

[268] See `https://oeis.org/A042978`. Recent research seems to confirm that any other Stern prime must be larger than 2×10^{13}.
[269] See `https://oeis.org/A007597`.
[270] Also see `https://t5k.org/primes/page.php?id=89907`.
[271] See `https://oeis.org/A051634`. We did not find sufficiently reliable information about the largest known strong prime (noting that strong primes are very common and hence they are not a record-setting type or category with sufficient rarity or distinction to be recorded and documented as such).
[272] This condition can be obtained from the above inequality by multiplying it by 2 and rearranging its terms.
[273] The proof(s) of the infinitude of strong primes should be proof(s) for the infinitude of prime numbers (see § 1.6) if such proof(s) do not assume the infinitude of primes.

6. The idea of strong primes can be extended to higher orders (similar to the generalization of balanced and weak primes; see Point 5 of § 2.1.1 and Point 6 of § 2.1.89).

Also see § 2.1.26.

2.1.80 Supersingular Primes

"Supersingular prime" refers to two seemingly-different (but deeply-linked) concepts:

1. One related to algebraic number theory which means (according to some references) prime p for which an elliptic curve becomes supersingular (modulo p).[274] Accordingly, any supersingular elliptic curve has infinitely many such primes (which seemingly belong specifically to that curve).
2. One related to group theory (or monstrous moonshine theory) which means (according to some references) the set of prime numbers that divide the group order of the monster group. Accordingly, there are only 15 supersingular primes which are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71.[275]

The references that we consulted about supersingular primes are seemingly inconsistent. Moreover, this type of primes is discussed and investigated in very specialized literature (some of which is not related to number theory such as string theory). Hence, we refer the interested readers to the relevant literature.

2.1.81 Thabit Primes

A Thabit prime (which may also be called 321 prime) is a Thabit number that is prime (see the upcoming Note). We note:

1. The first 9 Thabit primes of the first kind (i.e. those $< 10^{10}$) are: 2, 5, 11, 23, 47, 191, 383, 6143, 786431 (corresponding to $n = 0$, 1, 2, 3, 4, 6, 7, 11, 18 in the sequence of Thabit numbers of the first kind).[276] Apparently, there are currently (March 2026) only 69 known Thabit primes of the first kind.[277]
2. The largest known Thabit prime of the first kind is apparently $2^{23157875} \cdot 3 - 1$ (with about 6.97 million decimal digits).[278]
3. The first 9 Thabit primes of the second kind (i.e. those $< 10^{12}$) are: 7, 13, 97, 193, 769, 12289, 786433, 3221225473, 206158430209 (corresponding to $n = 1$, 2, 5, 6, 8, 12, 18, 30, 36 in the sequence of Thabit numbers of the second kind).[279] Apparently, there are currently (March 2026) only 50 known Thabit primes of the second kind.[280]
4. The largest known Thabit prime of the second kind is apparently $2^{16408818} \cdot 3 + 1$ (with about 4.94 million decimal digits).[281]
5. Thabit primes are linked to amicable numbers and hence they are used (historically and currently) in the investigation and search for amicable numbers.[282]
6. It is conjectured that there are infinitely many Thabit primes (of each kind).
7. There are Thabit twin prime pairs (i.e. one of the first kind and the other of the second kind with the same exponent n), e.g. (5, 7) and (11, 13).

---

[274] An elliptic curve is a smooth plane algebraic curve defined over a field K and typically described by the cubic equation $y^2 = x^3 + ax + b$ where a, b are coefficients in K.

[275] See `https://oeis.org/A002267`.

[276] See `https://oeis.org/A007505` and `https://oeis.org/A002235`.

[277] See `https://pzktupel.de/Primetables/Table321`.

[278] See `https://www.primegrid.com/primes/primes.php?project=321` and `https://pzktupel.de/Primetables/Table321`.

[279] See `https://oeis.org/A039687` and `https://oeis.org/A002253`.

[280] See `https://pzktupel.de/Primetables/Table321`.

[281] See `https://www.primegrid.com/download/321-16408818.pdf` and `https://pzktupel.de/Primetables/Table321`.

[282] The first to investigate these primes and their link to amicable numbers is Thabit ibn Qurra (lived in the ninth century AD) who formalized a rule for using these primes to generate pairs of amicable numbers. We note that amicable numbers are pairs of positive integers where the sum of the proper divisors of each number equals the other number, e.g. (220, 284). See `https://oeis.org/A259180`.

Note: The *Thabit numbers* were historically defined as integers of the form $2^n \cdot 3 - 1$ ($n \in \mathbb{N}_0$). More recently, integers of the form $2^n \cdot 3 + 1$ ($n \in \mathbb{N}_0$) have been termed Thabit numbers of the second kind; thus, integers of the original form (i.e. $2^n \cdot 3 - 1$) are now referred to as Thabit numbers of the first kind. We note:

A. The first 12 Thabit numbers of the first kind (i.e. those $< 10^4$) are: 2, 5, 11, 23, 47, 95, 191, 383, 767, 1535, 3071, 6143.[283]

B. The first 12 Thabit numbers of the second kind (i.e. those $< 10^4$) are: 4, 7, 13, 25, 49, 97, 193, 385, 769, 1537, 3073, 6145.[284]

2.1.82 Tribonacci Primes

Tribonacci primes are Tribonacci numbers which are prime (see the upcoming Note). We note:

1. The first 5 Tribonacci primes (i.e. those $< 10^{25}$) are: 2, 7, 13, 149, 19341322569415713958901 (corresponding to $n = 4$, 6, 7, 11, 87 in the Tribonacci sequence).[285]
2. The largest known Tribonacci prime is apparently T_{96879} (with about 26 thousand decimal digits).[286]
3. It is conjectured that there are infinitely many Tribonacci primes (apparently independently rather than as an instance or implication of a broader general conjecture, noting that it is heuristically supported).

Note: The *Tribonacci numbers* are the numbers of the *Tribonacci sequence* which is defined recursively by the formula:

$$T_0 = T_1 = 0,\ T_2 = 1 \qquad \text{and} \qquad T_n = T_{n-3} + T_{n-2} + T_{n-1} \text{ (for } 2 < n \in \mathbb{N})$$

We note:

A. The first 18 Tribonacci numbers (i.e. those $< 10^4$) are: 0, 0, 1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 504, 927, 1705, 3136, 5768.[287]

B. Every positive integer can be expressed as a sum of distinct Tribonacci numbers (and hence the Tribonacci sequence is described as a *complete sequence*).

2.1.83 Truncatable Primes

A truncatable prime is a prime number that remains prime when digits are truncated from either side or both sides (simultaneously or alternately). We note:

1. Being truncatable is base-dependent (where 10 is the conventional base).
2. As indicated already, there are four main types of truncatable primes: left-truncatable, right-truncatable, left-and-right truncatable, and two-sided truncatable.
3. A *left-truncatable prime* is a prime number that remains prime at every stage as its leftmost digits are removed successively until only a single-digit prime number remains. An example of a left-truncatable prime is 9137 because 9137, 137, 37 and 7 are all primes. Left-truncatable primes must not contain the digit 0. There are only 4260 left-truncatable primes in base 10 (according to some references). The first 33 left-truncatable primes in base 10 (i.e. those < 500) are: 2, 3, 5, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97, 113, 137, 167, 173, 197, 223, 283, 313, 317, 337, 347, 353, 367, 373, 383, 397, 443, 467.[288] The largest left-truncatable prime is 357686312646216567629137 (according to some sources).

---

[283] See `https://oeis.org/A055010`.

[284] See `https://oeis.org/A181565`.

[285] See `https://oeis.org/A092836` and `https://oeis.org/A303263`.

[286] See `https://oeis.org/A303263`. From this record, it seems that there are currently only 11 known Tribonacci primes (with some being probable). The record also indicates that T_{96879} is probable rather than proven.

[287] See `https://oeis.org/A000073`.

[288] See `https://oeis.org/A024785`. Single-digit numbers may be excluded (otherwise they are "left-truncatable primes" in a trivial sense).

4. A *right-truncatable prime* is a prime number that remains prime at every stage as its rightmost digits are removed successively until only a single-digit prime number remains. An example of a right-truncatable prime is 7393 because 7393, 739, 73 and 7 are all primes. Multi-digit right-truncatable primes must not contain the digits 0, 2, 4, 5, 6, 8 (except for the leftmost digit which can be 2 or 5). There are only 83 right-truncatable primes in base 10 (according to some references). The first 27 right-truncatable primes in base 10 (i.e. those < 2000) are: 2, 3, 5, 7, 23, 29, 31, 37, 53, 59, 71, 73, 79, 233, 239, 293, 311, 313, 317, 373, 379, 593, 599, 719, 733, 739, 797.[289] The largest right-truncatable prime is 73939133 (according to some sources).
5. A *left-and-right truncatable prime* (which may also be called a *simultaneously truncatable prime*) is a prime number that remains prime at every stage as its leftmost and rightmost digits are removed simultaneously and successively until only a single-digit or double-digit prime number remains. An example of a left-and-right truncatable prime is 1825711 because 1825711, 82571, 257 and 5 are all primes. Appropriate digit restrictions must be imposed to avoid breach of primality or triviality at each successive stage of truncation (e.g. 0 is not allowed while 2, 4, 5, 6, 8 are not allowed in certain positions). There are only about 920.7 million left-and-right truncatable primes in base 10 (according to some references). The first 33 left-and-right truncatable primes in base 10 (i.e. those < 200) are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 127, 131, 137, 139, 151, 157, 173, 179.[290] The largest left-and-right truncatable prime is a 104-digit number (according to some sources).
6. A *two-sided truncatable prime* is a prime number that is both left-truncatable and right-truncatable. In other words, two-sided truncatable primes are precisely the primes in the intersection of the primes of Points 3 and 4. An example of a two-sided truncatable prime is 797 because it is simultaneously left-truncatable (since 797, 97 and 7 are all primes) and right-truncatable (since 797, 79 and 7 are all primes). The aforementioned digit restrictions of both left-truncatable and right-truncatable primes must be imposed on two-sided truncatable primes. There are only 15 two-sided truncatable primes in base 10 (according to some references) which are: 2, 3, 5, 7, 23, 37, 53, 73, 313, 317, 373, 797, 3137, 3797, 739397.[291]
7. As indicated above, there are only finitely many truncatable primes in base 10.[292]

2.1.84 Twin Primes

Twin primes are a pair of prime numbers which are 2 apart (like 11 and 13). We note:

1. Although 2 and 3 are consecutive primes they are not twin primes because their difference is not 2. Hence, the first (or lowest) twin prime pair is (3, 5).
2. $(3, 5)$ and $(5, 7)$ are the only consecutive pairs of twin primes. In other words, 5 is the only prime number that is shared by two different pairs of twin primes.[293]
3. The sum of any twin primes other than $(3, 5)$ is divisible by 12. In other words, any twin prime pair other than $(3, 5)$ can be expressed as $(6n - 1, 6n + 1)$ where $n \in \mathbb{N}$.[294]

[289] See `https://oeis.org/A024770`. Single-digit numbers may be excluded (otherwise they are "right-truncatable primes" in a trivial sense).

[290] See `https://oeis.org/A077390`. Single- and double-digit numbers may be excluded (otherwise they are "left-and-right truncatable primes" in a trivial sense).

[291] See `https://oeis.org/A020994`. Single-digit numbers may be excluded (otherwise they are "two-sided truncatable primes" in a trivial sense).

[292] Seemingly, it is conjectured that truncatable primes are finite in every base (apparently with certain restrictions and conditions). So, what is proven is only their finitude in base 10 (and possibly some other bases). The precise status of the various claims in the literature requires further investigation.

[293] (3, 5, 7) may be called *twin-triplet primes*, noting that triplet primes is usually used more generally to refer to a set of three consecutive primes separated from each other by a gap of certain size such as (47, 53, 59) which have a gap of 6 or (199, 211, 223) which have a gap of 12.

[294] This can be used as a test to rule out (but not in) being twin primes (i.e. it is a necessary but not sufficient condition

4. The number between a twin prime pair is obviously composite (since it is an even number > 2).
5. According to some Internet sources, the number of known twin prime pairs (below 10^{18}) is about 808.7 trillion.
6. The first 35 twin prime pairs (i.e. those < 1000) are: (3, 5) (5, 7) (11, 13) (17, 19) (29, 31) (41, 43) (59, 61) (71, 73) (101, 103) (107, 109) (137, 139) (149, 151) (179, 181) (191, 193) (197, 199) (227, 229) (239, 241) (269, 271) (281, 283) (311, 313) (347, 349) (419, 421) (431, 433) (461, 463) (521, 523) (569, 571) (599, 601) (617, 619) (641, 643) (659, 661) (809, 811) (821, 823) (827, 829) (857, 859) (881, 883).[295]
7. The largest known twin prime pair is apparently $2996863034895 \times 2^{1290000} \pm 1$ (with about 388 thousand digits).[296]
8. A prime number that is not part of a twin prime pair is called an *isolated prime*, e.g. 23 and 37 (see § 2.1.35). Such a prime may also be called *single prime* or *non-twin prime*. It is worth noting that "isolated prime" may be used more generally to refer to a prime that is not associated with neighboring primes such as being part of a cousin pair (see § 2.1.10) or a sexy pair (see § 2.1.74) as well as a twin pair, although this seems to depend on the context and hence "isolated" in such generalization may not be conventional or technical.
9. Noting that the only twin prime triplet is (3, 5, 7), in a twin prime pair (p_n, p_{n+1}) where $p_n > 5$ the gap to the previous prime p_{n-1} and the gap to the next prime p_{n+2} are always greater than 2. Hence, in a twin prime pair (p_n, p_{n+1}) where $p_n > 5$, p_n is always a strong prime and p_{n+1} is always a weak prime (see § 2.1.79 and § 2.1.89).
10. All lower members of twin prime pairs are necessarily Chen primes (see § 2.1.6), but only some upper members of twin prime pairs are Chen primes. Also see § 4.7.3.
11. It is unknown if there are infinitely many twin primes or not (and this is called the twin prime problem). According to the twin prime conjecture (which is supported by partial evidence), there are infinitely many twin primes (see Point 1 of § 6.1.34 and Point 16 of § 8.5).[297]

2.1.85 Unique Primes

A unique prime is a prime number (other than 2 and 5 in base 10; see Point 26 of § 1.4) whose reciprocal has a period length that is not shared by any other prime. For example, 3, 11, 37 are unique primes because $1/3, 1/11, 1/37$ $(= 0.\overline{3}, 0.\overline{09}, 0.\overline{027})$ have a period length of 1, 2, 3 (respectively) that is not shared by any other prime number. On the other hand, 7 and 13 are not unique primes because both have a reciprocal period length of 6 ($7 = 0.\overline{142857}$ and $13 = 0.\overline{076923}$). We note:

1. Being unique is base-dependent (where 10 is the conventional base).
2. The first 8 decimal unique primes (i.e. those $< 10^7$) are: 3, 11, 37, 101, 9091, 9901, 333667, 909091 (corresponding to period lengths of 1, 2, 3, 4, 10, 12, 9, 14).[298]
3. Currently (March 2026), there are only about 50 known unique primes (according to some sources).[299]
4. The largest known *generalized unique prime* is apparently $516693^{2097152} - 516693^{1048576} + 1$ (which is

for being twin primes).

[295] See `https://oeis.org/A001359`.

[296] See `https://t5k.org/largest.html`.

[297] According to Brun's theorem (see § 5.1.5), the sum of the reciprocals of twin primes converges to a finite value (known as Brun's constant). Although this does not imply that the set of twin primes is finite, it shows that twin primes are significantly sparser than primes in general.

[298] See `https://oeis.org/A040017` and `https://oeis.org/A051627`. The decimal reciprocals of these 8 unique primes are (respectively): $0.\overline{3}, 0.\overline{09}, 0.\overline{027}, 0.\overline{0099}, 0.\overline{0001099989}, 0.\overline{000100999899}, 0.\overline{000002997}, 0.\overline{00000109999989}$.

[299] Unique primes are exceptionally rare (where according to some sources, there are only 18 decimal unique primes below 10^{50} despite there being more than 10^{47} primes below 10^{50}; see for instance `https://t5k.org/glossary/page.php?sort=UniquePrime`). The aforementioned "50 known unique primes" seem to include some probable decimal unique primes and some *generalized unique primes* (where "generalized" extends the concept to other bases; see for instance `https://oeis.org/A217611`). So, the readers should check all these details.

currently the ninth largest known prime and consists of about 12 million decimal digits).[300]

5. Every decimal repunit prime (see § 2.1.69) is a unique prime in base 10, and hence repunit primes are a proper subset of unique primes.
6. It is conjectured that there are infinitely many unique primes in base 10. This conjecture appears to be based largely on broader conjectural and heuristic considerations concerning the occurrence of primes in certain sequences rather than on considerations specific to unique primes (see for instance Point 5). Moreover, there seems to be a more general conjecture predicting the infinitude of unique primes in every base.

2.1.86 Untouchable Primes

These are prime numbers that are untouchable numbers (see the upcoming Note). We note:

1. There are only two known untouchable primes: 2 and 5 (i.e. one even and one odd).
2. It is widely believed (and conjectured) that there are no untouchable primes other than 2 and 5.

Note: An *untouchable number* (which may also be called *nonaliquot number*) is a natural number that cannot be expressed as the sum of the proper divisors of any positive integer. We note:

A. The first 10 untouchable numbers (i.e. those < 200) are: 2, 5, 52, 88, 96, 120, 124, 146, 162, 188.[301]
B. All known untouchable numbers are even except 5. In fact, it is widely believed (and conjectured) that 5 is the only odd untouchable number.
C. There are some links between untouchable numbers and Goldbach's conjecture (see § 6.1.19). There are also some links between untouchable numbers and perfect numbers (see Note 2 in 2.1.41). These links are worthy of investigation by those who are interested in any one of these subjects. Also see § 9.11.
D. There are infinitely many untouchable numbers.

2.1.87 Wagstaff Primes

A Wagstaff prime W_p is a prime number of the form $W_p = (2^p + 1)/3$ where p is an odd prime. For example, 3 and 11 are Wagstaff primes because $3 = (2^3 + 1)/3$ and $11 = (2^5 + 1)/3$. We note:

1. The first 9 Wagstaff primes (i.e. those $< 10^{12}$) are: 3, 11, 43, 683, 2731, 43691, 174763, 2796203, 715827883 (corresponding to $p = 3$, 5, 7, 11, 13, 17, 19, 23, 31).[302]
2. Seemingly, only 36 proven Wagstaff primes are currently known, i.e. those corresponding to the first 36 entries in the OEIS sequence A000978. A few more probable Wagstaff primes are also known.
3. The largest known proven Wagstaff prime is apparently $(2^{141079} + 1)/3$ (with about 42.5 thousand decimal digits).[303]
4. Wagstaff primes are related to Mersenne numbers (see Note 1 in § 2.1.41), as can be seen by rearranging (with some basic manipulation) the definition $W_p = (2^p + 1)/3$ to obtain $3W_p - 2 = 2^p - 1$, i.e. $3W_p - 2 = M_p$ where M_p is a Mersenne number. We also note that Wagstaff primes are referred to within the new Mersenne conjecture (see § 6.1.24).
5. Wagstaff primes are cyclotomic and hence Wagstaff primes are a proper subset of cyclotomic primes (see § 2.1.14), that is: $W_p = (2^p + 1)/3 = \Phi_{2p}(2)$ where p is an odd prime and W_p is a Wagstaff prime (associated with p).
6. Every Wagstaff prime is a Jacobsthal prime (see § 2.1.36) and vice versa (excluding $J_4 = 5$ which is a Jacobsthal prime but not a Wagstaff prime).

[300] See `https://t5k.org/top20/page.php?id=3`.
[301] See `https://oeis.org/A005114`.
[302] See `https://oeis.org/A000979` and `https://oeis.org/A000978`.
[303] See `https://t5k.org/top20/page.php?id=67`. The largest known probable Wagstaff prime is seemingly $(2^{15135397}+1)/3$ (with about 4.6 million decimal digits).

7. All Wagstaff primes are of the form $4k-1$ for some $k \in \mathbb{N}$ (or equivalently $4k+3$ for some $k \in \mathbb{N}_0$), i.e. the Wagstaff primes are a proper subset of the non-Pythagorean primes (see § 2.1.66).
8. It is conjectured that there are infinitely many Wagstaff primes. This conjecture is consistent with broader heuristics in number theory concerning the distribution of prime numbers, although it remains unproved. It is also related to the conjectured infinitude of Jacobsthal primes.

2.1.88 Wall-Sun-Sun Primes

These may also be called *Fibonacci-Wieferich primes* and are related to the Fibonacci numbers modulo p^2 (see the Note in 2.1.21). More specifically, a Wall-Sun-Sun prime is a prime number p such that p^2 divides the Fibonacci number $\mathcal{F}_{p-\left(\frac{p}{5}\right)}$ where $\left(\frac{p}{5}\right)$ is the Legendre symbol. We note:

1. No Wall-Sun-Sun prime has ever been found despite extensive computational searches to very large bounds (up to 2^{64} according to some sources).
2. It is conjectured that there are infinitely many Wall-Sun-Sun primes (apparently based on heuristic considerations).[304]

2.1.89 Weak Primes

A weak prime (p_n) is a prime number that is less than the average of the primes immediately before and after it, that is:

$$p_n < \frac{p_{n-1} + p_{n+1}}{2} \tag{32}$$

where n is the prime index in the sequence of prime numbers. For example, 3 and 7 are weak primes because $3 < (2+5)/2$ and $7 < (5+11)/2$. We note:

1. The first 12 weak primes (i.e. those < 100) are: 3, 7, 13, 19, 23, 31, 43, 47, 61, 73, 83, 89.[305]
2. In terms of prime gap, the gap preceding a weak prime is smaller than the gap succeeding it, i.e. $(p_n - p_{n-1}) < (p_{n+1} - p_n)$.[306] Hence, in a twin prime pair (p_{n-1}, p_n) where $p_{n-1} > 5$, p_n is always a weak prime because the gap to the next prime (i.e. $p_{n+1} - p_n$) is greater than 2 (see Point 9 of § 2.1.84).
3. There are infinitely many weak primes.[307]
4. Balanced primes (see § 2.1.1), strong primes (see § 2.1.79), and weak primes partition the set of odd prime numbers.
5. "Weak prime" may be used in cryptography with a different meaning (also see Point 5 of § 2.1.79), and hence the readers should be cautious. We also note that "weak prime" is different from "weakly prime" (see § 2.1.15).
6. The idea of weak primes can be extended to higher orders (similar to the generalization of balanced primes and strong primes; see Point 5 of § 2.1.1 and Point 6 of § 2.1.79).

Also see § 2.1.26.

2.1.90 Wieferich Primes

A Wieferich prime is a prime number p where p^2 divides $(2^{p-1} - 1)$. We note:

---

[304] Such claim can be found on the Internet but this requires further investigation. In fact, there may be contradicting suggestions or conjectures, i.e. there are only finitely many of these hypothetical numbers or they are even nonexistent.

[305] See `https://oeis.org/A051635`. We did not find sufficiently reliable information about the largest known weak prime (noting that "weak prime" is very common and hence it is not a record-setting type or category with sufficient rarity or distinction to be recorded and documented as such).

[306] This condition can be obtained from the above inequality by multiplying it by 2 and rearranging its terms.

[307] The proof(s) of the infinitude of weak primes should be proof(s) for the infinitude of prime numbers (see § 1.6) if such proof(s) do not assume the infinitude of primes.

1. There are only two known Wieferich primes: 1093 and 3511 (despite extensive search up to 2^{64} according to some Internet sources).[308]
2. Wieferich primes are linked to Fermat's little theorem (see § 5.1.15) noting that the given condition for Wieferich prime [i.e. $p^2|(2^{p-1}-1)$] is stronger than the condition of Fermat's little theorem, i.e. $p|(2^{p-1}-1)$.
3. Historically, Wieferich primes have emerged in the context of investigating Fermat's last theorem and remain closely associated with it.
4. Wieferich primes are also linked to Mersenne numbers (see Note 1 in § 2.1.41) although a Mersenne prime cannot be a Wieferich prime.
5. The similarity between Wieferich prime and Mirimanoff prime is obvious (see § 2.1.46).
6. The concept of "Wieferich prime" may be generalized to bases other than 2 (and hence it becomes base-dependent in this sense). For instance, a base-3 Wieferich prime is a prime number p such that $p^2|(3^{p-1}-1)$, and hence Mirimanoff primes become base-3 generalized Wieferich primes.
7. It is unknown if there are infinitely many Wieferich primes (noting that the infinitude of Wieferich primes is conjectured based seemingly on heuristic models).[309] The infinitude of non-Wieferich primes is also conjectured.
8. Whether there exists a prime that is simultaneously a Wieferich prime and a Mirimanoff prime is a long standing open problem in number theory. Heuristic considerations seem to suggest such primes may exist, but apparently there is no commonly recognized conjecture asserting their existence.[310]

2.1.91 Wilson Primes

A Wilson prime is a prime number p where p^2 divides $(p-1)!+1$. We note:
1. These primes are obviously linked to Wilson's theorem (see § 5.1.43) and this should explain their name.[311]
2. There are only three known Wilson primes: 5, 13 and 563 (despite the search up to 2×10^{13} according to some Internet sources).[312]
3. It is unknown if there are infinitely many Wilson primes (noting that the infinitude of Wilson primes is conjectured).
4. The concept of "Wilson prime" may be generalized to higher orders, where a generalized Wilson prime of order n ($n\in\mathbb{N}$) is defined as a prime p ($p\geq n$) where p^2 divides $(n-1)!(p-n)!-(-1)^n$. Under this definition, the classical Wilson primes correspond to the case $n=1$.[313]

2.1.92 Wolstenholme Primes

A Wolstenholme prime is a prime number p that satisfies the following congruence relation:

$$C_{p-1}^{2p-1}\equiv 1 \pmod{p^4} \tag{33}$$

[308] See `https://oeis.org/A001220`.

[309] Apparently, the conjectured infinitude extends to all bases >1 (i.e. not only base 2).

[310] According to some internet sources, it is unknown if a prime can satisfy both the (base-2) Wieferich and (base-3) Mirimanoff conditions simultaneously, but this possibility is conjectured by some mathematicians. However, the reliability of this information should be investigated.

[311] Note that the given condition in the definition of Wilson primes [i.e. p^2 divides $(p-1)!+1$] is stronger than the condition in Wilson's theorem [i.e. p divides $(p-1)!+1$] and hence Wilson primes represent a proper subset of prime numbers (see the next points).

[312] `https://oeis.org/A007540`.

[313] See `https://oeis.org/A128666` and `https://oeis.org/A152413`. We note that the concept of "Wilson prime" may also be generalized to higher orders but in a different sense, where the n^{th} order ($n\in\mathbb{N}$) Wilson prime is defined as a prime p such that p^n divides $(p-1)!+1$. Under this definition, prime numbers correspond to the case $n=1$, while the classical Wilson primes correspond to the case $n=2$.

where C_m^n is the binomial coefficient. We note:
1. There are different (but largely equivalent) definitions of Wolstenholme primes. Conditions (such as $p > 3$ or $p > 7$) may also be imposed.
2. There are currently only two known Wolstenholme primes: 16843 and 2124679 (despite massive search up to 10^{11} according to some sources).[314]
3. Wolstenholme primes are related to the Bernoulli numbers, irregular primes, and Fermat's last theorem. In fact, Wolstenholme primes are a proper subset of irregular primes (see § 2.1.32).
4. The infinitude of Wolstenholme primes is an open problem where it is conjectured that there are infinitely many Wolstenholme primes. But there is seemingly an opposite conjecture, i.e. there are only finitely many Wolstenholme primes. Some mathematicians even seem to conjecture that the only Wolstenholme primes are the two currently known ones.

2.1.93 Woodall Primes

A Woodall prime is a Woodall number that is prime (see the upcoming Note). We note:
1. The first 4 Woodall primes (i.e. those $< 10^{24}$) are: 7, 23, 383, 32212254719 (corresponding to $n = 2$, 3, 6, 30).[315]
2. Seemingly, only 34 Woodall primes are currently known.[316]
3. The largest known Woodall prime is apparently the Woodall number with $n = 17016602$ (with about 5.12 million decimal digits).[317]
4. The index n of a Woodall prime cannot be congruent to 4 or 5 (modulo 6). This can be useful in searching for Woodall primes (see Point 27 of § 7.2).
5. There is no known n for which both $2^n n - 1$ and $2^n n + 1$ are prime, i.e. there is no known "Woodall-Cullen twin prime pair" (see § 2.1.12). In fact, it is currently unknown whether such a twin prime pair exists.
6. It is conjectured that there are infinitely many Woodall primes.

Also see § 2.1.12 and § 2.1.71.

Note: The *Woodall numbers* are natural numbers of the form $2^n n - 1$ where $n \in \mathbb{N}$. The first 7 Woodall numbers (i.e. those < 2000) are: 1, 7, 23, 63, 159, 383, 895.[318]

2.2 Tentative Types of Prime Numbers

Some types of prime numbers are rarely mentioned in the literature, or the terms referring to them are rarely used to denote conventional classes of prime numbers (e.g. Lucas-Wieferich primes). Hence, we did not include them in the previous section because they have received little attention, whether due to their rarity, lack of interest among mathematicians, or because they are too novel and have yet to become established as worthy of investigation. In fact, even the definitions of some of these types are not sufficiently clear and may vary across authors and sources.[319]

Overall, we can find in the literature many terms and labels which may suggest certain types of prime numbers but they do not actually represent standard and commonly recognized types or categories of

[314] See `https://oeis.org/A088164`.
[315] See `https://oeis.org/A050918` and `https://oeis.org/A002234`.
[316] See `https://oeis.org/A002234`.
[317] See `https://oeis.org/A002234` and `https://www.primegrid.com/primes/primes.php?project=WOO`.
[318] See `https://oeis.org/A003261`.
[319] Actually, some of these factors also exist in some of the types of the previous section, but the types of the present section represent a rather extreme case in these factors. We should also note that the list of prime types of the previous section does not necessarily include all the common and standard types of primes and hence this list is likely to be updated and extended in the future volumes.

prime numbers. For example, some of these terms may represent a combination of two distinct types of prime (e.g. because some prime numbers can fit into more than one type or category).[320] Also, some authors may improvise some terms (deliberately or mistakenly or laxly) which are not standard terminology and hence they do not represent conventional prime types.

Anyway, in the following subsections we list some examples of these types (listed alphabetically) with a brief investigation or discussion (noting that we advise the readers to be cautious about the provided information).

2.2.1 Chebyshev Primes

The definition of "Chebyshev primes" (which can be found in some research papers) is not clear, although it seems related to Chebyshev's (prime number) theorem (see § 5.1.7), Chebyshev's prime-counting functions (see § 8.2.5) and Chebyshev's bias (see § 8.7.1) and possibly Chebyshev's polynomials, rather than being a commonly recognized conventional type of prime numbers. Anyway, Chebyshev primes may be defined as an infinite set of prime numbers appearing in inequalities for Chebyshev's prime-counting functions. It may also be defined as an infinite set of prime numbers identified in the study of efficient prime-counting functions.[321]

According to some of these definitions, the first 11 Chebyshev primes (i.e. those < 300) are: 109, 113, 139, 181, 197, 199, 241, 271, 281, 283, 293.[322] There are a number of uncertainties about the finitude/infinitude of this type of primes (e.g. originating from conceptual uncertainty with regard to the meaning of "Chebyshev primes", as well as opinion-based uncertainty with regard to the source) even though the infinitude seems to be part of some of the aforementioned definitions (as indicated). Anyway, we refer the readers to the relevant literature about these issues.

2.2.2 Lucas-Wieferich Primes

These may be defined as Lucas primes satisfying the *generalized* Wieferich condition (see § 2.1.39 and § 2.1.90). If so, then 11 (which is a Lucas prime and a base-3 Wieferich prime) may be an example of Lucas-Wieferich primes. However, caution is required when dealing with this issue (as well as any other issue related to "Lucas-Wieferich primes") since there are seemingly more elaborate (and possibly different) definitions and conventions about this type of primes (as well as other sources of confusion and uncertainty).[323]

2.2.3 Weak Irregular Primes

Apparently, there is no standard and universally-accepted definition of this type of prime numbers. According to some sources, a prime number is weak irregular *iff* it is a Bernoulli irregular prime or an Euler irregular prime (refer to § 2.1.32 and § 2.1.33).[324] However, "weak irregular primes" may be extended to the Genocchi irregular primes (see § 2.1.34) and possibly to other types of "weak irregular primes".

---

[320] For example, 16843 is an irregular and Wolstenholme prime (see § 2.1.32 and § 2.1.92) and hence it may be called an irregular-Wolstenholme prime. Similarly, 11 is a safe and Sophie Germain prime and hence it may be called safe Sophie Germain prime (or Sophie Germain safe prime; see Point 6 of § 2.1.76).

[321] As indicated, this term may also be used loosely in the context of Chebyshev's theorem and Chebyshev's bias which describe the distribution and density of prime numbers (see § 5.1.7 and § 8.7.1)

[322] See `https://oeis.org/A196667`.

[323] See for example `https://t5k.org/curios/page.php/103.html`.

[324] See `https://oeis.org/A250216`.

2.3 Emerging Types of Prime Numbers

This section explores prime types that are mostly indicated in the existing literature (primarily through sequences cataloged in the OEIS database) but have not yet been widely recognized as conventional prime types or systematically investigated under standardized terminology. Consequently, these types warrant further study, including the development of consistent definitions and nomenclature. In the following subsections, we present a selection of such prime types, providing a foundational framework and proposing formal nomenclature to enhance their recognizability and facilitate further discussion. Furthermore, we elaborate on some of these types by introducing novel variations, sub-types, and related mathematical nuances and structures. However, before that we draw the reader's attention to the following remarks:

1. Some (or most) of these types may not be of any utility within the current framework of prime number theory (and number theory in general), and this may explain why they are not recognized as standard prime types. However, this does not rule out their potential utility in novel research areas (and even in ongoing research areas) and hence they deserve some attention.
2. Some of these types are actually classes of types rather than single types, and we propose them as extensions and generalizations of ordinary prime types (whether conventional or not).
3. Some of these prime types are trivial. However, even the commonly-recognized standard types of prime numbers include such trivial cases (especially in the field of recreational mathematics).

2.3.1 Bad Primes

We may define a bad prime as a prime number that is not a good prime (see § 2.1.26). For example, 2, 13, and 31 are bad primes. We note:

1. The first 30 bad primes (i.e. those < 200) are: 2, 3, 7, 13, 19, 23, 31, 43, 47, 61, 73, 79, 83, 89, 103, 107, 109, 113, 131, 137, 139, 151, 157, 163, 167, 173, 181, 193, 197, 199.[325]
2. A bad prime may also be defined as a prime number p_n that satisfies the condition $p_n^2 < p_{n-1}p_{n+1}$. This definition includes fewer primes, i.e. the bad primes of the previous definition are a proper superset of those of this definition. According to this definition, the first 23 bad primes (i.e. those < 200) are: 2, 3, 7, 13, 19, 23, 31, 43, 47, 61, 73, 83, 89, 103, 109, 113, 131, 139, 151, 167, 181, 193, 199.[326]
3. Apparently, there are infinitely many bad primes (considering each definition).
4. Bad and good primes (of corresponding definitions) partition the entire set of prime numbers (comprehensively and disjointly).

2.3.2 Complete Primes

We may define a complete prime as a prime number which all the sub-sequences of its digits are prime. We note:

1. Being complete prime is base-dependent (where we use base 10 in this discussion).
2. Complete primes can contain only the digits 2, 3, 5 and 7 (in base 10) and hence complete primes are a proper subset of D2357 primes (see § 2.3.5).
3. We may define several variations or sub-types of the complete primes type according to the conditions of *digits-order* and *digits-proximity*. The details are as follows:
   • Sub-type 1: complete prime with both conditions, i.e. the sub-sequences of its digits are restricted to those that keep digits-order and digits-proximity. For example, 373 is a complete prime of sub-type 1 because all the sub-sequences of its digits with these conditions (which are 3, 7, 37, 73, and 373) are prime, but if we drop the condition of digits-proximity then the sub-sequence 33 (which violates the condition of digits-proximity because the two 3's are not proximate) is not prime and hence 373 will

[325] See `https://oeis.org/A130903`.
[326] See `https://oeis.org/A068828` noting that 2 is included by convention.

not be qualified as a complete prime of a type that disregards this condition. It can be shown that no such primes exist beyond 373 in base 10. Hence, there are only 9 complete primes of sub-type 1 (in base 10), namely: 2, 3, 5, 7, 23, 37, 53, 73, 373.[327] Even though repetition of digits is allowed in this sub-type, the repeated digits must be separated.

• Sub-type 2: complete prime with none of these conditions. The primes of this sub-type cannot have more than 4 digits (because repetition of digits is not allowed as sub-sequences of repeated digits are composite), and hence must be less than 10^4 (and actually lower). So, if we inspect the D2357 primes which are $< 10^4$ we find that there are only 6 primes of this sub-type, namely: 2, 3, 5, 7, 37, 73. It is obvious that this sub-type is a proper subset of sub-type 1.[328]

• We may also define two other sub-types, i.e. one with only digits-order condition, and one with only digits-proximity condition. However, we leave this to the readers to work out the details (which are mostly trivial).[329]

4. Broadly speaking, complete primes (at least in some of their sub-types and variations) look like the opposite to minimal primes (see § 2.1.45). Hence, we may label complete primes as *maximal primes*.
5. As indicated already, there are only finitely many complete primes (at least in base 10 and some other bases, including none in base 2, noting that the possibility of their infinitude in some bases and/or some sub-types/variations requires further investigation even though their finitude in every base and sub-type/variation seems plausible).[330]

2.3.3 Composite-Indexed Primes

We may define a composite-indexed prime as a prime number whose index (in the prime number sequence) is composite. We note:

1. The first 15 composite-indexed primes (i.e. those < 100) are: 7, 13, 19, 23, 29, 37, 43, 47, 53, 61, 71, 73, 79, 89, 97.
2. Odd primes are partitioned (comprehensively and mutually exclusively) as prime-indexed (i.e. super primes; see § 2.1.62) and composite-indexed. To complete the partitioning of prime numbers (by including 2), we may define nonprime-indexed primes (i.e. primes whose index is not prime).[331]
3. The density of composite-indexed primes (relative to the density of prime-indexed primes) generally increases as we move higher on the number line (and hence prime numbers are overwhelmingly composite-indexed).[332]
4. There are infinitely many composite-indexed primes (since there are infinitely many composite numbers among the positive integers n, and p_n is prime for every n).

2.3.4 D014689 Primes

We may define a D014689 prime as a prime number whose digits are exclusively non-prime, i.e. 0, 1, 4, 6, 8, 9 in base 10 (noting that the name D014689 refers to these digits). For example, 11, 19 and 101 are D014689 primes. We note:

1. Being D014689 is base-dependent (where we use base 10 in this discussion including the naming, i.e. D014689).[333]

[327] See `https://oeis.org/A085823`.
[328] This makes inspecting 2, 3, 5, 7, 23, 37, 53, 73, 373 more reasonable than inspecting D2357 primes which are $< 10^4$.
[329] See for instance `https://oeis.org/A202263`.
[330] See `https://oeis.org/A309572`.
[331] See `https://oeis.org/A007821`.
[332] In fact, the proportion of composite-indexed primes among all primes tends to 1 as the numbers increase without bound, whereas the proportion of prime-indexed primes tends to 0. Thus, in the asymptotic sense, almost all primes are composite-indexed.
[333] For the name to be base-independent, we may label these primes as *nonprime-digit primes*.

2. The first 18 D014689 primes (i.e. those < 500 in base 10) are: 11, 19, 41, 61, 89, 101, 109, 149, 181, 191, 199, 401, 409, 419, 449, 461, 491, 499.[334]
3. It may be conjectured that there are infinitely many D014689 primes. More generally, one may conjecture that there are infinitely many nonprime-digit primes in each base $b > 2$.[335]

2.3.5 D2357 Primes

We may define a D2357 prime as a prime number whose digits are all prime, i.e. 2, 3, 5, 7 in base 10 (noting that the name D2357 refers to these digits). For example, 5, 23 and 37 are D2357 primes. We note:

1. Being D2357 is base-dependent (where we use base 10 in this discussion including the naming, i.e. D2357).[336]
2. The first 16 D2357 primes (i.e. those < 500 in base 10) are: 2, 3, 5, 7, 23, 37, 53, 73, 223, 227, 233, 257, 277, 337, 353, 373.[337]
3. It may be conjectured that there are infinitely many D2357 primes. More generally, one may conjecture that there are infinitely many prime-digit primes in each base $b \geq 3$.

2.3.6 D4689 Primes

We may define a D4689 prime as a prime number whose digits are exclusively composite (i.e. 4, 6, 8, 9). For example, 89, 449 and 4649 are D4689 primes. We note:

1. Being D4689 is base-dependent (where we use base 10 in this discussion including the naming, i.e. D4689).[338]
2. The first 22 D4689 primes (i.e. those $< 10^4$ in base 10) are: 89, 449, 499, 4649, 4889, 4969, 4999, 6449, 6469, 6689, 6869, 6899, 6949, 8669, 8689, 8699, 8849, 8969, 8999, 9649, 9689, 9949.[339]
3. It may be conjectured that there are infinitely many D4689 primes. More generally, one may conjecture that there are infinitely many composite-digit primes in each base $b \geq 5$.
4. D4689 primes are a sub-type (and hence a proper subset) of D014689 primes (see § 2.3.4). This extends to their generalizations to other bases.

2.3.7 Digit-Increasing and Digit-Decreasing Primes

We may define a digit-increasing prime as a multi-digit prime number whose digits are strictly increasing from left to right. For example, 13, 17, and 23 are digit-increasing primes. We may define a digit-decreasing prime as a multi-digit prime number whose digits are strictly decreasing from left to right. For example, 31, 41, and 43 are digit-decreasing primes. We note:

1. Being digit-increasing and digit-decreasing is base-dependent (where we use base 10 in this discussion).
2. The first 11 digit-increasing primes (i.e. those < 100 in base 10) are: 13, 17, 19, 23, 29, 37, 47, 59, 67, 79, 89.[340]
3. The first 9 digit-decreasing primes (i.e. those < 100 in base 10) are: 31, 41, 43, 53, 61, 71, 73, 83, 97.[341]

---

[334] See `https://oeis.org/A034844`.
[335] In base 2, this is established (rather than conjectured) since both binary digits (0 and 1) are nonprime, and hence every prime is a nonprime-digit prime in base 2.
[336] For the name to be base-independent, we may label these primes as *prime-digit primes*.
[337] See `https://oeis.org/A019546`.
[338] For the name to be base-independent, we may label these primes as *composite-digit primes*.
[339] See `https://oeis.org/A051416`.
[340] See `https://oeis.org/A052015`.
[341] See `https://oeis.org/A052014`.

4. Unlike some base-dependent prime types, there cannot be infinitely many digit-increasing or digit-decreasing primes in any fixed base. In fact, assuming the usual positional representation without leading zeros, a strictly increasing sequence of digits in base b can contain at most $b-1$ digits, while a strictly decreasing sequence can contain at most b digits. Consequently, there are only finitely many digit-increasing and digit-decreasing integers, and hence only finitely many corresponding primes, in every fixed base. A natural question is therefore to determine the number and distribution of such primes in a given base, or to study how these quantities behave as the base varies.

Note: Several other prime types (related to the digit-increasing and digit-decreasing prime types) can also be defined; for example:
• A *digit-nondecreasing prime* may be defined as a multi-digit prime number whose digits are non-decreasing from left to right. This type is a proper superset of the set of digit-increasing primes. We note that repunit primes are a proper subset of this type. It may be conjectured that there are infinitely many digit-nondecreasing primes in any base.
• A *digit-nonincreasing prime* may be defined as a multi-digit prime number whose digits are non-increasing from left to right. This type is a proper superset of the set of digit-decreasing primes. Again, repunit primes are a proper subset of this type. It may be conjectured that there are infinitely many digit-nonincreasing primes in any base.
• A *digit-oscillating prime* may be defined as a multi-digit prime number whose digits are neither non-decreasing nor nonincreasing (i.e. its digit sequence contains at least one up-down or down-up cycle). It may be conjectured that there are infinitely many digit-oscillating primes in any base.[342]

We note that every multi-digit prime number belongs to at least one of these three prime types.[343]

2.3.8 Index-Added Primes I

We may define an index-added prime of the first kind (denoted as an index-added prime I) as a prime number p_n such that $p_n + n$ is also prime (where p_n is the n^{th} prime in the sequence of prime numbers). For example, 2, 3, and 7 are index-added primes I because 3, 5, and 11 are also primes. We note:
1. The first 17 index-added primes I (i.e. those < 500) are: 2, 3, 7, 13, 61, 79, 89, 101, 131, 139, 181, 223, 317, 349, 359, 421, 479 (corresponding to $n = 1$, 2, 4, 6, 18, 22, 24, 26, 32, 34, 42, 48, 66, 70, 72, 82, 92).[344]
2. It may be conjectured that there are infinitely many index-added primes I.

2.3.9 Index-Added Primes II

We may define an index-added prime of the second kind (denoted as an index-added prime II) as a prime number of the form $p_n + n$ (where p_n is the n^{th} prime in the sequence of prime numbers). For example, 3, 5, and 11 are index-added primes II. We note:
1. The first 15 index-added primes II (i.e. those < 500) are: 3, 5, 11, 19, 79, 101, 113, 127, 163, 173, 223, 271, 383, 419, 431 (corresponding to $n = 1$, 2, 4, 6, 18, 22, 24, 26, 32, 34, 42, 48, 66, 70, 72).[345]
2. It may be conjectured that there are infinitely many index-added primes II.
3. There is a one-to-one correspondence between index-added primes I and index-added primes II. Accordingly, the primes of these two types can be paired as $(p_n, p_n + n)$.

---

[342] In fact, this type can be split to several other sub-types (i.e. up-down and/or down-up with various number of cycles) where each one of these can be treated as a stand-alone type.
[343] In fact, only repunit primes are common among these types (i.e. common to the digit-nondecreasing primes and digit-nonincreasing primes); otherwise the three types are disjoint.
[344] See `https://oeis.org/A061067` and `https://oeis.org/A064402`. For all $n > 1$, n is even.
[345] See `https://oeis.org/A061068` and `https://oeis.org/A064402`. For all $n > 1$, n is even.

2.3.10 Index-Subtracted Primes I

We may define an index-subtracted prime of the first kind (denoted as an index-subtracted prime I) as a prime number p_n such that $p_n - n$ is also prime (where p_n is the n^{th} prime in the sequence of prime numbers). For example, 5, 7, and 13 are index-subtracted primes I because 2, 3, and 7 are also primes. We note:

1. The first 20 index-subtracted primes I (i.e. those < 500) are: 5, 7, 13, 19, 29, 43, 53, 61, 107, 113, 181, 193, 229, 251, 317, 337, 383, 433, 463, 491 (corresponding to $n = 3$, 4, 6, 8, 10, 14, 16, 18, 28, 30, 42, 44, 50, 54, 66, 68, 76, 84, 90, 94).[346]
2. It may be conjectured that there are infinitely many index-subtracted primes I.

2.3.11 Index-Subtracted Primes II

We may define an index-subtracted prime of the second kind (denoted as an index-subtracted prime II) as a prime number of the form $p_n - n$ (where p_n is the n^{th} prime in the sequence of prime numbers). For example, 2, 3, and 7 are index-subtracted primes II. We note:

1. The first 21 index-subtracted primes II (i.e. those < 500) are: 2, 3, 7, 11, 19, 29, 37, 43, 79, 83, 139, 149, 179, 197, 251, 269, 307, 349, 373, 397, 491 (corresponding to $n = 3$, 4, 6, 8, 10, 14, 16, 18, 28, 30, 42, 44, 50, 54, 66, 68, 76, 84, 90, 94, 110).[347]
2. It may be conjectured that there are infinitely many index-subtracted primes II.
3. There is a one-to-one correspondence between index-subtracted primes I and index-subtracted primes II. Accordingly, the primes of these two types can be paired as $(p_n, p_n - n)$.

2.3.12 Jump Primes

We may define a jump prime as a prime number p_n whose gap from its immediate predecessor p_{n-1} is greater than any previous gap in the sequence of prime numbers, i.e.

$$(p_n - p_{n-1}) > (p_k - p_{k-1}) \tag{34}$$

for all $1 < k < n$. We note:

1. The first 11 jump primes (i.e. those $< 10^4$) are: 3, 5, 11, 29, 97, 127, 541, 907, 1151, 1361, 9587.[348]
2. There are infinitely many jump primes.[349]

2.3.13 Mixed-Digit Primes

We may define a mixed-digit prime as a multi-digit prime number whose digits are a mix of primes (i.e. 2, 3, 5, 7 in base 10) and non-primes (i.e. 0, 1, 4, 6, 8, 9 in base 10). We note:

1. Being mixed-digit is base-dependent (where we use base 10 in this discussion).
2. The first 27 mixed-digit primes (i.e. those < 200 in base 10) are: 13, 17, 29, 31, 43, 47, 59, 67, 71, 79, 83, 97, 103, 107, 113, 127, 131, 137, 139, 151, 157, 163, 167, 173, 179, 193, 197.[350]
3. It may be conjectured that there are infinitely many mixed-digit primes (and actually in any base $b \geq 3$).
4. D014689 primes (see § 2.3.4), D2357 primes (see § 2.3.5) and mixed-digit primes (as well as their generalizations to other bases) partition the entire set of prime numbers.

[346] See `https://oeis.org/A227420` and `https://oeis.org/A064269`. For all $n > 3$, n is even.
[347] See `https://oeis.org/A064270` and `https://oeis.org/A064269`. For all $n > 3$, n is even.
[348] See `https://oeis.org/A000101` noting that 3 vacuously satisfies the given condition. Also see `https://oeis.org/A002386`.
[349] This is because there are arbitrarily large gaps between consecutive primes.
[350] See `https://oeis.org/A152426`.

2.3.14 Nesting and Non-Nesting Primes

We may define a nesting prime as a prime number that contains another smaller prime as a *strict* sub-string.[351] For example, 13, 23, 29, 113, and 167 are nesting primes. We may define a non-nesting prime as a prime number that does not contain any smaller prime as a *strict* sub-string. For example, 11, 41, 61, 89, and 101 are non-nesting primes. We note:

1. Being nesting and non-nesting is base-dependent (where we use base 10 in this discussion, although the names are general).
2. The first 33 nesting primes (i.e. those < 200 in base 10) are: 13, 17, 23, 29, 31, 37, 43, 47, 53, 59, 67, 71, 73, 79, 83, 97, 103, 107, 113, 127, 131, 137, 139, 151, 157, 163, 167, 173, 179, 191, 193, 197, 199.[352]
3. The first 13 non-nesting primes (i.e. those < 200 in base 10) are: 2, 3, 5, 7, 11, 19, 41, 61, 89, 101, 109, 149, 181.[353]
4. All multi-digit non-nesting primes are D014689 primes (see § 2.3.4), and hence multi-digit non-nesting primes are a proper subset of D014689 primes (noting, for instance, that 199 is a D014689 nesting prime because it nests 19).
5. All mixed-digit primes (see § 2.3.13) are nesting primes, and hence mixed-digit primes are a proper subset of nesting primes (noting, for instance, that 37 is a nesting, but not a mixed-digit, prime).
6. All multi-digit D2357 primes (see § 2.3.5) are nesting primes, and hence multi-digit D2357 primes are a proper subset of nesting primes (noting that mixed-digit primes are nesting, but not D2357, primes).
7. It may be conjectured that there are infinitely many nesting primes and infinitely many non-nesting primes (in any base $b \geq 2$).
8. Nesting and non-nesting primes partition the entire set of prime numbers (comprehensively and disjointly).

2.3.15 Primes with and without Repeated Digits

Examples of primes with repeated digits are: 11, 101, and 113. Examples of primes without repeated digits are: 13, 17, and 19. We note

1. Being with and without repeated digits is base-dependent (where we use base 10 in this discussion).
2. The first 8 primes with repeated digits (i.e. those < 200 in base 10) are: 11, 101, 113, 131, 151, 181, 191, 199.[354]
3. The first 38 primes without repeated digits (i.e. those < 200 in base 10) are: 2, 3, 5, 7, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 103, 107, 109, 127, 137, 139, 149, 157, 163, 167, 173, 179, 193, 197.[355]
4. In any base, there are infinitely many primes with repeated digits and only finitely many primes without repeated digits. In fact, for each base we have a minimal threshold above which all primes (and actually all integers) are with repeated digits. For instance:
   • In base 2 (i.e. binary system) all prime numbers excluding 2 (and actually all non-negative integers excluding 0, 1, 2) are with repeated digits.
   • In base 3 (i.e. ternary system) all prime numbers excluding 2, 3, 5, 7, 11, 19 (and actually all integers > 21) are with repeated digits.
5. These two types of prime numbers partition the entire set of primes.

[351] "Sub-string" (in a strict sense) is necessary because otherwise every prime number will be nesting.
[352] See `https://oeis.org/A179924`.
[353] See `https://oeis.org/A033274`.
[354] See `https://oeis.org/A073064`. Also see `https://oeis.org/A098227`.
[355] See `https://oeis.org/A029743`. Also see `https://oeis.org/A073532`.

2.3.16 Prime-Sum Primes

We may define a prime-sum prime p_{S_n} as a prime number that is the sum of the first n prime numbers, that is:

$$p_{S_n} = \sum_{k=1}^{n} p_k \tag{35}$$

where p_{S_n} is a prime number. For example, the integers 2 and 5 are prime-sum primes corresponding to $n = 1$ and 2. We note

1. The first 8 prime-sum primes (i.e. those $< 10^4$) are: 2, 5, 17, 41, 197, 281, 7699, 8893 (corresponding to $n = 1$, 2, 4, 6, 12, 14, 60, 64).[356]
2. It may be conjectured that there are infinitely many prime-sum primes.

2.3.17 Product-Digit Primes

We may define a product-digit prime as a prime number for which the product of its digits is also prime. For example, 2 and 13 are product-digit primes. We note

1. Being product-digit prime is base-dependent (where we use base 10 in this discussion).
2. The first 13 product-digit primes (i.e. those < 1000 in base 10) are: 2, 3, 5, 7, 13, 17, 31, 71, 113, 131, 151, 211, 311.[357]
3. The only product-digit primes are the single-digit primes (i.e. 2, 3, 5, 7 in base 10) and the primes which have a single prime digit (i.e. 2, 3, 5, 7) with the rest of their digits being 1, e.g. 13, 17, 211, 1117, 1151.
4. In base 2 (i.e. binary system) there is no product-digit prime (because the product of the digits in this base is either 0 or 1). In other bases, it may be conjectured that there are infinitely many product-digit primes.

2.3.18 Residue Primes

We may define an m-residue prime (modulo n) as a prime number p such that $p \overset{n}{=} m$ where $m, n \in \mathbb{N}$ and $n > 1$. For example:

- 2, 7, 17, 37, 47, 67 are 2-residue primes (modulo 5).[358]
- 3, 11, 19, 43, 59, 67 are 3-residue primes (modulo 8).[359]
- 7, 17, 37, 47, 67, 97 are 7-residue primes (modulo 10).[360]
- 5, 31, 83, 109, 239, 317 are 5-residue primes (modulo 13).[361]

We note:

1. "Residue Primes" denotes a class of prime types (rather than a single type of primes). Each member of this class is associated with a particular pair of m and n.
2. There are infinitely many m-residue primes (modulo n) for every pair of coprime m, n satisfying $1 \leq m < n$ (according to Dirichlet's theorem; see § 5.1.11).

[356] See `https://oeis.org/A013918` and `https://oeis.org/A013916`.
[357] See `https://oeis.org/A046703`.
[358] See `https://oeis.org/A045380`.
[359] See `https://oeis.org/A007520`.
[360] See `https://oeis.org/A030432`.
[361] See `https://oeis.org/A102732`.

2.3.19 Sum-Minus Primes

We may define a sum-minus prime p_{N-} as a prime number that is the sum of the first N positive integers minus 1, i.e.

$$p_{N-} = \left(\sum_{k=1}^{N} k\right) - 1 \tag{36}$$

There are only two sum-minus primes, namely: 2 and 5 (corresponding to $N = 2$ and 3). This is because the underlying expression can be factored as:

$$p_{N-} = \left(\sum_{k=1}^{N} k\right) - 1 = \frac{N(N+1)}{2} - 1 = \frac{(N-1)(N+2)}{2} \tag{37}$$

i.e. for $N > 3$, p_{N-} is composite.[362]

2.3.20 Sum-Plus Primes

We may define a sum-plus prime p_{N+} as a prime number that is the sum of the first N positive integers plus 1, i.e.

$$p_{N+} = \left(\sum_{k=1}^{N} k\right) + 1 \tag{38}$$

We note:

1. The first 9 sum-plus primes (i.e. those < 200) are: 2, 7, 11, 29, 37, 67, 79, 137, 191 (corresponding to $N = 1$, 3, 4, 7, 8, 11, 12, 16, 19).[363]
2. It may be conjectured that there are infinitely many sum-plus primes.[364]

2.3.21 Transformed and Image Primes

We may define a transformed prime as a prime number whose image under a specified mathematical transformation is also prime. The resulting prime is called the corresponding image prime. For example:

• The integers 3, 7, 13 are transformed primes (corresponding to image primes 19, 67, 199) under the quadratic transformation $p^2 + 2p + 4$.

• The integers 2, 3 are transformed primes (corresponding to image primes 11, 29) under the exponential transformation $3^p + 2$.

• The integers 2, 3, 5 are transformed primes (corresponding to image primes 3, 7, 31) under the Mersenne transformation $2^p - 1$ (see § 2.1.41 and § 2.1.43).

• The integers 2, 3, 5 are transformed primes (corresponding to image primes 5, 7, 11) under the Sophie Germain transformation $2p + 1$ (see § 2.1.72 and § 2.1.76).

---

[362] When $N > 3$, the integers $(N - 1)$ and $(N + 2)$ are both greater than 2. Since one of these integers must be even, dividing by 2 still leaves a product of two integers that are both strictly greater than 1. Consequently, p_{N-} is composite for all $N > 3$.

[363] See `https://oeis.org/A055469` and `https://oeis.org/A067186`.

[364] Unlike sum-minus primes (see § 2.3.19), the algebraic form of p_{N+} expands as:

$$p_{N+} = \left(\sum_{k=1}^{N} k\right) + 1 = \frac{N(N+1)}{2} + 1 = \frac{N^2 + N + 2}{2} \tag{39}$$

Because the quadratic polynomial $N^2 + N + 2$ is irreducible over the integers, it does not factor into lower-degree polynomials with integer coefficients. Thus, unlike the sum-minus case, there is no corresponding algebraic factorization that forces p_{N+} to be composite for all sufficiently large N.

• The integers 2, 3, 5 are transformed primes (corresponding to image primes 3, 5, 11) under the prime-indexing transformation (see § 2.1.62).[365]
• The integers 3, 5, 7 are transformed primes (corresponding to image primes 3, 11, 43) under the Wagstaff transformation (see § 2.1.87).
• The integers 2, 3, 7 are transformed primes (corresponding to image primes 3, 5, 11) under the index-addition transformation (see § 2.3.8 and § 2.3.9).
• The integers 5, 7, 13 are transformed primes (corresponding to image primes 2, 3, 7) under the index-subtraction transformation (see § 2.3.10 and § 2.3.11).

We note:
1. "Transformed and Image Primes" denotes a class of prime types (rather than a single type of primes). Each member of this class is associated with a particular transformation. In fact, transformed primes and the corresponding image primes of each transformation represent two distinct types.
2. The infinitude of transformed primes and image primes depends on the specific types (which depends on the specific transformation). The infinitude of the transformed primes and image primes in the above examples may be conjectured (excluding the case of prime-indexing transformation where the infinitude of both is proven; see § 1.6 and § 2.1.62).
3. For each specified transformation, if the transformation between transformed primes and image primes is injective, there is a one-to-one correspondence between the transformed primes and their image primes. Accordingly, they may be paired as (p_t, p_i) where p_t and p_i denote the transformed prime and its corresponding image prime respectively. An example of such transformation is the Sophie Germain transformation where p_t represents a Sophie Germain prime and p_i represents a safe prime (see § 2.1.72 and § 2.1.76).

2.3.22 Type-Indexed Primes I

We may define a type-indexed prime of the first kind (denoted as a type-indexed prime I) as a prime number of a certain type whose index in the sequence of prime numbers is also a prime number of that type. Formally, a prime p_n is a type-indexed prime I of type T *iff* $p_n \in T$ and $n \in T$. For instance:
• The integers 5, 11, 17 are cluster-indexed cluster primes I because they are cluster primes whose indices in the sequence of prime numbers are $n = 3, 5, 7$ which are also cluster primes (see § 2.1.8).
• The integers 157, 991, 1217 are emirp-indexed emirp primes I because they are emirp primes whose indices in the sequence of prime numbers are $n = 37, 167, 199$ which are also emirp primes (see § 2.1.17).
• The integers 3, 5, 11 are Higgs-indexed Higgs primes I because they are Higgs primes whose indices in the sequence of prime numbers are $n = 2, 3, 5$ which are also Higgs primes (see § 2.1.29).
• The integers 41, 109, 157 are Pythagorean-indexed Pythagorean primes I because they are Pythagorean primes whose indices in the sequence of prime numbers are $n = 13, 29, 37$ which are also Pythagorean primes (see § 2.1.66).

We note:
1. "Type-Indexed Primes I" denotes a class of prime types (rather than a single type of primes). Each member of this class is associated with a particular underlying prime type T.
2. Being type-indexed prime I can be base-dependent, i.e. when the underlying prime type T is base-dependent (e.g. emirp-indexed emirp primes I are base-dependent).
3. For a given underlying prime type T, the corresponding type-indexed primes I form a subset of T. For example, the emirp-indexed emirp primes I form a subset of the emirp primes.
4. The idea of type-indexed prime I may be extended to higher levels of indexing and hence we get higher orders of such primes.

[365] The transformed primes in this case represent the entire set of prime numbers.

5. The infinitude of type-indexed primes I depends on the specific type (although it may be conjectured for many types). More specifically, the infinitude of type-indexed primes I of type T implies the infinitude of the underlying type T, but the converse is not true in general.
6. Composite-indexed primes (see § 2.3.3) cannot have type-indexed primes I. This may also apply to other types of prime numbers (noting that some types have no known type-indexed primes I even though such primes may exist in principle).

2.3.23 Type-Indexed Primes II

We may define a type-indexed prime of the second kind (denoted as a type-indexed prime II) as a prime number of a certain type T whose index in that type is also a prime number of type T. For instance:
• The integers 2, 5, 233 are Fibonacci-indexed Fibonacci primes II because they are Fibonacci primes whose indices as Fibonacci primes ($\mathcal{F}_n$) are $n = 3$, 5, 13 which are also Fibonacci primes (see § 2.1.21).
• The integers 3, 29, 199 are Lucas-indexed Lucas primes II because they are Lucas primes whose indices as Lucas primes (L_n) are $n = 2$, 7, 11 which are also Lucas primes (see § 2.1.39).
• The integers 7, 127, 2147483647 (and all double Mersenne primes) are Mersenne-indexed Mersenne primes II because they are Mersenne primes whose indices as Mersenne primes (M_p) are $p = 3$, 7, 31 which are also Mersenne primes (see Point 14 of § 2.1.41).

We note:
1. "Type-Indexed Primes II" denotes a class of prime types (rather than a single type of primes). Each member of this class is associated with a particular underlying prime type T.
2. Type-indexed primes II arise primarily from prime types whose elements are prime numbers occurring in an indexed integer sequence. Consequently, each such prime has an index representing its position in the underlying sequence.
3. For a given underlying prime type T, the corresponding type-indexed primes II form a subset of T. For example, the Fibonacci-indexed Fibonacci primes II form a subset of the Fibonacci primes.
4. The idea of type-indexed prime II may be extended to higher levels of indexing and hence we get higher orders of such primes.
5. The infinitude of type-indexed primes II depends on the specific type. For instance, double Mersenne primes are conjectured to be finite (with the 4 known instances potentially being the only ones in existence, even though their infinitude may also be conjectured; see Point 14 of § 2.1.41), while the infinitude of Fibonacci-indexed Fibonacci primes II and Lucas-indexed Lucas primes II may be conjectured. In any case, the infinitude of type-indexed primes II of type T implies the infinitude of the underlying type T, but the converse is not true in general.

2.4 Primes with Infinitely Many Members

This section is about types and categories[366] of prime numbers which are proven to have infinitely many members.[367] However, this issue will be investigated in § 5.2.4 and hence the readers should refer to that subsection.

[366] "Types" refers to the rather conventional sense that we used in the previous sections, while "categories" refers to more loose sense like "kind" or "class" or "sub-type". Anyway, this is a trivial issue.
[367] For those types which are conjectured to have infinitely many members we refer the readers to chapter 6 (see for instance § 6.2.4).

2.5 Primes with Finitely Many Members

In this section we list examples of common types and categories of prime numbers which are proven to have only finitely many members:[368]

1. Catalan primes: there are only 2 Catalan primes, i.e. 2 and 5 (see § 2.1.4).
2. Even primes: there is only one even prime number, i.e. 2.
3. Fermat primes $2^n + 1$ with odd n: there is only one such prime, i.e. 3 (see § 2.1.20).
4. Fibonacci primes with a composite index: there is only one, i.e. $\mathcal{F}_4 = 3$ (see § 2.1.21).
5. Higgs primes of the first order: there are only 4 Higgs primes of the first order, i.e. 2, 3, 7, 43 (see § 2.1.29).
6. Jacobsthal primes with a composite index: there is only one, i.e. $J_4 = 5$ (see § 2.1.36).
7. Minimal primes: there are only 26 minimal primes in base 10 (see § 2.1.45).
8. Palindromic primes of even number of digits (in base 10): there is only 1 such prime, i.e. 11 (see § 2.1.53).
9. Primes with specific number of digits in specific bases, e.g. there is only 4 primes with one digit and only 21 primes with two digits (in base 10).
10. Repunit primes in certain perfect power bases, e.g. there is only 1 repunit prime in base-4 which is 5 (see § 2.1.69).
11. Repunit primes with even number of digits in base 10 (only 11).[369]
12. Supersingular primes (group theory): there are only 15 supersingular primes, i.e. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71 (see § 2.1.80).
13. Truncatable primes in base 10: refer to § 2.1.83 for details.

Also see § 1.5 for examples of forms or kinds of prime numbers that have only finitely many members.

2.6 Primes with Few Known Members

In this section we list common types of primes which have only few or counted known examples.[370] The importance of this (which justifies the creation of this section) is that this is a good indication of their rarity and sparsity (which is important to know in the context of investigations of density and distribution of primes). Moreover, some of these types (with certain favoring indications) may be good candidates for having only finitely many elements (i.e. they can be suspected as being finite sets).

1. Carol primes: seemingly only 44 are known (see § 2.1.3).
2. Cullen primes: only 16 are known (see § 2.1.12).
3. Double Mersenne primes: only 4 are known, i.e. those with $p = 2, 3, 5, 7$ (see Point 14 of § 2.1.41).
4. Factorial primes: only 53 are known (see § 2.1.19).
5. Fermat primes: only 5 are known, i.e. 3, 5, 17, 257, 65537 (see § 2.1.20).
6. Fibonacci primes: only 37 (or 57 including 20 probable) are known (see § 2.1.21).
7. Lucas primes: seemingly only 52 (or 69 including 17 probable) are known (see § 2.1.39).
8. Mersenne primes: only 52 are known (see § 2.1.41).
9. Mirimanoff primes: only 2 are known, i.e. 11 and 1006003 (see § 2.1.46).
10. Non-generous primes: only 3 are known, i.e. 2, 40487, 6692367337 (see § 2.1.50).

[368] This issue will be investigated in § 5.2.5 but in a rather broader and less specific way (noting as well that in the present section we provide some details about the count, and potentially the list, of the finitely many members). For those types which are conjectured to have only finitely many members we refer the readers to chapter 6 (see for instance § 6.2.5).

[369] In fact, this is included in Point 8.

[370] We note that "few" here includes zero. We should also note that we include in this section some types and categories with well-documented counted members although their known members are not few in the literal or usual sense (e.g. 52 or 69). So, "Few" in the title represents "few or counted" (as stated in the text).

11. Non-repunit permutable primes (in base 10): only 21 are known, i.e. 2, 3, 5, 7, 13, 17, 31, 37, 71, 73, 79, 97, 113, 131, 199, 311, 337, 373, 733, 919, 991 (see § 2.1.58).
12. NSW primes: seemingly only 26 are known (see § 2.1.51).
13. Primorial primes: only 52 are known (see § 2.1.64).
14. Repunit primes (in base 10): only 11 are known (possibly including some probable), i.e. those with the following indices: 2, 19, 23, 317, 1031, 49081, 86453, 109297, 270343, 5794777, 8177207 (see § 2.1.69).
15. Permutable primes (in base 10) including repunits: only 32 are known (see Points 11 and 14).
16. Smarandache-Wellin primes: only 8 are known, i.e. those resulting from the concatenation of the first 1, 2, 4, 128, 174, 342, 435, 1429 primes (see § 2.1.75).
17. Stern primes: only 8 are known, i.e. 2, 3, 17, 137, 227, 977, 1187, 1493 (see § 2.1.77).
18. Thabit primes of the first (second) kind: only 69 (50) are known (see § 2.1.81).
19. Unique primes (decimal): only about 50 are known (see § 2.1.85).
20. Untouchable primes: only 2 are known, i.e. 2 and 5 (see § 2.1.86).
21. Wagstaff primes: seemingly only 36 proven (with a few more probable) are known (see § 2.1.87).
22. Wieferich primes: only 2 are known, i.e. 1093 and 3511 (see § 2.1.90).
23. Wilson primes: only 3 are known, i.e. 5, 13 and 563 (see § 2.1.91).
24. Wolstenholme primes: only 2 are known, i.e. 16843 and 2124679 (see § 2.1.92).
25. Woodall primes: seemingly only 34 are known (see § 2.1.93).

2.7 Primes with no Known Members

In the following list we give two examples of types of prime numbers with no known members (even though in theory they can have some members, or it is not proven that they cannot have some members):
1. Generalized Wieferich primes (see § 2.1.90) in some bases (e.g. base 47 and base 72).[371]
2. Wall-Sun-Sun primes (see § 2.1.88).

2.8 Primes with no Members

In the following list we give examples of categories of prime numbers with no members (i.e. they represent empty sets in theory not because they have no known members):
1. Centered k-gonal prime for $k = 8$ and $k = 9$ (see § 2.1.5).
2. Even prime greater than 2.
3. Mersenne prime $2^n - 1$ with composite n (see § 2.1.41).
4. Pandigital prime in base 10 if the "exactly once" condition is applied (see § 2.1.55).
5. Pell prime with a composite index (see § 2.1.57).
6. Permutable prime in base 10 that contains more than two distinct digits (see § 2.1.58).
7. Prime p_n with $n \geq p_n$ (where p_n is the n^{th} prime number).
8. Prime of the form $n^k - 1$ where $2 < n \in \mathbb{N}$ and $1 < k \in \mathbb{N}$.
9. Repunit prime in specific perfect power bases, e.g. there are no repunit primes in base 9 (see § 2.1.69).
10. Repunit prime with a composite number of digits (see § 2.1.69).

Also see § 5.2.3.

2.9 General Remarks

We present in the following points some general remarks about prime numbers and their types in some extended classifications and meanings which are largely beyond what we investigated (and sometimes even beyond what we should investigate) in the previous sections of this chapter:

[371] See `https://www.fermatquotient.com/FermatQuotienten/FermQ_Sort.txt`.

1. There are some terms (within the terminology of number theory) which are related to the size of large primes and hence these terms do not represent types of primes in the conventional sense, i.e. classifications based on their mathematical properties as already investigated in the previous sections (mostly in § 2.1). The main terms among these are: *titanic primes* (at least 1000 decimal digits), *gigantic primes* (at least 10000 decimal digits), and *megaprimes* (at least one million decimal digits). A seemingly less common and less established term is *bevaprimes* (also sometimes referred to as *gigaprimes*), which refer to primes with at least one billion decimal digits. However, it should be noted that these terms, and similar terms if any, are not standard classifications in mainstream number theory, and their usage and degree of standardization vary according to the literature and context. In particular, while some of these terms have relatively well-established conventional thresholds, they are primarily descriptive terms used in the literature on large and recreational primes rather than universally standardized mathematical classifications. Therefore, readers of the literature should be careful about assuming that such terms always have the same meaning in every context. Also see § 3.1.8.
2. The term "record primes" is commonly used in the literature to refer to the largest discovered prime numbers. Also, "world record prime" is used to refer to the largest known prime number which is currently (March 2026) the 41024320-digit Mersenne prime $2^{136279841} - 1$.[372] Anyway, these "types" of prime numbers are not really types of primes in the sense of those investigated early in this chapter because being a record prime, for example, is not something related to the nature of the number itself but it is something incidental and determined by our progress in the search and investigation of primes. Moreover, being a record prime is subject to abrupt changes and alterations (e.g. what is a world record prime may lose its status as such to another prime, or what is the fourth largest of record primes may suddenly become the fifth or sixth largest, and so on). Also see § 3.1.5.
3. We find in the literature of number theory and prime numbers terms that may suggest a type or class of prime numbers, although they actually describe configurations or groupings of primes. For example, a "prime triplet" (or "prime quadruplet") refers to a particular configuration of three (or four) prime numbers with a certain relationship among them rather than to a type of prime numbers in the sense considered in the previous sections (see § 2.1 and § 2.2). Yes, in standard usage a prime triplet usually refers to a set of three consecutive primes whose smallest and largest members differ by 6.[373] Similarly, in standard usage a "prime quadruplet" normally refers to the specific configuration $(p, p+2, p+6, p+8)$ of four consecutive prime numbers. So, in their generic usage such terms do not (and should not) represent types of primes in the conventional sense, but in their standard and explicitly-defined usage such terms deserve to represent (configuration-based or relational-based) types of primes in the conventional sense (like Chen, twin, cousin and sexy primes) even though such primes are not normally treated as prime types (on equal footing with Chen, twin, cousin and sexy primes).
4. *Semiprimes* are not a type (or class or category) of prime numbers and hence they are not within the main scope of this book, but we will discuss them briefly later on (see § 9.5) due to their link to the prime numbers since their investigation is complementary to the investigation of prime numbers. For instance, some prime types (e.g. Chen primes; see § 2.1.6) and prime-related theorems (e.g. Chen's theorems; see § 5.1.8 and § 5.1.9) and conjectures (e.g. Lemoine's conjecture; see § 6.1.23) involve semiprimes. The same can be said about *almost-primes* noting that semiprimes are a type of almost-primes, i.e. they are 2-almost-primes (see § 9.6).
5. What we said already in the previous point about semiprimes applies similarly to *pseudoprimes* (see § 9.7; also see § 7.9.5).
6. The main subject of this book is the prime numbers in their ordinary meaning and conventional sense (i.e. as a subset or type of natural numbers), and hence all the investigated types in the previous sections

[372] See `https://www.mersenne.org/primes/` and `https://t5k.org/largest.html`.
[373] Apart from (3, 5, 7), such triplets have the form $(p, p+2, p+6)$ or $(p, p+4, p+6)$.

are instances of primes in this ordinary sense. However, there are extensions and generalizations of the concepts of "prime number" and "primality" that go beyond the ordinary meaning and conventional sense and hence they include types of numbers which are not natural numbers (and hence are labeled as "prime numbers" in some sense). For example, *Gaussian primes* (see § 9.4.1) are "prime numbers" within the complex number system in a way similar to the ordinary primes within the system of integers. So, these are "primes" in the set of complex integers $\mathbb{Z}[i]$ and hence they are not the ordinary (or conventional) prime numbers which are in the set of integers $\mathbb{Z}$. Similarly, *Eisenstein primes* (see § 9.4.3) are not ordinary prime numbers but they are "prime numbers" in an extended or generalized meaning of primality. These types of "prime numbers" and related issues will be investigated later on (see § 9.4).

Chapter 3
Categorizations of Primes

In this chapter we investigate the categorizations of prime numbers (and their types) from various perspectives and according to different criteria. Before we delve deeply into this investigation we note the following:

1. Some of these categorizations are exhaustive (i.e. include all prime numbers) and mutually exclusive (i.e. each prime number belongs to one and only one category), while other categorizations are not (i.e. they lack at least one of these properties).
2. We classify the categorizations of prime numbers into two main classes: basic categorizations (which are the subject of § 3.1), and more elaborate and technical categorizations and comparisons of prime types (which are the subject of § 3.2).
3. As indicated already, some categorizations are essentially based on comparisons and similarities (and this largely applies to the categorizations of § 3.2).
4. What we present in this chapter about categorizations and comparisons is rather limited because *complete* investigation of categorizations and comparisons of prime numbers and their types (if possible at all) is very lengthy. So, the investigation in this chapter is about common samples and examples of this subject presented in a rather brief and concise fashion. However, this investigation will be extended horizontally and vertically in the forthcoming volumes of this book.

3.1 Generic Categorizations of Primes

By "generic categorizations" we mean classifications based on basic criteria or on non-inherent (or contextual) considerations from a mathematical perspective. In short, we present in the following subsections some common examples of such "generic" categorizations or classifications of prime numbers (and these examples should clarify the idea of these "generic categorizations" and the objective of this section). However, before we go through these details it is useful to note the following points:

1. As indicated, the following are common examples (but not the only examples) of such categorizations. Careful inspection of the relevant literature should reveal other examples especially when we go beyond the conventional and commonly recognized conceptualizations and terminology of this field where certain individual researchers or groups have their own conceptualizations and categorizations.
2. The following categorizations may also include some extensions or generalizations of the concepts of "prime numbers" and "primality".
3. As indicated, some categorizations represent classifications of the entire set of prime numbers (usually in the form of "partitions"), while others include only some primes (or certain types).
4. For ease of access, we order the following subsections alphabetically (a policy we have largely adopted throughout this book due to its encyclopedic nature).

3.1.1 Certainty of Primality

Most known prime numbers are of small or medium size (in terms of the number of digits) and they are usually found and tested by deterministic sieves and primality tests and hence they are proven primes, i.e. their primality is 100% certain. However, many primes (especially the exceptionally large ones) are often

discovered and tested by heuristic techniques and probabilistic primality tests and hence their primality is not 100% certain (although their primality is usually very high probabilistically). Accordingly, prime numbers may be categorized (especially in the literature of very large and record-breaking primes) as *proven primes* (whose primality is absolutely certain) and *probable primes* (whose primality is highly probable or almost certain but not absolutely certain). Similar terms may also be used in this regard (e.g. *verified* or *confirmed primes* and *probabilistic primes*).

3.1.2 Modularity

The prime numbers can be fully partitioned (i.e. comprehensively and disjointly) according to their residues modulo 4 (and hence we get three distinct parts): number 2, the odd primes of the form $4k-1$, and the odd primes of the form $4k+1$ (where $k \in \mathbb{N}$; see § 5.1.33). Similarly, the prime numbers can be fully partitioned according to their residues modulo 6 (and hence we get four distinct parts): number 2, number 3, the primes > 3 of the form $6k-1$, and the primes > 3 of the form $6k+1$ (where $k \in \mathbb{N}$; see § 5.1.34). Other modularity-based categorizations can also be found in the literature (and in this book as well; see for instance Points 27 and 28 of § 5.2.13). Also see § 2.3.18.

3.1.3 Parity

This is the most basic categorization of prime numbers, where they are partitioned (i.e. comprehensively and disjointly) into even primes (consisting solely of the number 2) and odd primes (consisting of all other primes).

3.1.4 Real vs Complex

The concept of "prime numbers" (which originally means ordinary integers > 1 divisible only by 1 and themselves) may be extended to the set of complex numbers (mainly represented by the Gaussian integers; see footnote [776] in § 9.4.1), where prime numbers (or rather Gaussian primes and similar concepts) then loosely refers to complex numbers $a + \mathrm{i}b$ that cannot be factorized into simpler complex integers (see for instance § 9.4.1 and § 9.4.3). Accordingly, the concept of "prime numbers" becomes more general to include both real prime numbers and complex prime numbers as two categories of prime numbers (noting that "complex primes" include some real primes and exclude others).

In any case, we should note that "Real vs Complex" (i.e. the title of the present subsection which largely refers to the Gaussian primes) does not tell the entire story of generalizing and extending the concepts of prime numbers and primality beyond their ordinary meanings (i.e. ordinary integers > 1 divisible only by 1 and themselves). As we will see later (refer to the subsections of § 9.4), there are other types of generalizations and extensions of these concepts (e.g. Hurwitz primes in the ring of Hurwitz quaternions; see § 9.4.4). In fact, "dimensionality", which is largely the basis and criterion of the generalizations of § 9.4, may not be the only basis for generalizing and extending the concepts of prime numbers and primality.

We should also note that this book is about the ordinary prime numbers (in the ordinary meaning of primality) and hence complex prime numbers, along with any other generalizations and extensions, are beyond the scope of this book, although examples of such generalizations will be investigated briefly in § 9.4 due to their conceptual and practical links to the ordinary prime numbers.

3.1.5 Record

The largest discovered prime numbers (whether in general or of certain types such as Fermat or Mersenne primes) are referred to as *record primes* or *record-breaking primes* and hence they can be seen as a "category" (or "categories") of prime numbers. It is obvious that this categorization (whether from the

perspective of "which is in and which is out" or from other perspectives such as having new types of record numbers) is subject to change and modification from time to time, where regular updates are required. We indicated, almost systematically, some of the record primes in the subsections of § 2.1. Moreover, we indicated this issue in Point 2 of § 2.9.

3.1.6 Recreation

A large part of the current literature of prime numbers is related to recreational mathematics. While the study of prime numbers serves as a cornerstone of rigorous and serious number theory and pure mathematics in general (as well as some related subjects like modern cryptography), a significant part of the contemporary literature in number theory (and prime numbers in particular) remains deeply connected to recreational mathematics. This is partly justified by the fascination with integers and prime numbers which often originates from the "elusive" and "mystic" nature of integers and prime numbers and their types and patterns which captivate professional mathematicians as well as hobbyists and amateur mathematicians. These recreational investigations (and related research and mathematical activities) often establish a useful connection between serious academic inquiries and mathematical play and fun, which contribute to the thrive and enrichment of mathematics in general and number theory in particular. This is in line with the fact that the entire subject of number theory is mostly about curiosity, excitement and satisfaction, noting that its theoretical utilizations (beyond its own domain) and real life applications are rather limited (see chapter 10). Accordingly, many types and categories of prime numbers are based on recreational grounds and considerations. This categorization will be investigated further in § 3.2.9.

3.1.7 Relation to Other Disciplines

Some prime numbers, or types of prime numbers, are involved in certain subjects and disciplines, which are mainly branches of pure and applied mathematics and computing. Accordingly, they may be given certain labels and identifications, and hence they become practically a sort of "prime category". In short, prime numbers with specific properties are frequently grouped into "categories" or "classes" based on their utility in certain disciplines or their unique structural properties which are relevant and useful in some disciplines or investigations.

For example, large primes of certain size and types and with properties relevant to use in cryptography may be referred to (and hence categorized as) *cryptographic primes* or *RSA primes*. We may also find similar labels in other disciplines or in certain types of research, such as group theory and related research, and hence we get other discipline-based prime categories like *group-theoretic primes*. Also see § 2.1.80.

3.1.8 Size

The very large prime numbers are categorized according to their size (as measured by the number of their digits, usually based on their decimal representation, or by their binary bit-length). This categorization was investigated briefly in Point 1 of § 2.9 and hence we do not repeat.

3.1.9 Theoretical Involvement in Certain Theories

Prime numbers are often classified not just by their inherent properties, but by the functional and behavioral roles which they play within certain mathematical theories and in connection to specific theoretical structures. More specifically, some prime numbers (or types of prime numbers) play certain functional roles in some mathematical theories and hence they are labeled and categorized according to their theoretical or behavioral roles in these theories. Prominent examples of such prime number categories can be found in algebraic number theory which often categorizes certain prime numbers as *inert primes* or

ramified primes or *split primes* (and so on) according to their functional and behavioral roles in particular algebraic extensions and within certain theoretical contexts. Also see § 2.1.80.

3.2 Categorizations and Comparisons of Prime Types

The basis of categorizations in this section is different from the basis in the previous section. The categorizations in this section are essentially based on the types of primes that were investigated in chapter 2 (mostly in § 2.1), and hence they are "more fundamental" than those of the previous section which are somewhat "incidental" or "casual". Anyway, it is important to note the following points about the categorizations of the present section:

1. These categorizations are generally not exhaustive and/or mutually exclusive since each categorization usually involve very few (and sometimes single) types of primes which are usually representing small subsets of prime numbers with potential overlap in many cases.
2. The purpose of categorization in the present section is to highlight and demonstrate certain structural aspects within the set of prime numbers and their types (i.e. of chapter 2) as well as certain relational aspects among these types (where similarities among prime types, such as in their algebraic form or structure, are central to these classifications).
3. These categorizations are mostly approximate and may largely represent comparisons more than categorizations or classifications in a strict sense (as indicated by "and Comparisons" in the title of this section). In fact, this is in line with the essence of the previous point.
4. Whether a prime type or types belong to this category or that category is, in many cases, subject to personal judgment and subjective factors in which various aspects and characteristics of the concerned prime type(s) are taken into consideration where some aspects and characteristics are actually (or judged as) stronger or more relevant to the situation and context. Therefore, in many cases, these issues are not completely clear cut.
5. All base-dependent prime types are assumed to be in base 10 (unless stated otherwise).
6. All types mentioned in this section refer to types of prime numbers unless stated otherwise. For example, "repunit" means "repunit prime" rather than "repunit number" in general.
7. As indicated, the investigation in this section is related to the common prime types that were investigated in § 2.1, and hence we will not investigate types mentioned or discussed in other parts of the book (e.g. those discussed in § 2.2 and § 2.3).
8. For ease of access, the following subsections are arranged alphabetically.

3.2.1 Algebraic Form

In this subsection we group and categorize prime types which are mainly characterized by their algebraic forms. These types are defined primarily by specific algebraic expressions and mathematical formulae. The prime types of this category that we investigate in this subsection are: Carol, Catalan, centered, compositorial, cuban, Cullen, cyclotomic, Euler, factorial, Fermat, fortunate, generalized Fermat, generalized Mersenne, Jacobsthal, Kynea, Leyland, Mersenne, Mersenne prime exponent, n^2+1, n^4+1, near-square, NSW, Pierpont, primorial, Proth, Pythagorean, quartan, Riesel, Thabit, Wagstaff, and Woodall. Further classifications of these prime types are given in the following points:

1. We may group the following prime types in one category based on their algebraic form of *exponential type I*:
   - Fermat: $2^{2^k}+1$ where $k \in \mathbb{N}_0$.
   - Fermat (generalized): $b^{2^n}+1$ for $b, n \in \mathbb{N}_0$ and $b > 1$.
2. We may group the following prime types in one category based on their algebraic form of *exponential type II*:

- Mersenne: $2^p - 1$ where $p \in \mathbb{P}$.
- Mersenne (generalized): see § 2.1.25.

3. We may group the following prime types in one category based on their algebraic form of *exponential type III*:
   - Carol: $4^n - 2^{n+1} - 1$ where $n \in \mathbb{N}$.
   - Kynea: $4^n + 2^{n+1} - 1$ where $n \in \mathbb{N}_0$.
4. We may group the following prime types in one category based on their algebraic form of *exponential type IV*:
   - Jacobsthal: $\left[2^n - (-1)^n\right]/3$ where $n \in \mathbb{N}$.[374]
   - Wagstaff: $(2^p + 1)/3$ where p is an odd prime.
5. We may group the following prime types in one category based on their algebraic form of *exponential type V*:
   - Pierpont: $2^a \cdot 3^b + 1$ for $a, b \in \mathbb{N}_0$.
   - Thabit: $2^n \cdot 3 \pm 1$ where $n \in \mathbb{N}_0$ (minus for the first kind and plus for the second kind).
6. We may group the following prime type in one category based on its algebraic form of *exponential type VI*:
   - NSW: $\left[(1+\sqrt{2})^{2n+1} + (1-\sqrt{2})^{2n+1}\right]/2$ where $n \in \mathbb{N}_0$.
7. We may group the following prime type in one category based on its algebraic form of *exponent type*:
   - Mersenne prime exponent: $p \in \mathbb{P}$ such that $2^p - 1$ is prime (i.e. Mersenne prime).
8. We may group the following prime types in one category based on their algebraic form of *polynomial type*:
   - Centered: $[(3n^2 - 3n)/2] + 1$ where $n \in \mathbb{N}$ (triangular), $2n^2 + 2n + 1$ where $n \in \mathbb{N}$ (square), $(5n^2 + 5n + 2)/2$ where $n \in \mathbb{N}$ (pentagonal), and so on.
   - Cuban: $3y^2 + 3y + 1$ (for the first kind) and $3y^2 + 6y + 4$ (for the second kind) where $y \in \mathbb{N}$.[375]
   - Euler: $n^2 + n + 41$ where $n \in \mathbb{N}_0$.
   - Near-square: $n^2 + k$ where $n \in \mathbb{N}$ and k is an integer of small magnitude.
   - $n^2 + 1$ primes where $n \in \mathbb{N}$.
   - $n^4 + 1$ primes where $n \in \mathbb{N}$.
   - Pythagorean: $4n + 1$ where $n \in \mathbb{N}$.
9. We may group the following prime types in one category based on their algebraic form of *polynomial-like type*:
   - Cuban: $(x^3 - y^3)/(x - y)$ where $x, y \in \mathbb{N}$ and $x = y + 1$ or $x = y + 2$.[376]
   - Pythagorean: $x^2 + y^2$ where $x, y \in \mathbb{N}$.[377]
   - Quartan: $x^4 + y^4$ where $x, y \in \mathbb{N}$.
10. We may group the following prime types in one category based on their algebraic form of *exponential-polynomial type I*:
    - Cullen: $2^n n + 1$ where $n \in \mathbb{N}$.
    - Proth: $2^n k + 1$ where $n \in \mathbb{N}$, $0 < k \in \mathbb{O}$ and $k < 2^n$.
    - Riesel: $2^n k - 1$ where $n \in \mathbb{N}$, $0 < k \in \mathbb{O}$ and $k < 2^n$.
    - Woodall: $2^n n - 1$ where $n \in \mathbb{N}$.
11. We may group the following prime type in one category based on its algebraic form of *exponential-polynomial type II*:

---

[374] We note that Jacobsthal numbers (and hence primes) may also be defined formally by: $J_n = \lfloor 2^n/3 \rceil$ where $n \in \mathbb{N}_0$ (see § 2.1.36).

[375] Cuban may also be given by the form $(x^3 - y^3)/(x - y)$ where $x, y \in \mathbb{N}$ and $x = y + 1$ or $x = y + 2$.

[376] Cuban may also be given by the form $3y^2 + 3y + 1$ (for the first kind) and $3y^2 + 6y + 4$ (for the second kind) where $y \in \mathbb{N}$.

[377] If $x^2 + y^2$ should be equivalent to $4n + 1$ then 2 should be excluded, i.e. $x^2 + y^2$ must be odd.

• Leyland: $x^y + y^x$ for integers $x, y > 1$.

12. We may group the following prime type in one category based on its algebraic form of *factorial type*:
• Factorial: $n! \pm 1$ where $n!$ is the factorial of $n \in \mathbb{N}$.
13. We may group the following prime types in one category based on their algebraic form of *primorial type*:
• Fortunate: $q - p_n\#$ where $p_n\#$ is the n^{th} primorial number of the first kind, q is the smallest prime number strictly greater than $p_n\# + 1$, and $n \in \mathbb{N}$.
• Primorial: $p_n\# \pm 1$ where $p_n\#$ is the n^{th} primorial number of the first kind.
14. We may group the following prime type in one category based on its algebraic form of *factorial-primorial type*:
• Compositorial: $(n!/n\#) \pm 1$ where $n!$ is the factorial of $n \in \mathbb{N}$ and $n\#$ is the n^{th} primorial number of the second kind.
15. We may group the following prime type in one category based on its algebraic form of *combinatorics type*:
• Catalan: $C_n^{2n}/(n+1)$ where C_n^{2n} is the binomial coefficient.
16. We may also consider cyclotomic primes [i.e. those of the form $\Phi_n(2)$, where $\Phi_n(x)$ is the n^{th} cyclotomic polynomial] as a broad class in the "algebraic form" category.

3.2.2 Base Dependency

In this subsection we group and categorize prime types which are distinguished by being base-dependent (where "base" refers to the numeral system used in their expression such as binary and decimal). These types are characterized largely by having digit-related (or string-related) properties and features which are mostly taken in their definitions and classifications. The base-dependent prime types that we investigate in this subsection are: circular, delicate, dihedral, emirp, full reptend, happy, home, minimal, palindromic, palindromic wing, pandigital, permutable, primeval, repunit, reversible, self, Smarandache-Wellin, strobogrammatic, truncatable, and unique. Further classifications of these prime types are given in the following points:[378]

1. We may group the following prime types in one category based on the criterion of *digit manipulation*:
• Circular: remains prime under all cyclic permutations of its digits.
• Delicate: becomes composite if any one of its digits is replaced.
• Emirp: results in another prime when its digits are reversed.
• Happy: iterative sum of squares of its digits eventually reaches 1.
• Palindromic (including palindromic wing): remains the same when its digits are reversed.
• Permutable: remains prime under any permutation of its digits.
• Primeval: the number of distinct primes that can be obtained by permuting some or all of its digits is larger than the number of primes that can be obtained in the same way for any smaller positive integer.
• Reversible: remains prime when its digits are reversed.
• Self: cannot be expressed as a sum of a positive integer and its digit sum.[379]
• Truncatable: remains prime when digits are truncated from either side or both sides.
2. We may group the following prime types in one category based on the criterion of *digital pattern*:
• Dihedral: remains prime under certain reflectional and rotational visual symmetries.
• Pandigital: includes in its significant digits every digit used in its base at least once.
• Repunit: all its digits are 1.
• Strobogrammatic: its numeral appears the same when rotated 180 degrees.

[378] It should be noted that in all groupings and categorizations of prime types that are base-dependent we assume they have a common base (which is usually base 10) unless stated otherwise.
[379] This classification may be questioned because digit manipulation does not belong to the prime itself.

3. We may group the following prime type in one category based on the criterion of *primality of its sub-sequences*:
   • Minimal: does not contain any other prime as a sub-sequence of its digits.
4. We may group the following prime type in one category based on the criterion of *prime concatenation*:
   • Smarandache-Wellin: formed by concatenating the first n prime numbers in their increasing order.
5. We may group the following prime type in one category based on the criterion of *prime factor concatenation*:
   • Home: results from repetitive application of prime factorization to the successive concatenation of the prime factors of a natural number n and the numbers obtained by concatenating those factors.
6. We may group the following prime types in one category based on the criterion of *reciprocal pattern*:
   • Full reptend: the decimal expansion of its reciprocal has a repeating period of length $(p-1)$ digits.
   • Unique: its reciprocal has a period length that is not shared by any other prime.

3.2.3 Divisibility and Modularity

In this subsection we group and categorize prime types which are distinguished by being identified by certain divisibility or modularity properties (where these properties are mostly taken in their definitions and characterizations). The prime types that we investigate in this subsection are: harmonic, Higgs, irregular/regular (i.e. of Bernoulli, Euler, and Genocchi types), Mersenne divisor, Mirimanoff, Pillai, Pythagorean, Wall-Sun-Sun, Wieferich, Wilson, and Wolstenholme. Further classifications of these prime types are given in the following points:

1. We may group each one of the following prime types in one category based on the criterion of *its divisibility attribute* (i.e. they represent four independent categories not one category):
   • Harmonic: divides the numerators of exactly three harmonic numbers.
   • Higgs: its totient evenly divides the square of the product of the smaller Higgs primes.
   • Mersenne divisor: prime divisor of Mersenne numbers with prime exponents.
   • Pillai: $p \in \mathbb{P}$ for which there is an $n \in \mathbb{N}$ such that $p|(n!+1)$ and $n \not| (p-1)$.
2. We may group the following prime types in one category based on the criterion of *their divisibility attribute*:
   • Mirimanoff: $p \in \mathbb{P}$ where p^2 divides $(3^{p-1}-1)$.
   • Wall-Sun-Sun: $p \in \mathbb{P}$ such that p^2 divides the Fibonacci number $\mathcal{F}_{p-\left(\frac{p}{5}\right)}$.
   • Wieferich: $p \in \mathbb{P}$ where p^2 divides $(2^{p-1}-1)$.
   • Wilson: $p \in \mathbb{P}$ where p^2 divides $(p-1)!+1$.
   • Wolstenholme: $p \in \mathbb{P}$ where p^4 divides $C_{p-1}^{2p-1}-1$.
3. We may group the following prime types in one category based on the criterion of *their divisibility-related irregularity/regularity attribute*:
   • Bernoulli irregular: odd prime p that divides the numerator of at least one of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$ (and B-regular otherwise).
   • Euler irregular: odd prime p that divides at least one of the Euler numbers $E_2, E_4, \ldots, E_{p-3}$ (and E-regular otherwise).
   • Genocchi irregular: odd prime p that divides at least one of the Genocchi numbers $G_2, G_4, \ldots, G_{p-3}$ (and G-regular otherwise).
4. We may group the following prime type in one category based on the criterion of *its modularity attribute*:
   • Pythagorean: $p \in \mathbb{P}$ where $p \overset{4}{=} 1$.

Also see § 3.1.2.

3.2.4 Expressibility

In this subsection we group and categorize prime types which are distinguished by being identified by certain expressibility properties (where these properties are mostly taken in their definitions and characterizations).[380] The prime types that we investigate in this subsection are: self, Stern, and untouchable. Further classifications of these prime types are given in the following points:

1. We may group the following prime type in one category based on the property of its members (denoted p) *being inexpressible as the sum of a positive integer and its digit sum*:
   • Self: $p \in \mathbb{P}$ where $p \neq k + S(k)$ for any $k \in \mathbb{N}$ where $S(k)$ is the sum of the digits of k.
2. We may group the following prime type in one category based on the property of its members (denoted p) *being inexpressible as the sum of a smaller prime and twice a perfect square*:
   • Stern: $p \in \mathbb{P}$ where $p \neq q + 2b^2$ for any $\mathbb{P} \ni q < p$ and $b \in \mathbb{N}$.
3. We may group the following prime type in one category based on the property of its members *being inexpressible as the sum of the proper divisors of any positive integer*:
   • Untouchable: $p \in \mathbb{P}$ where $p \neq s(n)$ for any $n \in \mathbb{N}$ where $s(n)$ is the restricted divisor function of n.

3.2.5 Grouping and Association

There are certain types of prime numbers whose nature (or definition) requires or implies a kind of association or grouping among them (e.g. by pairing or "setting"). The following notes should clarify the idea of this kind of categorization:

1. Cousin (see § 2.1.10), emirp (see § 2.1.17), sexy (see § 2.1.74), and twin primes (see § 2.1.84) come in pairs (i.e. specifically) where both members of the pair equally hold the given qualification (i.e. cousin prime, emirp prime, etc.). For example, both 13 and 31 are equally qualified as "emirp prime" in this group. Similarly, 11 and 13 in the twin pair (11, 13) are both equally qualified as "twin prime" in this group.[381]
2. Safe and Sophie Germain primes also come in pairs but in the given sense (which is different from the pairing in the previous point; see § 2.1.72 and § 2.1.76), and hence each comes as a single in its specific qualification, i.e. being safe prime and Sophie Germain prime (see Point 5).[382]
3. Circular (see § 2.1.7), dihedral (see § 2.1.16), and permutable primes (see § 2.1.58) generally come in sets (which can be of any non-zero cardinality) where each member of the set equally holds the given qualification. For example, 113, 131 and 311 are equally qualified as circular primes (and permutable primes as well). Similarly, 1181 and 1811 are equally qualified as dihedral primes (which also applies to 120121, 121021, and 150151, 151051).
4. Truncatable primes (see § 2.1.83) also come in sets but in a rather different sense to the sense of Point 3. For example, the left-truncatable prime number 197 is associated with the primes 97 and 7 but in a rather different sense to the association of the circular prime 197 with the primes 719 and 971 which are circular primes on equal footing in this "circular relation" and "circular qualification".
5. The other types of prime numbers (e.g. balanced, Fermat, harmonic, Leyland, Wilson, etc.) generally come as single numbers (i.e. they are not associated with other primes in a particular way as those that come in pairs or sets which we investigated in the previous points). For example, 3 is a Fermat

[380] It should be noted that "expressibility" here excludes algebraic expressibility (which is about "Algebraic Form" that we investigated in § 3.2.1).

[381] Palindromic prime (including palindromic wing prime) results in the same prime and hence it does not belong to this group (see § 2.1.53 and § 2.1.54). This also applies to strobogrammatic prime (see § 2.1.78). Regarding reversible prime (see § 2.1.70), with the exclusion of palindromic prime it represents emirp prime only (which is already counted).

[382] In fact, this should apply even to prime-indexed prime types (such as Mersenne primes M_p and Wagstaff primes W_p) which cannot be included in this category because, despite the pairing of the prime index with the indexed prime (i.e. p with M_p or W_p in the given examples), the index and the indexed are generally not of the same prime type. Yes, when they are (e.g. in the case of double Mersenne primes; see Point 14 in § 2.1.41), the inclusion may be justified.

prime regardless of any other Fermat prime (unlike 3 as a twin prime which is in association with 5 as the other twin prime in this relation).

Also see Point 3 in § 2.9.

3.2.6 Indexing

In this subsection we group and categorize prime types which are distinguished by having specific types of indices (or index-like identifications) according to their definitions or classifications (or even as a characteristic property regardless of their definitions and classifications). We can identify two main kinds of these primes: prime types whose members are indexed (or identified, possibly with some exceptions) by prime numbers, and prime types whose members are indexed (or identified, possibly with some exceptions) by composite numbers (or non-prime numbers to be more general). These two kinds will be investigated in the following two paragraphs.

Regarding prime indexing, we note first that "prime indexing" (or rather prime-indexed[383] primes) refers to those types of prime numbers whose members are indexed or identified with prime numbers (possibly with very few exceptions) according to their definitions or classifications or as a characteristic property of their own. We should also note that "indexing" here refers to the index or label that identifies them within their class or group (according to their definition or classification or as a property), and hence "indexing" here has different meanings (depending on the specific types) and is not unique (and may even refer loosely to their formal identification in general). We may identify two main categories in the *prime indexing*-based prime types:

1. Those types of primes which prime indexing (or identification) is in their formal definition. These types include:[384]
   - Mersenne primes: $M_p = 2^p - 1$ for some $p \in \mathbb{P}$ (see § 2.1.41).[385]
   - Prime-indexed primes: p_n where $n \in \mathbb{P}$ (see § 2.1.62).
   - Primorial primes: $P^{\pm}_{p_n} = p_n\# \pm 1$ where p_n is the n^{th} prime and $p_n\#$ is its primorial of the first kind (see § 2.1.64).
   - Safe primes: $S_p = 2p + 1$ where $p \in \mathbb{P}$ (see § 2.1.72).
   - Wagstaff primes: $W_p = (2^p + 1)/3$ where p is an odd prime (see § 2.1.87).
2. Those types of primes which prime indexing is not in their definition or identification but they are actually prime-indexed, i.e. prime indexing is a characteristic property of their own. These types include:
   - Fibonacci primes excluding 3, i.e. $\mathcal{F}_4$ (see § 2.1.21).
   - Jacobsthal primes excluding 5, i.e. J_4 (see § 2.1.36).
   - Pell primes without exception (see § 2.1.57).
   - Repunit primes without exception (see § 2.1.69).

Regarding composite (or non-prime) indexing, we note that "composite indexing" (or rather composite-indexed primes) refers to those types of prime numbers whose members are indexed by composite numbers (possibly with very few exceptions) according to their definitions or classifications (or even as a property regardless of their definitions and classifications). The obvious example of this category is Fermat primes (as defined to be prime numbers of the form $F_n = 2^n + 1$ and hence they are indexed by $n \in \mathbb{N}$; see § 2.1.20). Noting that n must be a non-negative power of two, all Fermat primes greater than 5 are necessarily composite-indexed. However, we should note that Fermat primes may also be indexed by k (as defined to be prime numbers of the form $F_k = 2^{2^k} + 1$ where $k \in \mathbb{N}_0$) and hence Fermat primes

[383] "Prime-indexed" here is a general adjective, i.e. it is not a label to super primes (see § 2.1.62).

[384] We note that the following prime types have a kind of prime-identification feature: Mirimanoff, Stern, Wieferich, Wilson, and Wolstenholme. However, we do not include them in this category.

[385] This should include double Mersenne primes (see Point 14 in § 2.1.41).

can be indexed without such restriction (noting that the five known Fermat primes are indexed with $k = 0, 1, 2, 3, 4$).[386]

3.2.7 Interval Relationship

In this subsection we group and categorize prime types which are distinguished by being identified by interval[387] relationships of their members with neighboring primes or semiprimes or non-primes. In other words, these prime types are characterized by being defined according to the relationship of the primes of these types with neighboring integers from the perspective of "spacing" or "proximity". The *interval relationship*-based prime types that we investigate in this subsection are: Chen, cousin, isolated, sexy, and twin. Further classifications of these prime types are given in the following points:

1. We may group the following prime types in one category based on the criterion of *proximity of their members to neighboring primes*:
   - Cousin: $(p, p + 4)$ where p and $p + 4$ are prime.
   - Sexy: $(p, p + 6)$ where p and $p + 6$ are prime.
   - Twin: $(p, p + 2)$ where p and $p + 2$ are prime.
2. We may group the following prime type in one category based on the criterion of *proximity of its members to neighboring primes or semiprimes*:
   - Chen: $p \in \mathbb{P}$ such that $p + 2$ is either prime or semiprime.
3. We may group the following prime type in one category based on the criterion of *proximity of its members to neighboring non-primes*:
   - Isolated: $p \in \mathbb{P}$ where $p - 2$ and $p + 2$ are both non-prime.

Also see Point 3 in § 2.9.

3.2.8 Magnitude Comparison

In this subsection we group and categorize prime types which are distinguished by being identified by the magnitude of their members in comparison to the magnitude of combinations of other primes. More specifically, these prime types are characterized by being defined on the basis of the magnitude of their members in comparison to the magnitude of the arithmetic and geometric means of the neighboring or surrounding primes. The *magnitude comparison*-based prime types that we investigate in this subsection are: balanced, good, strong, and weak. Further classifications of these prime types are given in the following points:

1. We may group the following prime types in one category based on the criterion of *the magnitude of their members relative to the magnitude of the arithmetic mean of the neighboring primes*:[388]
   - Balanced: $p_n = (p_{n-1} + p_{n+1})/2$.
   - Strong: $p_n > (p_{n-1} + p_{n+1})/2$.
   - Weak: $p_n < (p_{n-1} + p_{n+1})/2$.
2. We may group the following prime type in one category based on the criterion of *the magnitude of its members relative to the magnitude of the geometric mean of the surrounding primes*:[389]
   - Good: $p_n > \sqrt{p_{n-i}p_{n+i}}$ for all $1 \leq i \leq (n - 1)$.

   Also see § 2.3.1.

[386] In fact, the best example of this category is composite-indexed primes (see § 2.3.3). However, "Emerging Types of Prime Numbers" (see § 2.3) are not included in the investigation of this section (see Point 7 of § 3.2).

[387] "Interval" is more general than "gap" which has a specific technical meaning in association with prime numbers (i.e. prime gap).

[388] "Neighboring" may be replaced by "surrounding" in connection with Point 6 of § 2.1.89.

[389] "Surrounding" may be replaced by "neighboring" in connection with Point 2 of § 2.1.26.

3.2.9 Recreation

In this subsection we investigate the categorization of prime numbers on the basis of being typified and used for recreational purposes, as opposite to serious purposes (such as professional mathematical investigation and research, and important mathematical applications like cryptography and computing). In fact, there is no obvious and formal boundary between "recreational" and "serious" prime types noting that large parts of mathematics (and number theory in particular) are mainly motivated by curiosity and self-satisfaction rather than usefulness and need, and hence they are recreational in some sense. Moreover, many playful mathematical constructions have inspired serious investigations and real research and vice versa. So, there is no clear cut border between the two, i.e. recreational and serious prime types.

However, there are lots of prime types that are mostly studied for the purpose of curiosity, aestheticism, patterns, puzzles (and similar purposes and motives) rather than deep theoretical importance or practical benefit. Broadly speaking, recreational prime types are often defined by their visual patterns, digital properties, or unusual relationships and odd characteristics rather than their utility in theoretical investigations (like advanced number theory) or applied mathematical fields (like cryptography). In short, recreational prime types are typified and categorized on bases and factors which have little to do with their fundamental mathematical nature and properties. In fact, many (and possibly most) of the recreational prime types come from the base-dependent prime types (which were largely investigated in § 3.2.2).

We outline in the following list some of the main categorization bases that characterize recreational prime types with some examples of these prime types:

1. Digit and string manipulation: most of the base-dependent prime types (see § 3.2.2) fall in this category of recreational prime types. These types are characterized by being based on attributes that hardly have any inherent connection with the primality of the integers of these types; instead they are based on or related to extrinsic and amusing considerations (or rather acrobatic gimmicks) such as removing digits or replacing them or changing their positions and so on. Examples of this category of recreational prime types are: circular, delicate, emirp, happy, palindromic, permutable, primeval, self, and truncatable primes.[390]
2. Digital pattern: this category is based on the digital and string patterns of the primes of these types and their sub-sequences (or sub-strings); which are mostly unrelated to any intrinsic mathematical attribute of these numbers themselves or their primality (or at least these mathematical attributes are marginal or irrelevant to any serious purpose or aspect of these primes). Examples of this category of recreational prime types are: minimal, pandigital and Smarandache-Wellin primes.
3. Visual pattern: this category is based on the visual patterns of the primes of these types which have no significance or any serious mathematical purpose or perspective. These visual patterns are mostly demonstrated and exemplified by certain visual symmetries like reflection and rotation. Examples of this category of recreational prime types are: dihedral and strobogrammatic primes.
4. Playful definition: this category is based on mathematically-arbitrary (and rather playful) definitions and hence these prime types are void of any real mathematical significance or theoretical substance. Examples of this category of recreational prime types are: happy and lucky primes.

3.2.10 Sequencing Form

In this subsection we group and categorize prime types which are distinguished by being identified as prime types whose members are occurring in certain recursively-defined integer sequences (and hence they are defined inherently by specific recurrence relations). The *sequencing form*-based prime types that we investigate in this subsection are: Bell, Fibonacci, Jacobsthal, Lucas, NSW, Padovan, partition, Pell,

[390] It is worth noting that some of these recreational prime types (like circular and truncatable primes) are involved in real research areas and serious mathematical applications such as number bases and automation.

Perrin, and Tribonacci. Further classifications of these prime types are given in the following points:

1. We may group the following prime type in one category based on the criterion of *representing set partitioning*:
   • Bell: $\mathscr{B}_{n+1} = \sum_{k=0}^{n} C_k^n \mathscr{B}_k$ where $\mathscr{B}_0 = 1$ and C_k^n is the binomial coefficient.[391]
2. We may group the following prime type in one category based on the criterion of being *part of a* 1^{st} *order recursively-defined sequence*:
   • Jacobsthal: $J_0 = 0$ and $J_{n+1} = 2^n - J_n$ $\left[\text{or } J_{n+1} = 2J_n + (-1)^n\right]$ (for $0 \leq n \in \mathbb{N}_0$).
3. We may group the following prime types in one category based on the criterion of being *part of* 2^{nd} *order recursively-defined sequences*:
   • Fibonacci: $\mathcal{F}_0 = 0$, $\mathcal{F}_1 = 1$ and $\mathcal{F}_n = \mathcal{F}_{n-2} + \mathcal{F}_{n-1}$ (for $1 < n \in \mathbb{N}$).
   • Jacobsthal: $J_0 = 0$, $J_1 = 1$ and $J_n = 2J_{n-2} + J_{n-1}$ (for $1 < n \in \mathbb{N}$).
   • Lucas: $L_0 = 2$, $L_1 = 1$ and $L_n = L_{n-2} + L_{n-1}$ (for $1 < n \in \mathbb{N}$).
   • NSW: $N_0 = 1, N_1 = 7$ and $N_n = 6N_{n-1} - N_{n-2}$ (for $1 < n \in \mathbb{N}$).
   • Pell: $\mathcal{P}_0 = 0$, $\mathcal{P}_1 = 1$ and $\mathcal{P}_n = \mathcal{P}_{n-2} + 2\mathcal{P}_{n-1}$ (for $1 < n \in \mathbb{N}$).
4. We may group the following prime types in one category based on the criterion of being *part of* 3^{rd} *order recursively-defined sequences*:
   • Padovan: $P_0 = P_1 = P_2 = 1$ and $P_n = P_{n-3} + P_{n-2}$ (for $2 < n \in \mathbb{N}$).
   • Perrin: $\mathsf{P}_0 = 3$, $\mathsf{P}_1 = 0$, $\mathsf{P}_2 = 2$ and $\mathsf{P}_n = \mathsf{P}_{n-3} + \mathsf{P}_{n-2}$ (for $2 < n \in \mathbb{N}$).
   • Tribonacci: $T_0 = T_1 = 0$, $T_2 = 1$ and $T_n = T_{n-3} + T_{n-2} + T_{n-1}$ (for $2 < n \in \mathbb{N}$).
5. We may group the following prime type in one category based on the criterion of *representing integer partitioning*:
   • Partition: $P(a) = 0$ for $a < 0$, $P(0) = 1$, and

$$P(n) = \sum_{k=1}^{\infty} (-1)^{k-1} \left[P\left(n - \frac{k(3k-1)}{2}\right) + P\left(n - \frac{k(3k+1)}{2}\right) \right] \qquad \text{(for } n \geq 1\text{)} \qquad (40)$$

3.2.11 Other Considerations

In this subsection we group and categorize prime types whose categories have only one or two types (and hence they are not worth of having an entire subsection).

1. We may group the following prime type in one category based on the property of its members (denoted p) that *all even positive integers up to* $p - 3$ *occur as differences of primes bounded by* p:
   • Cluster: odd prime p where every even integer m $(2 \leq m \leq p - 3)$ can be written as the difference between two primes which are less than or equal to p.
2. We may group the following prime types in one category based on the property of their members *having totient-related properties*:
   • Higgs: its totient evenly divides the square of the product of the smaller Higgs primes.
   • Highly cototient: $p \in \mathbb{P}$ for which the equation $x - \phi(x) = p$ has more solutions x than any smaller positive integer greater than 1 (where ϕ is the totient function).
3. We may group the following prime type in one category based on the property of its members *being lucky numbers*:
   • Lucky: prime number that survives the sieve of lucky numbers.
4. We may group the following prime type in one category based on the property of its members *being generated via a specific double exponential function involving Mills' constant*:
   • Mills: prime obtained by Mills' constant through applying the floor function to the Mills constant powers.

[391] The Bell sequence does not have a fixed order (or degree) because it is defined by a variable-order recurrence relation.

5. We may group the following prime type in one category based on the property of its members (denoted p) that *their least positive primitive root fails to be a primitive root modulo* p^2:
   • Non-generous: $p \in \mathbb{P}$ whose least positive primitive root is not a primitive root modulo p^2.
6. We may group the following prime type in one category based on the property of its members (denoted R_n) *being the smallest primes that guarantee* $\pi(x) - \pi(x/2) \geq n$ *for all* $x \geq R_n$:
   • Ramanujan: smallest prime R_n such that there are at least n primes between $x/2$ and x for all $x \geq R_n$.
7. We may group the following prime types in one category based on the criterion of *structural relationships between their members*:[392]
   • Safe: $2p + 1$ is a safe prime *iff* p is also prime (i.e. Sophie Germain prime).
   • Sophie Germain: p is a Sophie Germain prime *iff* $2p + 1$ is also prime (i.e. safe prime).
8. We may group the following prime type in one category based on the property of its members *having a modularity property related to elliptic curves*:
   • Supersingular: p for which an elliptic curve becomes supersingular (modulo p).

[392] "Their members" means the members of one type and the corresponding members of the other type.

Chapter 4
Relationships of Primes

In this chapter we investigate the relationships between the types of prime numbers which we investigated in chapter 2 (and in section § 2.1 in particular). In the following sections we outline common relationships between these prime types. However, before we go through this investigation it is useful to note the following remarks:

1. What we present in this chapter about the relationships between prime types is limited because *complete* investigation of these relationships (if possible at all) is very lengthy and hence it is beyond the intended size of the present volume. So, the investigation in this chapter is actually about common examples of these relationships to demonstrate and illustrate the basic idea about such relationships. However, this investigation should be extended horizontally and vertically in the forthcoming volumes of this book.
2. All integer types that we mention in this chapter refer to prime numbers (e.g. "repunit" means "repunit prime" rather than repunit in general) unless stated otherwise. Moreover, all base-dependent types are assumed to be in base 10 (unless stated otherwise).
3. The investigation of these relationships is mostly based on the categorizations and comparisons of prime types (as investigated largely in § 3.2), and hence the reader should refer to § 3.2 for more clarity. In fact, the sections of the present chapter mostly mirror (in relationships and comparisons) the subsections of § 3.2 (which are essentially about grouping and categorization).
4. We may use graphical illustrations (in the form of Venn diagrams) to demonstrate the relationships when such demonstrations are relevant and useful. However, the provided graphics are just samples and examples (with no commitment to do so systematically).
5. The investigation of the relationships between the prime types in this chapter is largely based on comparisons between these types considering common features and similarities between them (as reflected in the definitions and characteristics of these prime types). We note that these comparison-based relationships are not necessarily fundamental or inherent to the nature and behavior of the prime numbers of these types.
6. For ease of access, we order the following sections alphabetically.

4.1 Algebraic Form

We investigate in this section the relationships between the prime types that are characterized mainly by their algebraic forms (where the investigation will be structured within the subsections of the present section to identify and outline these relationships).[393] The prime types that we investigate in this section are: Carol, Catalan, centered, compositorial, cuban, Cullen, cyclotomic, Euler, factorial, Fermat, fortunate, generalized Fermat, generalized Mersenne, Jacobsthal, Kynea, Leyland, Mersenne,[394] Mersenne prime exponent, $n^2 + 1$, $n^4 + 1$, near-square, Pierpont, primorial, Proth, Pythagorean, quartan, Riesel,

[393] As indicated, this section is essentially about the relationships and comparisons between the prime types that have been investigated (i.e. grouped and categorized) in § 3.2.1. So, the present section is a "twin" section to the § 3.2.1 subsection. This similarly applies to most sections of this chapter.

[394] Double Mersenne primes are, by definition, Mersenne primes, and hence they are not treated as a separate category in this chapter. While they are included in our general discussion of Mersenne primes without formal distinction, their unique properties and relationships should be investigated independently in our future work.

Thabit, Wagstaff, and Woodall primes.[395]

4.1.1 Carol , Kynea and Near-Square Primes

The algebraic forms of these types of prime numbers are:
- Carol: $(2^n - 1)^2 - 2$ where $n \in \mathbb{N}$ (see § 2.1.3).
- Kynea: $(2^n + 1)^2 - 2$ where $n \in \mathbb{N}_0$ (see § 2.1.37).
- Near-square: $n^2 + k$ where $n \in \mathbb{N}$ and k is an integer of small magnitude (see § 2.1.49).

As we see, these types have similarities in their algebraic form. The relationships between these prime types are outlined in the following points:
1. Carol, Kynea: despite the striking similarity in the algebraic form of these types, the actual relationship between them is less fundamental (considering their members). The fundamental relationship is actually between Carol *numbers* and Kynea *numbers* (rather than Carol *primes* and Kynea *primes*) because the primality is rather random in connection with the algebraic form (i.e. no inherent correlation between primality and algebraic form). In fact, the specific algebraic forms of these types make them mutually exclusive except in number 7 which is the only prime number that is Carol and Kynea simultaneously.
2. Carol, near-square: Carol primes are a special case of the primes of the form $m^2 - 2$ (where $m = 2^n - 1$) which are a kind of near-square primes, i.e. Carol primes are a proper subset of near-square primes.
3. Kynea, near-square: like Carol primes, Kynea primes are a proper subset of near-square primes (with $m = 2^n + 1$).

4.1.2 Catalan Primes

As seen earlier (refer to § 2.1.4), Catalan primes are of the form $C_n^{2n}/(n+1)$ where C_n^{2n} is the binomial coefficient. The algebraic form of the Catalan primes does not look like that of any other types of prime numbers and hence this type is a category of its own with no inherent relationship with other types of the *algebraic form*-based prime types. In fact, the rarity of the Catalan primes (i.e. 2 and 5 are the only Catalan primes; see § 2.1.4) which indicates the unique nature of this prime type should confirm this observation.

4.1.3 Cullen, Fermat, Pierpont and Proth Primes

The algebraic forms of these types of prime numbers are:
- Cullen: $2^n n + 1$ where $n \in \mathbb{N}$ (see § 2.1.12).
- Fermat: $2^{2^m} + 1$ where $m \in \mathbb{N}_0$ (see § 2.1.20).[396]
- Pierpont: $2^a 3^b + 1$ where $a, b \in \mathbb{N}_0$ (see § 2.1.60).
- Proth: $2^n k + 1$ where $n \in \mathbb{N}$, k is an odd positive integer, and $k < 2^n$ (see § 2.1.65).

As we see, these types have similarities in their algebraic form. The relationships between these prime types are outlined in the following points:
1. Cullen, Fermat: 3 is the only prime that is Cullen and Fermat simultaneously.[397]
2. Cullen, Pierpont: Cullen primes are Pierpont for $n = a = 3^b$, and hence Cullen primes and Pierpont primes overlap in this case (i.e. they overlap partially). An example of a Cullen Pierpont prime is

[395] We note that other types of prime numbers may also be included in this section within the "Algebraic Form" category. For example, safe and Sophie Germain primes may also be classified in this category but we will investigate them as a "Structure Based" category (see § 4.11.1) as this seems more relevant and appropriate to their nature.

[396] We are using m (instead of k which is the commonly-used index) because k is used in Proth.

[397] By equating $2^n n + 1$ (Cullen) to $2^{2^m} + 1$ (Fermat) we can conclude that no integer (whether prime or not) other than 3 can be of these forms simultaneously. So, 3 is the only integer (not only prime) that is both a Cullen number and a Fermat number.

3 (where $n = 1 = a = 3^0$).[398] Examples of Cullen primes which are not Pierpont are Cullen with $n = 141, 4713, 5795$. Examples of Pierpont primes which are not Cullen are 2, 5, 7, 13.

3. Cullen, Proth: although their forms suggest that they have only partial overlap, in practice (considering the condition $k < 2^n$) all Cullen primes are Proth primes and hence Cullen primes are a proper subset of Proth primes. Examples of Proth primes which are not Cullen are: 5, 13, 17.
4. Fermat, Pierpont: Fermat primes are a special case of Pierpont primes (i.e. Pierpont with $a = 2^m$ and $b = 0$), and hence Fermat primes are a proper subset of Pierpont primes. Examples of Pierpont primes which are not Fermat are: 7, 13, 19.
5. Fermat, Proth: Fermat primes are a special case of Proth primes (i.e. Proth with $n = 2^m$ and $k = 1$), and hence Fermat primes are a proper subset of Proth primes. Examples of Proth primes which are not Fermat are: 13, 41, 97, 113.
6. Pierpont, Proth: Pierpont and Proth primes partially overlap. Examples of Pierpont primes which are not Proth are: 2, 7, 19, 37. Examples of Proth primes which are not Pierpont are: 41, 113, 241, 353. Examples of Pierpont Proth primes are: 3, 5, 13, 17, 97.
7. Cullen, Fermat, Pierpont, Proth: the relationships between these prime types are depicted graphically in the Venn diagram of Figure 1. Examples of (where "zone" refers to the labeled areas in Figure 1):
   - Zone 1 (i.e. none): 11, 23, 29, 43.
   - Zone 2 (i.e. all): 3.[399]
   - Zone 3 (i.e. Cullen-Proth but not Fermat, Pierpont): Cullen with $n = 141, 4713, 5795$.
   - Zone 4 (i.e. Fermat-Pierpont-Proth but not Cullen): 5, 17, 257, 65537.
   - Zone 5 (i.e. Pierpont only): 7, 19, 37, 73.
   - Zone 6 (i.e. Proth only): 41, 113, 353, 1217.
   - Zone 7 (i.e. Pierpont-Proth but not Cullen, Fermat): 13, 97, 577.
   - Zone 8 (i.e. Cullen-Pierpont-Proth but not Fermat): seemingly there are no known examples of such primes (and hence it is apparently an empty set).[400]

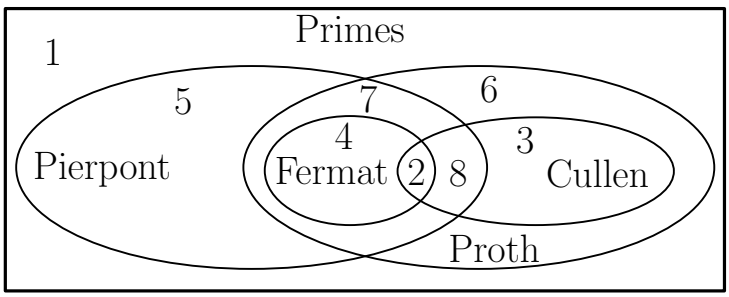


Figure 1: Venn diagram demonstrating the relationships between primes of the indicated types (see Point 7 of § 4.1.3).

We should finally refer to the obvious fact that Fermat primes are a proper subset of generalized Fermat primes (which have the form $b^{2^n}+1$ for $b, n \in \mathbb{N}_0$ and $b > 1$). The relationships between generalized Fermat primes and Cullen, Pierpont and Proth can be inferred from this form (while utilizing the discussion in the previous points).

[398] Number 3 seems to be the only known Cullen Pierpont prime. Whether or not there exists a Cullen Pierpont prime other than 3 seems to be an open problem.

[399] In fact, 3 is the only integer (and consequently the only prime) that is simultaneously a Cullen, Fermat, Pierpont, and Proth number (see footnote [397]).

[400] In fact, the existence (or non-existence) of such primes can be an open problem where conjectures can be formulated and proofs can be sought (e.g. "there are no prime numbers which are Cullen, Pierpont, and Proth simultaneously but they are not Fermat primes" or "3 is the only Cullen, Pierpont, and Proth prime simultaneously").

4.1.4 Centered Primes

These primes are generally defined by polynomial expressions (see § 2.1.5), and hence they have a similarity to other prime types which are also defined by polynomial expressions (see Point 8 in § 3.2.1). But in general there is no fundamental relationship between centered primes and those types. However, we may find some exceptions (e.g. every cuban prime of the first kind is a centered hexagonal prime).

4.1.5 Mersenne, Riesel and Woodall Primes

The algebraic forms of these types of prime numbers are:
- Mersenne: $M_p = 2^p - 1$ where $p \in \mathbb{P}$ (see § 2.1.41).
- Riesel: $2^n k - 1$ where $n \in \mathbb{N}$, $0 < k \in \mathbb{O}$ and $k < 2^n$ (see § 2.1.71).
- Woodall: $2^n n - 1$ where $n \in \mathbb{N}$ (see § 2.1.93).

As we see, these types have similarities in their algebraic form. The relationships between these prime types are outlined in the following points:

1. Mersenne, Riesel: Mersenne primes are a proper subset of Riesel primes (corresponding to $k = 1$).
2. Mersenne, Woodall: Mersenne and Woodall primes overlap partially (noting that Woodall primes are rarer than Mersenne primes). The known examples of this overlap are: 7 and $M_{521} = 2^{521} - 1 = 2^{512} \cdot 512 - 1$. The potential existence of other example(s) seems to be an open problem.[401] Examples of Mersenne primes which are not Woodall are: 3, 31, 127, 8191. Examples of Woodall primes which are not Mersenne are: 23, 383, 32212254719.
3. Riesel, Woodall: every Woodall prime is a Riesel prime (but not the reverse), and hence Woodall primes are a proper subset of Riesel primes.[402] Examples of prime numbers which are Woodall (and hence Riesel as well) are: 7, 23, 383, 32212254719. Examples of Riesel primes which are not Woodall are: 3, 11, 31, 47, 79.
4. Mersenne, Riesel, Woodall: the relationships between these prime types are depicted graphically in the Venn diagram of Figure 2. Examples of (where "zone" refers to the labeled areas in Figure 2):
   - Zone 1 (i.e. none): 2, 5, 13, 17, 19.
   - Zone 2 (i.e. all): 7, $M_{521} = 2^{521} - 1$.[403]
   - Zone 3 (i.e. Mersenne-Riesel but not Woodall): 3, 31, 127, 8191.
   - Zone 4 (i.e. Woodall-Riesel but not Mersenne): 23, 383, 32212254719.
   - Zone 5 (i.e. Riesel only): 11, 47, 79.

We should finally refer to the obvious fact that Mersenne primes are a proper subset of generalized Mersenne primes (at least according to some definitions; see § 2.1.25). The relationships between generalized Mersenne primes and Riesel and Woodall primes may be inferred from the given forms (or definitions) of generalized Mersenne primes (while utilizing the discussion in the previous points). We should also remember here that Mersenne primes are a proper subset of Mersenne divisors (see § 2.1.42).

---

[401] The existence of other examples depends on whether p of Mersenne can be of the form $m + 2^m$ for some $m \in \mathbb{N}$ while simultaneously resulting in a prime number (noting that this is a necessary but not sufficient condition).

[402] We note that $n < 2^n$ for all $n \in \mathbb{N}$. Moreover, if n is odd then Woodall prime is a Riesel prime corresponding to $k = n$, while if n is even then it can be written as $n = 2^m \cdot k$ where $0 < k \in \mathbb{O}$ and hence $2^n n - 1 = 2^{n+m} k - 1$ which is Riesel (noting that $k \leq n < 2^n < 2^{n+m}$).

[403] As indicated already, 7 and M_{521} are the only *known* examples of Mersenne Woodall primes (and hence the only *known* examples of Mersenne Riesel Woodall primes). However, "whether these two numbers are the only *known* examples of such primes or they are the only *possible* such primes" seems to be a valid open problem (which we did not find any mention of it in the available literature), and hence it can be a new open problem with possible formulation of conjectures about it, e.g. 7 and M_{521} are the only possible prime numbers which are Mersenne and Woodall (and hence Mersenne, Riesel and Woodall) simultaneously.

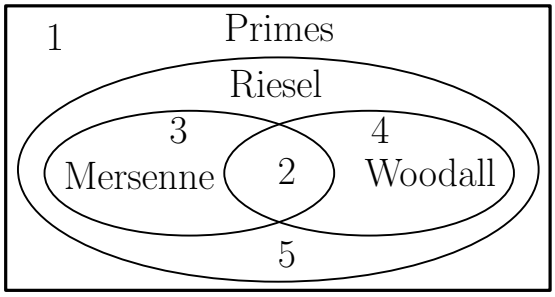


Figure 2: Venn diagram demonstrating the relationships between primes of the indicated types (see Point 4 of § 4.1.5).

4.1.6 Mersenne Prime Exponents

As seen earlier (refer to § 2.1.43), a Mersenne prime exponent is a prime p such that $2^p - 1$ is prime (i.e. Mersenne prime). The algebraic form (or formal condition) of the Mersenne prime exponents does not have similarity with any other types of prime numbers, and hence this type is a category of its own with no essential relationship with other types of the *algebraic form*-based prime types.[404]

4.1.7 Mersenne and Pythagorean Primes

The algebraic forms of these types of prime numbers are:
- Mersenne: $M_p = 2^p - 1$ where $p \in \mathbb{P}$ (see § 2.1.41).
- Pythagorean: $4k + 1$ where $k \in \mathbb{N}$ (see § 2.1.66).

Noting that $M_p = 2^p - 1 = 4(2^{p-2}) - 1$, we can see that all Mersenne primes are non-Pythagorean and hence Mersenne and Pythagorean primes are disjoint sets (formally as well as practically). However, we should note that they have a common geometric meaning and significance since both Mersenne and Pythagorean primes are linked to right-angle triangles, i.e. a Mersenne prime can represent the odd leg of a primitive Pythagorean triangle with consecutive even leg and hypotenuse, while every Pythagorean prime can represent the hypotenuse of a right triangle with integer legs (also see Point 4 in § 4.1.14).

4.1.8 Pierpont, Proth and Thabit Primes

The algebraic forms of these types of prime numbers are:
- Pierpont: $2^a 3^b + 1$ where $a, b \in \mathbb{N}_0$ (see § 2.1.60).
- Proth: $2^n k + 1$ where k is an odd positive integer, $n \in \mathbb{N}$ and $k < 2^n$ (see § 2.1.65).
- Thabit (of the second kind): $2^n \cdot 3 + 1$ where $n \in \mathbb{N}_0$ (see § 2.1.81).

As we see, these types have similarities in their algebraic form. The relationships between these prime types are outlined in the following points:

1. Pierpont, Proth: see Point 6 in § 4.1.3.
2. Pierpont, Thabit: Thabit primes are a proper subset of Pierpont primes (by setting $a = n$ and $b = 1$).
3. Proth, Thabit: Proth and Thabit are the same for $n > 1$ and $k = 3$, e.g. $2^2 \cdot 3 + 1 = 13$, $2^5 \cdot 3 + 1 = 97$ and $2^6 \cdot 3 + 1 = 193$.[405] Examples of Proth which are not Thabit are: 3, 5, 17, 41. An example of Thabit which is not Proth is: 7.[406]

[404] In fact, even being an *algebraic form*-based prime type is rather arbitrary (i.e. to find some place within our categorizations to this unique prime type).
[405] In fact, if $n > 1$ then Thabit primes (of the second kind) are a subset of Proth primes.
[406] In fact, 7 is the only Thabit prime (of the second kind) that is not a Proth prime.

4. Pierpont, Proth, Thabit: the relationships between these prime types are depicted graphically in the Venn diagram of Figure 3. Examples of (where "zone" refers to the labeled areas in Figure 3):
   - Zone 1 (i.e. none): 11, 23, 29, 31.
   - Zone 2 (i.e. all): 13, 97, 193.
   - Zone 3 (i.e. Pierpont-Proth but not Thabit): 3, 5, 17, 257.
   - Zone 4 (i.e. Pierpont only): 2, 19, 37, 73.
   - Zone 5 (i.e. Proth only): 41, 113, 241, 353.
   - Zone 6 (i.e. Pierpont-Thabit but not Proth): only 7.

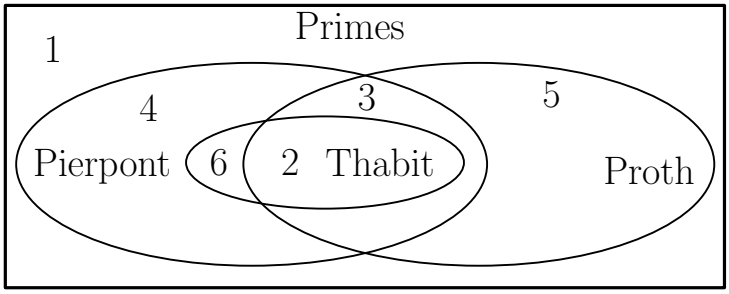


Figure 3: Venn diagram demonstrating the relationships between primes of the indicated types (noting that Thabit is of 2^{nd} kind; see Point 4 of § 4.1.8).

4.1.9 Riesel, Thabit and Woodall Primes

The algebraic forms of these types of prime numbers are:
- Riesel: $2^n k - 1$ where $n \in \mathbb{N}$, $0 < k \in \mathbb{O}$ and $k < 2^n$ (see § 2.1.71).
- Thabit (of the first kind): $2^n \cdot 3 - 1$ where $n \in \mathbb{N}_0$ (see § 2.1.81).
- Woodall: $2^n n - 1$ where $n \in \mathbb{N}$ (see § 2.1.93).

As we see, these types have similarities in their algebraic form. The relationships between these prime types are outlined in the following points:

1. Riesel, Thabit: Riesel and Thabit are the same for $n > 1$ and $k = 3$, e.g. $2^2 \cdot 3 - 1 = 11$ and $2^3 \cdot 3 - 1 = 23$.[407] Examples of Riesel which are not Thabit are: 3, 7, 31, 79. Examples of Thabit which are not Riesel are: 2, 5.
2. Riesel, Woodall: see Point 3 in § 4.1.5.
3. Thabit, Woodall: Thabit and Woodall are the same for $n = 3$, i.e. 23. They may also overlap in other cases (i.e. when the n of Woodall is of the form $2^m \cdot 3$, e.g. $2^7 \cdot 3 - 1 = 2^6 \cdot 6 - 1 = 383$). Examples of Thabit which are not Woodall are: 2, 5, 11, 47, 191. Examples of Woodall which are not Thabit are: 7, 32212254719.[408]
4. Riesel, Thabit, Woodall: the relationships between these prime types are depicted graphically in the Venn diagram of Figure 4. Examples of (where "zone" refers to the labeled areas in Figure 4):
   - Zone 1 (i.e. none): 13, 17, 19, 29.
   - Zone 2 (i.e. all): 23, 383.
   - Zone 3 (i.e. Riesel-Thabit but not Woodall): 11, 47.
   - Zone 4 (i.e. Riesel only): 3, 31, 79.
   - Zone 5 (i.e. Thabit only): 2, 5.
   - Zone 6 (i.e. Riesel-Woodall but not Thabit): 7, 32212254719, 283341988972187128217599.

[407] In fact, if $n > 1$ then Thabit primes are a subset of Riesel primes.
[408] We note that $32212254719 = 2^{30} \cdot 30 - 1 = 2^{31} \cdot 3 \cdot 5 - 1$ and hence it is a Woodall but not Thabit.

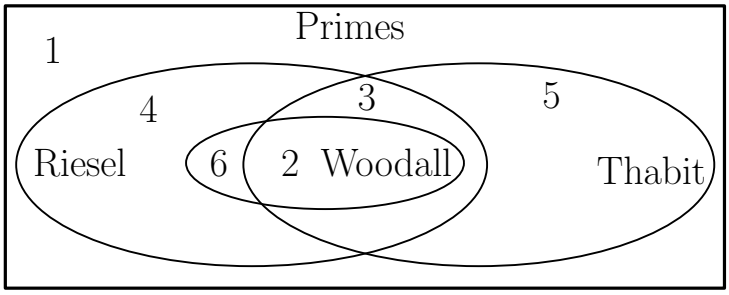


Figure 4: Venn diagram demonstrating the relationships between primes of the indicated types (noting that Thabit is of 1^{st} kind; see Point 4 of § 4.1.9).

4.1.10 n^2+1, n^4+1, Near-Square and Quartan Primes

The algebraic forms of these types of prime numbers are:
- n^2+1 where $n \in \mathbb{N}$ (see § 2.1.47).
- n^4+1 where $n \in \mathbb{N}$ (see § 2.1.48).
- Near-square: n^2+k where $n \in \mathbb{N}$ and k is an integer of small magnitude (see § 2.1.49).
- Quartan: x^4+y^4 where $x, y \in \mathbb{N}$ (see § 2.1.67).

As we see, these types have similarities in their algebraic form. The relationships between these prime types are outlined in the following points:

1. n^2+1, n^4+1: the n^4+1 primes are a proper subset of the n^2+1 primes.
2. n^2+1, near-square: n^2+1 primes are a proper subset of near-square primes.
3. n^2+1, quartan: these prime types partially overlap (e.g. 2, 17, 257 are of both types, and 5, 37, 101 are of n^2+1 type only, while 97, 337, 641 are quartan only).
4. n^4+1, near-square: the n^4+1 primes are a proper subset of the near-square primes.
5. n^4+1, quartan: the n^4+1 primes are a proper subset of the quartan primes.
6. Near-square, quartan: these prime types partially overlap (e.g. 2, 17, 257 are of both types,[409] and 7, 23, 47, 79 are of near-square type only,[410] while 3697, 4177, 4721 are quartan only).
7. n^2+1, n^4+1, near-square, quartan: the relationships between these prime types are depicted graphically in the Venn diagram of Figure 5. Examples of (where "zone" refers to the labeled areas in Figure 5):
   - Zone 1 (i.e. none): 347, 421.
   - Zone 2 (i.e. all): 2, 17, 257.
   - Zone 3 (i.e. near-square only): 7, 23, 47, 79.
   - Zone 4 (i.e. near-square and n^2+1 only): 37, 101, 197, 401.
   - Zone 5 (i.e. near-square, n^2+1 and n^4+1 but not quartan): none (see Point 5).
   - Zone 6 (i.e. near-square and quartan only): 97.
   - Zone 7 (i.e. near-square, n^2+1 and quartan but not n^4+1): we did not find an example within the available OEIS data for these prime types.
   - Zone 8 (i.e. quartan only): 3697, 4177, 4721.

4.1.11 Jacobsthal and Wagstaff Primes

The algebraic forms of these types of prime numbers are:
- Jacobsthal: $\left[2^n-(-1)^n\right]/3$ where $n \in \mathbb{N}$ (see § 2.1.36).[411]

[409] These are of the form n^2+1.
[410] These are of the form n^2-2.
[411] It is worth noting that Jacobsthal primes are also classified within the "Recursive Sequencing" category due to their multiple characterizing definitions (see § 4.10). Moreover, Jacobsthal primes are also defined by the following algebraic

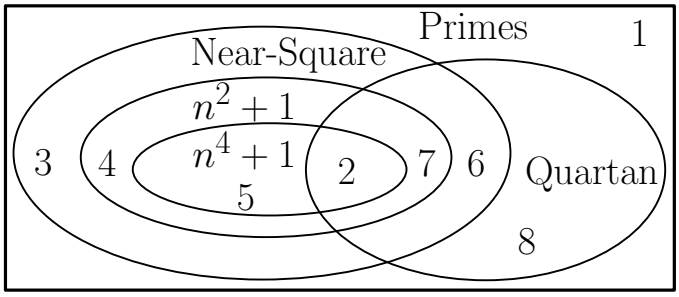


Figure 5: Venn diagram demonstrating the relationships between primes of the indicated types (see Point 7 of § 4.1.10).

• Wagstaff: $W_p = (2^p + 1)/3$ where p is an odd prime (see § 2.1.87).

As indicated previously, every Jacobsthal prime is a Wagstaff prime and vice versa excluding $J_4 = 5$ which is a Jacobsthal prime but not a Wagstaff prime (see § 2.1.36 and § 2.1.87). In fact, the indices n of the Jacobsthal primes (excluding $J_4 = 5$) are the same indices p of the Wagstaff primes. This means that the indices of the Jacobsthal primes (excluding $J_4 = 5$) are all prime numbers, and hence $J_4 = 5$ is the only Jacobsthal prime with a composite index. Also see § 3.2.6.

4.1.12 Factorial, Primorial and Compositorial Primes

The algebraic forms of these types of prime numbers are:
• Factorial: $n! \pm 1$ where $n \in \mathbb{N}$ (see § 2.1.19).
• Primorial: $P^{\pm}_{p_n} = p_n\# \pm 1$ (see § 2.1.64).
• Compositorial: $(n!/n\#) \pm 1$ where $n \in \mathbb{N}$ (see § 2.1.9).

As we see, these types have some similarities in their algebraic form (which reflects structural similarities). The relationships between these prime types are outlined in the following points:

1. Factorial, primorial: apart from the broad structural similarity between these types of prime as products of a sequence of smaller integers (i.e. all integers up to n for factorial, and all primes up to p_n for primorial) ± 1, these types of prime numbers do not seem to have inherent common features. The only known (and likely the only possible) primes which are factorial and primorial simultaneously are: 2, 3, 5, 7. Also see Point 4.
2. Factorial, compositorial: apart from the broad structural similarity between these types of prime as products of a sequence of smaller integers (i.e. all integers up to n for factorial, and all non-primes up to n for compositorial) ± 1, these types of prime numbers do not seem to have inherent common features. The only known (and likely the only possible) primes which are factorial and compositorial simultaneously are: 2, 3, 5, 23. Also see Point 4.
3. Primorial, compositorial: apart from the broad structural similarity between these two types of prime as products of a sequence of smaller integers ± 1, these types of prime numbers do not seem to have inherent common features. The only known (and likely the only possible) primes which are primorial and compositorial simultaneously are: 2, 3, 5. Also see Point 4.
4. Factorial, primorial, compositorial: these types of prime numbers have some common (but broad) features. The most obvious of these features are outlined in the following points:
   • Structural similarity: these types of prime numbers arise from a shared construction idea by taking a product of a sequence of natural numbers with a highly structured meaning followed by adding or subtracting 1 to ensure that the resulting integer is not divisible by any member of the underlying

form: $J_n = \lfloor 2^n/3 \rceil$ (i.e. the nearest integer to $2^n/3$) where $n \in \mathbb{N}_0$.

sequence, thereby eliminating a large set of potential divisors. In short, these types of prime numbers are structurally similar in a rather broad sense (as explained in the previous points).

• Extremely rapid growth: the primes defined by the algebraic forms of these types (as given above) grow in size very quickly. Accordingly, finding and prime-testing of these primes are mostly difficult and computationally demanding, and this makes the number of the known primes of these types relatively small. What makes the search and test of these primes more difficult is the lack of specialized and exceptionally-fast primality tests (or other specialized and efficient methods) for these primes, unlike, for instance, Mersenne primes which benefit (in search and test) from specialized and exceptionally-fast deterministic tests like Lucas-Lehmer test (see § 7.3.10).[412]

• Sparsity: The extremely rapid growth of the underlying factorial, primorial, and compositorial sequences (see the previous point) suggests that primes of these types are all expected to be very sparse. However, while they share this qualitative feature, their actual sparsity may differ because the density of candidates and the probability of primality depend on the specific form of each sequence.

• Possibility of twin prime pairs: the ± 1 in the algebraic forms of these types (as given above) makes these primes potential candidates for twin prime pairs (or rather raise the curiosity or draw the attention to being twin primes if an integer is identified as a prime of one of these types, noting that there is no special reason to have a twin prime pair in such situation in the absence of other indications). An example of factorial twin primes is (5, 7) which is the only known (and possibly the only existing) twin factorial prime pair with the same n (i.e. $n = 3$), noting that (3, 5) is another example but with different n (i.e. $n = 2$ for 3 and $n = 3$ for 5). Examples of primorial twin prime pairs are (3, 5), (5, 7) and (29, 31) where the pairs in the latter two arise from the same primorial base, i.e. $p_n = 3$ for (5, 7) and $p_n = 5$ for (29, 31), noting that for (3, 5) we have $p_n = 2$ for 3 and $p_n = 3$ for 5. Examples of compositorial twin prime pairs are (3, 5) and (191, 193) noting that the pairs in these two share the same index (i.e. $n = 4$ and $n = 8$ respectively).

• Euclidean-type: the factorial, primorial, and compositorial primes may be considered to be of "Euclidean-type" because they follow the construction style of Euclid's proof of the infinitude of primes. However, the "strict" Euclidean-type should be restricted to the primorial primes of the form $p_n\# + 1$ (see Point 1 of § 2.1.64).

We should finally note that the factorial, primorial, and compositorial primes have rare (and coincidental) overlap. Such overlap occurs mostly (and possibly only) among the very small primes. Examples of primes which are factorial, primorial, and compositorial simultaneously are: 2, 3, 5.[413]

4.1.13 Fortunate Primes

The algebraic form of this type of prime numbers is:

• Fortunate: $q - p_n\#$ where $p_n\#$ is the n^{th} primorial number of the first kind, q is the smallest prime number strictly greater than $p_n\# + 1$, and $n \in \mathbb{N}$ (see § 2.1.22).

Despite the appearance of this form (which has similarity with the form of the primorial primes), we did not include the fortunate prime type in the previous subsection (see § 4.1.12) because the nature and properties of this type (as indicated in its definition) are different from those of the types of § 4.1.12. So, there is no significant relationship between this type and those of § 4.1.12. This may be indicated by the seemingly high density (or frequency) of fortunate primes compared to the low density of those of § 4.1.12

[412] We should note that the coprimality of any prime of these types to all of its constituent factors (i.e. the factors of $n!$, $p_n\#$, $n!/n\#$ respectively) should have some (although little) beneficial computational efficiency. We should also note that substantial computational efficiency gain may be obtained from some tests for specific types of these primes due to their specific form (e.g. Lucas test for factorial primes) although these are not analogous to the Lucas-Lehmer test in terms of efficiency or universality.

[413] In fact, the overlap beyond 5 is very unlikely (and seemingly unknown or even impossible, which may result in an open problem or conjecture regarding the existence of more overlapping primes of these types).

(as may be revealed by inspecting the growth rate of the size of the numbers in the sequences of these prime types). However, there is some overlap among these types especially within the very small prime numbers. For example, 3, 5, 23 are common to the fortunate, factorial and compositorial primes, while 3, 5, 7 are common to the fortunate, factorial and primorial primes.

4.1.14 Cuban, Euler and Pythagorean Primes

The algebraic forms of these types of prime numbers are:

• Cuban: $3y^2 + 3y + 1$ (for the first kind) and $3y^2 + 6y + 4$ (for the second kind) where $y \in \mathbb{N}$ (see § 2.1.11).[414]

• Euler: $n^2 + n + 41$ where $n \in \mathbb{N}_0$ (see § 2.1.18).

• Pythagorean: $4k + 1$ where $k \in \mathbb{N}$ (see § 2.1.66).

As we see, these types have similarities in their algebraic form (mainly as being represented by polynomial expressions). The relationships between these prime types are outlined in the following points:

1. Cuban, Euler: these types have an obvious similarity in their algebraic form, i.e. they are both defined by quadratic polynomials and hence they are both "quadratic primes". In fact, both types highlight and demonstrate how certain quadratic forms can generate sequences of prime numbers. Also, both types may be studied as examples of how algebraic structures can influence primality of integers. Beyond this, no deeper structural (or systematic) relationships between these types of prime numbers are known and hence their overlap is coincidental and sporadic. Examples of primes which are cuban and Euler simultaneously are: 61, 547.
2. Cuban, Pythagorean: these types have some similarity in their algebraic form, i.e. they are both defined by polynomial expressions. They also have a structural similarity because of their modular similarity since $4k + 1 \overset{4}{=} 1$, and $3y^2 + 3y + 1 \overset{4}{=} 1$ for the cases $y \overset{4}{=} 0, 3$, and $3y^2 + 6y + 4 \overset{4}{=} 1$ for the cases $y \overset{4}{=} 1, 3$ (which makes cuban primes expressible as $4k + 1$ in these cases and hence be Pythagorean). So, all cuban primes of the first kind for $y \overset{4}{=} 0, 3$ and of the second kind for $y \overset{4}{=} 1, 3$ are Pythagorean (i.e. the two sets overlap for half of the modular values generated by the cuban prime polynomials).[415] Accordingly, these types have a significant overlap, e.g. 13, 37, 61, 109, 193, and 397 are a few examples of primes which are cuban and Pythagorean simultaneously.
3. Euler, Pythagorean: these types have some similarity in their algebraic form, i.e. they are both defined by polynomial expressions. They also have a structural similarity because of their modular similarity since $4k + 1 \overset{4}{=} 1$ and $n^2 + n + 41 \overset{4}{=} 1$ for the cases $n \overset{4}{=} 0, 3$ (which makes Euler primes expressible as $4k + 1$ in these cases and hence be Pythagorean). So, all Euler primes for $n \overset{4}{=} 0, 3$ are Pythagorean (i.e. the two sets overlap for half of the modular values generated by Euler's prime polynomial). Accordingly, these types have a significant overlap, e.g. 41, 53, 61, 97, and 113 are a few examples of primes which are Euler and Pythagorean simultaneously.
4. Cuban, Euler, Pythagorean: these types of prime numbers are connected through the ways they are expressed as special algebraic forms. They share a deep foundation in quadratic forms and modular arithmetic. Pythagorean primes are the broadest of these types as their modular form is common among prime numbers (noting that odd primes are either of the form $4k + 1$ or of the form $4k - 1$ where $k \in \mathbb{N}$). However, prime numbers which are cuban, Euler, and Pythagorean simultaneously are rare; the known example of such primes (at least among low value primes) is 61. We should finally notice that all these types of prime numbers share the property of having some geometric meaning and significance as outlined below:

   • As indicated earlier (see Point 5 in § 2.1.11), every cuban prime of the first kind is a centered hexagonal

[414] Cuban may also be given by the form $(x^3 - y^3)/(x - y)$ where $x, y \in \mathbb{N}$ and $x = y + 1$ or $x = y + 2$.

[415] In reality, all the cuban primes of the second kind are Pythagorean, while only some of the cuban primes of the first kind are Pythagorean. This is related to the modular parity of y which we indicated already.

number (which possesses an obvious geometric significance). We should also note that $3y^2+3y+1$ and $3y^2+6y+4$ represent parabolic curves (which is another geometric significance).

• Euler primes are given by the quadratic form n^2+n+41 (for some values of $n \in \mathbb{N}_0$) which geometrically represents parabolic curves.

• Pythagorean primes have the most direct geometric meaning (as suggested by their name), i.e. every Pythagorean prime represents the square length of hypotenuse of a right triangle with integer legs.[416] We should note in this context that Pythagorean primes can be uniquely expressed as a sum of two perfect squares (remembering Fermat's two-square theorem which requires an odd prime to be a sum of two squares *iff* it is of the form $4k+1$; see § 5.1.41). In fact, Pythagorean primes have another geometric significance in the context of Gaussian integers where each such prime represents the norm of a Gaussian prime, corresponding to the squared distance from the origin of a lattice point in the complex plane (see § 9.4.1).

4.1.15 Fermat and Pythagorean Primes

The algebraic forms of these types of prime numbers are:

• Fermat: $2^{2^m}+1$ where $m \in \mathbb{N}_0$ (see § 2.1.20).

• Pythagorean: $4n+1$ where $n \in \mathbb{N}$ (see § 2.1.66).

For $m > 0$ Fermat primes can be written as $2^2 \times 2^{2^m-2}+1 = 4(2^{2^m-2})+1$, i.e. they are of the form $4k+1$. Accordingly, all Fermat primes (excluding 3 which corresponds to $m = 0$) are Pythagorean primes.

4.1.16 Leyland Primes

As seen earlier (refer to § 2.1.38), the Leyland primes are of the form x^y+y^x (and of the form x^y-y^x for the second kind) for integers $x, y > 1$. The algebraic form of Leyland primes does not look like that of any other type of prime numbers and hence this unique type is a category of its own with no inherent relationship with other types of the *algebraic form*-based prime types. In fact, the distinction of the Leyland primes in their algebraic form (as exemplified by having two non-correlated variables) and the rather arbitrariness of their structure (as seen in their "strange" algebraic form) should justify the uniqueness of this type.[417]

4.1.17 Cyclotomic Primes

Cyclotomic primes are of the form $\Phi_n(2)$, where $\Phi_n(x)$ is the n^{th} cyclotomic polynomial (see § 2.1.14), and hence they are also characterized by their algebraic form (even though this algebraic form is broad and rather vague). Therefore, they deserve some attention in this section. In fact, the relationships between the cyclotomic primes and the other types of prime numbers of the "Algebraic Form" category are rather lengthy and involved subject (noting that many traditional prime types are specific cyclotomic instances at $x = 2$). However, we need to refer to some basic facts in this regard which the reader must be aware of (noting that these facts are just a sample of such facts):

1. Cuban primes (see § 2.1.11) are not cyclotomic although they have some overlap, e.g. 7, 13 and 127 are cuban and cyclotomic simultaneously.[418]

[416] Actually, the converse is also true for odd primes, i.e. every odd prime that represents the square length of hypotenuse of a right triangle with integer legs is a Pythagorean prime. We should also note that every Pythagorean prime is itself the length of hypotenuse in a primitive Pythagorean triple.

[417] We note that although cuban primes are defined by an algebraic form of two variables, these two variables are correlated and hence cuban primes are essentially defined by a single variable. This is demonstrated by the fact that cuban primes are actually defined by the single-variable formulae: $3y^2+3y+1$ and $3y^2+6y+4$ (see Points 1 and 7 of § 2.1.11).

[418] Whether there are infinitely many primes which are cuban and cyclotomic simultaneously seems to be an open problem. We note that "are not cyclotomic" means inherently and intrinsically (and hence overlap is justified).

2. Cullen primes (see § 2.1.12) are not cyclotomic although they have some overlap, e.g. 3 is Cullen and cyclotomic simultaneously.[419]
3. Euler primes (see § 2.1.18) are not cyclotomic although they have some overlap, e.g. 43 and 151 are Euler and cyclotomic simultaneously.
4. Fermat, Mersenne, and Wagstaff primes (see § 2.1.20, § 2.1.41, and § 2.1.87) are cyclotomic, i.e. they are proper subsets of cyclotomic primes. Examples of cyclotomic primes which are not Fermat nor Mersenne nor Wagstaff are: 13, 73, 151.
5. The relationship between cyclotomic and generalized Fermat primes is complicated and it depends on the definition of generalized Fermat primes (see § 2.1.24). But in general there is some overlap between these two types of prime numbers (where the extent of overlap generally depends on the definition adopted for generalized Fermat primes).
6. The relationship between cyclotomic and generalized Mersenne primes is even more complicated and it depends on the definition of generalized Mersenne primes (which involves more complications; see § 2.1.25). But in general there is some overlap between these two types (where the extent of overlap generally depends on the definition adopted for generalized Mersenne primes).
7. Leyland primes (see § 2.1.38) are not cyclotomic but they overlap in numbers like 17 (and 7 of the second kind) noting that such examples are very rare (as these types are fundamentally different in their algebraic form and structure).
8. Pierpont primes (see § 2.1.60): there is a partial overlap between cyclotomic primes and Pierpont primes, but the overlap consists partly (and possibly essentially) of the Fermat primes. Examples of primes which are cyclotomic but not Pierpont include most large Mersenne and Wagstaff primes. Examples of primes which are Pierpont but not cyclotomic are: 19, 37, 97, 109. Examples of primes which are cyclotomic and Pierpont simultaneously are Fermat primes (as well as 7 and 73 of non-Fermat).
9. Proth primes (see § 2.1.65): there is a partial overlap between cyclotomic primes and Proth primes. Examples of primes which are cyclotomic but not Proth are: 7, 31, 73, 151. Examples of primes which are Proth but not cyclotomic are: 41, 97, 113, 193. Examples of primes which are cyclotomic and Proth simultaneously are: 3, 5, 13, 17.
10. Riesel primes (see § 2.1.71): there is a partial overlap between cyclotomic primes and Riesel primes. Examples of primes which are cyclotomic but not Riesel are: 5, 13, 17, 43, 73. Examples of primes which are Riesel but not cyclotomic are: 23, 47, 79. Examples of primes which are cyclotomic and Riesel simultaneously are: 3, 7, 11, 31.
11. Woodall primes (see § 2.1.93): it seems that the only known prime numbers which are cyclotomic and Woodall simultaneously are $M_3 = 2^3 - 1 = 2^2 \cdot 2 - 1 = 7$ and $M_{521} = 2^{521} - 1 = 2^{512} \cdot 512 - 1$ (but this requires further checks). If so then we may have an open problem (and possible conjecture), e.g. the only prime numbers which are both cyclotomic and Woodall are M_3 and M_{521}.

4.1.18 Accidental Overlaps

There are many overlaps between the prime types of different algebraic forms, and we label such overlaps as "accidental" (or coincidental or casual) to distinguish them from inherent overlaps (i.e. those between prime types of similar forms such as Cullen and Pierpont).[420] Examples of accidental overlaps are:

[419] Apparently, 3 is the only known Cullen and cyclotomic prime simultaneously. Whether 3 is the only possible such prime (or there are other finitely-many/infinitely-many such primes) seems to be an open problem. We note that such potential open problems (i.e. the possibility of uniqueness of the given examples, or the existence of finitely-many/infinitely-many such primes) apply to some of the following points (and hence we do not repeat such footnote, noting that the possibility of such open problems and their nature can usually be determined from the specific case and context).

[420] Actually, we may define "accidental overlaps" more specifically as those overlaps between dissimilar types due to the lack of formal and structural relationships between these types (i.e. they have no common features in their algebraic form or structural properties).

1. Fermat and Mersenne primes overlap in number 3 (which is the only prime that is Fermat and Mersenne simultaneously).
2. Mersenne and Pierpont primes overlap in numbers 3 and 7 (which are the only primes of Mersenne and Pierpont types simultaneously).[421]
3. Some of the previous overlaps (e.g. in the cyclotomic category; see § 4.1.17) may also be regarded as accidental overlaps (e.g. due to the lack of formal and structural relationships between cyclotomic primality and some of the other types of primality).
4. There are many examples of overlap between Wagstaff and other types of primes.[422] For instance:
   - Wagstaff and Fermat primes overlap in number 3 only.
   - Wagstaff and Mersenne primes overlap in number 3 only.
   - Wagstaff and Pierpont primes overlap in number 3 only.
   - Wagstaff and Proth primes overlap in number 3 only.
   - Wagstaff and Riesel primes overlap in 3 and 11 only.

4.2 Digit Manipulation and Pattern

This section is supposed to investigate the relationships and comparisons between the base-dependent prime types which were investigated (i.e. grouped and categorized) in § 3.2.2. However, what we actually investigate in this section are the relationships and comparisons between the base-dependent prime types that are characterized mainly by their digit manipulation and pattern (where the investigation will be structured within the following subsections to identify and outline such relationships and comparisons). This is because there are hardly any relationships that deserve attention and investigation among the base-dependent prime types which are not characterized by digit manipulation and pattern. However, we will refer to these (non-digit) types occasionally and briefly in this section to complete the investigation of base-dependent prime types (even though the title of this section is chosen to reflect the actual content of this section).

Before we go through this investigation we would like to draw the attention to the following remarks (which are mainly about the prime types of § 3.2.2 noting that the present section partially mirrors § 3.2.2 as indicated already):

1. The base-dependent prime types may be classified with regard to digit manipulation and pattern operations (which characterize certain primality types according to the formal definitions of those types) into three main categories:[423]
   - Digit manipulation category which includes the following prime types: circular, delicate, emirp, happy, minimal, palindromic, permutable, primeval, reversible, self, and truncatable.
   - Digit pattern category which includes the following prime types: dihedral, pandigital, repunit, and strobogrammatic.
   - Neither (manipulation nor pattern) category which includes the following prime types: full reptend, home, Smarandache-Wellin, and unique.
2. Full reptend primes (see § 2.1.23), happy primes (see § 2.1.27), home primes (see § 2.1.31), primeval primes (see § 2.1.63), self primes (see § 2.1.73), and unique primes (see § 2.1.85) are unique in their definitions and characteristics and hence they have no fundamental relationships with other prime types (whether among themselves or with prime types of this section or with other prime types in general).
3. All relationships and comparisons of prime types which are base-dependent assume having a common

[421] We mean Pierpont primes of the first kind noting that Mersenne primes are a proper subset of Pierpont primes of the second kind.

[422] As noted earlier, Wagstaff primes are a proper subset of cyclotomic primes (noting that this is beyond "accidental overlap", i.e. it is structural). We should also note that there is no known intersection between Wagstaff and Woodall primes (noting that the impossibility of such intersection can be an open problem and a subject of conjectures).

[423] In fact, this classification is not exact with regard to some of these types.

base (which is usually base 10) unless stated otherwise.

4.2.1 Circular, Permutable, and Repunit Primes

These types of prime numbers are defined as follows:
• Circular: remains prime under all cyclic permutations of its digits (see § 2.1.7).
• Permutable: remains prime under any permutation of its digits (see § 2.1.58).
• Repunit: all its digits are 1 (see § 2.1.69).

The relationships between these prime types are depicted graphically in the Venn diagram of Figure 6. We note the following:
1. Examples of circular primes that are not permutable are: 197, 1193, 3779.
2. Examples of permutable (and hence circular) primes that are not repunit are: 79, 113, 199, 337.
3. Examples of repunit (and hence permutable and circular) primes are: U_2, U_{19}, U_{23}.

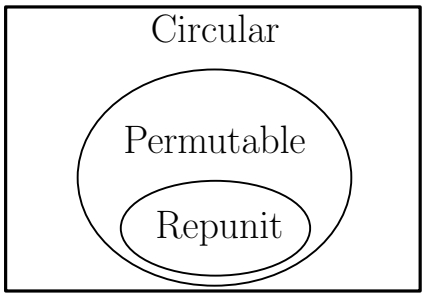


Figure 6: Venn diagram demonstrating the relationships between primes of the indicated types (see § 4.2.1).

4.2.2 Emirp, Palindromic, Repunit, and Reversible Primes

These types of prime numbers are defined as follows:
• Emirp: results in another prime when its digits are reversed (see § 2.1.17).
• Palindromic: (and palindromic wing) remains the same when its digits are reversed (see § 2.1.53 and § 2.1.54).
• Repunit: all its digits are 1 (see § 2.1.69).
• Reversible: remains prime when its digits are reversed (see § 2.1.70).

The relationships between these prime types are depicted graphically in the Venn diagram of Figure 7. We note the following:
1. Emirp and palindromic primes partition the entire set of reversible primes (and hence no prime belongs to the zone outside the zones of "Emirp" and "Palindromic" in Figure 7).[424]
2. By definition, repunit primes are palindromic but not palindromic wing.
3. Examples of each one of these types are given in the subsections of § 2.1.

4.2.3 Emirp, Permutable, Repunit, and Reversible Primes

These types of prime numbers are defined as follows:
• Emirp: results in another prime when its digits are reversed (see § 2.1.17).
• Permutable: remains prime under any permutation of its digits (see § 2.1.58).
• Repunit: all its digits are 1 (see § 2.1.69).

[424] We note that single-digit primes, which are palindromic, are "reversible".

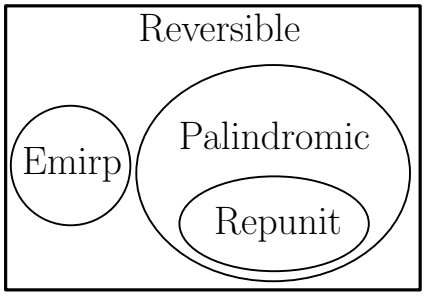


Figure 7: Venn diagram demonstrating the relationships between primes of the indicated types (see § 4.2.2).

• Reversible: remains prime when its digits are reversed (see § 2.1.70).

The relationships between these prime types are depicted graphically in the Venn diagram of Figure 8. We note the following:

1. Emirp and permutable primes do not partition reversible primes (i.e. there are reversible primes which are neither emirp nor permutable; moreover, emirp and permutable primes overlap).
2. Examples of reversible primes which are neither emirp nor permutable (i.e. zone 1 of Figure 8) are: 151, 181, 191, 353, 383.
3. Examples of emirp primes which are also permutable (i.e. zone 2) are: 37, 79, 113, 199, 337.
4. Examples of emirp primes which are not permutable (i.e. zone 3) are: 107, 149, 157, 167, 179.
5. Examples of permutable primes which are neither emirp nor repunit (i.e. zone 4) are: 131, 373, 919.

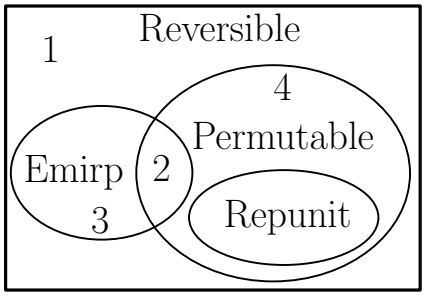


Figure 8: Venn diagram demonstrating the relationships between primes of the indicated types (see § 4.2.3).

4.2.4 Palindromic, Permutable, Repunit, and Reversible Primes

These types of prime numbers are defined as follows:

• Palindromic: (and palindromic wing) remains the same when its digits are reversed (see § 2.1.53 and § 2.1.54).

• Permutable: remains prime under any permutation of its digits (see § 2.1.58).

• Repunit: all its digits are 1 (see § 2.1.69).

• Reversible: remains prime when its digits are reversed (see § 2.1.70).

The relationships between these prime types are depicted graphically in the Venn diagram of Figure 9. We note the following:

1. Palindromic and permutable primes do not partition reversible primes (i.e. there are reversible primes which are neither palindromic nor permutable; moreover, palindromic and permutable primes overlap).

2. Examples of reversible primes which are neither palindromic nor permutable (i.e. zone 1 of Figure 9) are: 107, 149, 157, 167, 179.
3. Examples of palindromic primes which are also permutable but not repunit (zone 2) are: 131, 373, 919.
4. Examples of palindromic primes which are not permutable (zone 3) are: 151, 181, 191, 313, 353, 383.
5. Examples of permutable primes which are not palindromic (zone 4) are: 97, 113, 311, 199, 991, 337, 733.

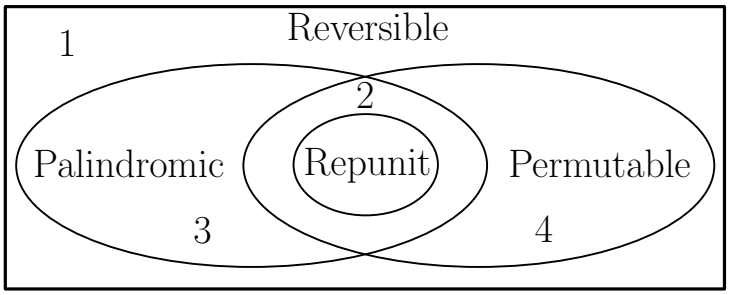


Figure 9: Venn diagram demonstrating the relationships between primes of the indicated types (see § 4.2.4).

4.2.5 Minimal and Truncatable Primes

These types of prime numbers are defined as follows:
- Minimal: does not contain any other prime as a sub-sequence of its digits (see § 2.1.45).
- Truncatable: remains prime when digits are truncated from either side or both sides (see § 2.1.83).

The relationships between these prime types (in base 10) are outlined in the following points:
1. Minimal primes vs (left-, right- and two-sided) truncatable primes: these types overlap only in single-digit primes. This is because any multi-digit (left-, right- and two-sided) truncatable prime necessarily contains a smaller prime sub-sequence, and hence it cannot satisfy the definition of minimal prime.
2. Minimal primes vs (left-and-right) truncatable primes: these types overlap only in the set {2, 3, 5, 7, 11, 19, 41, 61, 89}. For primes with more than two digits, these types are disjoint sets because any multi-digit (left-and-right) truncatable prime necessarily contains a smaller prime sub-sequence, and hence it cannot be a minimal prime.

We should finally note that minimal and truncatable primes have a common feature of having only finitely many members (at least in base 10; see § 2.5).

4.2.6 Delicate and Minimal Primes

These types of prime numbers are defined as follows:
- Delicate: becomes composite if any one of its digits is replaced (see § 2.1.15).
- Minimal: does not contain any other prime as a sub-sequence of its digits (see § 2.1.45).

The common feature of these prime types is that they are about the stability (or fragility) of their primality under specific digit-based manipulations, even though the two types work on different rules (i.e. delicate is about the effect of digit substitution, while minimal is essentially about digit deletion). Anyway, considering that there are only 26 minimal primes (in base 10) none of which is delicate, we can say that these prime types are disjoint sets.

4.2.7 Dihedral, Palindromic, Pandigital, Repunit and Strobogrammatic Primes

These types of prime numbers are defined as follows:
• Dihedral: remains prime under certain reflectional and rotational visual symmetries (noting that it is restricted to base 10 and within a seven-segment display; see § 2.1.16).
• Palindromic: (and palindromic wing) remains the same when its digits are reversed (see § 2.1.53 and § 2.1.54).
• Pandigital: includes in its significant digits every digit used in its base at least once (see § 2.1.55).
• Repunit: all its digits are 1 (see § 2.1.69).
• Strobogrammatic: its numeral appears the same when rotated 180 degrees (see § 2.1.78).

The main characteristic feature of these prime types is that they are mainly about digit pattern (rather than digit manipulation or something else; see § 3.2.2).[425] The relationships between these prime types are outlined in the following points:
1. Dihedral, palindromic: palindromic primes made entirely of the digits 0, 1, and 8 are dihedral primes.
2. Dihedral, repunit: repunit primes are a proper subset of dihedral primes.
3. Dihedral, strobogrammatic: strobogrammatic primes made entirely of the digits 0, 1, and 8 are dihedral primes.
4. Palindromic, repunit: repunit primes are a proper subset of palindromic primes.
5. Palindromic, strobogrammatic: strobogrammatic primes made entirely of the digits 0, 1, and 8 are palindromic primes.
6. Repunit, strobogrammatic: repunit primes are a proper subset of strobogrammatic primes.
7. Dihedral, palindromic, strobogrammatic: dihedral primes made entirely of the digits 0, 1, and 8 and are also palindromic are strobogrammatic.
8. Pandigital: pandigital primes and dihedral/repunit/strobogrammatic primes do not overlap even casually, i.e. no number can be a pandigital prime and one of these three prime types in the same base (which is base 10 in the present context). Accordingly, pandigital primes and these prime types are pairwise disjoint sets (both conceptually and in practice). Regarding palindromic primes, there are known examples of pandigital palindromic primes (e.g. 1023985674765893201 in base 10).[426] There are similar examples in other bases (e.g. 101 in base 2 which represents 5 in decimal, and 20102 in base 3 which represents 173 in decimal). Whether pandigital palindromic primes exist in every base requires further investigation.

4.2.8 Smarandache-Wellin and Truncatable Primes

These types of prime numbers are defined as follows:
• Smarandache-Wellin: formed by concatenating the first n prime numbers in their increasing order (see § 2.1.75).
• Truncatable: remains prime when digits are truncated from either side or both sides (simultaneously or alternately; see § 2.1.83).

There is no fundamental or direct mathematical relationship between Smarandache-Wellin and truncatable primes. However, they share a broad structural feature of digit construction/destruction, i.e. one involves constructing numbers by concatenation while the other involves destroying numbers by truncation. Moreover, there is some casual overlap between them (which is rare and seems to occur only in very small numbers).[427]

[425] In fact, palindromic can be both.
[426] See `https://t5k.org/curios/page.php/1023985674765893201.html`.
[427] Apparently, the only known prime numbers that are Smarandache-Wellin and truncatable simultaneously are 2 and 23. In fact, (at least) for right-truncatable primes (and hence two-sided truncatable as well), it can be proven that 2 and 23 are the only possible such primes. For $n \geq 3$, every Smarandache-Wellin number begins with 235, and successive right

4.2.9 Fragile and Robust Primality under Digit Operations

From the perspective of the stability of primality (in various senses and degrees) of prime numbers under the (actual or virtual) operations related to *digit manipulation and pattern*, we may classify (most of) the prime types in the group of *digit manipulation and pattern* into two broad categories:[428]

1. Fragile primes, i.e. those primes which lose their primality under the designated operations. The following prime types fall into this category: delicate and minimal primes.[429]
2. Robust primes, i.e. those primes which keep their primality under the designated operations. The following prime types fall into this category: circular, emirp, palindromic, permutable, reversible, truncatable, dihedral, and strobogrammatic.[430]

4.3 Divisibility and Modularity

The present section is dedicated to the relationships and comparisons between the prime types which are characterized by having some divisibility or modularity element in their identification (as indicated in their formal definitions). In fact, these types were grouped and categorized in § 3.2.3, and hence the present section (with regard to relationships and comparisons) is the twin section to that section (with regard to grouping and categorization). In fact, we can hardly find fundamental relationships (apart from the common feature of divisibility and modularity which mostly is also superficial) among these prime types (i.e. among themselves as well as with prime types of other groups and categories). However, we will investigate in the following subsections two groups (one characterized by irregularity/regularity and the other by having a similar kind of divisibility requirement) as the similarity between the types of each of these groups is sufficiently strong (and hence their relationships and comparisons deserve attention and investigation).

The other types in the "Divisibility and Modularity" class of this section (namely: harmonic, Higgs, Mersenne divisor, Pillai, and Pythagorean primes)[431] will not be investigated in this section as they lack sufficient similarities (among themselves or with other types) that can be the basis for significant relationships and comparisons. Yes, there are some accidental overlaps (among themselves or with other types). In fact, Pythagorean primes are so broad and abundant (as they make almost half of the primes; but also see § 8.7.1) that is there is hardly any prime type without significant overlap with them (at least in theory).[432]

4.3.1 Irregular and Regular Primes

These types of prime numbers are defined as follows:

• Bernoulli irregular: odd prime p that divides the numerator of at least one of the Bernoulli numbers B_n for $n = 2, 4, \ldots, p-3$; otherwise, it is B-regular (see § 2.1.32).

• Euler irregular: odd prime p that divides at least one of the Euler numbers E_n for $n = 2, 4, \ldots, p-3$; otherwise, it is E-regular (see § 2.1.33).

truncation eventually produces 235, which is composite. Further investigation is required for non-decimal bases.

[428] We note that this subsection is essentially philosophical and epistemological in nature, inviting a more contemplative mode of reflection. Although it may not fit well within the present section, we have not found a more suitable place for it elsewhere in the book.

[429] For minimal primes, we virtually remove digits to obtain sub-sequences (and hence the operation in this case is digit deletion).

[430] If we stretch the given criterion for robust primes, we may even include primeval primes.

[431] We note that Pythagorean primes have been investigated previously within the category of "Algebraic Form" (see § 4.1) based on their characterization by the algebraic form $4k + 1$. In this regard we should remind the reader of Point 7 of § 2.1.66 which is important for the distinction between the two definitions of Pythagorean primes.

[432] But we should note (for instance) that Mersenne primes (which are a proper subset of Mersenne divisors) are non-Pythagorean (see § 4.1.7). Wagstaff primes (see § 2.1.87) and safe primes excluding 5 (see § 2.1.72) are also non-Pythagorean.

• Genocchi irregular: odd prime p that divides at least one of the Genocchi numbers G_n for $n = 2, 4, \ldots, p-3$; otherwise, it is G-regular (see § 2.1.34).

The relationships and comparisons between these prime types are discussed briefly in the following remarks:

1. The main relationships between these prime types lie in their shared connection to certain number theoretic sequences that embed subtle divisibility properties. In fact, there are significant relationships between some of these types of prime numbers based on their common feature of irregularity/regularity. For example, there is a structural alignment between some of these types that stems from explicit identities connecting their underlying sequences, such as the relation $G_n = 2(1 - 2^n)B_n$ that links Bernoulli and Genocchi numbers (see Point 2 of § 2.1.34). A deeper investigation of these issues will be given in the future volumes.
2. Every prime number that is Bernoulli irregular is also Genocchi irregular, but the converse is not true in general (e.g. 17, 31, 41, and 43 are Genocchi irregular but they are Bernoulli regular).[433]
3. Apart from the "total overlap" of the previous point (i.e. the Bernoulli irregular primes are a proper subset of the Genocchi irregular primes), there are sporadic overlaps among these prime types, e.g. 67 and 101 are common to Bernoulli and Euler irregulars, while 31 and 43 are common to Euler and Genocchi irregulars.
4. Bernoulli (ir)regularity is largely related to the study of cyclotomic fields, while Euler (ir)regularity is largely related to the study of quadratic fields, noting that Genocchi (ir)regularity seems to provide a bridge between the two.
5. Regular primes (of the B-, E- and G-types) attract less attention and research interest from mathematicians than irregular primes, and hence we ignore them here (but we should consider them in the future volumes of this book).
6. Referring to the previous point, there are several potential reasons for the more attention to irregular primes. For example:

   • Irregular primes represent the exceptions[434] (as reflected in their name "irregular") which challenges the existing mathematical frameworks in various topics and aspects (but we may note that they are the "regular" ones when it comes to the issue of infinitude as their infinitude is proven and this could be another reason for the more attention to them as this is linked to a number of mathematical problems and issues).[435]

   • Another reason is the historical significance of irregular primes (and the Bernoulli type in particular) noting that their study was motivated and driven by Fermat's last theorem and the search for its proof (which was until fairly recently the focus of massive search and research).

   • We may also note their link to some modern problems and conjectures since research into the irregular and regular primes often intersects with such topics and investigations (e.g. the cyclotomic and quadratic fields, the Kummer-Vandiver conjecture, and the Iwasawa theory).[436]
7. The relationships between the B-, E- and G-irregular prime types are depicted graphically in the Venn diagram of Figure 10. Examples of (where "zone" refers to the labeled areas in Figure 10):

   • Zone 1 (i.e. none): 2, 3, 5, 7, 11, 13, 23 (noting that 2 is explicitly excluded from the definitions because it is even).

---

[433] It is worth noting in this regard that the Bernoulli numbers and Genocchi numbers are linked through the identity $G_{2k} = 2(1 - 2^{2k})B_{2k}$ for $k \in \mathbb{N}$ (see the Note in § 2.1.34).

[434] In fact, they are the "exception" not only in their characteristics and behavior, but even on a statistical basis (noting that regular primes are statistically more common among known primes).

[435] While the infinitude of irregular primes is proven (in contrast with the conjectured infinitude of regular primes), we should remember that irregular primes are statistically less common than regular primes among listed primes. So, proven/unproven infinitude and statistical abundance among listed primes are logically and practically independent issues.

[436] In fact, this reason is shared between irregular and regular.

- Zone 2 (i.e. all): 67, 101, 149.
- Zone 3 (i.e. B- and G-irregular but not E-irregular): 59, 103, 131.
- Zone 4 (i.e. E- and G-irregular but not B-irregular): 31, 43, 137.
- Zone 5 (i.e. E-irregular only): 19, 47, 61.
- Zone 6 (i.e. G-irregular only): 17, 41, 73.

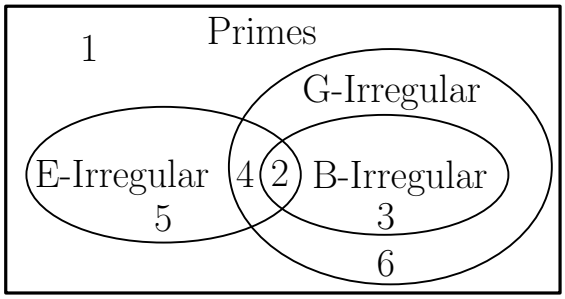


Figure 10: Venn diagram demonstrating the relationships between primes of the indicated types (see Point 7 of § 4.3.1).

4.3.2 Mirimanoff, Wall-Sun-Sun, Wieferich, Wilson and Wolstenholme Primes

These types of prime numbers are defined as follows:

- Mirimanoff: $p \in \mathbb{P}$ where p^2 divides $(3^{p-1} - 1)$. See § 2.1.46.
- Wall-Sun-Sun: $p \in \mathbb{P}$ such that p^2 divides the Fibonacci number $\mathcal{F}_{p-\left(\frac{p}{5}\right)}$. See § 2.1.88.
- Wieferich: $p \in \mathbb{P}$ where p^2 divides $(2^{p-1} - 1)$. See § 2.1.90.
- Wilson: $p \in \mathbb{P}$ where p^2 divides $(p-1)! + 1$. See § 2.1.91.
- Wolstenholme: $p \in \mathbb{P}$ where p^4 divides $C_{p-1}^{2p-1} - 1$. See § 2.1.92.

The relationships and comparisons between these prime types are outlined in the following remarks:

1. There are no common features among these classes apart from the divisibility element (of particular type) in their definition.[437]
2. These types are distinguished by their extreme rarity.[438]
3. There is no known overlap among these types (noting their rather bizarre nature and extreme rarity as indicated in the previous point).
4. Mirimanoff primes may be seen as a base-3 generalized Wieferich primes.

Finally, it is worth noting that the Wolstenholme primes are a proper subset of the Bernoulli irregular primes (and this may be seen as a link between the types of this subsection and the types of the previous subsection; see § 4.3.1).

4.4 Expressibility

Referring to § 3.2.4, the relationships between the prime types in this group (i.e. self, Stern and untouchable) do not exceed their broad similarity as being characterized by expressibility (or rather non-expressibility) in their formal definitions which may indicate their rather strange nature (and potential rarity; see Point 1). However, it is useful to note the following:

[437] In fact, some other (rather minor) features may also be added such as their historical link (mostly) to Fermat's last theorem.

[438] The only known Mirimanoff primes are 11 and 1006003. There is no known Wall-Sun-Sun prime. The only known Wieferich primes are 1093 and 3511. The only known Wilson primes are 5, 13 and 563. The only known Wolstenholme primes are 16843 and 2124679.

1. Stern and untouchable primes are extremely rare, i.e. there are only eight known Stern primes (which are: 2, 3, 17, 137, 227, 977, 1187, 1493) and only two known untouchable primes (which are: 2 and 5).
2. While it is conjectured that there are infinitely many self prime numbers (in every even base, noting that it is established for odd bases), it is conjectured that there are only finitely many Stern and untouchable primes. In fact, it is conjectured that the eight known Stern primes and the two known untouchable primes are the only such primes.[439]

4.5 Grouping and Association

Referring to § 3.2.5, the prime types whose members are characterized by having an element of association (or pairing or grouping) with other primes or integers (according to the definitions of these types) may be classified into two main kinds:

1. Those types which are explicitly and fundamentally defined by such associations (e.g. Chen, cousin, sexy, and twin primes).[440] These types of primes have been investigated (i.e. from the perspective of relationships and comparisons) as such within other sections (see for instance § 4.7).
2. Those types whose nature (according to their definitions) requires such associations implicitly (e.g. circular and permutable primes). Such associations are implicit and among the primes of each one of these types (e.g. the primes 13 and 31 which are associated as circular primes are both circular) and hence they do not deserve or incur relationships and comparisons on the basis of "Grouping and Association" (i.e. in the sense of this section, as between different prime types). Yes, such types deserve attention (from the perspective of relationships and comparisons) on other bases, which are directly and fundamentally taken in their definitions, such as "Digit Manipulation and Pattern" which belong to other sections of this chapter (see for instance § 4.2.1).

4.6 Indexing

In § 3.2.6 we grouped and categorized a number of prime types on the basis of "indexing", i.e. the members of these types are prime indexed by definition or formal identification (Mersenne, super, primorial, safe, Wagstaff), or they are prime indexed in reality but not formally (Fibonacci, Jacobsthal, Pell, repunit) or they are composite indexed (Fermat). Regarding the relationships between these types of prime numbers, we note that there is no fundamental relationship (based on their "indexing" status) between these types, i.e. neither between the types of each category nor between the types of different categories. So, if there is any relationship among these types it should be based on another criterion or status. There are also casual and rare overlaps among (the very small members of) some of these prime types. For example:

- 3 and 31 are common to the Mersenne and super primes.
- 3 and 5 are common to the super and Fibonacci primes.
- 3 and 5 are common to the Fibonacci and Jacobsthal primes.
- 3 and 5 are common to the super (as well as Fibonacci and Jacobsthal) and Fermat primes.

4.7 Interval Relationship

We investigate in this section the relationships and comparisons between the prime types that are characterized broadly by having interval-based relationships of their members with other primes or integers in their vicinity (see § 3.2.7). The prime types that we investigate in this section are: Chen, cousin, isolated, sexy, and twin.

[439] Regarding untouchable primes, the specific conjecture is that 5 is the only odd untouchable number (and hence prime). But since 2 is the only even prime, if this conjecture holds then 2 and 5 will necessarily be the only untouchable primes.

[440] In fact, even safe and Sophie Germain primes may be included in this kind if we extend the association to include such relationships.

4.7.1 Cousin, Sexy and Twin Primes

These types of prime numbers are defined as follows:
- Cousin: $(p, p+4)$ where p and $p+4$ are prime (see § 2.1.10).
- Sexy: $(p, p+6)$ where p and $p+6$ are prime (see § 2.1.74).
- Twin: $(p, p+2)$ where p and $p+2$ are prime (see § 2.1.84).

There are two kinds of comparison between cousin, sexy and twin prime numbers:
1. As pairs: these prime types are mutually exclusive, i.e. no pair of one of these types can be a pair of another type.
2. As individual numbers: prime numbers are partitioned (i.e. exhaustively and disjointly) with respect to their membership in the twin, cousin, and sexy prime types, into eight categories: none (e.g. 2), only twin (e.g. 149), only cousin (e.g. 487), only sexy (e.g. 251), only twin-cousin (e.g. 3), only twin-sexy (e.g. 5), only cousin-sexy (e.g. 23), twin-cousin-sexy (e.g. 7).

4.7.2 Isolated and Twin Primes

These types of prime numbers are defined as follows:
- Isolated: $p \in \mathbb{P}$ where $p-2$ and $p+2$ are both non-prime (see § 2.1.35).
- Twin: $(p, p+2)$ where p and $p+2$ are prime (see § 2.1.84).

Isolated primes and twin prime members partition the entire set of prime numbers. This should be obvious from the other name of isolated primes (i.e. non-twin primes; see § 2.1.35).[441]

4.7.3 Chen and Twin Primes

These types of prime numbers are defined as follows:
- Chen: $p \in \mathbb{P}$ such that $p+2$ is either prime or semiprime (see § 2.1.6).
- Twin: $(p, p+2)$ where p and $p+2$ are prime (see § 2.1.84).

There are two kinds of comparison between Chen and twin prime numbers:
1. As pairs: if we label $(p, p+2)$ a "Chen prime pair" (i.e. when p is a Chen prime), then we can say: twin prime pairs are a proper subset of Chen prime pairs. Examples of "Chen prime pairs" which are not twin prime pairs are (7, 9), (19, 21) and (23, 25).
2. As individual numbers: as indicated already (see § 2.1.6 and § 2.1.84), all lower members of twin prime pairs are necessarily Chen primes, but only some upper members of twin prime pairs are Chen primes. So, prime numbers are partitioned (i.e. exhaustively and disjointly) into four categories: primes which are both twin and Chen (e.g. 3, 5, 11), primes which are only Chen (e.g. 37, 53), primes which are only twin (e.g. 43, 73), and primes which are neither (e.g. 97).

4.8 Magnitude Comparison

We investigate in this section the relationships and comparisons between the prime types that are characterized broadly by the magnitude of their members in comparison to the (arithmetic or geometric) average of other primes in their surroundings (see § 3.2.8). The prime types that we investigate in this section are: balanced, good, strong, and weak.

4.8.1 Balanced, Strong and Weak Primes

These types of prime numbers are defined as follows:
- Balanced: $p_n = (p_{n-1} + p_{n+1})/2$ (see § 2.1.1).

[441] It should also be obvious that an isolated prime can be a member of cousin or sexy primes (e.g. 23).

• Strong: $p_n > (p_{n-1} + p_{n+1})/2$ (see § 2.1.79).
• Weak: $p_n < (p_{n-1} + p_{n+1})/2$ (see § 2.1.89).

We note the following:
1. Number 2 is the only prime that is neither balanced nor strong nor weak.
2. Balanced, strong and weak primes partition the set of the remaining primes (i.e. all odd primes).

So in short, prime numbers are partitioned into four categories: the number 2, balanced, strong, and weak.

4.8.2 Good Primes

Good primes are defined as follows:
• Good: $p_n > \sqrt{p_{n-i}p_{n+i}}$ for all $1 \leq i \leq (n-1)$. See § 2.1.26.

Good prime is obviously defined on the basis of its magnitude relative to the geometric mean of other primes in its surroundings (i.e. "equi-distance" on both sides in the sequence of prime numbers). So, it is unique in its nature (as characterized by its definition) and hence it is a category of its own with no fundamental relationships with other prime types. The closest analogue to good prime is strong prime[442] and hence the good primes type may be compared (based on a broad similarity) to the strong primes type (and more broadly to the category of balanced, strong, and weak primes which we investigated already in § 4.8.1). In this regard we note the following:
1. Both good and strong primes are defined by a "greater than" (i.e. $>$) comparison relation.
2. While good prime is related to geometric mean, strong prime is related to arithmetic mean.
3. While good prime looks at *all surrounding primes* (in the given sense of "equi-distance" on both sides), strong prime looks only at its immediate prime neighbors on both sides. Yes, if we adopt the second definition of good prime (see Point 2 in § 2.1.26) or extend the idea of strong prime to all surrounding primes (see Point 6 of § 2.1.79) then the correspondence (or similarity) is exact from this perspective.

4.9 Recreation

Referring to § 3.2.9, recreation is obviously a peripheral (or incidental or extraneous) basis for grouping and categorization of prime types as it is unrelated to the fundamental properties of prime numbers (or their types) and their mathematical nature or behavior (noting that "recreation" is about human rather than mathematical entities such as integers or primes). Hence, recreation is not a valid basis (neither theoretically nor in practice) for mathematically substantial or legitimate relationships and comparisons between the prime types.

Yes, most of the prime types within the recreation category of § 3.2.9 have other (and potentially more fundamental) bases for grouping and categorization (such as "digit and string manipulation" or "digital pattern" which were indicated in § 3.2.9), and they actually participate in groupings and categorizations of mathematical significance and nature. Such bases justify the search for legitimate relationships and comparisons of essential mathematical significance and value (i.e. under groupings and categorizations other than "recreation", as we did for instance in § 4.2).

4.10 Recursive Sequencing

We investigate in this section the relationships and comparisons between the prime types that are characterized mainly by being identified as prime types whose members are occurring in certain recursively-defined integer sequences (and hence they are defined inherently by specific recurrence relations). The

[442] The analogy becomes stronger if we adopt the second definition of good prime or extend the idea of strong prime (see Point 2 of § 2.1.26 and Point 6 of § 2.1.79).

prime types that we investigate in this section are: Bell, Fibonacci, Jacobsthal, Lucas, NSW, Padovan, partition, Pell, Perrin, and Tribonacci (see § 3.2.10).

4.10.1 Fibonacci, Jacobsthal, Lucas, NSW, Padovan, Pell, Perrin and Tribonacci Primes

The recursive formulae of the integer sequences to which the members of these prime types belong are:

- Fibonacci: $\mathcal{F}_0 = 0,\, \mathcal{F}_1 = 1$ & $\mathcal{F}_n = \mathcal{F}_{n-2} + \mathcal{F}_{n-1}$ (for $1 < n \in \mathbb{N}$). See § 2.1.21.
- Jacobsthal: $J_0 = 0,\, J_1 = 1$ & $J_n = 2J_{n-2} + J_{n-1}$ (for $1 < n \in \mathbb{N}$). See § 2.1.36.
- Lucas: $L_0 = 2,\, L_1 = 1$ & $L_n = L_{n-2} + L_{n-1}$ (for $1 < n \in \mathbb{N}$). See § 2.1.39.
- NSW: $N_0 = 1, N_1 = 7$ & $N_n = 6N_{n-1} - N_{n-2}$ (for $1 < n \in \mathbb{N}$). See § 2.1.51.
- Padovan: $P_0 = P_1 = P_2 = 1$ & $P_n = P_{n-3} + P_{n-2}$ (for $2 < n \in \mathbb{N}$). See § 2.1.52.
- Pell: $\mathcal{P}_0 = 0,\, \mathcal{P}_1 = 1$ & $\mathcal{P}_n = \mathcal{P}_{n-2} + 2\mathcal{P}_{n-1}$ (for $1 < n \in \mathbb{N}$). See § 2.1.57.
- Perrin: $\mathsf{P}_0 = 3,\, \mathsf{P}_1 = 0,\, \mathsf{P}_2 = 2$ & $\mathsf{P}_n = \mathsf{P}_{n-3} + \mathsf{P}_{n-2}$ (for $2 < n \in \mathbb{N}$). See § 2.1.59.
- Tribonacci: $T_0 = T_1 = 0,\, T_2 = 1$ & $T_n = T_{n-3} + T_{n-2} + T_{n-1}$ (for $2 < n \in \mathbb{N}$). See § 2.1.82.

In general, there are no fundamental relationships between these types of prime numbers apart from the broad similarity in their sequence-based definitions and some rare and occasional overlaps. However, some relationships and comparisons (as well as other relevant observations) are outlined in the following points:

1. All these prime types (or rather their parent sequences) are defined by linear recurrence relations with constant coefficients.
2. Fibonacci and Jacobsthal sequences differ only in the coefficient of the $n-2$ term in the sum of their recursive formulae.
3. Fibonacci and Lucas sequences differ only in their initial term, i.e. the zeroth term.
4. Fibonacci and Pell sequences differ only in the coefficient of the $n-1$ term in the sum of their recursive formulae.
5. Jacobsthal primes are also defined (through their parent sequence) by the following first order recurrence relations:
   $J_0 = 0$ and $J_{n+1} = 2^n - J_n$ $\left[\text{or } J_{n+1} = 2J_n + (-1)^n\right]$ (for $0 \leq n \in \mathbb{N}_0$).
6. Jacobsthal primes are also classified within the "Algebraic Form" category due to the multiple characterizing definitions of this type of prime (see § 4.1.11).
7. As indicated already, there are occasional overlaps among these types of primes. For instance, 3 and 5 are common to Fibonacci, Jacobsthal and Padovan primes, and 2 and 3 are common to Fibonacci, Lucas and Padovan primes, while 2 and 5 are common to Fibonacci, Padovan and Pell primes. However, such overlaps are generally among the very low-value primes, with seemingly no such overlaps observed among the very high-value primes of these types.

4.10.2 Bell Primes

The recursive formula of the integer sequence to which the members of the Bell primes belong is:

- Bell: $\mathscr{B}_{n+1} = \sum_{k=0}^{n} C_k^n \mathscr{B}_k$ where $\mathscr{B}_0 = 1$ and C_k^n is the binomial coefficient (see § 2.1.2).

As we see, this prime type is unique in its definition and characteristics with no obvious similarity to other prime types (apart from very broad features such as being recursively-defined which do not incur fundamental relationships with other prime types). The Bell sequence (unlike the sequences of § 4.10.1) does not have a fixed order (or degree) because it is defined by a variable-order recurrence relation.

4.10.3 Partition Primes

The recursive formula of the integer sequence to which the members of the partition primes belong is:

• Partition (see § 2.1.56): $P(a) = 0$ for all $a < 0$, $P(0) = 1$, and

$$P(n) = \sum_{k=1}^{\infty}(-1)^{k-1}\left[P\left(n - \frac{k(3k-1)}{2}\right) + P\left(n - \frac{k(3k+1)}{2}\right)\right] \qquad \text{(for } n \geq 1\text{)} \qquad (41)$$

As we see, this prime type is unique in its definition and characteristics, and hence what has been said already about Bell primes (see § 4.10.2) applies to partition primes. Similarly, the partition sequence (unlike the sequences of § 4.10.1) is defined by a variable-order recurrence relation (also see footnote [198]).

4.11 Other Considerations

Referring to § 3.2.11, it is obvious that the prime types in the "Other Considerations" group have various considerations (or bases) for grouping and categorization (and that is why they are grouped and categorized as "Other Considerations"). Hence, in general there are no fundamental relationships among the prime types of this group or between them and other prime types of other groups (other than what has been indicated already in that subsection). In the following two subsections we briefly discuss two categories of the "Other Considerations" group as examples for the nature of potential relationships and comparisons in this group and its categories.

4.11.1 Safe and Sophie Germain Primes

These types of prime numbers are defined as follows:
• Safe: $2p + 1$ is a safe prime *iff* p is also prime (see § 2.1.72).
• Sophie Germain: p is a Sophie Germain prime *iff* $2p + 1$ is also prime (see § 2.1.76).

As we see, these types of prime numbers are obviously related structurally, i.e. $p \in \mathbb{P}$ is a Sophie Germain prime *iff* $2p + 1$ is a safe prime, or alternatively $q \in \mathbb{P}$ is a safe prime *iff* $(q - 1)/2$ is a Sophie Germain prime.

4.11.2 Ramanujan Primes

This type of prime numbers is defined as follows:
• Ramanujan: smallest prime R_n such that there are at least n primes between $x/2$ and x for all $x \geq R_n$ (see § 2.1.68).[443]

As we see, the Ramanujan prime is unique in its nature (as characterized by its definition) which is based on its link to the distribution of other primes through the prime-counting function in this distinctive manner. Hence, there is no other type of primes (among the common types of prime numbers) that can be associated with it in one category or have a fundamental relationship or comparison with it, and hence the Ramanujan prime is a category of its own.

Yes, if we go beyond the prime types of § 2.1, then we may find some proper categorizations of the Ramanujan primes (and hence relationships and comparisons) with other prime types. For instance, the Ramanujan primes may be classified with the Chebyshev primes (see § 2.2.1) into one "distribution-based" category noting that both these prime types are defined by their relationship to the prime-counting function (or functions) at least according to some definitions of the Chebyshev primes.[444] Nevertheless, we do not see any fundamental relationship between the Ramanujan and Chebyshev prime types beyond

[443] This may also be stated more formally by the relation: $\pi(x) - \pi(x/2) \geq n$ for all $x \geq R_n$ (where $n \in \mathbb{N}$ and π is the prime-counting function; see § 8.2.1).
[444] In fact, even other potential definitions of the Chebyshev primes include an element of counting and distribution (see § 2.2.1).

their broad common feature as being related to the distribution and counting of prime numbers through the prime-counting function (or functions), noting that coincidental overlap does exist between these two types (as it usually exists between various types of prime numbers). For example, 181, 241, and 281 are Ramanujan and Chebyshev primes simultaneously (according to some definitions of the Chebyshev primes; see § 2.2.1).[445]

[445] Also see `https://oeis.org/A196667`.

Chapter 5
Theorems of Primes

In this chapter, we present a selected collection of common theorems and results (including corollaries of major theorems) concerning prime numbers, as well as closely related facts. These are organized and classified under a range of subject-based headings and categories, reflecting the rich diversity of topics and approaches to the subject. By examining prime numbers from multiple aspects and perspectives we aim to provide a broad and coherent overview that highlights both their fundamental properties and their deeper mathematical significance. We will also briefly investigate the relationships among these theorems and results. Alongside their classification, this should deepen our understanding of this collection of fundamental theorems and results, as well as of the theory of prime numbers more broadly.

5.1 Common Theorems on Primes

In the following subsections we list alphabetically and discuss briefly a number of common theorems about (or related to) prime numbers. This collection of selected theorems (alongside other "minor" theorems, corollaries and results which will be listed in the classification section; see the subsections of § 5.2) forms the main body of our current proven theoretical knowledge on prime numbers at the level of the present volume.

5.1.1 Baker-Harman-Pintz Theorem

This theorem is regarded as a landmark result in analytic number theory regarding the maximum gap between consecutive prime numbers. The theorem asserts that there is at least one prime number in the interval $[x - x^{0.525}, x]$ for any sufficiently large x. This result provides an upper bound on the difference between consecutive primes, showing that $(p_{n+1} - p_n) < p_n^{0.525}$ for large enough n. Unconditionally, the exponent 0.525 represents the tightest proven upper bound on maximum prime gaps achieved without assuming the unproven Riemann hypothesis (see § 6.1.29). If the Riemann hypothesis is eventually proven, this theoretical bound would narrow further to $O(\sqrt{p_n}\,\log p_n)$.

The significance of the Baker-Harman-Pintz theorem lies in its improvement over previous estimates for prime gaps and its contribution to understanding the distribution of prime numbers. Although it does not determine the exact size of the largest gaps between primes, it demonstrates that primes cannot become arbitrarily sparse as numbers increase. The result represents an important step toward the broader goal of proving stronger bounds on prime gaps, such as the long-standing Cramer conjecture that maximum gaps between consecutive primes grow only as the square of the logarithm (see § 6.1.12). Also see § 5.1.20.

5.1.2 Bertrand's Postulate

Bertrand's postulate is a fully proven theorem, not a conjecture or hypothesis, despite its name which suggests otherwise (noting that the "postulate" label is because it was originated by Bertrand as a conjecture). It was first proven by Chebyshev and hence it is also called *Chebyshev theorem* and *Bertrand-Chebyshev theorem*. According to this postulate, for any $1 < n \in \mathbb{N}$ there is at least one $p \in \mathbb{P}$ such that $n < p < 2n$ (noting that if $n = 1$ then $n < p \leq 2n$ is true). This simply means that prime numbers are sufficiently abundant to always exist between any number and its double.

In fact, Bertrand's postulate has an important implication, that is: it can be used as a proof for the infinitude of prime numbers (assuming that the proof of Bertrand's postulate is not based explicitly or implicitly on this infinitude; see § 1.6). Also see Point 2 in § 2.1.68 regarding the relationship between Bertrand's postulate and Ramanujan primes.

5.1.3 Binary Quadratic Prime Theorem

The theorem states that every primitive, irreducible, positive-definite binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ (where $a, b, c \in \mathbb{Z}$) represents infinitely many prime numbers. In this context, "primitive" means that the greatest common divisor of its coefficients (a, b, c) is 1, while "positive-definite" means that $f(x, y) > 0$ for all $(x, y) \neq (0, 0)$. The condition that the form is irreducible means that it does not factor into linear factors over $\mathbb{Z}$ (or equivalently that its discriminant is not a perfect square). This theorem may be regarded as a multi-variable analogue of Bunyakovsky's conjecture (see § 6.1.11).

The binary quadratic prime theorem holds profound significance in analytic number theory because it bridges the gap between quadratic forms and the distribution of prime numbers. While Dirichlet's theorem on arithmetic progressions (see § 5.1.11) establishes prime distribution in linear forms, this result reaches the more complex topic of degree-two polynomial representations. It demonstrates that the arithmetic structure of quadratic forms is rich enough to guarantee the occurrence of primes, even when the values are generated through a two-variable polynomial rather than a simple sequence. It also provides a deep connection between the theory of quadratic forms, algebraic number theory, and the distribution of prime numbers. In particular, it shows that primes are not confined to specific numerical patterns but appear infinitely often within broader families of Diophantine equations.

5.1.4 Bombieri-Vinogradov Theorem

The essence of the Bombieri-Vinogradov theorem is that primes are evenly distributed across arithmetic progressions on average over moduli. It is an unconditional, average substitute for the generalized Riemann hypothesis (GRH), as it provides a powerful error bound that matches what the GRH predicts, but without requiring unproven assumptions. Hence, it is commonly described as an unconditional average substitute for the GRH. Formally, the Bombieri-Vinogradov theorem states: for any given constant $A > 0$, there exists a corresponding constant $B(A) > 0$ such that:

$$\sum_{q \leq Q} \max_{y \leq x} \max_{\substack{1 \leq a \leq q \\ (a,q)=1}} \left| \psi(y; q, a) - \frac{y}{\phi(q)} \right| \ll_A x(\log x)^{-A} \tag{42}$$

where ψ is the second Chebyshev function (see § 8.2.5), ϕ is the totient function, and the upper limit of the sum is defined as $Q = x^{1/2}(\log x)^{-B}$.

5.1.5 Brun's Theorem

According to Brun's theorem, the series formed by the sum of the reciprocals of twin primes converges to a finite value (known as Brun's constant $\mathcal{B}_2$) which is estimated to be about 1.90216058,[446] that is:

$$\mathcal{B}_2 = \sum_{\substack{p \in \mathbb{P} \\ p+2 \in \mathbb{P}}} \left(\frac{1}{p} + \frac{1}{p+2} \right) = \left(\frac{1}{3} + \frac{1}{5} \right) + \left(\frac{1}{5} + \frac{1}{7} \right) + \left(\frac{1}{11} + \frac{1}{13} \right) + \left(\frac{1}{17} + \frac{1}{19} \right) + \cdots \tag{43}$$

[446] See `https://oeis.org/A065421`.

This theorem is related to the density of twin primes (i.e. they are significantly sparser than prime numbers in general),[447] even though this does not imply that the set of twin primes is finite.

The significance of Brun's theorem lies in its deep implications for the density and distribution of twin primes. By proving convergence, the theorem demonstrates that if an infinite number of twin prime pairs does exist, they must be very rare and distributed with a very low density throughout the number line. Because the series converges regardless of whether the set is finite or infinite, the theorem also illustrates a major challenge in analytic number theory which is the inability to use simple arithmetic accumulation to prove the infinitude of subsets of primes. Also see § 7.4.6.

5.1.6 Brun-Titchmarsh Theorem

This theorem is an important result in analytic number theory that provides an upper bound on the number of primes p in an arithmetic progression within a given interval. According to this theorem:

$$\pi(x;q,a) \leq \frac{2x}{\phi(q)\ln(x/q)} \tag{44}$$

for all $q < x$ where ϕ is the totient function, and $\pi(x;q,a)$ is the number of prime numbers $p \leq x$ with $p \overset{q}{=} a$ and $\gcd(a,q) = 1$ [i.e. $\pi(x;q,a)$ counts the number of primes up to x in the sequence $a, a+q, a+2q, \ldots$]. Although the Brun-Titchmarsh theorem does not provide an exact asymptotic equality, it provides a reliable and rigorous upper bound that holds uniformly for all $q < x$. In fact, it provides the correct order of magnitude over a massive range of values where standard analytical methods fail to do so.

The importance of the Brun-Titchmarsh theorem lies in its ability to give useful information about the distribution of primes in arithmetic progressions without relying on unproven hypotheses such as the generalized Riemann hypothesis. Its uniformity with respect to the modulus q makes it especially valuable in situations where q is relatively large compared with x, a regime in which stronger asymptotic results, such as those arising from the prime number theorem for arithmetic progressions (see § 5.1.32), are often unavailable or ineffective. Consequently, the theorem has become an important tool in sieve theory and analytic number theory, with applications to problems involving gaps between primes, the distribution of primes in residue classes, and estimates used throughout modern research.

5.1.7 Chebyshev's Theorem

Historically, this theorem was the first major step toward proving the prime number theorem which describes the asymptotic distribution of prime numbers (see § 5.1.31). The Chebyshev theorem essentially establishes the order of magnitude for the distribution of prime numbers, and hence it is commonly described as a "weak version" of the prime number theorem. The Chebyshev theorem states that there are constants a and A such that the prime-counting function $\pi(x)$ (see § 8.2.1) satisfies the following inequality for all $x \geq 2$:

$$a\frac{x}{\ln x} \leq \pi(x) \leq A\frac{x}{\ln x} \tag{45}$$

From a historical viewpoint, this result was a major breakthrough because it confirmed that the number of primes less than or equal to x is approximately proportional to $x/\ln x$, although the theorem did not provide the exact asymptotic limit of 1 that the proof of the prime number theorem established later on. In fact, Chebyshev proved unconditionally that for all sufficiently large x, the ratio $\pi(x)/(x/\ln x)$ is bounded between about 0.92129 and 1.10555. Moreover, he showed that if the limit of the ratio $\pi(x)/(x/\ln x)$ does exist as x approaches infinity, then this limit must be 1 (although he was not able to prove that the limit

[447] We note that the sum of the reciprocals of all prime numbers diverges (see § 9.2.1) and this is one of the proofs for the infinitude of prime numbers (see Point 2 in § 1.6).

does exist actually). Chebyshev also used his estimate for $\pi(x)$ to prove the Bertrand postulate (see § 5.1.2).

5.1.8 Chen's Theorem I

This theorem (regarding even integers) states that every sufficiently large even number can be expressed as the sum of either two primes or a prime and a semiprime (see § 9.5).[448] This theorem can be seen as an approach for proving the (strong) Goldbach's conjecture (see § 6.1.19) since it establishes a result that differs mainly from the conjecture by allowing one of the summands to be a semiprime rather than requiring both summands to be prime. So, although the theorem does not resolve Goldbach's conjecture, it demonstrates that every sufficiently large even integer is "very close" to having the conjectured representation. Therefore, it is regarded as one of the strongest partial results toward Goldbach's conjecture and represents a major achievement in additive number theory.

Chen's theorem (as one of the closest theoretical approximations to Goldbach's conjecture achieved so far) provides a crucial mathematical bridge between strict prime pairs and broader structures. By relaxing the requirement that both terms of the sum be prime and allowing one term to be a semiprime, the theorem establishes a theoretical ceiling on how far a large even integer can deviate from a pure prime-pair sum. We should also note that the innovative sieve methods developed in the course of proving this theorem have profoundly influenced modern analytic number theory, offering deep insights into the distribution of "near-primes" and refining our approach to the overall structure of integers. We should finally note that if p is a Chen prime (see § 2.1.6) then $2p+2$ (which is $p+[p+2]$) satisfies the conclusion of this theorem, in the sense that it provides an example of such a representation.

5.1.9 Chen's Theorem II

This theorem (which is related to the twin prime conjecture) states that there are infinitely many primes p such that $p+h$ (where h is a positive even integer) is either prime or a semiprime.[449] This theorem is obviously related to Chen primes, i.e. it establishes the infinitude of Chen primes which correspond to $h=2$ (see § 2.1.6). Moreover, it can be an important route (but not the only route) toward proving the twin prime conjecture (see § Point 1 in § 6.1.34). In fact, this theorem may be regarded as the closest proven result toward proving the twin prime conjecture (i.e. with regard to the composition of the numbers rather than the bound on the gap).

As indicated, this theorem is generalized to include every non-zero even integer h (noting that it is trivial for $h=0$).[450] This general form highlights the broader principle that shifted primes with a fixed even separation exhibit strong regularity when the second member is permitted to be a semiprime. As with Chen's theorem I (see § 5.1.8), the methods used in establishing this theorem (particularly advanced sieve techniques) have played a fundamental role in modern analytic number theory and have contributed significantly to the study of prime distributions and the patterns of almost-primes (see § 9.6).

5.1.10 Clement's Theorem

This is an extension of Wilson's theorem (see § 5.1.43) related to twin primes. It provides a necessary and sufficient condition for two integers to be twin primes, where it formulates the condition for twin primality within a single modular arithmetic congruence relation. This theorem states: for any integer $n>1$, the

[448] "Sufficiently large" means above a certain specified threshold.

[449] It is claimed that Chen extended this theorem later by proving the theorem for any non-zero even integer h (noting that the generalization may be from the beginning). Such historical discrepancies should be investigated by the readers.

[450] For example, we can say: there are infinitely many primes p such that $p-2$ is also prime or semiprime (which is a "twin prime" instance of Chen's theorem II).

pair of numbers $(n, n+2)$ are twin primes *iff*

$$4(n-1)! + 4 + n \equiv 0 \pmod{n^2 + 2n} \tag{46}$$

As a theoretical basis for a primality test, the Clement theorem is not practical due to the rapid factorial explosion which makes any computations involving even relatively small n either computationally very expensive or prohibitive. So, Clement's theorem (like Wilson's theorem) is primarily of theoretical interest rather than practical computational use. Also see § 7.3.19 and § 7.3.21.

5.1.11 Dirichlet's Theorem on Arithmetic Progressions

This theorem states: for any two coprime numbers $a, d \in \mathbb{N}$, there are infinitely many primes of the form $a + kd$ (where $k \in \mathbb{N}_0$). Noting that all primes (excluding 2) are of the form $2k + 1$, this theorem may be considered as an elaboration to the generic proofs of the infinitude of prime numbers (i.e. the proofs that establish the infinitude of prime numbers in general). As indicated previously, any proof of this theorem is a proof of the infinitude of prime numbers (assuming that such proofs do not presume the infinitude of primes).

In essence, Dirichlet's theorem asserts that if an arithmetic progression has the ability to contain prime numbers (as implied by the coprimality condition), it will eventually contain infinitely many primes. This (in part) makes this theorem an essential result for understanding the distribution of prime numbers among the integers, beyond what is given by the prime-counting function $\pi(x)$ and related theorems (such as the prime number theorem and the Mertens theorems; see § 5.1.31 and § 5.1.28).

As such, Dirichlet's theorem establishes a connection between simple counting of primes and how primes actually behave along different "tracks" of integers. In other words, while the prime number theorem indicates how many primes are there in total, the Dirichlet theorem shows that primes do not just aggregate in one place or distribute arbitrarily within the sequence of integers, but they are infinitely and uniformly distributed among all possible arithmetic progressions (within the imposed condition of coprimality). In short, the distribution of primes within the integers is governed by certain patterns; one of which is being in infinitely long "queues" within arithmetic progressions.

5.1.12 Erdos-Kac Theorem

The essence of this theorem is that the number of distinct prime factors of a typical large integer n follows probabilistically a normal distribution centered around a mean (average) value of $\log(\log n)$ with a spread (standard deviation) of $\sqrt{\log(\log n)}$. It is noteworthy that this theorem may also be called the *fundamental theorem of probabilistic number theory* although there seems to be no single such theorem (i.e. this label may apply to other theorems even though this theorem seems to be the most prominent of such theorems).

The deep significance of this result lies in its bridging of two traditionally separate realms of mathematics: deterministic number theory and probability theory. Primes are intrinsically exact and governed by strict arithmetic rules. However, the theorem reveals that their collective distribution as factors of large integers mimics random independent trials, structured neatly by a classic normal distribution curve. The theorem also demonstrates how universal statistical laws can emerge from the large-scale behavior of integers, even when individual numbers appear entirely unpredictable. Also see § 5.1.18.

5.1.13 Euler's Criterion

This criterion provides a necessary and sufficient condition for an integer n to be a quadratic residue modulo an odd prime p. It is therefore used as a test for the solvability of quadratic congruences modulo

odd primes. According to Euler's criterion, the quadratic congruence relation $x^2 \overset{p}{=} n$ has a solution *iff* $n^{(p-1)/2} \overset{p}{=} 1$ (where $n \in \mathbb{Z}$, p is an odd prime and $p \nmid n$). This may be expressed in terms of Legendre's symbol $\left(\frac{n}{p}\right)$ as:

$$\left(\frac{n}{p}\right) \overset{p}{=} n^{(p-1)/2} \qquad (n \in \mathbb{Z},\ p \text{ is an odd prime},\ p \nmid n) \tag{47}$$

Euler's criterion provides an efficient way for determining whether an integer is a quadratic residue modulo a prime without explicitly searching for a solution to the congruence. This result is significant because it connects the algebraic structure of modular arithmetic with the theory of quadratic residues and forms the basis for several important results in number theory, including quadratic reciprocity (see § 5.1.35). Furthermore, the criterion illustrates the usefulness of group-theoretic methods in studying congruences, as the expression $n^{(p-1)/2}$ arises from the properties of the multiplicative group of non-zero residues modulo p. We finally note that Euler's criterion underpins fast primality tests like Solovay-Strassen (see § 7.3.18).

5.1.14 Euler's Product Formula

The essence of this formula is that the Riemann zeta function factors over all primes (and hence the formula expresses the Riemann zeta function ζ as an infinite product over all prime numbers), that is:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} \qquad \big[\text{for } \Re(s) > 1\big] \tag{48}$$

where $\Re(s)$ is the real part of the complex variable s. This factorization reveals that the distribution of prime numbers is deeply embedded within the analytic structure of $\zeta(s)$, a connection that underlies many central results in number theory, including the study of prime distribution through the zeros of the zeta function. The formula therefore serves as an analytical bridge between the discrete world of prime numbers and the continuous world of complex analysis.

It is worth noting that the link between the infinite sum and the infinite product in this formula ultimately comes from the unique prime factorization of integers (see § 1.7) aided by the representation of $(1 - p^{-s})^{-1}$ as a geometric series. Both the infinite sum and the infinite product converge absolutely in the $\Re(s) > 1$ region (where "convergence" for the product is technically defined via the convergence of its corresponding sequence of partial products).

5.1.15 Fermat's Little Theorem

According to this theorem, if p is a prime number and a is an integer then $a^p \overset{p}{=} a$. Equivalently, if $p \nmid a$ then $a^{p-1} \overset{p}{=} 1$. It is worth noting that the converse of Fermat's little theorem is not true in general. This means that there are composite numbers that satisfy the congruence relation of Fermat's little theorem for every integer a and these composite numbers ($2 < n \in \mathbb{N}$ and $n \notin \mathbb{P}$) are called *Carmichael numbers* (i.e. $a^n \overset{n}{=} a$ for all $a \in \mathbb{Z}$, or equivalently $a^{n-1} \overset{n}{=} 1$ for all $a \in \mathbb{Z}$ where a and n are coprime). Accordingly, Carmichael numbers may be described as *Fermat pseudoprimes* or *absolute Fermat pseudoprimes* (but note that "Fermat pseudoprime" is more general than "Carmichael number"; see § 9.7.1 and § 9.7.6).

Apart from its obvious significance and usefulness in pure mathematics (and number theory in particular), Fermat's little theorem is useful for various applications such as primality testing (see for instance § 7.3.6, § 7.3.9 and § 7.3.12) and cryptography (e.g. in key generation and decryption in some cryptosystems; see § 10.1) as well as numerous applications in computational number theory. Also see § 2.1.90.

5.1.16 Goldbach's Ternary Conjecture

The Goldbach ternary (or weak) conjecture was proven recently (or rather its proof was finalized recently), and hence it is listed in this section (which is about proven theorems). According to this theorem, every odd integer > 5 can be expressed as a sum of three prime numbers (whether they are different or not). Also see § 5.1.42 and § 6.1.19.

Even though this theorem does not seem to be about the counting and distribution of prime numbers, it is intimately linked to the counting and distribution of primes because it implies that primes are so dense that they can represent any odd integer > 5 (as a sum of three primes). In fact, the theorem does not only imply that primes are "sufficiently dense", but it also implies that primes are "sufficiently well-distributed" among integers, i.e. by their sufficient abundance and regular distribution they can represent any odd integer > 5 as a sum of three primes.

5.1.17 Green-Tao Theorem

In simple words, this theorem states that the sequence of prime numbers contains arbitrarily long arithmetic progressions. More formally, for any $n \in \mathbb{N}$ there exist n prime numbers:

$$p, p+d, p+2d, \ldots, p+(n-1)d \qquad (d \in \mathbb{N}) \tag{49}$$

This means that no matter how large n is, one can always find n prime numbers that are equally spaced.

The theorem is remarkable because prime numbers become increasingly sparse as numbers grow larger, yet they still exhibit this surprising level of regularity. Its significance lies in revealing that despite the seemingly chaotic and unpredictable distribution of prime numbers, they still contain highly structured, deterministic patterns. The result also established a deep connection between number theory and additive combinatorics and is regarded as one of the major results in modern number theory.

5.1.18 Hardy-Ramanujan Theorem

This theorem describes the "typical" number of distinct prime factors of a positive integer. It estimates that the number of distinct prime factors of a natural number n is approximately equal to $\log(\log n)$ for almost all integers. More formally, the theorem states that the normal order of the number $\omega(n)$ of distinct prime factors of a natural number n is $\log(\log n)$, that is:[451]

$$\omega(n) \simeq \log(\log n) \tag{51}$$

The theorem is one of the fundamental results in probabilistic number theory (noting that it is essentially about the distribution of prime factors inside integers).

By demonstrating that the vast majority of integers behave in a highly predictable manner regarding their factorization, this result challenges the stereotype that prime distribution as factors of integers is random. Rather than describing exceptional cases, the theorem characterizes what happens for the overwhelming majority of integers. The theorem also laid the foundation for stronger results, most notably the Erdos-Kac theorem (see § 5.1.12) which shows that the number of distinct prime factors of an integer is not only concentrated around $\log(\log n)$ but is also asymptotically normally distributed (after appropriate normalization). The insights offered by this theorem provide a profound theoretical basis for understanding the statistical structure of natural numbers.

[451] More precisely: for any $\epsilon > 0$, the inequality:

$$|\omega(n) - \log(\log n)| < \big[\log(\log n)\big]^{1/2+\epsilon} \tag{50}$$

holds for almost all integers n.

5.1.19 Hensel's Theorem

This theorem (commonly known as Hensel's lemma) provides a practical method for solving polynomial congruences modulo powers of primes, making it a fundamental tool for solving univariate polynomial congruence equations in general. According to this theorem, if:
• $P(m)$ is a polynomial with integer coefficients and P' is its derivative,
• p is a prime number,
• $P(m) \equiv 0 \pmod{p^d}$ and $P'(m) \not\equiv 0 \pmod{p}$,
then there is a unique $c \pmod{p}$ such that the lifted solution $m_{\text{new}} \equiv m + cp^d \pmod{p^{d+1}}$ satisfies $P(m + cp^d) \equiv 0 \pmod{p^{d+1}}$ where c is given by:

$$c \equiv -\left[P'(m)\right]^* \frac{P(m)}{p^d} \pmod{p} \tag{52}$$

with $\left[P'(m)\right]^*$ being the multiplicative inverse of $P'(m)$ modulo p.

The importance of Hensel's lemma lies in its ability to transform a difficult congruence problem modulo a high power of a prime into a sequence of simpler problems modulo increasing powers of that prime. In particular, it shows that a solution modulo p^d can be systematically extended to a solution modulo p^{d+1}, and repeated application allows extension to higher powers of p, provided that the derivative condition is satisfied. This lifting process is fundamental in number theory and has applications in areas such as p-adic analysis, Diophantine equations, algebraic number theory, and computational methods for solving polynomial equations over modular arithmetic systems. The theorem also illustrates the close relationship between local solutions (considered modulo powers of individual primes) and broader solutions to polynomial equations.

5.1.20 Hoheisel's Theorem

Historically, this theorem was the first result to prove (unconditionally) that prime numbers can be guaranteed in sub-linear short intervals without relying on the unproven Riemann hypothesis (and this was an improvement to the then-proven Bertrand's postulate; see § 5.1.2). Hoheisel's theorem states that there exists a constant $\eta < 1$ such that for all sufficiently large x the interval $[x, x + x^\eta]$ always contains at least one prime number. Since its appearance in 1930, the constant η has shrunk in size to reach currently 0.525.[452] If the Riemann hypothesis is eventually proven, the constant η could shrink even further.

This theorem marked a major milestone in analytic number theory by showing that non-trivial bounds on gaps between consecutive primes can be established unconditionally. It also initiated a long line of research aimed at reducing the admissible value of η, with successive refinements relying on increasingly sophisticated estimates for the distribution of zeros of the Riemann zeta function and related analytic techniques. Although the current unconditional estimate of η remains well above the conjectured optimal values, Hoheisel's theorem laid the foundation for much of the modern theory of primes in short intervals and continues to serve as a benchmark in the study of the local distribution of prime numbers. Also see § 5.1.1.

5.1.21 Iwaniec's Theorem

According to this theorem, there are infinitely many integers of the form $n^2 + 1$ that are either prime or have exactly two prime factors (i.e. semiprimes; see § 9.5). The significance of Iwaniec's theorem lies in the fact that it provides the strongest known unconditional result toward Landau's fourth problem, which asks whether there are infinitely many primes of the form $n^2 + 1$ (see § 2.1.47). Although the theorem does

[452] A very recent preprint claims an improvement to 0.52 (but this requires check).

not prove that infinitely many values of $n^2 + 1$ are prime, it shows that this sequence contains infinitely many numbers that are almost-prime, namely numbers with at most two prime factors (see § 9.6). Thus, Iwaniec's theorem demonstrates that values of the quadratic polynomial $n^2 + 1$ come arbitrarily close to being prime infinitely many times.

Iwaniec's theorem represents an important advancement in modern sieve theory, bridging the gap between classical multiplicative number theory and unsolved polynomial prime-generation problems. From the perspective of Landau's fourth problem, Iwaniec's theorem shows that the obstacle is not the complete absence of arithmetic structure in the sequence n^2+1, but rather the difficulty of excluding the possibility of a second prime factor. In other words, the theorem establishes that sieve methods are powerful enough to prove that infinitely many values of $n^2 + 1$ have at most two prime factors, yet current techniques fall short of proving that one of those factors can be eliminated altogether. Consequently, Iwaniec's theorem is widely regarded as the closest unconditional approximation to a solution of Landau's fourth problem and serves as a standard against which later advances on primes represented by quadratic polynomials are measured.

5.1.22 Lagrange's Theorem on Polynomial Congruences

According to this theorem, if $f(x)$ is a polynomial of degree $n \in \mathbb{N}$ with integer coefficients whose leading coefficient is not divisible by the prime p, then the congruence $f(x) \stackrel{p}{=} 0$ has at most n incongruent solutions modulo p. The significance of this theorem lies in the fact that it provides a fundamental upper bound on the number of solutions of polynomial congruences modulo a prime. It guarantees that a non-zero polynomial cannot vanish (modulo p) at more residue classes than its degree, mirroring the familiar result for polynomial equations over fields.

This theorem is regarded as a cornerstone of elementary and algebraic number theory and has numerous applications, including the study of quadratic and higher-power residues, the analysis of polynomial equations over finite fields, and the estimation of exponential sums. It also serves as a basic ingredient in many proofs involving congruences, finite fields and arithmetic functions, and underlies several important results in cryptography, coding theory and computational number theory.

5.1.23 Legendre's Formula

This formula (also known as *Polignac's formula*) gives the exact power s of a prime p in $n!$, that is:

$$s = \sum_{i=1}^{\infty} \text{floor}\left(\frac{n}{p^i}\right) \tag{53}$$

where floor is the floor function. It is important to note that the sum is formally infinite but effectively finite, i.e. all the terms of the sum will vanish after a given i because there will always be an integer k such that $p^i > n$ for all $i \geq k$ and hence all the terms with $i \geq k$ will vanish.

Beyond its theoretical elegance, this formula serves as a fundamental building block in computational number theory and combinatorics. It provides an efficient method for computing the prime factorization of large factorials without the need to calculate the massive factorial value itself. Practically, this is the foundational mechanism used to determine how many trailing zeros a factorial has by finding the exponent of 5 in its factorization. Furthermore, Legendre's formula is used in proving Kummer's theorem, which determines the p-adic valuation of binomial coefficients and connects the formula directly to the study of carry operations in base-p arithmetic.[453]

[453] Kummer's theorem states that the exponent of the highest power of a prime p dividing the binomial coefficient C_k^n is equal to the number of carries when adding k and $n - k$ in base p.

5.1.24 Linnik's Theorem

This theorem is a fundamental result in analytic number theory that bounds the size of the smallest prime number in an arithmetic progression. While Dirichlet's theorem (see § 5.1.11) asserts the existence of infinitely many primes in such a progression, Linnik's theorem provides an upper bound on how far we have to look to find the first one. The theorem states that for any two coprime positive integers a and d, the least prime $p_{a,d}$ in the arithmetic progression $a + nd$ (where $n \in \mathbb{N}_0$) is bounded by the following relation:

$$p_{a,d} \leq cd^L \tag{54}$$

where c and L are positive absolute constants (i.e. they are independent of both a and d). It is worth noting that the current best upper bound for L (which is known as Linnik's constant) is $L \leq 5$.

Establishing this bound is highly significant because it guarantees that the first prime is relatively "small" compared to the modulus d, preventing the need for an exhaustive, computationally prohibitive search. While the theorem provides a crucial unconditional upper bound, conditionally assuming the generalized Riemann hypothesis dramatically sharpens this relation, implying that the true value of L could be as low as 2 or even lower for large moduli.

As for its relation to Dirichlet's theorem, Linnik's theorem may be regarded as a quantitative version of Dirichlet's theorem in the sense that: rather than merely guaranteeing the existence of primes in an arithmetic progression (as required by Dirichlet's theorem), Linnik's theorem describes how large the first such prime can be in relation to the modulus d. This result has important consequences in areas where primes in specific residue classes are required, such as computational number theory and the study of prime distributions.

5.1.25 Littlewood's Theorem

Historically, it was widely believed that the logarithmic integral $\mathrm{Li}(x)$, which provides an asymptotic approximation to the prime-counting function $\pi(x)$ in the prime number theorem, always overestimates $\pi(x)$ and hence the difference $\pi(x) - \mathrm{Li}(x)$ is always negative (see § 5.1.31 and § 8.2.2). However, it was later proved that $\pi(x) - \mathrm{Li}(x)$ changes sign infinitely many times (a result known as Littlewood's theorem).

In this context we should refer to the Skewes conjecture and the Skewes number which are linked to this issue. Regarding the Skewes conjecture, we refer the readers to § 6.5. As for the Skewes number, it is defined as the smallest positive integer x for which the prime-counting function $\pi(x)$ exceeds the logarithmic integral function $\mathrm{Li}(x)$. More broadly, the term refers to the proven upper bounds for this first crossover point. While the detailed variations of these numbers are beyond our scope, current proofs establish that the first crossover is greater than 10^{19} but less than about 1.3972×10^{316}.

5.1.26 Maier's Theorem

The essence of this theorem is that the Cramer probabilistic model (which is a heuristic model that treats primes like random numbers with a specific density) is inaccurate for predicting primes in short intervals. More specifically, while the Cramer model suggests that the number of primes in a short interval should consistently follow a specific density, the Maier theorem proves that the density of primes in such interval actually fluctuates. The significance of this is that prime numbers have non-random structural properties which simple random models fail to capture. In other words, there are short intervals of specific length that contain significantly more primes than what is predicted by the Cramer model, and there are other such intervals that contain significantly fewer primes, and hence the density actually fluctuates by a specifically quantified factor.

Formally, Maier's theorem states:

$$\frac{\pi(x+\ln^{\lambda} x)-\pi(x)}{\ln^{\lambda-1} x} \tag{55}$$

does not have a limit as x tends to infinity, where π is the prime-counting function (see § 8.2.1) and $\lambda > 1$. In more precise terms, the limit inferior is less than 1 and the limit superior is greater than 1, that is:

$$\liminf_{x\to\infty} \frac{\pi(x+\ln^{\lambda} x)-\pi(x)}{\ln^{\lambda-1} x} < 1 \qquad \text{and} \qquad \limsup_{x\to\infty} \frac{\pi(x+\ln^{\lambda} x)-\pi(x)}{\ln^{\lambda-1} x} > 1 \tag{56}$$

and hence the limit cannot exist.

5.1.27 Mertens' First Theorem

This theorem provides an asymptotic estimate for a weighted sum of the logarithms of prime numbers. It states that for $2 \leq x \in \mathbb{R}$ the sum of $(\ln p)/p$ over all primes p up to x grows logarithmically with x (with the error term being bounded), that is:

$$\sum_{p\leq x} \frac{\ln p}{p} = \ln x + O(1) \qquad \text{or} \qquad \left| \left(\sum_{p\leq x} \frac{\ln p}{p} \right) - \ln x \right| \leq 2 \tag{57}$$

where $x \geq 2$ and O is the big O notation.

This theorem is essentially about the counting and distribution of prime numbers (but in a rather different sense to the prime number theorem and its analog), and is one of the important results in analytic number theory. Historically, this result was a precursor to the prime number theorem (see § 5.1.31). Despite the fact that it does not formulate the distribution of primes as precisely as the prime number theorem, it establishes that the density of primes is such that this weighted sum tracks the natural logarithm very closely.

5.1.28 Mertens' Second Theorem

This theorem is an important result related to the density of prime numbers, as it provides an asymptotic estimate for the sum of the reciprocals of primes up to a given positive real number x. It states that:[454]

$$\sum_{p\leq x} \frac{1}{p} \sim \ln(\ln x) \qquad (x \to \infty) \tag{59}$$

where $\sim$ is the asymptotic equivalence symbol. This means that the sum of the reciprocals of primes diverges, but it diverges very slowly (at logarithmic-logarithmic rate). In fact, this provides a weight (or density indicator) to how many primes exist compared to all positive integers (noting that the harmonic series of all positive integers $\sum_{n\in\mathbb{N}} 1/n$ diverges at a logarithmic rate which is much faster than the rate of the sum of the reciprocals of primes). In Figure 11 we plot the $1/n$ and $1/p$ series [alongside the theoretical $\ln x$ and $\ln(\ln x)$ functions] up to $x = 10^4$ to demonstrate and compare the behavior of these series.

Nevertheless, this very slow rate of growth of the $1/p$ series shows that even though the prime numbers

[454] This may also be given as an equation:

$$\sum_{p\leq x} \frac{1}{p} = \ln(\ln x) + M + O\left(\frac{1}{\ln x}\right) \tag{58}$$

where $M \approx 0.261497$ is the Meissel-Mertens constant and O is the big O notation.

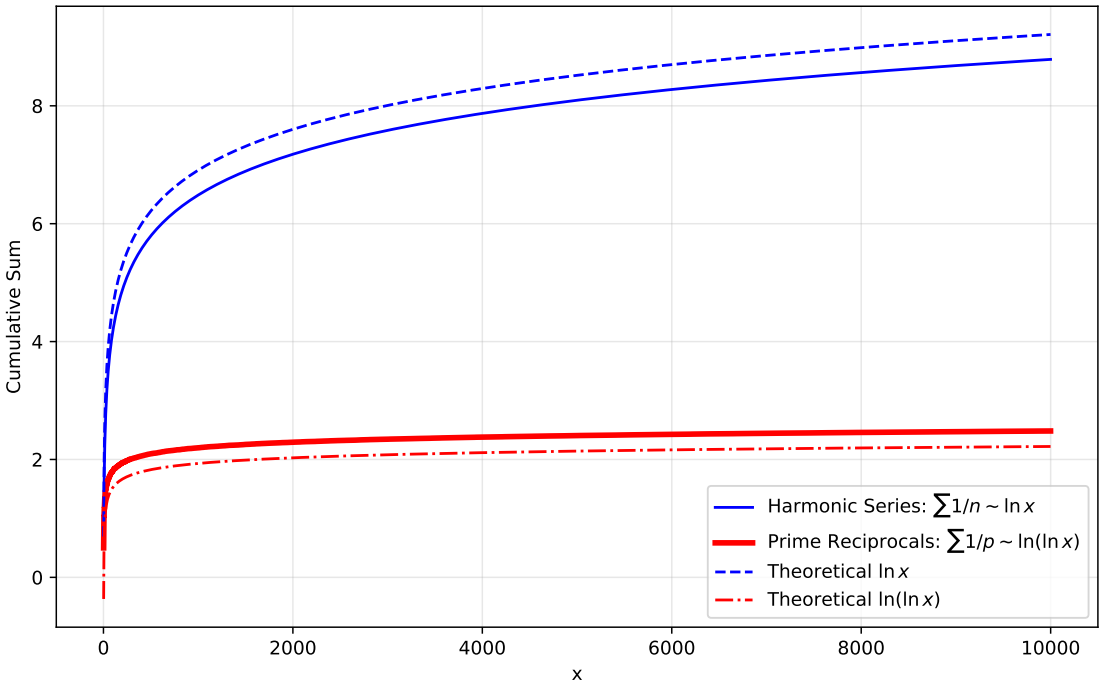


Figure 11: The $1/n$ and $1/p$ series as well as the theoretical $\ln x$ and $\ln(\ln x)$ functions (for $1 < x \leq 10^4$). See § 5.1.28.

become increasingly sparse among the positive integers, they are still sufficiently abundant to prevent the $1/p$ series from converging to a finite limit. In short, even though primes become sparse among integers as we go to infinity, they are not so sparse to force the $1/p$ series to converge (unlike, for instance, the sparsity of n^2 which forces the $1/n^2$ series to converge to $\pi^2/6$). Anyway, Mertens' second theorem should imply (indirectly) the infinitude of prime numbers which is supported by tens, if not hundreds, of other proofs (also see Point 2 of § 1.6 and § 9.2.1).[455]

Finally, it is worth noting that Mertens' second theorem is closely related to the prime number theorem (see § 5.1.31). In fact, Mertens' second theorem can be derived from the prime number theorem using partial summation.

5.1.29 Mertens' Third Theorem

This theorem is an important result in analytic number theory that describes the asymptotic behavior of a specific product over prime numbers. It states that:

$$\lim_{x\to\infty} \ln x \prod_{p\leq x} \left(1 - \frac{1}{p}\right) = e^{-\gamma} \tag{60}$$

[455] In fact, this indirect proof should be stronger, more significant and more informative than the direct proofs of infinitude of primes (such as Euclid's proof) because Euclid's proof and similar arguments just establish the infinitude of prime numbers while this indirect proof adds information about the (rather high) density of primes and their distribution, noting that the infinitude in itself does not guarantee the divergence (as we see in the convergence of the $1/n^2$ series despite the infinitude of n^2).

where γ is the Euler-Mascheroni constant (≈ 0.57721566).[456] It is also frequently written in its equivalent asymptotic notation:

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\ln x} \qquad (x \to \infty) \tag{61}$$

While the prime number theorem (see § 5.1.31) is about the density of primes, Mertens' third theorem specifically quantifies the density of numbers not divisible by any prime up to x. This theorem may be regarded as the exponentiated version of Mertens' second theorem which deals with the sum of the reciprocals of primes (see § 5.1.28).

5.1.30 Mills' Theorem

This theorem states that there exists a real constant $A > 1$ (i.e. Mills' constant) such that floor $\left(A^{3^n}\right)$ is a prime number for every positive integer n.[457] The value of Mills' constant depends on the first prime chosen for the sequence. This means that the value of A depends on identifying a sequence of primes in advance, and hence to compute A precisely we need a sequence of primes that fit the pattern.

Accordingly, this theorem is not constructive (but rather "formative" or "formulative"). In other words, the theorem is not about discovering or "generating" new primes in a computationally useful way. So, the primary value of the theorem lies in demonstrating that primes (which often appear random) can be ordered (or arranged) by a rather simple analytic formula, and hence they have a more organized structure than they may be thought.[458]

If we assume the validity of the Riemann hypothesis (see § 6.1.29) and start the sequence with the smallest possible primes, then the value of Mills' constant is approximately $A \approx 1.306377883863080690468 6$.[459] It is worth noting that Mills' constant is irrational (a result proven very recently). Also see § 2.1.44 and Point 1 of § 9.1.8.

5.1.31 Prime Number Theorem

This is one of the most important results in number theory (and the topic of prime numbers in particular). It describes the asymptotic growth of the prime-counting function $\pi(x)$, and hence it establishes a connection between the discrete nature of prime numbers and the smooth nature of continuous functions. According to this theorem, the number of prime numbers less than or equal to x (as represented by the prime-counting function; see § 8.2.1) is asymptotically equivalent to $x/\ln x$ as x tends to infinity, that is:

$$\pi(x) \sim \frac{x}{\ln x} \quad (x \to \infty) \qquad \text{or} \qquad \lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1 \tag{62}$$

In fact, this theorem gives a general idea about the distribution of prime numbers among integers since it shows that prime numbers become sparser as integers grow larger (because $x/\ln x$ grows slower than x itself, which means that the density of prime numbers among integers decreases as $x \to \infty$).[460]

The term $x/\ln x$ in Eq. 62 may be replaced by the (offset) logarithmic integral function $\mathrm{Li}(x)$, yielding:

$$\lim_{x \to \infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1 \tag{63}$$

[456] See `https://oeis.org/A001620`.

[457] More precisely, "Mills' constant" is used for the least possible value of A (noting the dependency of the value of A on the starting sequence as will be explained next), but in this subsection we are using "Mills' constant" rather laxly for ease of presentation. See footnote [168].

[458] But note that although the resulting sequence consists entirely of primes, it does not include all prime numbers.

[459] See `https://oeis.org/A051021`.

[460] This can be seen more easily by writing $\pi(x)/x \sim 1/\ln x$ $(x \to \infty)$ because $1/\ln x \to 0$ as $x \to \infty$.

In fact, $\mathrm{Li}(x)$ provides a significantly better approximation to $\pi(x)$ than $x/\ln x$ for finite values of x.

In Figure 12 we compare the convergence of Eqs. 62 and 63 for $x \leq 10^{20}$ (evaluated at $x = 10, 10^2, \ldots, 10^{20}$) using the actual number of primes $\leq x$ to represent $\pi(x)$. As we see, Eq. 63 provides a better and faster convergence as x increases (for $x \leq 10^{20}$). It is noteworthy that the Figure may suggest that $\mathrm{Li}(x)$ is always greater than $\pi(x)$. However, it is proven that the difference $\pi(x) - \mathrm{Li}(x)$ changes sign infinitely many times (a result known as Littlewood's theorem; see § 5.1.25).

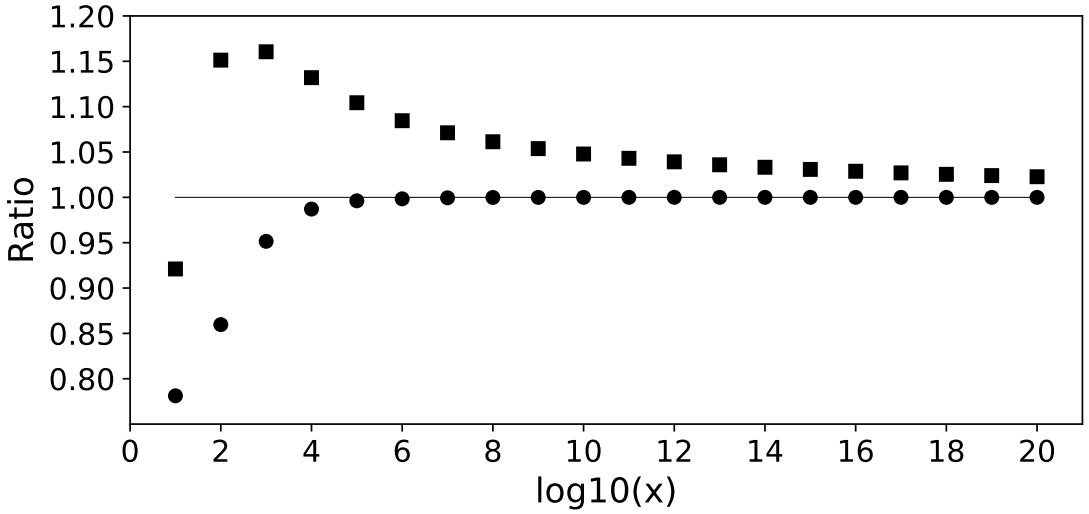


Figure 12: The plot of the ratio $\pi(x)/(x/\ln x)$ of Eq. 62 (squares) and the ratio $\pi(x)/\mathrm{Li}(x)$ of Eq. 63 (circles) versus $\log_{10}(x)$ for $x \leq 10^{20}$. See § 5.1.31.

To sum up, three main factors should be considered when comparing $\mathrm{Li}(x)$ and $x/\ln x$, all of which generally make $\mathrm{Li}(x)$ the superior choice for estimating the prime-counting function $\pi(x)$:

• Rate of convergence: while both functions are asymptotically equivalent [i.e. their respective ratios with $\pi(x)$ approach 1 as $x \to \infty$], $\mathrm{Li}(x)$ approaches this limit at a much faster rate.

• Accuracy: because $\mathrm{Li}(x)$ converges much faster than $x/\ln x$, it generally provides a significantly more accurate estimate of $\pi(x)$ for finite values of x. This is formally revealed by the asymptotic expansion of $\mathrm{Li}(x)$, i.e.

$$\mathrm{Li}(x) \sim \frac{x}{\ln x} + \frac{x}{(\ln x)^2} + \frac{2x}{(\ln x)^3} + \cdots \tag{64}$$

where we can see that $\mathrm{Li}(x)$ includes correction terms beyond $x/\ln x$ (which only constitutes the first term of the expansion).

• Direction of error: the approximation $x/\ln x$ consistently underestimates $\pi(x)$ for all sufficiently large values of x. In contrast, $\mathrm{Li}(x)$ typically overestimates $\pi(x)$ for accessible values, although it eventually keeps oscillating and hence crossing the value of $\pi(x)$ infinitely many times.

5.1.32 Prime Number Theorem for Arithmetic Progressions

This theorem goes beyond the prime number theorem (see § 5.1.31) as it gives the asymptotic distribution of primes in arithmetic progressions. According to this theorem:

$$\pi(x; q, a) \sim \frac{1}{\phi(q)} \frac{x}{\ln x} \qquad (x \to \infty) \tag{65}$$

where q, a are coprime integers with fixed $q \geq 2$, ϕ is the totient function, and $\pi(x; q, a)$ is the number of primes $p \leq x$ with $p \overset{q}{=} a$. In words, this theorem does not only imply that there are infinitely many such primes, but it also says that they are asymptotically equidistributed among the reduced residue classes modulo q. Since this asymptotic formula implies the infinitude of primes in arithmetic progressions (which is the essence of Dirichlet's theorem; see § 5.1.11), the prime number theorem for arithmetic progressions is stronger than the Dirichlet theorem. In fact, if we allow q to be 1, then we can recover the prime number theorem (see § 5.1.31) as a special case of the PNTAP.

Beyond establishing equidistribution, this theorem serves as a foundational result for modern analytic number theory and cryptography. The distribution of primes described by this theorem has practical implications for computational number theory and cryptography, particularly in understanding the abundance and generation of large primes used in cryptographic systems. Compared with Dirichlet's theorem, PNTAP provides a more precise description of the distribution of primes than Dirichlet's theorem, which only guarantees the existence of infinitely many primes in each admissible arithmetic progression. In particular, it quantifies how frequently primes occur in each residue class and shows that no reduced residue class is favored in the long term. This equidistribution property is a fundamental insight into the apparent randomness of prime numbers and plays an important role in analytic number theory.

5.1.33 Primes Modulo 4 Theorem

This theorem states: every odd prime must be either of the form $(4k + 1)$ or of the form $(4k - 1)$ where $k \in \mathbb{N}$. This classification holds because every integer is congruent to 0, 1, 2, or 3 (modulo 4). As odd primes cannot be congruent to 0 or 2 (since these correspond to even numbers) the only possible congruence classes are 1 and 3 (which is congruent to -1 modulo 4).

Moreover, there are infinitely many primes of the form $(4k + 1)$ and of the form $(4k - 1)$. This result represents a specific case of Dirichlet's theorem on arithmetic progressions (see § 5.1.11). It is also an important refinement of Euclid's theorem on the infinitude of primes, showing that prime numbers are infinitely distributed across both of these residue classes rather than being confined to just one.

5.1.34 Primes Modulo 6 Theorem

This theorem states: every prime greater than 3 must be either of the form $(6k+1)$ or of the form $(6k-1)$ where $k \in \mathbb{N}$. This classification holds because every integer is congruent to 0, 1, 2, 3, 4, or 5 (modulo 6). Any integer congruent to 0, 2, or 4 (mod 6) is even, while any integer congruent to 3 (mod 6) is divisible by 3. Consequently, a prime greater than 3 cannot belong to any of these residue classes, leaving only the congruence classes 1 and 5 (which is congruent to -1 modulo 6).

Moreover, there are infinitely many primes of the form $(6k + 1)$ and of the form $(6k - 1)$. Again, this result represents a specific case of Dirichlet's theorem on arithmetic progressions (see § 5.1.11). It is also an important refinement of Euclid's theorem on the infinitude of primes. This theorem and the primes modulo 4 theorem (see § 5.1.33) are frequently used in elementary number theory to characterize the possible forms of prime numbers. They also serve as useful starting points for studying the distribution of primes.

5.1.35 Quadratic Reciprocity Law

According to the law of quadratic reciprocity, if p and q are distinct odd primes then:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \tag{66}$$

where $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ denote the Legendre symbols. For an integer a and an odd prime p, the Legendre symbol $\left(\frac{a}{p}\right)$ indicates whether a is a quadratic residue modulo p (i.e. it is equal to 1 if a is a non-zero quadratic residue mod p, -1 if it is a quadratic non-residue mod p, and 0 if p divides a). The law of quadratic reciprocity provides a remarkable relationship between the quadratic residuosity of p modulo q and that of q modulo p. In particular, if at least one of the primes is congruent to 1 (mod 4), then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, whereas if both primes are congruent to 3 (mod 4), then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

This theorem is one of the central results of elementary number theory, as it greatly simplifies the computation of the Legendre symbol by allowing the numerator and denominator to be interchanged under a predictable sign change. Together with Euler's criterion (see § 5.1.13) and the supplementary laws [e.g. for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$; see Point 38 of § 1.4], it provides an efficient method for determining whether an integer is a quadratic residue modulo an odd prime.

5.1.36 Riemann-von Mangoldt Formula

The Riemann-von Mangoldt formula describes the distribution of the zeros of the Riemann zeta function $\zeta(s)$. Specifically, it provides an estimate for the number of non-trivial zeros $N(T)$, counted with multiplicity, in the critical strip with imaginary parts between 0 and T. This result is linked to the distribution of prime numbers. In fact, this formula is one of the cornerstones of analytic number theory because it connects the zeros of the zeta function to the distribution of prime numbers. The standard form of this formula is:

$$N(T) = \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T) \qquad (T \to \infty) \tag{67}$$

where $N(T)$ is the number of non-trivial zeros, counted with multiplicity, of the zeta function with imaginary part greater than 0 and less than or equal to T, and $O(\log T)$ denotes the error term in the big O notation. This formula may also be given as:

$$N(2\pi T) = T \log T - T + O(\log T) \qquad (T \to \infty) \tag{68}$$

The relatively small error term $O(\log T)$ shows that the average distribution of zeros is highly predictable as T grows, even though the exact spacing between individual zeros varies. By describing the density of non-trivial zeros, the formula provides essential information for studying the explicit connections between the zeros of the zeta function and the error term in the prime number theorem (see § 5.1.31).

The Riemann-von Mangoldt formula is significant because it gives a precise asymptotic description of how the non-trivial zeros of the zeta function are distributed as their height increases. Although it does not determine the exact locations of individual zeros, it reveals that their average density follows a highly structured pattern. This result provides a foundation for further investigations into the relationship between the zeros of the zeta function and the distribution of prime numbers through the explicit formulae of analytic number theory. The formula also plays an important role in the study of the Riemann hypothesis, which concerns the locations of the non-trivial zeros (see § 6.1.29).

5.1.37 Robin's Theorem

This theorem asserts that the Riemann hypothesis (see § 6.1.29) is true *iff* for all integers $n > 5040$ the following inequality holds:

$$\sigma(n) < e^{\gamma} n \ln \ln n \tag{69}$$

where $\sigma(n)$ is the divisor function and γ is the Euler-Mascheroni constant.

Robin's theorem transforms an analytic problem concerning the zeros of the Riemann zeta function into

a purely arithmetic statement about the distribution of divisors. The threshold of 5040 is structurally significant, as it represents a highly composite number (specifically 7!) where the density of divisors is exceptionally large. In fact, 5040 is the largest known integer that violates this inequality.[461] If any integer greater than 5040 was found to violate this bound, it would immediately disprove the Riemann hypothesis by implying the existence of an unexpected irregularity in the distribution of prime numbers. Consequently, verifying the inequality for every integer greater than 5040 would establish the Riemann hypothesis, while the existence of a single integer $n > 5040$ for which the inequality fails would disprove it. This equivalence illustrates the deep connections between the distribution of prime numbers and the behavior of divisor functions, making Robin's theorem an important result in analytic number theory.

5.1.38 Selberg's Formula

This is an elementary formula that served as the foundation for the first elementary proof of the prime number theorem (see § 5.1.31). Before the emergence of this formula, proofs of the prime number theorem depended heavily on the Riemann zeta function and complex analysis. The formula is:

$$\sum_{p\leq x}(\ln p)^2+\sum_{pq\leq x}\ln p\ln q=2x\ln x+O(x) \tag{70}$$

where $p, q \in \mathbb{P}$ and O is the big O notation. Selberg's formula may also be given as:

$$\psi(x)\ln x+\sum_{n\leq x}\Lambda(n)\psi\left(\frac{x}{n}\right)=2x\ln x+O(x) \tag{71}$$

where $\psi(x)$ is the second Chebyshev function (see § 8.2.5), and $\Lambda(n)$ is the von Mangoldt function.[462] This formula provides strong information about the distribution of primes and, together with further elementary arguments, leads to the prime number theorem, establishing that $\pi(x) \sim x/\ln x$ as $x \to \infty$.

5.1.39 Siegel-Walfisz Theorem

This is an important result of analytic number theory and may be regarded as a refinement of the prime number theorem (see § 5.1.31) that provides an estimate for the distribution of primes in arithmetic progressions. Formally, the theorem states: for any fixed positive real number A, there exists a positive constant C_A such that:

$$\pi(x;q,a)=\frac{\operatorname{Li}(x)}{\phi(q)}+O_A\left(xe^{-C_A\sqrt{\ln x}}\right) \tag{73}$$

where $\pi(x; q, a)$ is the number of primes $\leq x$ which are congruent to $a \pmod q$, ϕ is the totient function, Li is the offset logarithmic integral function (see § 8.2.2), O_A is the big O notation (in which the implied constant may depend on A), $q \leq (\ln x)^A$, and $\gcd(a, q) = 1$. The Siegel-Walfisz theorem is an important ingredient in analytic number theory and is related to stronger results on the average distribution of primes in arithmetic progressions, such as the Bombieri-Vinogradov theorem (see § 5.1.4).

---

[461] It has been proven that within the range $2 \leq n \leq 5040$, the inequality of Eq. 69 fails for exactly 27 integers and holds for all others. See `https://oeis.org/A091901` and `https://oeis.org/A067698`.

[462] The von Mangoldt function $\Lambda(n)$ is an arithmetic function defined for positive integers n, that is:

$$\Lambda(n)=\begin{cases}\ln p & \text{if } n=p^k \text{ where } p\in\mathbb{P} \text{ and } 1\leq k\in\mathbb{N}\\ 0 & \text{otherwise}\end{cases} \tag{72}$$

5.1.40 Sylvester-Schur Theorem

According to this theorem, if $k, n \in \mathbb{N}$ and $n > k$ then in the set of k consecutive integers $\{n, n+1, n+2, \ldots, n+k-1\}$ there is at least one number possessing a prime factor strictly greater than k. This theorem may also be stated (through the use of binomial coefficients) as: if $n \geq 2k$ then the binomial coefficient C_k^n always has a prime factor $p > k$. The Sylvester-Schur theorem may be viewed as a broad generalization of Bertrand's postulate (see § 5.1.2), noting that Bertrand's postulate may be obtained from the Sylvester-Schur theorem by setting $n = k + 1$.

The Sylvester-Schur theorem plays an important role in understanding the distribution of large prime factors in short intervals. The theorem has many applications, particularly in the study of prime divisors of products of consecutive integers and of binomial coefficients. It is frequently used in proofs concerning the irreducibility of polynomials, the existence of primitive prime divisors, and the arithmetic properties of combinatorial quantities. The theorem also illustrates the principle that sufficiently long blocks of consecutive integers cannot be composed solely of "small" prime factors, ensuring the appearance of relatively large primes. Its elementary nature, together with its broad applicability, has made it a common tool in both elementary and analytic number theory.

5.1.41 The Sum of Two Squares Theorem

According to this theorem (which is attributed to Fermat and is commonly known as Fermat's theorem on sums of two squares), a prime $p > 2$ can be expressed uniquely (up to changing signs and exchanging terms) as a sum of two perfect squares *iff* $p = 4k + 1$ for some $k \in \mathbb{N}$. We note that 2 is also expressible as a sum of two squares, i.e. $2 = 1^2 + 1^2$.

This theorem is one of the earliest and most influential results in the study of quadratic forms and has played an important role in the development of number theory. It provides a direct link between the arithmetic properties of primes and their representation by quadratic expressions, illustrating the relationship between congruence conditions and Diophantine equations. The theorem also serves as a foundation for the more general theory of sums of squares, including the characterization of integers expressible as sums of two, three, or four squares. Furthermore, the theorem has important consequences in algebraic number theory, particularly through its connection with Gaussian integers (see footnote [776] in § 9.4.1), where primes congruent to 1 (modulo 4) factor into non-trivial products. Its simplicity, elegance and wide-range implications have made it a focal example of the interaction between elementary and advanced areas of number theory (and even mathematics in general).

5.1.42 Vinogradov's Theorem

The theorem asserts that every sufficiently large odd integer can be expressed as the sum of three primes. In fact, this theorem is a weaker version of the Goldbach ternary conjecture (which is a proven theorem; see § 5.1.16 and § 6.1.19) because the latter asserts this expressibility for all odd integers > 5. The theorem was one of the major achievements of analytic number theory in the 20^{th} century and provided the first general proof that the Goldbach ternary problem has an affirmative answer for all sufficiently large odd integers.

It is worth noting that according to the (historical) Waring conjecture for prime numbers:[463] every odd integer ≥ 5 is either a prime number or the sum of three prime numbers. The recent proof of the Goldbach ternary conjecture makes this conjecture a proven theorem (noting that 5 is prime and "or" in

[463] Waring's conjecture for prime numbers is also known (possibly more commonly) as *Waring's problem* for prime numbers. We should also note that, according to some sources, the classical Waring problem is about powers of primes rather than primes (so please check).

the statement of Waring's conjecture is not exclusive; moreover ≥ 5 can be replaced by ≥ 3 and hence ≥ 5 seems to be for historical reasons).

5.1.43 Wilson's Theorem

According to this theorem, an integer $n > 1$ is prime *iff*

$$(n-1)! + 1 \equiv 0 \pmod{n} \tag{74}$$

The significance and usefulness of Wilson's theorem should be obvious as it provides a necessary and sufficient condition for primality, and hence it is met in many situations and contexts in number theory and related areas of mathematics (although it is not efficient for primality testing due to the fast factorial growth; see § 7.3.19). Also see § 2.1.91.

In fact, Wilson's theorem is largely used for educational and theoretical purposes (such as proving elementary theorems in number theory) rather than as a practical tool for computation (such as primality testing and sieving) even though it is involved in such practical applications in many situations and contexts indirectly through establishing theoretical foundations for practically-used theorems (as well as many minor results and corollaries). For example, it is used to prove Euler's criterion for the Legendre symbol, which in turn provides a foundation for the Solovay-Strassen test (see § 5.1.13 and § 7.3.18). So in short, the significance and usefulness of Wilson's theorem is mainly theoretical, while its practical utility manifests indirectly by establishing foundations for other results, methods and algorithms. Also see § 5.1.10 and § 7.3.21.

5.1.44 Zhang's Theorem

According to this theorem, the gaps between consecutive prime numbers are bounded infinitely often. More precisely, the theorem establishes that there exists a fixed upper bound c such that there are infinitely many pairs of consecutive primes differing by at most c. The size of this gap was originally about 70 million, but subsequent collaborative research reduced this value to 246.[464] The theorem is directly related to the twin prime conjecture (see Point 1 of § 6.1.34), which would be proven true if the bound c could be unconditionally reduced to 2. Analogously, reducing the bound to 4 or 6 would prove the infinitude of at least one gap size up to those bounds, which represents a major step toward proving the existence of infinitely many cousin or sexy primes (see § 2.1.10 and § 2.1.74).[465]

While Zhang's theorem is often referred to as the *bounded gaps theorem*, the latter term is broader. Zhang's result represents a specific instantiation of the bounded gaps theorem (which asserts that there exists a finite constant c such that there are infinitely many pairs of consecutive primes that differ by at most c). More generally, "bounded gaps theorem" can refer to a wider class of results and variations concerning the size, distribution, and characteristics of intervals between consecutive prime numbers, and hence we could have "bounded gaps theorems".

5.1.45 Zsigmondy's Theorem

This theorem is a fundamental result in number theory concerning the prime divisors of sequences of the form $a^n - b^n$ where $1 < n \in \mathbb{N}$. It states that for any two coprime positive integers $a > b > 0$, the expression $a^n - b^n$ will always have at least one primitive prime divisor (i.e. a prime number that divides $a^n - b^n$ but does not divide $a^k - b^k$ for any positive integer $1 \leq k < n$) except in two cases:

[464] Very recent claims have further reduced the bound to 240, and even to 186, but these results have not yet received independent verification.

[465] For example, if reduced to 6, it would guarantee the infinitude of at least one gap size up to 6, proving that at least one of twin, cousin, or sexy prime pairs occurs infinitely often.

• $n = 2$: $a + b$ is a power of 2 (e.g. $3^2 - 1^2 = 8$ whose only prime factor is 2, which already divides $3^1 - 1^1 = 2$).
• $n = 6$: $a = 2$ and $b = 1$ (giving $2^6 - 1^6 = 63 = 3^2 \times 7$. None of these primes are primitive, as 3 divides $2^2 - 1^2 = 3$ and 7 divides $2^3 - 1^3 = 7$).

The Zsigmondy theorem provides a powerful result about the divisibility of numbers and the prime factors involved in powers of integers. In short, it has many uses and applications in mathematics. For example, it is a valuable tool for proving that certain Diophantine equations have no solutions by showing that the prime factors required by the theorem cannot exist within the constraints of the equation. It may also be used in group theory to establish the existence of certain prime divisors of group orders and related quantities, which can help distinguish possible group orders except in specific known cases. While the theorem is not concerned with the overall distribution of prime numbers, it shows that, apart from its explicitly stated exceptional cases, new prime divisors continue to appear in sequences of the form $a^n - b^n$, making it an important tool in the study of divisibility properties of integer sequences.

We should finally note that Zsigmondy's theorem is a generalization of Bang's theorem which is the special case $b = 1$ of Zsigmondy's theorem. In turn, Carmichael's theorem may be viewed as a further generalization of Zsigmondy's theorem, since it extends the existence of primitive prime divisors from geometric sequences to the more general class of Lucas sequences.

5.2 Classification of Theorems

In this section we classify the theorems, results and facts about (or related to) prime numbers. Although the theorems of § 5.1 will be a major part of this classification, many other theorems (especially "small" ones) and results will be included. This classification is not comprehensive by any means, but it should give a good idea about the landscape of prime number theory in its basic substance and structure. This topic (like any other topic of this volume) should be extended substantially in the forthcoming volumes of this book.

5.2.1 Foundations

In this subsection, we list a collection of mostly elementary and foundational theorems (of rather general content) concerning prime numbers (or related to prime numbers) which are frequently encountered in elementary number theory:
1. Dirichlet's theorem on arithmetic progressions (see § 5.1.11).
2. Euclid's lemma (and generalized Euclid's lemma; see Point 19 in § 1.3).
3. Euclid's theorem on the infinitude of prime numbers (see § 1.6).
4. Euler's criterion (see § 5.1.13).
5. Euler's product formula (see § 5.1.14).
6. Fermat's little theorem (see § 5.1.15).
7. Fundamental theorem of arithmetic (see § 1.7).
8. Hensel's theorem (see § 5.1.19).
9. Lagrange's theorem on polynomial congruences (see § 5.1.22).
10. Legendre's formula (see § 5.1.23).
11. Prime number theorem (see § 5.1.31).
12. Prime number theorem for arithmetic progressions (see § 5.1.32).
13. Primes modulo 4 theorem (see § 5.1.33).
14. Primes modulo 6 theorem (see § 5.1.34).
15. Quadratic reciprocity law (see § 5.1.35).
16. Sum of two squares theorem (see § 5.1.41).

17. Wilson's theorem (see § 5.1.43).
18. There are many other basic theorems and results that we met earlier in this book that fall into this category (see for instance § 1.3 and § 1.4).

5.2.2 Existence

There are many theorems and facts about the existence of prime numbers of certain types (or in particular situations or conditions) or mathematical entities (e.g. numbers or sequences) related to primes. We list in the following some examples of these theorems and facts:

1. Baker-Harman-Pintz theorem (see § 5.1.1).
2. Bertrand's postulate (see § 5.1.2).
3. Chebyshev's theorem (i.e. the existence of constants a and A; see § 5.1.7).
4. Dirichlet's theorem (i.e. the existence of infinitely many primes in arithmetic progressions; see § 5.1.11).
5. Fundamental theorem of arithmetic (i.e. for every integer $n > 1$ there exists a unique factorization into prime numbers; see § 1.7).
6. Goldbach's ternary conjecture (i.e. the existence of a sum of three primes representing any odd integer $n \geq 7$; see § 5.1.16).
7. Green-Tao theorem (see § 5.1.17).
8. Hoheisel's theorem (see § 5.1.20).
9. Ingham's theorem [i.e. there exists at least one prime between n^3 and $(n+1)^3$ for all sufficiently large n].
10. Linnik's theorem (see § 5.1.24).[466]
11. Maynard's theorem (i.e. for every $m \in \mathbb{N}$, there exists a constant H_m such that there are infinitely many intervals of length H_m containing at least m distinct primes).
12. Mills' theorem (see § 5.1.30).
13. Nagura's theorem (i.e. for any $n \geq 25$, there exists at least one prime between n and $1.2n$).
14. Prime number theorem for arithmetic progressions (i.e. it implies the existence of infinitely many primes in arithmetic progressions; see § 5.1.32).
15. Siegel-Walfisz theorem (see § 5.1.39).
16. Sierpinski's theorem (i.e. there exist infinitely many positive odd integers k such that $2^n k + 1$ is composite for all $n \geq 1$; see § 7.9.4).
17. Sylvester-Schur theorem (see § 5.1.40).
18. Wilson's theorem [i.e. for every prime p there exists a congruence $(p-1)! + 1 \stackrel{p}{=} 0$; see § 5.1.43].
19. Wright's theorem.[467]
20. Zsigmondy's theorem (i.e. the existence of a primitive prime divisor; see § 5.1.45).[468]
21. There exist arbitrarily large prime numbers (as a consequence of the Euclid theorem on the infinitude of prime numbers; see § 1.6).
22. For every $n \geq 3$ there exists a prime p $(n < p < 2n)$ that divides the central binomial coefficient C_n^{2n}.[469]
23. For every $\varepsilon > 0$ and sufficiently large n there exists at least one prime p with $n < p < n(1+\varepsilon)$.[470]

[466] I.e. there exist positive constants c and L such that the smallest prime in an arithmetic progression $a \pmod d$ is less than cd^L where a and d are positive coprime integers and $1 \leq a \leq d-1$. The essence of this theorem is that it asserts the existence of a bound on the smallest prime in an arithmetic progression.

[467] Wright's theorem states: there exists a real number α (i.e. Wright's constant) such that $\lfloor g_n \rfloor$ is prime for all $n \geq 1$ (where $g_0 = \alpha$, and $g_{n+1} = 2^{g_n}$ for all $n \geq 0$).

[468] We may also include Bang's theorem (as a special case of Zsigmondy's theorem) and Carmichael's theorem (as a generalization of Zsigmondy's theorem) as existence statements (see § 5.1.45).

[469] This is essentially equivalent to Bertrand's postulate (see § 5.1.2) and the properties of this binomial coefficient are used in an elementary proof of the postulate.

[470] This is a consequence of the prime number theorem (see § 5.1.31).

24. There exists a sexy prime quintuplet, i.e. (5, 11, 17, 23, 29) only (see § 2.1.74).
25. There exists a twin prime triplet, i.e. (3, 5, 7) only (see § 2.1.84).
26. There exist arbitrarily large gaps between consecutive primes.[471]
27. There exist composite numbers n for which $a^n \overset{n}{=} a$ for all integers a (i.e. Carmichael numbers; see § 5.1.15, § 7.9.2 and § 9.7.1).
28. If a composite solution n to $\phi(n)|(n-1)$ does exist then it must be odd, square-free, and divisible by at least 14 distinct primes.[472] Moreover, it must be a Carmichael number (see § 6.1.22).
29. If an odd perfect number N does exist then its prime factorization must be of the form $N = q^k n^2$ where q is prime, $k \in \mathbb{N}$, $n \in \mathbb{Z}$, $q \overset{4}{=} 1$, $k \overset{4}{=} 1$, and $\gcd(q, n) = 1$.
30. If an odd perfect number (i.e. $N = q^k n^2$) exists then its non-Eulerian component must strictly exceed its Eulerian prime factor component (i.e. $q^k < n^2$).
31. If an odd perfect number N exists then it must have at least 10 distinct prime factors. Moreover, if $3 \nmid N$ then it must have at least 12 distinct prime factors.
32. We may also include in this category Bourgain's theorem on prime numbers with prescribed digits (which asserts the existence of primes in which a significant proportion of their digits are pre-selected or follow a specified pattern).
33. Theorems about infinitude (see § 5.2.4) are essentially about existence (i.e. of infinitely many). In fact, some of the theorems about finitude (see § 5.2.5) should also be so (i.e. they are essentially about existence of only finitely many).

5.2.3 Non-Existence

We refer first to § 2.8. The following are some other examples of the non-existence of prime numbers of certain types or categories or under certain conditions (or non-existence of something related to prime numbers):[473]

1. There is no "largest prime" (see § 1.6).
2. There is no integer > 1 with two distinct prime factorizations (ignoring the order of factors; see § 1.7).[474]
3. There is no integer > 1 with no prime divisor (see § 1.7).
4. There is no even prime beyond 2.
5. There is no prime p_n with $n \geq p_n$.
6. There is no prime in the sequence of $n-1$ consecutive integers: $n!+2, n!+3, \ldots, n!+n$ $(n \geq 2)$.
7. There is no prime p such that $p+4, p+8, p+12$ are all primes.
8. There is no multi-digit prime (in base 10) that ends in 0, 2, 4, 5, 6, or 8.
9. There is no prime of the form $4k+3$ $(k \in \mathbb{N}_0)$ that can be expressed as a sum of two perfect squares (see § 5.1.41).
10. There is no prime with more than one representation (up to changing signs and exchanging terms) as a sum of two squares (see § 5.1.41).
11. There is no prime of the form $2^n + 1$ where $n \in \mathbb{N}$ is not a power of 2 (see § 2.1.20).
12. There is no prime of the form $a^n + 1$ where $1 < a \in \mathbb{N}$ and $n \in \mathbb{N}$ is not a power of 2 (see § 2.1.24).
13. There is no prime of the form $2^n - 1$ with a composite index $n \in \mathbb{N}$ (see § 2.1.41).
14. There is no prime of the form $a^n - b^n$ where $1 < n \in \mathbb{N}$, $a, b \in \mathbb{N}$ and $|a-b| > 1$.[475]
15. There is no prime of the form $a^n + b^n$ where $1 < n \in \mathbb{O}$, $a, b \in \mathbb{N}$ and $a + b \neq 2$.

[471] Alternatively: there exist arbitrarily long sequences of consecutive composite numbers.
[472] According to a rather recent study, "at least 15 distinct primes" with $n > 10^{30}$ (but please check).
[473] For base-specific statements in which no numeral system is specified, the default is base 10.
[474] We note that 0 and 1 have no prime factorization. Negative integers (excluding -1) possess a unique factorization consisting of the factor -1 together with the prime factorization of their positive counterparts.
[475] As a special case: there is no prime of the form $a^n - 1$ where $2 < a \in \mathbb{N}$ and $1 < n \in \mathbb{N}$.

16. There is no prime of the form $2n^2 + 3n + 1$ (where $n \in \mathbb{N}$).
17. There is no prime of the form $3^n + 1$ (where $n \in \mathbb{N}$).
18. There is no prime of the form $n^3 + 1$ for $n > 1$ ($n \in \mathbb{N}$).
19. There is no prime of the form $n^4 + 4^n$ for $n > 1$ ($n \in \mathbb{N}$).
20. There is no prime of the form $n^n - 1$ for $n > 2$ ($n \in \mathbb{N}$).
21. There is no prime of the form $p^2 + 2$ for $p > 3$ (where $p \in \mathbb{P}$).
22. There is no centered k-gonal primes for $k = 8$ and $k = 9$ (see § 2.1.5).
23. There is no 10-digit pandigital prime in base 10 (see § 2.1.55).
24. There is no multi-digit circular prime that contains digits other than 1, 3, 7, and 9 (see § 2.1.7).
25. There is no dihedral prime that contains digits other than 0, 1, 2, 5, and 8 (see § 2.1.16).
26. There is no multi-digit permutable prime that contains digits other than 1, 3, 7, and 9 (see § 2.1.58).
27. There is no strobogrammatic prime that contains digits other than 0, 1, 6, 8, and 9 (see § 2.1.78).
28. There is no permutable prime that uses more than two distinct digits (see § 2.1.58).
29. There is no Fibonacci prime > 3 with a composite index (see § 2.1.21).
30. There is no Jacobsthal prime > 5 with a composite index (see § 2.1.36).
31. There is no Pell prime with a composite index (see § 2.1.57).
32. There is no repunit prime with a composite index (see § 2.1.69).
33. There is no prime number such that for every digit position and every replacement by a different digit, the resulting number is still prime.[476]
34. There is no prime p such that p^2 divides the central binomial coefficient C_p^{2p}.
35. There is no prime of the form $4k + 3$ that divides a number of the form $n^2 + 1$.
36. There is no odd prime p for which the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ is not cyclic.
37. There is no prime $p > 3$ that divides $2^p + 1$.
38. There is no prime $p > 5$ for which the period of $1/p$ in base 10 is not a divisor of $p - 1$.
39. There is no prime triple of the form $(p, p + 2, p + 4)$ beyond (3, 5, 7).
40. There are no two consecutive Fibonacci numbers that are both prime beyond (2, 3) and (3, 5).
41. There are no four primes forming an arithmetic progression with common difference less than 6 and first term greater than 3.
42. There is no non-constant infinite arithmetic progression consisting solely of prime numbers.
43. There is no non-constant polynomial $P(n)$ with integer coefficients that yields a prime number for every integer n.[477]
44. There is no rational function that generates the entire set of primes exclusively.[478]
45. There is no prime gap of 1 beyond (2, 3).[479]
46. There is no upper limit on the gap between consecutive primes.
47. There is no finite period for the sequence of gaps between consecutive primes.
48. There is no zero of the Riemann zeta function on the line $\Re(s) = 1$ where $\Re(s)$ is the real part of the complex variable s.[480]
49. There is no Fermat number that is a Carmichael number.[481]
50. Theorems about finitude (see § 5.2.5) are, in a sense, about non-existence (i.e. beyond the finitely many). This similarly applies to oddities and exceptions (see § 1.5).

---

[476] In a sense, this is the opposite of Erdos' theorem on delicate primes (see § 2.1.15).

[477] This may be stated with "every positive integer".

[478] A rational function $f(n)$ means $f(n) = \frac{P(n)}{Q(n)}$ where P and Q are polynomials. "Exclusively" means it does not output any non-prime values.

[479] Alternatively, there is no prime pair $(p, p + 1)$ beyond $p = 2$.

[480] Although there is no mention of primes in this statement, it is essential for the proof of the prime number theorem (see § 5.1.31).

[481] Alternatively, there is no Fermat number that is a pseudoprime to every base coprime to it.

5.2.4 Infinitude

In § 1.6 we discussed the infinitude of prime numbers in general (i.e. there are infinitely many prime numbers according to Euclid's theorem). In this subsection we discuss the infinitude of certain types (or categories or sequences) of prime numbers whose status (as having infinitely many members) has been established as proven theorems or facts. The following are common examples of such theorems and facts (where for brevity we only list the names or labels of the infinite types and categories):

1. Chen primes (see § 2.1.6).
2. Delicate primes (in any base; see § 2.1.15).
3. Good primes (of each version; see § 2.1.26).
4. Irregular primes of Bernoulli type (see § 2.1.32).
5. Irregular primes of Euler type (see § 2.1.33).
6. Irregular primes of Genocchi type (see § 2.1.34).
7. Isolated primes (see § 2.1.35).[482]
8. Mersenne divisors (see § 2.1.42).
9. Mills' primes (see § 2.1.44).
10. Non-Pythagorean primes (a consequence of Dirichlet's theorem and PNTAP; see Point 24).
11. Pillai primes (see § 2.1.61).
12. Prime-indexed primes (see § 2.1.62).
13. Pythagorean primes (a consequence of Dirichlet's theorem and PNTAP; see Point 24).[483]
14. Ramanujan primes (see § 2.1.68).
15. Self primes in every odd base (see § 2.1.73).
16. Strong primes (see § 2.1.79).
17. "Supersingular primes" related to elliptic curves (see § 2.1.80).
18. Weak primes (see § 2.1.89).
19. Primes of Chen's theorem II (see § 5.1.9) noting the relationship to Chen primes which we listed already (see Point 1), i.e. Chen primes are a special case of this type of primes.
20. Odd primes (i.e. there are infinitely many odd primes).
21. Primes that divide zero (i.e. all primes).
22. Primes ending in 1, 3, 7, or 9.[484]
23. Primes that do not contain a specific digit (such as 7) in their decimal expansion.
24. Primes of the form $a + kd$ (i.e. primes in arithmetic progressions; see § 5.1.11 and § 5.1.32).[485]
25. Primes of the form $x^2 + y^2$ where x, y are integers (as a consequence of the infinitude of Pythagorean primes; see § 5.1.41).
26. Primes of the form $x^2 + y^4$ where x and y are integers (Friedlander-Iwaniec theorem).[486]
27. Primes of the form $x^2 + ny^2$ where $n \in \mathbb{N}$ is fixed and x, y are integers (subject to certain restrictions), e.g. $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$ and $x^2 + 7y^2$.
28. Primes of the binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ (see § 5.1.3).[487]
29. Primes of the form $x^3 + 2y^3$ where x and y are integers (Heath-Brown theorem).
30. Primes that divide numbers of the form $a^n - 1$ where $a, n \in \mathbb{N}$ and $a > 1$.[488]

[482] This should trivially establish the infinitude of primes p such that $p - 2$ (or $p + 2$) is composite.

[483] The infinitude of Pythagorean primes (as primes of the form $x^2 + y^2$) is also proven independently (see Point 27).

[484] This is a direct consequence of Dirichlet's theorem on arithmetic progressions (see § 5.1.11).

[485] Primes of the forms $(4k + 1)$, $(4k + 3)$, $(6k + 1)$ and $(6k + 5)$ are common examples of the primes of the form $a + kd$ (see § 5.1.33 and § 5.1.34).

[486] It is worth noting that the variables x and y in the expression $x^2 + y^4$ must be able to vary independently for the theorem to work, and hence this theorem does not imply, for instance, the infinitude of $n^2 + 1$ primes (whose infinitude is only conjectured; see § 2.1.47).

[487] This is a generalization of Point 27.

[488] This is a generalization of Point 8.

31. Primes that divide at least one Fibonacci number.[489]
32. Primes that divide at least one term of any non-degenerate linear recurrence sequence.
33. Primes that divide at least one Catalan number.[490]
34. Primes that divide at least one Fermat number.
35. Primes that divide at least one Mersenne number.
36. Primes p such that p divides the numerator of at least one harmonic number.[491]
37. Primes p such that $p-1$ is divisible by any fixed prime q.
38. Primes p such that $p-1$ is square-free.
39. Primes p such that $p+1$ is square-free.
40. Primes p such that $p-1$ has a prime factor greater than $p^{1/2}$.[492]
41. Primes p such that $p-1$ has a prime factor exceeding p^c for some constant $c > 1/2$.
42. Primes p such that $p-1$ has a prime factor greater than $p^{2/3}$.
43. Primes p such that $p+1$ has a prime factor exceeding p^c for some constant $c > 1/2$.[493]
44. Primes that are sums of three squares.[494]
45. Primes p such that $p-1$ is a sum of two squares.
46. Primes of the form $x^2 + y^2 + z^c$ ($x, y, z \in \mathbb{Z}$ and for any $c \in \mathbb{N}$).[495]
47. Primes of the form $\text{floor}(n^c)$ where $n \in \mathbb{N}$ and $1 < c < 243/205$.[496]
48. Primes of the form $\lfloor \alpha n + \beta \rfloor$ where $n = 1, 2, \ldots$ with irrational $\alpha > 1$ and $\beta \in \mathbb{R}$ (primes in the Beatty sequence).[497]
49. Primes that do not contain any specific digit from 0-9 in their decimal expansion.[498]
50. Primes whose expansion begins with any fixed prefix (not starting with zero).
51. Primes containing any fixed finite digit string as a sub-string.[499]
52. Primes with an even sum of digits, and primes with an odd sum of digits.[500]
53. Primes whose sum of digits is prime.
54. Primes that are not of the form $2^a 3^b + 1$.[501]
55. Primes p such that the Legendre symbol $\left(\frac{2}{p}\right) = 1$ $\left[\text{and similarly for } \left(\frac{2}{p}\right) = -1\right]$.[502]
56. Primes p such that the prime gap after p is smaller than the average $\ln p$.
57. Pairs of primes (p, q) such that $|p - q| < H$ where H is a finite constant (Zhang's theorem; see §

---

[489] In fact, a much stronger statement is true, that is: every prime number divides at least one Fibonacci number.

[490] In fact, a much stronger statement is true, that is: every prime number divides infinitely many Catalan numbers.

[491] In fact, a stronger statement is true, that is: every prime $p \geq 5$ divides the numerator of at least one harmonic number.

[492] In fact, there are stronger results than this (see for instance the next points).

[493] It is widely believed that there are infinitely many primes p such that both $p-1$ and $p+1$ have a prime factor exceeding p^c for some constant $c > 1/2$. This seems to be proven rather recently (but please check).

[494] This is a corollary of Legendre's three square theorem which states: a number $n \in \mathbb{N}$ can be expressed as a sum of three squares *iff* $n \neq 4^m(8k+7)$ where $m, k \in \mathbb{N}_0$. The actual proof of infinitude relies on Dirichlet's theorem (see § 5.1.11).

[495] Taking $z = 1$ reduces this to Point 45, i.e. the two statements are essentially identical. So please check if this statement is proved for general z (i.e. not only for $z = 1$). We suspect that for genuinely variable z (or for some $z \neq 1$), the statement is only conjectured.

[496] A recent paper seems to push this limit to $1 < c < 6/5$ (but further checks are required).

[497] Whether it is proven for every irrational $\alpha > 1$ and any real β should be checked.

[498] It seems that we can even exclude multiple digits and still find infinitely many primes (with some conditions). A related problem (which is not clear in the literature) is whether "there are infinitely many primes p such that the digits of p are all odd". The claimed validity of this proposition should be checked although it is more likely to be a yet-unproven conjecture.

[499] Some sources classify this as a conjecture, but it seems to be fully proven.

[500] In fact, each occurs with an asymptotic density $1/2$ among primes (i.e. they are "balanced" in a strong statistical meaning).

[501] In fact, the form $2^a 3^b + 1$ is just an example. There are many other forms to which this statement applies and can be proved.

[502] This is a result of Dirichlet's theorem on arithmetic progressions and prime number theorem for arithmetic progressions (see § 5.1.11 and § 5.1.32) noting that PNTAP shows that each has relative asymptotic density $1/2$ among the primes.

5.1.44).[503]

We should also list the following theorems and statements which are about (or related to) the infinitude of primes:

A. Iwaniec theorem (see § 5.1.21).
B. Maynard's theorem (i.e. for every $m \in \mathbb{N}$, there is a constant H_m such that there are infinitely many intervals of length H_m containing at least m distinct primes).
C. Green-Tao theorem (see § 5.1.17) implies that there are infinitely many distinct arithmetic progressions consisting entirely of prime numbers (although it does not imply the existence of a single infinite such sequence).[504]
D. There are infinitely many polynomial progressions of primes (Green-Tao-Ziegler theorem).
E. There are infinitely many primes in the Euclid-Mullin sequence (although it is unproven, but conjectured, that the sequence contains all primes). See § 9.1.4.
F. There are infinitely many Chebyshev primes (according to some definitions; see § 2.2.1).
G. There are infinitely many non-Wieferich primes (if the *abc* conjecture holds; see § 2.1.90 and § 6.1.1).
H. There are infinitely many $n > 0$ such that $2p_n < p_{n-i} + p_{n+i}$ for all $0 < i < n$.[505]
I. For every positive integer M, there exist infinitely many pairs of consecutive primes (p_n, p_{n+1}) such that $\gcd(p_n - 1, p_{n+1} - 1) > M$ (where p_n denotes the n^{th} prime number).
J. Every finite sequence of digits occurs in infinitely many primes.
K. There exists a real number α (i.e. Wright's constant) such that $\lfloor g_n \rfloor$ is prime for all $n \geq 1$ (where $g_0 = \alpha$, and $g_{n+1} = 2^{g_n}$ for all $n \geq 0$).[506]
L. There are infinitely many absolute pseudoprimes (i.e. Carmichael numbers; see § 9.7.1). This also applies to other types of pseudoprimes (see the subsections of § 9.7 such as § 9.7.3 and § 9.7.4).
M. There are infinitely many Riesel numbers (see § 7.9.3).
N. There are infinitely many Sierpinski numbers (see § 7.9.4).
O. Also see Point 3 of § 2.1.55 regarding the infinitude of non-strict pandigital primes.

5.2.5 Finitude

In this subsection we list common theorems about the finitude of certain types and categories of prime numbers (i.e. types and categories of prime numbers which have only finitely many members). For brevity, we only list the names or labels of the finite types and categories:

1. Catalan primes (see § 2.1.4).
2. Centered k-gonal primes for $k = 8$ and $k = 9$ (i.e. there are no centered k-gonal primes for $k = 8$ and $k = 9$; see § 2.1.5).
3. Higgs primes of the first order (see § 2.1.29).
4. Minimal primes (see § 2.1.45).[507]
5. Repunit primes (in perfect-power bases; see § 2.1.69).[508]
6. "Supersingular primes" related to monstrous moonshine theory (see § 2.1.80).
7. Truncatable primes (in base 10; see § 2.1.83).[509]
8. Even primes (i.e. there is exactly one even prime, namely 2).
9. Primes that divide a given non-zero integer (see § 1.7). This also applies to any finite set of non-zero

[503] We may also say: there are infinitely many intervals of bounded length containing at least two primes.
[504] In fact, there is no non-constant infinite arithmetic progression of primes.
[505] This is stronger than the infinitude of weak primes (see § 2.1.89).
[506] This is Wright's theorem.
[507] In fact, there are only finitely many minimal primes in any base $b \geq 2$.
[508] In short, if $b > 2$ is a perfect power, there is at most one repunit prime in base b, as a consequence of repunit factorization.
[509] Regarding other bases, see Point 7 of § 2.1.83.

integers.
10. Primes with exactly k digits in any fixed base $b \geq 2$, for any fixed $k \in \mathbb{N}$.
11. Primes p ($\neq 2, 5$) such that the period of $1/p$ has a specific fixed length n.[510]
12. We should also refer to § 1.5 for examples of forms or categories of prime numbers that have only finitely many members (e.g. the only prime of the form $n^3 - 1$ is 7).

5.2.6 Distribution

In this subsection we list some of the common theorems about the distribution of prime numbers (or related to their distribution) in various senses and contexts:[511]
1. Baker-Harman-Pintz theorem (see § 5.1.1).
2. Bertrand's postulate (see § 5.1.2).
3. Bombieri-Vinogradov theorem (see § 5.1.4).
4. Brun's theorem (see § 5.1.5).
5. Brun-Titchmarsh theorem (see § 5.1.6).
6. Chebyshev's theorem (see § 5.1.7).
7. Chen's theorem II (see § 5.1.9).
8. Dirichlet's theorem on arithmetic progressions (see § 5.1.11).
9. Erdos-Kac theorem (see § 5.1.12).
10. Euler's product formula (see § 5.1.14).
11. Goldbach's ternary conjecture (see § 5.1.16).
12. Green-Tao theorem (see § 5.1.17).
13. Hoheisel's theorem (see § 5.1.20).
14. Linnik's theorem (see § 5.1.24).
15. Littlewood's theorem (see § 5.1.25).
16. Maier's theorem (see § 5.1.26).
17. Mertens' first theorem (see § 5.1.27).
18. Mertens' second theorem (see § 5.1.28).
19. Mertens' third theorem (see § 5.1.29).
20. Prime number theorem (see § 5.1.31).
21. Prime number theorem for arithmetic progressions (see § 5.1.32).
22. Riemann-von Mangoldt formula (see § 5.1.36).
23. Robin's theorem (see § 5.1.37).
24. Selberg's formula (see § 5.1.38).
25. Siegel-Walfisz theorem (see § 5.1.39).
26. Sylvester-Schur theorem (see § 5.1.40).
27. Zhang's theorem (see § 5.1.44).

We should also list the following "minor" theorems and results about (or related to) the distribution of prime numbers:

A. Chen primes contain arbitrarily long arithmetic progressions (see § 2.1.6).
B. All lower members of twin prime pairs are Chen primes, but only some upper members of twin prime pairs are Chen primes (see § 2.1.6, § 2.1.84 and § 4.7.3).
C. In a twin prime pair (p_n, p_{n+1}) where $p_n > 5$, p_n is always a strong prime and p_{n+1} is always a weak prime (see § 2.1.79, § 2.1.84 and § 2.1.89).

[510] I.e. for any fixed positive integer n there are only finitely many primes p ($\neq 2, 5$) such that the decimal expansion of $1/p$ has minimal period exactly n.

[511] "Distribution" in the title of this section should be understood broadly, i.e. it should include things like: distribution, counting, density, gaps, arithmetic progressions, and so on (as well as things related to these concepts).

D. The prime gap preceding a cluster prime is always less than or equal to 6, i.e. 2 or 4 or 6 (see § 2.1.8).
E. There are arbitrarily large gaps between consecutive primes.
F. The only prime triplet of the form $(p, p+2, p+4)$ is (3, 5, 7). See § 2.1.10.
G. Prime numbers are equally distributed asymptotically among residue classes modulo 10 that are coprime to 10, i.e. 1, 3, 7, 9 (a consequence of Dirichlet's theorem and PNTAP; see § 5.1.11 and § 5.1.32).[512]
H. For a set of primes P_d whose leading digit is $d \in \{1, \ldots, b-1\}$ in base $b \geq 2$, the Dirichlet (analytic) density relative to the set of all primes is $\log_b(1 + 1/d)$.[513]
I. Asymptotically, prime numbers in any base ≥ 2 with odd/even number of digits have 50% frequency over the long term, in the sense of Dirichlet (analytic) density.
J. Asymptotically, the probability of a randomly chosen n-digit number being prime is inversely proportional to n (a consequence of the prime number theorem; see § 5.1.31).[514]
K. We may also include in the "Distribution" category the Bourgain theorem on prime numbers with prescribed digits (which we indicated earlier; see Point 32 of § 5.2.2).
L. We should also refer to the Chebyshev bias (see § 8.7.1) which is obviously related to the "Distribution" category of theorems.
M. We should also refer to the Lemke Oliver and Soundararajan bias (where consecutive prime numbers are significantly less likely to end in the same digit than would be expected if they were truly random).[515]
N. We should also refer to § 8.2 and § 8.3 which contain many mathematical relations (mainly formulae, equations and inequalities) that represent (or based on) theorems related to the distribution of prime numbers.
O. We may also broadly classify theorems concerning the infinitude and finitude of specific prime types and families (see for instance § 5.2.4 and § 5.2.5) under the "Distribution" category (or at least as closely related to it), since questions of infinitude and finitude concern the global distribution of these prime families, including their asymptotic behavior and whether they persist indefinitely. Although such theorems do not necessarily provide asymptotic densities or counting formulae, they nevertheless address the long-term occurrence and global behavior of these prime types and families.
P. Also see chapter 8 in general.

5.2.7 Algebraic Forms

In this subsection we list some of the common theorems and results about the algebraic forms of prime numbers and related issues:

A. Binary quadratic prime theorem (see § 5.1.3).
B. Dirichlet's theorem on arithmetic progressions (see § 5.1.11).
C. Mills' theorem (see § 5.1.30).
D. Iwaniec's theorem (see § 5.1.21).
E. Primes modulo 4 theorem (see § 5.1.33).
F. Primes modulo 6 theorem (see § 5.1.34).
G. Prime number theorem for arithmetic progressions (see § 5.1.32).
H. Sum of two squares theorem (see § 5.1.41).

We should also list the following "minor" theorems and supplementary results about (or related to) the

[512] More generally (and rather loosely), prime numbers are evenly distributed among residue classes coprime to the base of the numeral system.
[513] This is the same logarithmic distribution that appears in Benford's law.
[514] More precisely, for a fixed base $b \geq 2$, the probability that a uniformly chosen n-digit number is prime is asymptotic to $1/(n \log b)$.
[515] More clearly, consecutive primes are significantly less likely to share the same last digit (i.e. 1, 3, 7 and 9 in base 10) than 25%. However, this seems to be a computationally observed bias (within the investigated ranges) rather than an unconditional asymptotic theorem. Also see Point 23 of § 6.2.6.

forms of prime numbers:

1. Every odd prime can be expressed as a difference of two perfect squares.
2. For $2^n + 1$ to be prime, n must be a power of 2 (see § 2.1.20). More generally, if $a^n + 1$ (where $a, n \in \mathbb{N}$ and $a > 1$) is prime, then n must be a power of 2.
3. If $2^k + 1$ is prime then $2^k + 1 \neq m^p - n^p$ where $k, m, n \in \mathbb{N}$, $m > n$, and p is an odd prime.
4. No Fermat prime F_k can be expressed as $F_k = s^p - t^p$ where $s, t \in \mathbb{N}$ $(s > t)$ and p is an odd prime (see § 2.1.20).
5. All Fermat primes (except 3) are Pythagorean primes (see § 2.1.20 and § 2.1.66).
6. A prime of the form $n^n + 1$ is either 2 or a Fermat prime $(n \in \mathbb{N})$.
7. Every prime is expressible as a sum of four squares.[516]
8. The primes that can be written as the sum of two primes are exactly the larger elements of twin prime pairs (since one of the two primes in the sum must be 2).
9. Every Pythagorean prime can be uniquely expressed as a sum of two perfect squares. Conversely, every prime other than 2 that is a sum of two perfect squares is a Pythagorean prime (see § 2.1.66).
10. If $2^n - 1$ is prime then n is prime. Equivalently, if n is composite then $2^n - 1$ is composite (see § 2.1.41).
11. For $n \in \mathbb{N}_0$, the only prime of either form $3^n \pm 1$ is 2, i.e. $2 = 3^0 + 1 = 3^1 - 1$.
12. For $n \in \mathbb{Z}$, the only prime of the form $2n^2 + 3n + 1$ is 3 (i.e. when $n = -2$).
13. The only prime that is a factorial number is 2 (i.e. $2 = 2!$).[517]
14. The only factorial prime that can be generated by two distinct values of n is 2, i.e. $2 = 0! + 1$ and $2 = 1! + 1$ (see § 2.1.19).
15. The only primes p for which both $2p - 1$ and $2p + 1$ are prime are $p = 2$ and $p = 3$.
16. For $n \geq 3$, if $n + 1$ is prime then $n! + 1$ cannot be prime (see § 2.1.19).
17. The only prime that is a triangular number is 3.
18. The only prime of the form $2^m + 1$ (i.e. Fermat) and the form $2^n - 1$ (i.e. Mersenne) simultaneously is 3 (i.e. $m = 1$ and $n = 2$).
19. The only $n \in \mathbb{N}$ for which both $(2^n - 1)$ and $(2^n + 1)$ are prime is $n = 2$.
20. The only prime of the form $n^2 - 1$ is 3 $(n \in \mathbb{Z})$.
21. The only prime of the form $n^3 + 3n^2 + 5n + 6$ $(n \in \mathbb{Z})$ is 3 (corresponding to $n = -1$).
22. The only prime of the form $n^2 - 4$ is 5 (where $n \in \mathbb{Z}$).
23. The only prime of the form $2^p + 1$ is 5 (where $p \in \mathbb{P}$).[518]
24. The only prime that is the sum and difference (simultaneously) of pairs of distinct primes is 5, i.e. $5 = 2 + 3$ and $5 = 7 - 2$.
25. The only prime of the form $n^3 - 1$ is 7 $(n \in \mathbb{N})$.
26. The only prime of the form $4^{n+2} + 2^n$ $(n \in \mathbb{N}_0)$ is 17 (corresponding to $n = 0$).
27. The only value $n \in \mathbb{N}$ for which n, $n + 16$ and $n + 20$ are all primes is $n = 3$.
28. The only value $n \in \mathbb{N}$ for which n, $8n^2 + 1$ and $8n^2 + 2n + 1$ are all primes is $n = 3$.
29. A prime is expressible as a difference of two integer squares *iff* it is odd, in which case the two integers are consecutive.
30. A prime p is expressible as $p = x^2 + 3y^2$ $(x, y \in \mathbb{Z})$ *iff* $p = 3$ or $p \overset{3}{=} 1$.
31. A prime p is expressible as $x^2 + xy + y^2$ $(x, y \in \mathbb{Z})$ *iff* $p = 3$ or $p \overset{3}{=} 1$.
32. A prime p is expressible as $p = x^2 + 2y^2$ $(x, y \in \mathbb{Z})$ *iff* $p = 2$ or $p \overset{8}{=} 1$ or $p \overset{8}{=} 3$.
33. A prime p is expressible as $p = x^2 + 5y^2$ $(x, y \in \mathbb{Z})$ *iff* $p = 5$ or $p \overset{20}{=} 1$ or $p \overset{20}{=} 9$.
34. A prime p is expressible as $x^2 + 5y^2$ or $2x^2 + 2xy + 3y^2$ $(x, y \in \mathbb{Z})$ *iff* $p = 2$ or $p = 5$ or $p \overset{20}{=} 1, 3, 7$ or 9.

---

[516] In fact, this is Lagrange's four-square theorem (applied to primes) which states: every non-negative integer can be expressed as the sum of four integer squares.

[517] In fact, 2 is also a factorial prime, i.e. a prime of the form $n! + 1$ (corresponding to $n = 1$; see § 2.1.19).

[518] Actually, all integers of the form $2^n + 1$ are composite (where n is an odd integer greater than 1).

35. A prime $p > 2$ is expressible as $p = x^2 + 6y^2$ $(x, y \in \mathbb{Z})$ *iff* $p \overset{24}{\equiv} 1$ or $p \overset{24}{\equiv} 7$.
36. Every cuban prime of the first kind is a centered hexagonal number (see § 2.1.11).
37. All generalized Fermat primes with $n > 0$ are congruent to 1 modulo 4 (see § 2.1.24).
38. Any prime factor p of a Fermat number $2^{2^k} + 1$ $(k \geq 2)$ must be of the form $p = 2^{k+2} \cdot n + 1$ where $n \in \mathbb{N}$.
39. If an odd prime p is a generalized Fermat prime (with $n > 0$) then there is an integer c such that $p = c^2 + 1$.
40. All Jacobsthal primes (excluding $J_4 = 5$) are of the form $4k - 1$ for some $k \in \mathbb{N}$ (see § 2.1.36).
41. Any prime divisor of a Mersenne number $M_p = 2^p - 1$ (where p is an odd prime) is of the form $2kp + 1$ where $k \in \mathbb{N}$ (see § 2.1.41).
42. All Sophie Germain primes which are > 3 are of the form $6k - 1$ (where $k \in \mathbb{N}$).
43. There are no primes of the form $a^n - 1$ $(1 < n \in \mathbb{N})$ for any $2 < a \in \mathbb{N}$ (see § 2.1.41).
44. All Mersenne primes are Mersenne divisors (see § 2.1.41 and § 2.1.42).
45. All odd primes of the forms $n^2 + 1$ and $n^4 + 1$ have even n (see § 2.1.47 and § 2.1.48).
46. The form of a near-square prime may not be unique (see § 2.1.49).
47. All the prime factors of $(p - 1)$ are 2 or 3 where p is a Pierpont prime (see § 2.1.60).
48. All Pierpont primes (excluding 2 and Fermat primes) are of the form $6n + 1$ for some $n \in \mathbb{N}$ (see § 2.1.60).
49. For all quartan primes (except 2), x and y must have opposite parity (see § 2.1.67).
50. All quartan primes (except 2) can be expressed as $16n + 1$ for some $n \in \mathbb{N}$ (see § 2.1.67).
51. Every prime number (and actually every positive integer) can be expressed as a sum of distinct Tribonacci numbers (see § 2.1.82).
52. Any twin prime pair other than $(3, 5)$ can be expressed as $(6n - 1, 6n + 1)$ where $n \in \mathbb{N}$ (see § 2.1.84).
53. All Wagstaff primes are of the form $4k - 1$ for some $k \in \mathbb{N}$ (see § 2.1.87).
54. The primes of the form $4n + 1$ $(n \in \mathbb{N})$ and the odd primes of the form $x^2 + y^2$ $(x, y \in \mathbb{N})$ are the same.
55. Every odd prime of the form $n^2 + 1$ is congruent to 1 (mod 4).[519]
56. $(2m)^{2n+1} + 1$ cannot be prime (for all $m, n \in \mathbb{N}$).
57. A binomial coefficient C_k^n is prime *iff* n is prime and $k = 1$ or $k = n - 1$.
58. Also see § 5.2.3 for theorems about the non-existence of primes of certain algebraic forms (e.g. centered k-gonal primes for $k = 8$ and $k = 9$).
59. Also see § 5.2.4 for theorems about the infinitude of primes of certain algebraic forms (e.g. $x^2 + y^4$). Other subsections of this section also contain theorems relevant to the current subsection.

5.2.8 Numeric Forms

In this subsection we list some of the common theorems and facts about the numeric forms of prime numbers and related issues (which are mostly about the digit and string format of prime numbers and are normally base-dependent):[520]

1. The primality of any prime number is independent of the numeral system (e.g. binary or decimal) used to represent it and its digital format (see § 1.3).
2. The last digit of any multi-digit prime must be 1, 3, 7, or 9 (in decimal system; see § 1.4).
3. Asymptotically, decimal primes end in 1, 3, 7, or 9 with equal relative frequency of 25% each.[521]
4. A circular prime (except 2 and 5) can contain only the digits 1, 3, 7, and 9 (see § 2.1.7).

[519] Equivalently, every odd prime of the form $n^2 + 1$ is Pythagorean.

[520] For base-specific statements in which no numeral system is specified, the default is base 10.

[521] This is an instance of the prime number theorem for arithmetic progressions (see § 5.1.32), which establishes that primes are asymptotically equidistributed among the residue classes relatively prime to a fixed modulus. More generally, in base b, apart from the finitely many primes dividing b, the final digits that are relatively prime to b occur with equal asymptotic frequency $1/\phi(b)$, where ϕ is the totient function.

5. A dihedral prime can contain only the digits 0, 1, 2, 5, and 8 (see § 2.1.16).
6. A permutable prime (except 2 and 5) can contain only the digits 1, 3, 7, and 9 (see § 2.1.58).
7. A permutable prime cannot use more than two distinct digits (see § 2.1.58).
8. A strobogrammatic prime can contain only the digits 0, 1, 6, 8, and 9 (see § 2.1.78).
9. The only prime whose digits are all even is 2.
10. The only multi-digit prime numbers with identical digits are repunits (see § 2.1.69).
11. The number of digits of a repunit prime must be a prime number (see § 2.1.69).
12. In the binary number system, all Mersenne numbers (and hence all Mersenne primes) are repunits (see § 2.1.41 and § 2.1.69).
13. The last digit of all Fermat primes greater than 5 is 7 (see § 2.1.20).
14. A multi-digit minimal prime cannot contain any of the digits 2, 3, 5, or 7 (see § 2.1.45).
15. Every prime number in base 10 is either a minimal prime or it contains at least one minimal prime as a sub-sequence of its digits (see § 2.1.45).
16. The only even-length palindromic prime in base 10 is 11 (see § 2.1.53).
17. A palindromic wing prime must have an odd number of digits greater than or equal to 3 (see § 2.1.54).
18. Any pandigital prime in base 10 must contain at least 11 digits (see § 2.1.55).
19. There is no prime number such that for every digit position and every replacement by a different digit, the resulting number is still prime.
20. Asymptotically, the probability of a randomly chosen n-digit integer being prime is inversely proportional to n (a consequence of the prime number theorem; see § 5.1.31).
21. For a set of primes P_d whose leading digit is $d \in \{1, \ldots, b-1\}$ in base $b \geq 2$, the Dirichlet (analytic) density relative to the set of all primes is $\log_b(1 + 1/d)$.
22. Asymptotically, prime numbers in any base ≥ 2 with odd/even number of digits have 50% frequency over the long term, in the sense of Dirichlet (analytic) density.
23. The sum of digits of prime numbers is equidistributed in arithmetic progressions (Mauduit-Rivat theorem).[522]
24. For any prime p (other than 2 and 5) the decimal expansion of $1/p$ is always a purely repeating (i.e. periodic) decimal.
25. Noting that theorems like "there are infinitely many primes ending in 1, 3, 7, or 9" are a direct consequence of Dirichlet's theorem on arithmetic progressions (see § 5.1.11), we may also include Dirichlet's theorem in the category of "Numeric Forms" theorems. In fact, this should apply even to the prime number theorem for arithmetic progressions (see § 5.1.32 and footnote [521]).
26. We may also include in the "Numeric Forms" category Bourgain's theorem on prime numbers with prescribed digits (which we indicated earlier; see Point 32 of § 5.2.2).
27. We may also include in this category the Copeland-Erdos theorem which states that the constant formed by concatenating the decimal representations of the prime numbers in increasing order (i.e. $0.2357111317\ldots$) is normal in base 10.[523]
28. We may also refer to the Chebyshev bias (see § 8.7.1), which may cause certain last digits to appear more frequently than others in finite ranges of primes, through biases among the corresponding residue classes.[524]
29. We may also refer to the Lemke Oliver and Soundararajan bias (which we indicated earlier; see Point M of § 5.2.6).[525]

[522] This is a rough statement of this theorem. The readers should refer to the literature for a more precise version.

[523] A real number is normal in base b if, in its base-b expansion, every finite block of k digits occurs with limiting frequency b^{-k} for every positive integer k. In particular, each individual digit from 0 to $b-1$ appears with limiting frequency $1/b$. We note that the number $0.2357111317\ldots$ is called the Copeland-Erdos constant. See `https://oeis.org/A033308`.

[524] These biases are finite-range phenomena and hence they do not contradict the fact that, asymptotically, the relevant coprime residue classes occur with equal frequency (as stated earlier).

[525] But note that this is seemingly a computationally observed bias within certain ranges and hence it may not fit well

30. Also see § 5.2.4 for theorems about the infinitude of primes of certain numeric forms (e.g. infinitude of delicate primes, or primes that do not contain a specific digit, or primes ending in 1, 3, 7, or 9).
31. Also see § 5.2.5 for theorems about the finitude of primes of particular numeric forms or characters (e.g. finitude of minimal primes, or truncatable primes). Other subsections of this section also contain theorems relevant to the current subsection.

5.2.9 Role of Primes in the Number System

In this subsection we list some of the common theorems and facts regarding the role of prime numbers in the structure of the number system (mainly the integers) and related issues:[526]

1. The fundamental theorem of arithmetic (which is the main foundation for the role of prime numbers in building the integer number system; see § 1.7) .
2. Euclid's theorem on the infinitude of prime numbers (see § 1.6).
3. Generalized Euclid's lemma which states: a prime p is a factor of $(n_1 n_2 \dots n_k)$ *iff* p is a factor of n_i for some $1 \leq i \leq k$.
4. Brun's theorem (see § 5.1.5).
5. Chen's theorem I (see § 5.1.8).
6. Erdos-Kac theorem (see § 5.1.12).
7. Euler's product formula (see § 5.1.14).
8. Goldbach's ternary conjecture (see § 5.1.16).
9. Hardy-Ramanujan theorem (see § 5.1.18).
10. Iwaniec's theorem (see § 5.1.21).
11. Legendre's formula (see § 5.1.23).
12. Riemann-von Mangoldt formula (see § 5.1.36).
13. Vinogradov's theorem (and Waring's conjecture; see § 5.1.42).
14. Zsigmondy's theorem (see § 5.1.45).
15. Every integer greater than 1 has at least one prime factor.
16. The greatest common divisor (gcd) and the least common multiple (lcm) of any finite nonempty set of positive integers are fully determined by their prime factorizations.
17. Prime numbers are the atoms of the multiplicative monoid of positive integers.
18. The set of positive integers forms a free commutative monoid generated by the primes, and the divisibility relation is determined by coordinate-wise comparison of exponents.
19. The ring of integers $\mathbb{Z}$ is a unique factorization domain, and its irreducible elements are exactly the elements $\pm p$, where p is a positive prime integer.[527]
20. The product of any finite set of primes plus 1 is either prime or divisible by a prime not in the set.
21. A natural number n is the sum of two squares *iff* every prime of the form $4k+3$ occurs an even number of times in the prime factorization of n.
22. A number $n \in \mathbb{N}$ is an even perfect number *iff* $n = 2^{p-1}(2^p - 1)$ where $(2^p - 1)$ is prime, i.e. Mersenne prime (Euclid-Euler theorem).
23. Every even integer is a sum of at most six primes (not necessarily distinct; Ramare's theorem). Also see § 5.1.16 and § 5.1.42.
24. Any integer > 96 is a sum of distinct prime-indexed primes (see § 2.1.62).
25. If an odd perfect number N exists then its prime factorization must be of the form $N = q^k n^2$ where q is prime, $k, n \in \mathbb{N}$, $q \overset{4}{=} 1$, $k \overset{4}{=} 1$, and $\gcd(q, n) = 1$.

within the classification of theorems. Also see Point 4 of § 6.2.8.

[526] The title "Role of Primes in the Number System" of this subsection should be understood broadly, i.e. it should include things like expressing integers by primes and related issues.

[527] The statements of Points 17, 18 and 19 express the unique factorization of integers through increasingly sophisticated algebraic structures (moving from a simple atomic view, to order theory, and finally to full ring theory).

26. If an odd perfect number (i.e. $N = q^k n^2$) exists then its non-Eulerian component must strictly exceed its Eulerian prime factor component (i.e. $q^k < n^2$).
27. If an odd perfect number N exists then it must have at least 10 distinct prime factors. Moreover, if $3 \nmid N$ then it must have at least 12 distinct prime factors.
28. We may also include in the "Role of Primes in the Number System" category the Copeland-Erdos theorem (which we indicated earlier; see Point 27 of § 5.2.8).
29. We may also include in this category some of the distribution theorems (see § 5.2.6) such as Dirichlet's theorem on arithmetic progressions (see § 5.1.11), the prime number theorem (see § 5.1.31), and the prime number theorem for arithmetic progressions (see § 5.1.32).

Also see § 9.11.

5.2.10 Primality Testing and Sieving

In this subsection we list a number of common examples of theorems about testing and/or sieving of primes (or have some relation to primality testing and/or sieving):[528]

1. Brun's theorem (see § 5.1.5).
2. Brun-Titchmarsh theorem (see § 5.1.6).
3. Chen's theorem II (see § 5.1.9).
4. Clement's theorem (see § 5.1.10).
5. Euler's criterion (see § 5.1.13 and § 7.3.18).
6. Fermat's little theorem (see § 5.1.15).
7. Lucas primality test theorem (see § 7.3.9).
8. Morrison's primality test theorem (see § 7.3.13).
9. Pepin's primality test theorem (see § 7.3.15).
10. Pocklington's primality test theorem (see § 7.3.16).
11. Proth's theorem (see § 7.3.17).
12. Wilson's theorem (see § 5.1.43).
13. If $n \in \mathbb{N}$ is composite then n has a prime divisor $\leq \sqrt{n}$.
14. If n is prime then the only solutions to the congruence $x^2 \stackrel{n}{=} 1$ are $x \stackrel{n}{=} +1$ or $x \stackrel{n}{=} -1$.[529]
15. In base 10, a 10-digit pandigital integer cannot be prime (see § 2.1.55).
16. In base 10, a palindrome > 11 is composite if it is of even-length (the converse is untrue). See § 2.1.53 and § 2.1.54.
17. If $5 < n \in \mathbb{O}$ does not divide the Fibonacci number $\mathcal{F}_{n-\left(\frac{5}{n}\right)}$ then n is not prime, where $\left(\frac{5}{n}\right)$ is the Jacobi symbol (see § 7.3.7 and § 9.7.7).
18. If $2 < n \in \mathbb{O}$ does not divide the Pell number $\mathcal{P}_{n-\left(\frac{2}{n}\right)}$ then n is not prime, where $\left(\frac{2}{n}\right)$ is the Jacobi symbol (see § 7.3.14).
19. If n does not divide the n^{th} Perrin number P_n then n is not prime (see § 9.7.10).
20. There are odd $k \in \mathbb{N}$ such that $2^n k + 1$ is composite for all $n \geq 1$ (see § 7.9.4).
21. There are composite numbers n for which $a^n \stackrel{n}{=} a$ for all integers a (i.e. Carmichael numbers; see § 5.1.15, § 7.9.2 and § 9.7.1).
22. A composite integer $n > 1$ divides $a^n - a$ for all integers a *iff* n is square-free and $p - 1$ divides $n - 1$ for all the prime divisors p of n (Korselt's criterion for Carmichael numbers).
23. If a composite solution n to $\phi(n)|(n-1)$ does exist then it must be odd, square-free, and divisible by at

[528] The title "Primality Testing and Sieving" should be understood broadly to include for instance sieve theory and results obtained by sieve methods.

[529] We may also say: if there is an integer x such that $x^2 \stackrel{n}{=} 1$ but $x \stackrel{n}{\neq} \pm 1$ then n is composite. In fact, this is one of the theoretical foundations for the Miller-Rabin primality test, i.e. the absence of non-trivial square roots of 1 (modulo prime) is one of the key ideas underlying the Miller-Rabin primality test (see § 7.3.12).

least 14 distinct primes (see footnote [472]). Moreover, it must be a Carmichael number (see § 6.1.22).
24. $n! \pm 1$ is prime (i.e. a factorial prime; see § 2.1.19) *iff* it has no prime divisor p in the range $n < p \leq (n! \pm 1)^{1/2}$ (where $n \geq 1$ for $n! + 1$, and $n \geq 3$ for $n! - 1$).
25. $p_n\# \pm 1$ is prime (i.e. a primorial prime; see § 2.1.64) *iff* it has no prime divisor p in the range $p_n < p \leq (p_n\# \pm 1)^{1/2}$ (where $n \geq 1$ for $p_n\# + 1$, and $n \geq 2$ for $p_n\# - 1$).
26. We should also include in this category the theoretical foundations underlying some of the primality tests and prime sieves that will be investigated in § 7.3 and § 7.4 (and actually in chapter 7 in general). Refer for instance to the Solovay-Strassen test (see § 7.3.18) and the Selberg sieve (see § 7.4.10).
27. We may also include in this category many theorems and results in other categories (such as the "Infinitude" and "Distribution" categories; see § 5.2.4 and § 5.2.6) which have indirect implications and impacts on primality testing and sieving and related issues. A few examples of such theorems are: Dirichlet's theorem on arithmetic progressions (see § 5.1.11), the prime number theorem (see § 5.1.31), the prime number theorem for arithmetic progressions (see § 5.1.32), and Bertrand's postulate (see § 5.1.2).[530]

5.2.11 Indexing

In this subsection we list a number of common theorems and results about the indexing of prime numbers and related issues:
1. The index n of a Fermat prime (i.e. $2^n + 1$) must be a non-negative power of 2 (see § 2.1.20).
2. The only Fibonacci prime with a composite index is 3 (see § 2.1.21).
3. The only Jacobsthal prime with a composite index is 5 (see § 2.1.36).
4. The indices n of Jacobsthal primes (excluding $J_4 = 5$) and the indices p of Wagstaff primes W_p are identical (see § 2.1.36 and § 2.1.87).
5. The indices of Lucas primes are either 0, or a power of 2, or a prime number (see § 2.1.39).
6. All Pell primes have prime indices (see § 2.1.57).
7. Any integer > 96 is a sum of distinct prime-indexed primes (see § 2.1.62).
8. All repunit primes have prime indices (see § 2.1.69).
9. The index n of a Woodall prime cannot be congruent to 4 or 5 modulo 6 (see § 2.1.93).
10. $p_n > n$ for all $n \geq 1$.
11. $p_n > n \log n$ for all $n \geq 1$.
12. $p_n > n(\log n + \log \log n - 1)$ for all $n \geq 2$. Also see similar mathematical relationships in § 5.2.15.
13. We should also note that some prime types are indexed, by definition, with prime numbers; these include: Mersenne primes (see § 2.1.41), prime-indexed primes (see § 2.1.62), primorial primes (see § 2.1.64), safe primes (see § 2.1.72), and Wagstaff primes (see § 2.1.87). Also see § 3.2.6.

5.2.12 Subsets

In this subsection we list a number of theorems and facts about the subset relationships among prime types and categories (and related issues):
1. Bernoulli irregular primes are a proper subset of Genocchi irregular primes. See § 2.1.32 and § 2.1.34.
2. Carol primes are a proper subset of near-square primes. See § 2.1.3 and § 2.1.49.
3. Cullen primes are a proper subset of Proth primes. See § 2.1.12 and § 2.1.65.
4. Dihedral primes are a proper subset of reversible primes. See § 2.1.16 and § 2.1.70.
5. Double Mersenne primes are a proper subset of Mersenne primes. See § 2.1.41.
6. Emirp primes are a proper subset of reversible primes. See § 2.1.17 and § 2.1.70.
7. Fermat primes are a proper subset of cyclotomic primes. See § 2.1.14 and § 2.1.20.

[530] In fact, even results like the Bombieri-Vinogradov theorem may be included (see § 5.1.4 and § 7.4.8).

8. Fermat primes are a proper subset of generalized Fermat primes. See § 2.1.20 and § 2.1.24.
9. Fermat primes are a proper subset of Pierpont primes. See § 2.1.20 and § 2.1.60.
10. Fermat primes are a proper subset of Proth primes. See § 2.1.20 and § 2.1.65.
11. Fermat primes (except 3) are Pythagorean primes. See § 2.1.20 and § 2.1.66.
12. Odd primes of the form $n^n + 1$ are a proper subset of Fermat primes.
13. Kynea primes are a proper subset of near-square primes.[531] See § 2.1.37 and § 2.1.49.
14. Mersenne primes are a proper subset of cyclotomic primes. See § 2.1.14 and § 2.1.41.
15. Mersenne primes are a proper subset of generalized Mersenne primes (depending on the definition of generalized Mersenne primes). See § 2.1.25 and § 2.1.41.
16. Mersenne primes are a proper subset of Mersenne divisors. See § 2.1.41 and § 2.1.42.
17. Mersenne primes are a proper subset of non-Pythagorean primes. See § 2.1.41 and § 2.1.66.
18. Mersenne primes are a proper subset of Pierpont primes of the second kind. See § 2.1.41 and § 2.1.60.
19. Mersenne primes are a proper subset of Riesel primes. See § 2.1.41 and § 2.1.71.
20. Mirimanoff primes are a proper subset of generalized Wieferich primes. See § 2.1.46 and § 2.1.90.
21. $n^2 + 1$ primes are a proper subset of near-square primes. See § 2.1.47 and § 2.1.49.
22. $n^4 + 1$ primes are a proper subset of the $n^2 + 1$ primes. See § 2.1.47 and§ 2.1.48.
23. $n^4 + 1$ primes are a proper subset of the near-square primes. See § 2.1.48 and§ 2.1.49.
24. $n^4 + 1$ primes are a proper subset of the quartan primes. See § 2.1.48 and § 2.1.67.
25. $n^2 + 1$ and $n^4 + 1$ primes are proper subsets of the primes of the form $x^2 + y^2$ $(x, y \in \mathbb{Z})$. See § 2.1.47 and § 2.1.48.
26. Odd $n^2 + 1$ and $n^4 + 1$ primes are proper subsets of Pythagorean primes. See § 2.1.47, § 2.1.48 and § 2.1.66.
27. Palindromic primes are a proper subset of reversible primes. See § 2.1.53 and § 2.1.70.
28. Palindromic wing primes are a proper subset of palindromic primes. See § 2.1.53 and § 2.1.54.
29. Permutable primes are a proper subset of circular primes. See § 2.1.7 and § 2.1.58.
30. Permutable primes are a proper subset of reversible primes. See § 2.1.58 and § 2.1.70.
31. Pythagorean primes are a proper subset of the primes of the form $x^2 + y^2$ $(x, y \in \mathbb{Z})$.[532] See § 2.1.66.
32. Quartan primes are a proper subset of generalized Fermat primes. See § 2.1.24 and § 2.1.67.
33. Repunit primes are a proper subset of circular primes. See § 2.1.7 and § 2.1.69.
34. Repunit primes are a proper subset of dihedral primes. See § 2.1.16 and § 2.1.69.
35. Repunit primes are a proper subset of palindromic primes. See § 2.1.53 and § 2.1.69.
36. Repunit primes are a proper subset of permutable primes. See § 2.1.58 and § 2.1.69.
37. Repunit primes are a proper subset of reversible primes. See § 2.1.69 and § 2.1.70.
38. Repunit primes are a proper subset of strobogrammatic primes. See § 2.1.69 and § 2.1.78.
39. Repunit primes are a proper subset of unique primes. See § 2.1.69 and § 2.1.85.
40. Strict pandigital primes (if exist in a given base) are a subset of pandigital primes in that base. See § 2.1.55.
41. Thabit primes of the second kind are a proper subset of Pierpont primes. See § 2.1.60 and § 2.1.81.
42. For $n > 1$, Thabit primes of the first kind are a proper subset of Riesel primes. See § 2.1.71 and § 2.1.81.
43. For $n > 1$, Thabit primes of the second kind are a proper subset of Proth primes. See § 2.1.65 and § 2.1.81.
44. Twin prime pairs are a proper subset of Chen prime pairs. See § 2.1.6, § 2.1.84 and § 4.7.3.
45. Wagstaff primes are a proper subset of cyclotomic primes. See § 2.1.14 and § 2.1.87.

---

[531] Kynea primes are a special case of the primes of the form $m^2 - 2$ (which are a kind of near-square primes).
[532] The only exception is 2 which is of the form $x^2 + y^2$ but not Pythagorean.

46. Wagstaff primes are a proper subset of Jacobsthal primes.[533] See § 2.1.36 and § 2.1.87.
47. Wagstaff primes are a proper subset of non-Pythagorean primes. See § 2.1.66 and § 2.1.87.
48. Wolstenholme primes are a proper subset of Bernoulli irregular primes. See § 2.1.32 and § 2.1.92.
49. Woodall primes are a proper subset of Riesel primes. See § 2.1.71 and § 2.1.93.
50. In the binary number system, all Mersenne primes are repunit primes (and conversely). See § 2.1.41 and § 2.1.69.
51. Absolute pseudoprimes are a proper subset of Fermat pseudoprimes. See § 9.7.1 and § 9.7.6.
52. Euler-Jacobi pseudoprimes to a given base are a proper subset of Fermat pseudoprimes to that base. See § 9.7.4 and § 9.7.6.
53. Strong pseudoprimes to a given base are a proper subset of Euler-Jacobi pseudoprimes to that base, and hence are a proper subset of Fermat pseudoprimes to that base (refer to Point 52). See § 9.7.4, § 9.7.6 and § 9.7.12.

5.2.13 Divisibility and Modularity

In this subsection we list a number of theorems and facts about divisibility and modularity related to prime numbers (and connected issues):[534]

1. Carmichael's theorem which establishes the existence of primitive prime divisors for terms of Lucas sequences (with finitely many exceptions), similar to Zsigmondy's theorem for sequences of the form $a^n - b^n$ (see § 5.1.45).[535]
2. Clement's theorem (see § 5.1.10).
3. Euler's criterion (see § 5.1.13).
4. Fermat's little theorem (see § 5.1.15).
5. Hensel's theorem (see § 5.1.19).
6. Kummer's theorem which states that the exponent of the highest power of a prime p dividing the binomial coefficient C_k^n is equal to the number of carries when adding k and $n-k$ in base p.
7. Lagrange's theorem on polynomial congruences (see § 5.1.22).
8. Legendre's formula (i.e. it gives the exact power s of a prime p such that p^s divides $n!$). See § 5.1.23.
9. Lifting The Exponent (LTE) lemma which provides the exact power of a given prime p that divides $a^n \pm b^n$ under specific conditions.
10. Lucas's theorem which provides a method to compute binomial coefficients $C_k^n \pmod p$ using the base-p expansions of n and k.
11. Primes modulo 4 theorem (see § 5.1.33).
12. Primes modulo 6 theorem (see § 5.1.34).
13. Proth's theorem (see § 7.3.17).
14. Wilson's theorem (see § 5.1.43).
15. Zsigmondy's theorem (including Bang's theorem which is a special case; see § 5.1.45).
16. Every integer greater than 1 has at least one prime divisor.
17. $1 < n \in \mathbb{N}$ is prime *iff* it does not have a prime divisor $\leq \sqrt{n}$.
18. $1 < n \in \mathbb{N}$ is prime *iff* $\sigma(n) = 1 + n$ (where σ is the divisor function of n).
19. $1 < n \in \mathbb{N}$ is prime *iff* $s(n) = 1$ (where s is the restricted divisor function of n).
20. Every prime number is a divisor of some binomial coefficient.
21. The least positive divisor greater than 1 of any integer $n > 1$ is a prime number.
22. A prime p divides $(n_1 n_2 \dots n_k)$ *iff* p divides n_i for some $1 \leq i \leq k$ (generalized Euclid's lemma).

[533] The only exception is $J_4 = 5$ which is a Jacobsthal prime but not a Wagstaff prime.

[534] Due to the large number of theorems in this category and the limitation on the size of this volume, some theorems are only listed with minimal explanations. Further explanations and details about these theorems (as well as other theorems) will be provided in the upcoming volumes.

[535] In this sense, Carmichael's theorem may be regarded as an extension or generalization of Zsigmondy's theorem.

23. If a prime p divides a^n then p^n divides a^n.
24. For any prime number p and positive integer k, p^k has exactly $k+1$ positive divisors.
25. If $n \in \mathbb{N}$ is given in its prime decomposition as $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ ($a_i \in \mathbb{N}$, $1 \leq i \leq k$) then all the positive divisors of n (including 1 and n) are precisely the integers of the form:

$$p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \qquad (b_i \in \mathbb{N}_0,\, b_i \leq a_i,\, 1 \leq i \leq k) \tag{75}$$

where we consider all the possible combinations of b_i.
26. If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ then:

$$\tau(n) = \prod_{i=1}^{k} (a_i + 1) \tag{76}$$

where $\tau(n)$ is the divisor-counting function of n (see footnote [16]).
27. For any multi-digit prime p the following congruence always holds: $p \overset{10}{=} 1$, 3, 7, or 9.
28. For any prime $p > 5$ the following congruence always holds: $p \overset{30}{=} 1$, 7, 11, 13, 17, 19, 23, or 29.
29. Every prime divisor q of a Fermat number $2^{2^k} + 1$ ($k \geq 2$) must satisfy $q \overset{2^{k+2}}{=} 1$.[536]
30. There are infinitely many primes that divide Fermat numbers.
31. There are infinitely many primes that divide Mersenne numbers (valid for both $2^n - 1$ and $2^p - 1$). See Note 1 in § 2.1.41.
32. Every prime divisor q of a Mersenne number $2^p - 1$ is of the form $q = 2kp + 1$ (where $k \in \mathbb{N}$ and p is an odd prime).
33. Every prime divisor q of a Mersenne number $2^p - 1$ (where p is an odd prime) must satisfy $q \overset{2p}{=} 1$ and $q \overset{8}{=} \pm 1$ (prime divisors of Mersenne numbers).
34. If a prime $p > 3$ is of Sophie Germain type then $p \overset{6}{=} 5$.
35. If $p \overset{4}{=} 3$ is a Sophie Germain prime, then its corresponding safe prime $q = 2p + 1$ always divides the Mersenne number $2^p - 1$.[537]
36. For any integer a and prime p (where a and p are coprime), the multiplicative order of a (modulo p) always divides $p - 1$.
37. For any integer a and prime p (where a and p are coprime), the multiplicative order of a (modulo p^k) always divides $\phi(p^k) = (p-1)p^{k-1}$ (where $1 \leq k \in \mathbb{N}$).
38. An odd prime p is Pythagorean *iff* $p \overset{4}{=} 1$ (see § 2.1.66).[538]
39. An odd prime p is expressible as $p = x^2 + y^2$ *iff* $p \overset{4}{=} 1$.[539]
40. A prime $p > 3$ satisfies $p \overset{3}{=} 1$ *iff* it is expressible as $p = x^2 + xy + y^2$ for some integers x, y.[540]
41. An odd prime p satisfies $p \overset{8}{=} 1$ or $p \overset{8}{=} 3$ *iff* it is expressible as $p = x^2 + 2y^2$ for some integers x, y.
42. An odd prime p satisfies $p \overset{24}{=} 1$ or $p \overset{24}{=} 7$ *iff* it is expressible as $p = x^2 + 6y^2$ for some integers x, y.
43. $(p-1)! + 1$ has more than one prime divisor *iff* $p \geq 7$ ($p \in \mathbb{P}$).
44. The congruence $x^2 + 1 \overset{p}{=} 0$ has an integer solution x *iff* $p = 2$ or $p \overset{4}{=} 1$ ($p \in \mathbb{P}$).[541]
45. The congruence $x^2 + x + 1 \overset{p}{=} 0$ has an integer solution x *iff* $p = 3$ or $p \overset{3}{=} 1$ ($p \in \mathbb{P}$).
46. 2 is a quadratic residue (modulo an odd prime p) *iff* $p \overset{8}{=} \pm 1$.

---

[536] A weaker version of this statement (which may be called the *prime divisors of Fermat numbers theorem*) is: if q is an odd prime divisor of $2^{2^k} + 1$ then $q \overset{2^{k+1}}{=} 1$.

[537] Originally, the theorem excludes 3 (i.e. by imposing the condition $p > 3$) even though $q = 7$ divides $2^3 - 1 = 7$.

[538] We may also add (for clarity): an odd prime p is non-Pythagorean *iff* $p \overset{4}{=} 3$.

[539] We may also add (for clarity): an odd prime p is non-expressible as $p = x^2 + y^2$ *iff* $p \overset{4}{=} 3$. We may also extend it as: a prime p can be written as the sum of two squares *iff* $p = 2$ or $p \overset{4}{=} 1$.

[540] Regarding $p = 3$, we have $3 = 1^2 + 1 \times 1 + 1^2$ even though it does not satisfy $p \overset{3}{=} 1$.

[541] Equivalently, -1 is a quadratic residue (modulo a prime p) *iff* $p = 2$ or $p \overset{4}{=} 1$.

47. 3 is a quadratic residue (modulo a prime $p > 3$) *iff* $p \overset{12}{=} \pm 1$.
48. If p is a prime number that divides $x^2 + y^2$ where x, y are coprime integers, then $p = 2$ or $p \overset{4}{=} 1$.
49. If p is prime then p divides both $(p-1)^{mp-m} - 1$ and $(p+1)^{mp-m} - 1$ where $m \in \mathbb{N}$.
50. p divides $m^{n(p-1)+1} - m$ where $m \in \mathbb{Z}$, $n \in \mathbb{N}_0$, and $p \in \mathbb{P}$.[542]
51. If $p > n$ then $p \not| n!$ (p is prime).
52. p divides $(p-2)! - 1$ (p is prime).
53. p divides $2(p-3)! + 1$ (p is odd prime).
54. p divides $4(p-3)! + 2$ (p is odd prime).
55. n divides $(n-1)!$ ($n \geq 6$ is composite).
56. Every prime divides infinitely many Catalan numbers.
57. Every odd prime divides at least one Mersenne number (see § 2.1.41).
58. The sum of any twin prime pair other than $(3, 5)$ is divisible by 12 (see § 2.1.84).
59. For any pair of twin primes $(p, p+2)$ where $p > 3$, the product $p \times (p+2)$ satisfies: $p(p+2) \overset{9}{=} 8$.
60. Any prime divisor p of the n^{th} cyclotomic polynomial $\Phi_n(a) \neq 0$ is either a divisor of n or $p \overset{n}{=} 1$ (where $a \in \mathbb{Z}$).
61. The polynomial $x^{p-1} - 1$ has exactly $p - 1$ roots (modulo p) where p is prime.
62. Asymptotically, prime numbers are equidistributed among residue classes coprime to the base of the numeral system (a consequence of PNTAP; see § 5.1.32). In base 10 (as a special case), they are distributed evenly among the residue classes 1, 3, 7, and 9.
63. A Fermat number $F_k = 2^{2^k} + 1$ ($k \geq 1$) is prime *iff* F_k divides $3^{(F_k-1)/2} + 1$ (Pepin's theorem; see § 7.3.15).
64. A prime p divides C_n^p for all $1 \leq n \leq p-1$ where C_n^p is the binomial coefficient.
65. p^3 divides $C_{p-1}^{2p-1} - 1$ where $5 \leq p \in \mathbb{P}$ and C_{p-1}^{2p-1} is the binomial coefficient (Wolstenholme's theorem). Equivalently, for any prime $p \geq 5$, p^2 divides the numerator of the harmonic number $H_{p-1} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ when H_{p-1} is written in lowest terms.
66. For any prime $p \geq 5$, we have $C_p^{2p} \overset{p^3}{=} 2$ where C_p^{2p} is the binomial coefficient (a corollary to Wolstenholme's theorem).[543]
67. For $n \geq 3$ there exists a prime p with $n < p < 2n$ that divides the central binomial coefficient C_n^{2n}. Also see § 5.1.2.
68. Every prime $p \neq 2, 5$ divides at least one repunit number (in base 10).
69. For any prime p, $n = p-1$ is always a solution to $p|(n! + 1)$ (by Wilson's theorem). There may also exist smaller solutions $n < (p-1)$. However, no solutions exist for $n \geq p$.
70. If $p > 5$ is a primitive prime divisor of the n^{th} Fibonacci number $\mathcal{F}_n$ then $p \overset{n}{=} \pm 1$.
71. Any odd prime $p \neq 5$ divides the Fibonacci number $\mathcal{F}_{p-\left(\frac{5}{p}\right)}$ where $\left(\frac{5}{p}\right)$ is the Legendre symbol.[544]
72. If p is prime and $\mathcal{F}_n$ denotes the n^{th} Fibonacci number then:
    - If $p = 2$ then p divides $\mathcal{F}_{3k}$ for every $k \geq 1$.
    - If $p = 5$ then p divides $\mathcal{F}_{5k}$ for every $k \geq 1$.
    - If $p \overset{5}{=} 1$ or 4 then p divides $\mathcal{F}_{p-1}$ (see Point 71).
    - If $p \overset{5}{=} 2$ or 3 then p divides $\mathcal{F}_{p+1}$ (see Point 71).
73. Any prime $p \neq 2$ divides the Pell number $\mathcal{P}_{p-\left(\frac{2}{p}\right)}$ where $\left(\frac{2}{p}\right)$ is the Legendre symbol.
74. If n is prime then n divides the n^{th} Perrin number P_n.
75. If p is prime and $x^2 \overset{p}{=} 1$ then either $x \overset{p}{=} +1$ or $x \overset{p}{=} -1$.

[542] This may be viewed as a generalization of Fermat's little theorem (see § 5.1.15).

[543] The converse (i.e. no composite integer $n \geq 5$ satisfies $C_n^{2n} \overset{n^3}{=} 2$) is the open Jones conjecture.

[544] The exclusion of $p = 2$ is a direct consequence of the standard definition of the Legendre symbol, which requires an odd prime.

76. If $O_p a = d$, then $a^k \overset{p}{=} 1$ *iff* d divides k (where $a \in \mathbb{Z}$, $p \in \mathbb{P}$, $a \overset{p}{\neq} 0$).[545]
77. For $p \in \mathbb{P}$ and $d|(p-1)$, exactly $\phi(d)$ residue classes $a \pmod p$ have $O_p a = d$ (where ϕ is the totient function).
78. If p is an odd prime, g is a primitive root modulo p, and a is an integer such that $a \overset{p}{\neq} 0$, there exists a unique integer k in the range $0 \leq k < p-1$ such that: $g^k \overset{p}{=} a$.[546]
79. Referring to the previous points, if $k = \text{ind}_g a$ then:

$$O_p a = \frac{p-1}{\gcd(k, p-1)} \tag{77}$$

80. The integer a is a primitive root modulo p^k for all $k \geq 1$ *iff* it is a primitive root modulo p and $a^{p-1} \overset{p^2}{\neq} 1$ (where p is an odd prime and $a \overset{p}{\neq} 0$).
81. The number of primitive roots modulo a prime p is $\phi(p-1)$ where ϕ is the totient function.
82. For any prime $p > 5$ the period of $1/p$ in base 10 is a divisor of $p-1$.
83. A prime number p ($\neq 2, 5$) is a full reptend prime *iff* 10 is a primitive root (modulo p), i.e. $O_p 10 = p-1$.
84. The only prime p dividing $2^p + 1$ is $p = 3$.
85. Every even perfect number is divisible by a specific Mersenne prime.
86. The following congruence holds for Bell numbers: $\mathscr{B}_{p+k} \overset{p}{=} \mathscr{B}_k + \mathscr{B}_{k+1}$ where p is prime (Touchard's congruence).
87. A composite integer $n > 1$ divides $a^n - a$ for all integers a *iff* n is square-free and $p-1$ divide $n-1$ for all the prime divisors p of n (Korselt's criterion for Carmichael numbers). Also see § 5.1.15, § 7.9.2 and § 9.7.1.
88. Theorems about primes in arithmetic progressions (such as Dirichlet's theorem and PNTAP; see § 5.1.11 and § 5.1.32) can also be classified as theorems about divisibility and modularity.
89. Theorems (and theoretical foundations) about or related to primality tests (see § 7.2 and § 7.3) can often be classified as theorems about divisibility and modularity (see for instance § 7.3.1, § 7.3.4, § 7.3.7, § 7.3.10, § 7.3.15, § 7.3.16, and § 7.3.18).
90. We should also include in this category theorems and results in other categories such as the "Infinitude" category (see for instance Points 21, 30, 31, 32 and 33 in § 5.2.4), the "Finitude" category (see for instance Point 9 in § 5.2.5), the "Algebraic Forms" category (see for instance the expressibility statements starting from Point 30 in § 5.2.7), and the "Role of Primes in the Number System" category (see for instance Point 20 in § 5.2.9).
91. Primes p that split in $\mathbb{Z}[i]$ (i.e. Gaussian integers; see footnote [776]) always satisfy the following congruence: $p \overset{4}{=} 1$.[547]
92. Primes p that split in $\mathbb{Z}[\omega]$ (i.e. Eisenstein integers; see the Note in § 9.4.3) always satisfy the following congruence: $p \overset{3}{=} 1$.[548]

5.2.14 Calculation of Primes

In this subsection we list a number of theorems and formulae about (or related to) the calculation of prime numbers (which primarily means calculating the n^{th} prime number exactly although this will be extended to include generating and listing prime numbers in general as will be clarified next):

1. Gandhi's formula: this is a recurrence relation (based on the inclusion-exclusion principle) that deter-

[545] $O_p a = d$ is the order of a modulo p, which is the smallest positive integer such that $a^d \overset{p}{=} 1$. In particular, $d|(p-1)$.
[546] The integer k is called the discrete index (or discrete logarithm) of a base g and may be denoted as $\text{ind}_g a$.
[547] For odd primes, this is actually an *iff* statement.
[548] For primes > 3, this is actually an *iff* statement.

mines p_n from the previous $n-1$ primes using the Mobius function and the primorial $p_{n-1}\#$.

2. Hardy-Wright formula (or formulae): several references in the literature attribute such formula(e) to Hardy and Wright (often citing their book "An Introduction to the Theory of Numbers"). However, the precise origin and status of the formula(e) is unclear. We therefore encourage readers to consult the original sources and investigate the matter further.
3. Jones formula: this formula (which is based on Wilson's theorem; see § 5.1.43) utilizes a nested double summation and the monus operator to calculate the n^{th} prime, that is:

$$p_n = \sum_{i=0}^{n^2} \left[1 \dot{-} \left\{ \left(\sum_{j=0}^{i} (j \dot{-} 1)!^2 \mod j \right) \dot{-} n \right\} \right] \tag{78}$$

where $\dot{-}$ is the monus operator, which is defined as $x \dot{-} y = \max(x-y, 0)$, and $x \pmod 0$ is defined as x.

4. Rowland's formula: this is a recurrence formula that is commonly described as being naturally occurring generator of prime numbers. The rule of this formula is: start with $a(1) = 7$ and

$$a(n) = a(n-1) + \gcd\big[n, a(n-1)\big] \qquad (\text{for } n \geq 2) \tag{79}$$

The difference between the consecutive terms $\big[$i.e. $a(n) - a(n-1)\big]$ is either 1 or a prime number, and hence the sequence produced by this difference is a list of 1's and primes (i.e. not only primes). The first 40 terms of this sequence are:[549]

$$1, 1, 1, 5, 3, 1, 1, 1, 1, 11, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 23, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1$$

Rowland's formula is very simple (and possibly the simplest of such formulae) but it is extremely inefficient for computing primes (as the primes appear in this sequence very sparsely among loads of 1's). Moreover, it does not produce primes in a tidy and ordered fashion, and may not even produce all primes (let alone it produces some primes repeatedly like 3). Hence, it is not a formula for calculating the n^{th} prime number. In short, Rowland's formula is no more than a gimmick for mathematical curiosity rather than a tool for calculating or listing primes.

5. Sierpinski's formula: this formula uses a specific real number C whose decimal expansion encodes the sequence of prime numbers, that is:

$$C = \sum_{k=1}^{\infty} \frac{p_k}{10^{2^k}} = 0.020300050000000700\ldots \tag{80}$$

The n^{th} prime can then be recovered by:

$$p_n = \left\lfloor 10^{2^n} C \right\rfloor - 10^{2^{n-1}} \left\lfloor 10^{2^{n-1}} C \right\rfloor \tag{81}$$

Thus, the formula effectively encodes the sequence of primes into a single real number and subsequently extracts the individual primes from its decimal expansion. Accordingly, it is not a practical method for calculating the n^{th} prime, since determining C to the required precision requires prior knowledge of the primes being encoded. It is therefore better regarded as an encoding formula than as a genuinely generative or computationally efficient prime-generation method. In this computational sense, the formula is somewhat circular and provides no independent method for calculating the n^{th} prime.

6. Willans' formula: this is an exact formula that expresses p_n by using a nested double sum and the floor

[549] See `https://oeis.org/A132199`. Also see `https://oeis.org/A106108`.

function relying (in one of its variants) on a trigonometric representation as part of prime-detecting mechanism which in a sense plays the role of prime-counting function $\pi(x)$. The formula is based on Wilson's theorem (which acts within the formula as a "prime detector"). Moreover, it is "elementary" in the sense that it relies on standard functions (sums, factorials, floors, and trigonometry) rather than complex analysis or non-elementary integrals (for instance). In fact, Willans' formula is potentially one of the landmark results in this field noting that many of the subsequent results and formulae in this regard are based on or inspired by this formula. However, like other similar formulae, it is a theoretical tool rather than a computationally practical one due mainly to its computational inefficiency.

7. We should also remember in this context Mills' theorem (see § 5.1.30), which provides a prime-generating formula, although one that is theoretically significant rather than computationally practical. The resulting sequence consists entirely of primes, but it does not include all prime numbers. As indicated, the construction is also of limited practical use because it requires precise knowledge of the relevant constant (which depends on the first prime chosen for the sequence) and produces numbers that grow in size extremely fast.
8. We may similarly recall Wright's theorem (which is structurally and functionally similar to Mills' theorem), that is: there exists a real number α (known as Wright's constant) such that if $g_0 = \alpha$ and $g_{n+1} = 2^{g_n}$ for all $n \geq 0$, then $\text{floor}(g_n)$ is prime for all $n \geq 1$. Like Mills' construction, Wright's construction gives an infinite sequence of primes rather than an enumeration of all primes, and its practical computational value is severely limited by the extremely rapid growth of the sequence.

We finally note the following remarks:

1. In the above, we have primarily listed the theorems and formulae alongside brief, informal explanations, as a full treatment would be lengthy and of limited practical value in the present context. However, in the upcoming volumes we will present these theorems and formulae in a more technical and detailed manner.
2. As indicated, most of these formulae are computationally inefficient and practically useless for generating primes; hence, they are primarily regarded as theoretical curiosities. However, they possess significant value in demonstrating that prime numbers (despite their seemingly chaotic distribution) can be calculated and encoded by relatively simple formulae using elementary mathematical machinery. In this sense, they illustrate that the set of prime numbers admits remarkably concise mathematical descriptions, even though the distribution of primes among the integers remains highly irregular and is understood only in a broad asymptotic sense.
3. Some of these constructions (or formulae) output both primes and non-primes rather than only primes (e.g. Rowland's formula which outputs primes and 1's). Moreover, some output only sequences (rather than full list) of primes (e.g. Mills' and Wright's constructions). In short, there are several categories of these constructions; the main ones are outlines in the following list:[550]

   • Those which output all primes and nothing else (i.e. they do not output non-primes). These constructions are normally highly artificial as they essentially encode primes based on an advanced knowledge of their enumeration. Sierpinski's formula may be an example of this category.

   • Those which output all primes padded with non-primes. Jones formulae may be an example of this category (noting that its output includes non-prime values such as negative integers, but whose positive values are exactly the primes).

   • Those which output sequences (rather than full list) of primes but nothing else. Mills' and Wright's constructions may be examples of this category.

   • Those which output sequences (rather than full list) of primes padded with non-primes. Rowland's formula may be an example of this category.

[550] Further checks are required regarding the following classification and examples as we did not find sufficient (or consistent) information about some of these details.

4. The mathematical foundations (or approaches) for the prime-generating formulae vary in general. Examples of these approaches are:[551]
   • Enumerating the primes through certain recurrence relations such as the Gandhi approach.
   • Enumerating the primes through exploiting certain number-theoretic theorems (usually the Wilson theorem) and/or functions (usually the prime-counting function) such as the Willans, and (potentially) Hardy-Wright approaches.
   • Enumerating the primes through encoding their list (usually by using certain prime-counting arguments) such as the Sierpinski approach.
   • Generating primes (without systematic enumeration) through developing closed form formulae whose outputs are prime numbers (usually using certain constants or parameters in these formulae) such as the Mills and Wright approaches.
5. It is useful here to remember the following theorem: there is no non-constant polynomial $P(n)$ with integer coefficients that yields a prime number for every integer n (although it is not about generating all prime numbers).[552]

5.2.15 Estimation of p_n

In this subsection we list a number of theorems and formulae about (or related to) the estimates and approximations of the n^{th} prime number (where "Estimation" includes imposing bounds and restrictions on its size, e.g. by inequalities):

1. The following asymptotic formula is regarded as an equivalent statement of the prime number theorem (see § 5.1.31):
$$p_n \sim n \ln n \qquad (n \to \infty) \tag{82}$$
2. The following formula may be regarded as an equivalent statement of Bertrand's postulate (see § 5.1.2):
$$p_{n+1} < 2p_n \tag{83}$$
3. The following inequality can be easily proved (e.g. by Bertrand's postulate):
$$p_{n+1} < p_n^2 \qquad (\text{for all } n \geq 1) \tag{84}$$
4. According to Bonse's inequality:
$$p_{n+1}^2 < p_1 p_2 \dots p_n = p_n\# \qquad (\text{for } n \geq 4) \tag{85}$$
5. According to Cipolla's asymptotic expansion:
$$p_n = n\left[\ln n + \ln\ln n - 1 + \frac{\ln\ln n - 2}{\ln n} - \frac{(\ln\ln n)^2 - 6\ln\ln n + 11}{2(\ln n)^2} + \cdots\right] \qquad (n \to \infty) \tag{86}$$
6. The Dusart bounds (lower and upper) are:
$$p_n > n\left(\ln n + \ln\ln n - 1\right) \qquad (\text{for } n \geq 2) \tag{87}$$
$$p_n < n\left(\ln n + \ln\ln n\right) \qquad (\text{for } n \geq 6) \tag{88}$$

[551] We should note two things:
• "Prime-generating formulae" is more general than "formulae for calculating p_n" as the former include the latter plus formulae based on theorems like the Mills and Wright theorems.
• These examples are not based on the same theoretical foundation and hence they are not supposed to be exhaustive or mutually exclusive.

[552] This may be stated with "for every positive integer".

7. According to Rosser's theorem:

$$p_n > n \ln n \qquad \text{(for all } n \geq 1\text{)} \tag{89}$$

8. The Rosser-Schoenfeld bounds (lower and upper) are:

$$p_n > n\left(\ln n + \ln\ln n - \frac{3}{2}\right) \qquad \text{(for } n \geq 2\text{)} \tag{90}$$

$$p_n < n\left(\ln n + \ln\ln n - \frac{1}{2}\right) \qquad \text{(for } n \geq 20\text{)} \tag{91}$$

9. We should also refer to the Massias and Robin bounds, which provide refined explicit estimates for the n^{th} prime p_n, improving earlier lower and upper bounds and giving sharper control of the size of p_n (especially for large n).

5.3 Relationships between Theorems

In this section we briefly discuss relationships between theorems about (or related to) prime numbers. The following list provides some examples of such relationships:[553]

1. The fundamental theorem of arithmetic logically depends on Euclid's lemma (see § 1.7 and Point 19 of § 1.3).
2. Bertrand's postulate is a mathematical consequence (or corollary) of Chebyshev's theorem (see § 5.1.2 and § 5.1.7).
3. Bertrand's postulate is an asymptotic consequence of the prime number theorem for sufficiently large integers (see § 5.1.2 and § 5.1.31).
4. Brun-Titchmarsh theorem is weaker than the prime number theorem for arithmetic progressions in terms of sharp asymptotics, although it is stronger in terms of uniformity over the modulus (see § 5.1.6 and § 5.1.32).
5. Chebyshev's theorem is a "weak version" (or "weaker precursor") of the prime number theorem (see § 5.1.7 and § 5.1.31).[554]
6. Fermat's little theorem is a special case of Euler's totient theorem (obtained by setting the modulus equal to a prime number; see § 5.1.15).[555]
7. Although the Green-Tao theorem and Dirichlet's theorem are not direct consequences of one another, they are closely related in spirit, as both reveal deep regularity in the seemingly irregular distribution of prime numbers (see § 5.1.11 and § 5.1.17).
8. Linnik's theorem is stronger than what can be deduced from the Siegel-Walfisz theorem alone because it gives a uniform bound for the least prime in an arithmetic progression for arbitrary moduli, whereas Siegel-Walfisz applies only to relatively small moduli (see § 5.1.24 and § 5.1.39).
9. Mertens' first theorem was a precursor to the prime number theorem (see § 5.1.27 and § 5.1.31).
10. Mertens' second theorem can be derived from the prime number theorem using partial summation (see § 5.1.28 and § 5.1.31).
11. Mertens' second theorem can be derived from Mertens' first theorem using partial summation (see § 5.1.27 and § 5.1.28).
12. Mertens' third theorem can be derived from Mertens' second theorem by applying the logarithmic

[553] Some of these statements may be controversial (possibly because of different considerations and perspectives).

[554] In terms of logical implication (ignoring the historical development), Chebyshev's theorem can be obtained as a corollary of the prime number theorem. Historically, Chebyshev's theorem was an important precursor and partial step toward the proof of the prime number theorem.

[555] Euler's totient theorem states: if $m \in \mathbb{N}$ and $1 < k \in \mathbb{N}$ are coprime then $m^{\phi(k)} \overset{k}{=} 1$.

expansion of the Euler product (see § 5.1.28 and § 5.1.29).

13. Prime number theorem and the statement "$\zeta(s) \neq 0$ for all $\Re(s) = 1$" imply each other (potentially with some extra conditions; see § 5.1.31).[556]
14. Prime number theorem is equivalent to the statement "$\theta(x) \sim x$ as $x \to \infty$" (see § 5.1.31 and § 8.2.5).
15. Prime number theorem is equivalent to the statement "$\psi(x) \sim x$ as $x \to \infty$" (see § 5.1.31 and § 8.2.5).
16. Prime number theorem for arithmetic progressions is a more elaborate version of prime number theorem (see § 5.1.31 and § 5.1.32).[557]
17. Prime number theorem for arithmetic progressions is stronger than Dirichlet's theorem, since it provides an asymptotic formula for the distribution of primes in arithmetic progressions rather than merely proving their infinitude (see § 5.1.11 and § 5.1.32).
18. Schnirelmann's theorem has a broader domain of applicability than Goldbach's ternary conjecture and Vinogradov's theorem (see § 5.1.16 and § 5.1.42), but it is less specific in terms of the content and strength of its conclusions.[558]
19. Siegel-Walfisz theorem implies Dirichlet's theorem (see § 5.1.11 and § 5.1.39).[559]
20. Vinogradov's theorem is a weaker version of Goldbach's ternary conjecture (see § 5.1.16 and § 5.1.42).
21. Wilson's theorem is stronger than Fermat's little theorem, since it gives a necessary and sufficient condition for primality, whereas Fermat's little theorem provides only a necessary condition (see § 5.1.15 and § 5.1.43; also see § 7.3.6 and § 7.3.19).
22. We should also refer to the implication of various theorems (e.g. Dirichlet's theorem or the prime number theorem) and other established results (e.g. the divergence of the harmonic series of prime numbers) for Euclid's theorem on the infinitude of prime numbers (see for instance § 1.6).
23. Summaries: the following are examples of summaries of relationships between theorems (where $\Rightarrow$ means "implies"):[560]
    - Chebyshev $\Rightarrow$ Bertrand.
    - Euler totient $\Rightarrow$ Fermat.
    - Mertens1 $\Rightarrow$ Mertens2 $\Rightarrow$ Mertens3.
    - Mertens2 $\Rightarrow$ Euler ($\sum_{p \in \mathbb{P}} 1/p = \infty$).
    - PNT $\Rightarrow$ Bertrand (for sufficiently large numbers).
    - PNT $\Rightarrow$ {Chebyshev, Mertens2}.
    - PNTAP $\Rightarrow$ {Bertrand, Dirichlet, PNT}.
    - Siegel-Walfisz $\Rightarrow$ Dirichlet.

[556] We may also say: the prime number theorem is equivalent to the statement that the Riemann zeta function has no zeros on the line $\Re(s) = 1$.

[557] We may also say: PNTAP is a generalization of PNT, i.e. PNT is the special case $q = 1$ for PNTAP.

[558] Schnirelmann's theorem asserts that any integer greater than 1 can be expressed as the sum of at most C prime numbers (where C is an absolute constant).

[559] In fact, the Siegel-Walfisz theorem also provides an important ingredient and point of comparison in the development of more advanced results on primes in arithmetic progressions, such as the Bombieri-Vinogradov theorem (see § 5.1.4).

[560] We note that there are many other such summaries. Here, the symbol $\Rightarrow$ is intended primarily to indicate a broad mathematical implication; it does not necessarily specify the precise hypotheses, logical formulation, or method by which one result follows from another. Some relationships may also depend on the particular formulations of the theorems being compared. Many further relationships can be obtained by combining these and other related implications. Some classifications may likewise depend on the perspective adopted, for example whether one is considering strict logical implication, generalization, historical development, or another relationship.

Chapter 6
Conjectures of Primes

In this chapter we investigate open problems and conjectures (as well as "corollaries" of major conjectures) about primes or related to primes. However, before we start it is useful to be aware of the following points:

1. A conjecture is a mathematical proposition that is believed to be true but has not yet been proved. Usually, a conjecture is supported by theoretical considerations, computational evidence, or other indications, although such evidence does not constitute a formal and rigorous proof. An open problem or open question is a problem or question whose solution is not currently known. Thus, the terms are not mutually exclusive, i.e. a conjecture can be an open problem, as is the case with many famous conjectures concerning prime numbers. In some contexts, "open problem", "open question" and "conjecture" are used somewhat interchangeably, although "conjecture" specifically suggests an assertion that is believed to be true.
2. Most (or at least a significant number) of the major open problems and conjectures in number theory concern primes or are closely related to them. This concentration reflects the inherent complexity of prime numbers as both a mathematical structure and a focus of epistemic inquiry. It also highlights their foundational importance, as the intense research interest surrounding primes naturally and continuously generates new questions, which in turn lead to further open problems and conjectures.
3. There are many examples of conflicting conjectures, some of which have been noted previously and will be highlighted when necessary. For example, conjectures concerning whether certain types of prime numbers are finite or infinite make contradicting predictions. Such conflicting conjectures may arise from competing partial evidence, differing interpretations of the available evidence, or the subjective intuition of researchers (which may be ultimately based on different heuristic arguments or assumptions, or different deductions from known results and computational data).
4. The following collection of open problems and conjectures represents only a small fraction of the open problems and conjectures that circulate in the literature. Despite the extensive progress made in our understanding of prime numbers, many fundamental questions about their properties and distribution remain unresolved. In fact, what we do not know about prime numbers (which consequently appear as open problems and conjectures) is much more than (or at least comparable to) what we do know, and this should explain the huge number of open problems and conjectures related to the prime numbers. The large and continually growing body of open problems and conjectures reflects both the breadth of research on prime numbers and the depth of the questions that remain to be answered. The collection investigated in this chapter is therefore intended primarily as a representative sample of well known and frequently encountered examples in the literature on number theory and prime numbers, to give a good idea about the landscape of this topic. This collection is also intended to be extended and developed further in the future volumes of this book.
5. Our original plan was to classify the open problems and conjectures in this book into two categories: those concerning primes, in which primes are the central subject, and those related to primes, in which primes are involved but are not the central focus. However, we decided to abandon this classification because it would complicate the structure of the book without providing substantial benefit. Consequently, the collection of open problems and conjectures in the book, most of which are discussed in this chapter, includes both categories without making a formal distinction between them.

6.1 Open Problems and Conjectures about Primes

In the following subsections, we outline a selection of open problems and conjectures that are commonly discussed and frequently encountered in the literature on number theory in general and the theory of prime numbers in particular. We present these open problems and conjectures in largely alphabetical order.

6.1.1 *abc* Conjecture

The essence of this conjecture is that the product of the distinct prime factors of a, b, c cannot frequently be much smaller than c (where a, b, c are relatively prime positive integers with $c = a + b$). A more technical formulation of this conjecture is: for relatively prime positive integers a, b, c (where $c = a + b$) the radical $\text{rad}(abc)$ is typically at least $c^{1-\varepsilon}$ for any $\varepsilon > 0$, with only finitely many exceptions.[561]

While a claimed proof of the conjecture exists, it remains highly controversial and is not universally accepted by the mathematical community. The *abc* conjecture is widely regarded as one of the most important unsolved problems in Diophantine analysis. This is due to its impact on a number of open problems and conjectures,[562] and its profound implications for numerous other areas of number theory, including the distribution of prime numbers, a simplified proof of Fermat's last theorem, and Mihailescu's theorem (formerly known as Catalan's conjecture; see Point 5 of § 6.4).

6.1.2 Agoh-Giuga Conjecture

The Agoh-Giuga conjecture (also known as the Giuga conjecture) proposes a specific characterization of prime numbers using a summation formula. It states that an integer $n > 1$ is prime *iff* it satisfies the following congruence:

$$\sum_{i=1}^{n-1} i^{n-1} \equiv -1 \pmod{n} \tag{92}$$

The conjecture may also be formulated (equivalently) in terms of the Bernoulli numbers B_k, that is: $n > 1$ is prime *iff* it satisfies the following congruence:

$$nB_{n-1} \equiv -1 \pmod{n} \tag{93}$$

We remark that the conjecture is about the "*iff*" statement noting that the "only if" part of the statement is a proven theorem.

Extensive computational investigations have shown that any composite counterexample to the Agoh-Giuga conjecture must be extraordinarily large. The current best published results imply that any such counterexample must have at least 19908 decimal digits and at least 4771 distinct prime factors. Furthermore, it has been proved that every composite counterexample must be square-free. It has also been proved that a composite integer satisfies the summation congruence (or, equivalently, the Bernoulli congruence) *iff* it is simultaneously a Carmichael number (see § 5.1.15, § 7.9.2 and § 9.7.1) and a Giuga number.[563] Also see § 7.3.22 regarding the possibility (in principle) of the Agoh-Giuga conjecture to provide a "primality test".

[561] The "radical of n" in this context means the product of the distinct prime factors of n.
[562] See for instance Points 1, 2 and 30 of § 6.3.
[563] A Giuga number is a composite number n such that each of its distinct prime factors p_i satisfies $p_i^2 | (n - p_i)$.

6.1.3 Agrawal's Conjecture

According to this conjecture, if n and r are coprime positive integers and the following polynomial congruence condition holds:

$$(X-1)^n \equiv X^n - 1 \pmod{n, X^r - 1} \tag{94}$$

then either n is a prime number or $n^2 \equiv 1 \pmod{r}$. Broadly speaking, the conjecture serves as the theoretical base for optimizing the AKS primality test (see § 7.3.1) by reducing its run time.

It has been reported that the conjecture is verified computationally for $r < 100$ and $n < 10^{10}$.[564] However, a proposed heuristic argument claims that there are infinitely many counterexamples (none of which has been found yet). Moreover, it has been conjectured that if the Agrawal conjecture fails then a modified version of it may still hold.[565]

6.1.4 Andrica's Conjecture

According to this conjecture (which is essentially about prime gaps), the inequality $\left(\sqrt{p_{n+1}} - \sqrt{p_n}\right) < 1$ holds for all $n \in \mathbb{N}$ where p_n is the n^{th} prime number.[566] It has been claimed that the conjecture is verified for all prime numbers below 1.3002×10^{16} (noting that a more recent update seems to push this limit up to $2^{64} \approx 1.84 \times 10^{19}$). As a gap-regulating conjecture, Andrica's conjecture is related to other gap-regulating conjectures like the Legendre conjecture (see § 6.1.21) and the Oppermann conjecture (see § 6.1.25).[567]

6.1.5 Artin's Conjecture on Primitive Roots

This is one of the major open problems and conjectures in number theory (despite its relative simplicity). It states that any given integer a (which is not -1 or a perfect square) is a primitive root modulo infinitely many primes p. The conjecture also predicts the asymptotic density of these primes. For most square-free integers a, this density is expected to be Artin's constant C_A (which is about 0.3739558), which roughly means that about 37.4% of all primes will have a as a primitive root.

In fact, this conjecture has been proved conditionally, i.e. it holds true if the generalized Riemann hypothesis is true (see § 6.1.29). Moreover, it has been proven unconditionally that at least one of any three prime numbers (such as 2, 3, and 5) must be a primitive root for infinitely many primes (although it cannot be proved for a specific number like 2). This is because it has been shown that there are at most two exceptional square-free integers for which the conjecture could possibly fail.

6.1.6 Bateman-Horn Conjecture

This conjecture is essentially about the asymptotic distribution of prime values taken simultaneously by collections of polynomials,[568] i.e. it essentially predicts how often polynomials like n^2+1 and n^2+n+41 generate prime values (which should provide a quantitative estimate for the frequency of occurrence of these primes). It is described as "powerful" and "far-reaching" due to its implications and consequences which reach several theorems (like the Dirichlet and prime number theorems; see § 5.1.11, § 5.1.31 and § 6.4) and conjectures (like the n^2+1 and twin prime conjectures; see § 6.1.34 and § 6.3).

[564] A more recent research seems to push this limit to $n < 10^{17}$.

[565] The modified version imposes the additional congruence condition: $(X+2)^n \equiv X^n + 2 \pmod{n, X^r - 1}$.

[566] This conjecture may also be expressed (more explicitly as a gap-regulating conjecture) in terms of the prime gap as $g_n < 2\sqrt{p_n} + 1$ where g_n is the n^{th} prime gap which is given by $g_n = p_{n+1} - p_n$.

[567] With regard to the "strength" of these conjectures (concerning their implications for the prime gap size, i.e. how much they restrict the maximum possible size of prime gaps), we refer the reader to § 6.3.

[568] These polynomials must be irreducible over $\mathbb{Z}[x]$ with integer coefficients (and positive leading coefficients) and without local obstruction (i.e. there is no prime that divides the product of the polynomial values for every integer argument).

More technically, the Bateman-Horn conjecture predicts:

$$N(x) \sim \frac{C_{\text{BH}}}{D} \int_2^x \frac{dt}{(\ln\, t)^k} \tag{95}$$

where $N(x)$ is the number of prime-generating integers among the positive integers less than x (i.e. the number of integers $n \leq x$ such that all the k polynomials produce prime values), C_{BH} is the Bateman-Horn factor (which is a product over the sequence of primes), D is a product of the degrees of the aforementioned polynomials, and $\sim$ is the asymptotic equivalence symbol (which may be loosely replaced in some texts by $\approx$ or $\simeq$). Also see § 6.1.11 and § 6.1.17 (noting the resemblance in the formulae).

6.1.7 Bateman-Selfridge-Wagstaff Conjecture

According to this conjecture (also known as the *new Mersenne conjecture*), if a natural odd number p satisfies two of the following conditions then it must satisfy the third condition as well:
- p has the form $p = 2^k \pm 1$ or $p = 4^k \pm 3$ where $k \in \mathbb{N}$.[569]
- $2^p - 1$ is a prime number (i.e. Mersenne prime; see § 2.1.41).[570]
- $(2^p + 1)/3$ is a prime number (i.e. Wagstaff prime; see § 2.1.87).[571]

It is reported that this conjecture has been verified for all p up to the current search limit of Mersenne primes (i.e. there are no known cases where p meets exactly two conditions but fails the third). For example, 9 meets only the first condition, whereas 11 meets only the third condition. On the other hand, 3, 5, 7, and 13 meet all three conditions. It is worth noting that if p is composite then both conditions 2 and 3 are automatically false (see § 2.1.41 and § 2.1.87) and hence the conjecture holds trivially (because the antecedent of the conditional statement is false). In fact, this should explain the use of p.

6.1.8 Beal's Conjecture

According to this conjecture, if $A^x + B^y = C^z$ (where $A, B, C, x, y, z \in \mathbb{N}$ and $x, y, z > 2$) then A, B, C must have a common prime factor. This conjecture is related to Fermat's last theorem (FLT) and actually generalizes FLT from some aspects (noting, for example, that FLT is restricted to the case where $x = y = z$). The conjecture has been verified for a wide range of integers (in its six variables, i.e. bases and exponents), but because of its multi-variable and its multi-dimensional nature, there is no single and universal limit of verification. However, the conjecture is still unproven except in some special cases (notably FLT, i.e. $x = y = z$).[572]

6.1.9 Birch-Swinnerton-Dyer Conjecture

The essence of this conjecture is that the number of points on an elliptic curve (a plane algebraic curve defined over a field K and typically described by the cubic equation $y^2 = x^3 + ax + b$ where a, b are coefficients in K) modulo a prime p is deeply related to the rank of the group of rational points on the curve. In short, it establishes a definitive link between the algebraic properties of an elliptic curve and its analytic properties.

---

[569] See `https://oeis.org/A122834`.
[570] See `https://oeis.org/A000043`.
[571] See `https://oeis.org/A000978`.
[572] Fermat's last theorem states: no natural numbers A, B, C satisfy the equation $A^n + B^n = C^n$ for any $n \in \mathbb{N}$ greater than 2. So, Beal's conjecture is distinguished from FLT from two main aspects: the requirement of a common prime factor, and the relaxation of the equality of the three exponents. It is worth noting that FLT makes the conjecture vacuously true for equal exponents rather than providing a case where the common prime factor rule is actively tested and proven.

More specifically, the conjecture claims that the rank of the Abelian group of rational points, $E(\mathbb{Q})$, is exactly equal to the order of vanishing of its associated Hasse-Weil L-function, $L(E, s)$, at the point $s = 1$. Consequently, if $L(E, 1) = 0$, the rank is at least 1 and the number of rational points is infinite. Conversely, if $L(E, 1) \neq 0$, the rank is 0 and the group of rational points is finite.

The verification of this conjecture is currently limited to special cases (most notably for curves where the analytic rank is 0 or 1) supported by extensive statistical and numerical investigations. There are also occasional unverified claims of a general proof that lack recognition among the authoritative mathematical community. It is worth noting that the "strong" version of this conjecture provides an exact formula predicting the precise value of the leading Taylor coefficient of the L-function at $s = 1$ using the curve's geometric and arithmetic invariants.

6.1.10 Brocard's Conjecture

Brocard's conjecture (which is about the distribution and gap-regulation of primes) states: for every integer $n > 1$ there are at least four primes between p_n^2 and p_{n+1}^2 where p_n is the n^{th} prime number (noting that the condition $n > 1$ is to exclude the interval between 2^2 and 3^2 which embraces only two primes, i.e. 5 and 7). It has been reported that this conjecture is computationally verified for all $2 \leq n \leq 4 \times 10^5$.[573]

6.1.11 Bunyakovsky's Conjecture

This conjecture states that if $f(x)$ is an irreducible polynomial with integer coefficients, positive leading coefficient, and no fixed divisor [i.e. the greatest common divisor of the values $f(n)$, $n \in \mathbb{Z}$, is 1], then $f(n)$ is prime for infinitely many integers n. The conjecture remains open for every polynomial of degree at least two, although it is supported by extensive numerical evidence. Its linear case is precisely Dirichlet's theorem on arithmetic progressions (see § 5.1.11). Bunyakovsky's conjecture is a special case of Schinzel's hypothesis H which addresses the simultaneous primality of multiple polynomials (see § 6.1.30), while the Bateman-Horn conjecture (see § 6.1.6) provides a quantitative prediction for the asymptotic frequency of such prime values.

6.1.12 Cramer's Conjecture

This conjecture provides an estimate for the gap size between consecutive primes. It states:

$$p_{n+1} - p_n = O\left([\ln\, p_n]^2\right) \tag{96}$$

where p_n is the n^{th} prime number and O is the big O notation. In simple language, this conjecture means that the gap between two successive primes does not grow faster than the square of the logarithm of the first prime. In fact, Cramer suggested a specific limit for the gap, that is:

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\ln\, p_n)^2} = 1 \tag{97}$$

This was refined later by Granville where 1 was replaced by another constant (i.e. $2e^{-\gamma} \approx 1.1229$ where γ is the Euler-Mascheroni constant).[574] Cramer's conjecture is supported empirically by extensive verification of maximal prime gaps up to very high bounds (reportedly up to 2^{64}), though these finite computations remain far from the asymptotic regime.

[573] Other claims can also be found in the literature, e.g. it is verified for all n where $p_n^2 < 10^{18}$, or for all primes $p < 2^{32} \approx 4.294 \times 10^9$.

[574] It is widely believed among number theorists that Cramer's original limit of 1 is incorrect.

6.1.13 Dickson's Conjecture

According to this conjecture, for a set of k linear expressions with integer coefficients:

$$a_1n + b_1,\ a_2n + b_2,\ \ldots, a_kn + b_k \tag{98}$$

where the a's are all positive, there are infinitely many $n \in \mathbb{N}$ for which all these expressions are simultaneously prime *iff* there is no prime p that divides the product of all these expressions for every possible n. This conjecture implies or includes (as special cases) several famous conjectures and theorems, for example:

• Twin prime conjecture is represented by the case $k = 2$, $a_1 = a_2 = 1$, $b_1 = 0$ and $b_2 = 2$ (see Point 1 of § 6.1.34).

• The case $k = 1$ represents Dirichlet's theorem (noting that the condition that no prime p divides a_1n+b_1 for all n is equivalent to a_1 and b_1 being coprime; see § 5.1.11).

On the other hand, Dickson's conjecture may be regarded as a special case of other famous and more general conjectures (from various perspectives), e.g. the Bateman-Horn conjecture and Schinzel's hypothesis H (see § 6.1.6 and § 6.1.30). Also, Dickson's conjecture is more restrictive than the Bunyakovsky conjecture with respect to the degree of polynomials even though the Bunyakovsky conjecture is more restrictive with respect to the number of polynomials involved (since the Bunyakovsky conjecture is about a single polynomial; see § 6.1.11).[575]

Regarding the evidence for Dickson's conjecture, the strongest unconditional special case established so far is Dirichlet's theorem (which was proved long ago and was noted above). Progress on bounded gaps between primes (which is related to the twin-prime problem; see § 5.1.44) may also be viewed as indirect evidence in support of the conjecture. More generally, one may argue that the strongest evidence for Dickson's conjecture is the absence of any counterexample despite extensive theoretical, computational, and statistical investigation of the conjecture and related conjectures, such as the Bateman-Horn conjecture, the Bunyakovsky conjecture, and Schinzel's hypothesis H.

6.1.14 Elliott-Halberstam Conjecture

This conjecture is about the distribution of primes in arithmetic progressions (which is related to Dirichlet's theorem; see § 5.1.11). The essence of this conjecture is that prime numbers are distributed remarkably uniformly among arithmetic progressions, on average over the moduli. From this perspective, the Elliott-Halberstam conjecture can be seen as a substantial refinement of Dirichlet's theorem, i.e. whereas the theorem states that there are infinitely many primes in any arithmetic progression (satisfying the coprimality condition), the conjecture predicts a much stronger degree of uniformity in the distribution of prime numbers across different arithmetic progressions.

The Elliott-Halberstam conjecture is supported by significant partial results (such as the Bombieri-Vinogradov theorem; see § 5.1.4), together with extensive numerical evidence. Many important applications in sieve theory are based on or related to this conjecture. The conjecture (if proved) could also have a direct impact on the twin prime conjecture (see Point 1 of § 6.1.34).[576] The Elliott-Halberstam conjecture has been extended to stronger generalized forms to cover not only the distribution of primes

[575] It is worth noting that Schinzel's hypothesis H is more general than Bunyakovsky's conjecture (by removing the restriction to a single polynomial) and Dickson's conjecture (by removing the restriction to linearity).

[576] It has been shown that if the Elliott-Halberstam conjecture is true then the infinitude of prime pairs differing by at most 12 (which drops even further to 6 under its generalized form) can be proved (thereby improving the currently known unconditional bound of 246; see § 5.1.44) and hence we would be closer to the twin prime gap of 2 (which should boost our hope of proving the twin prime conjecture, even though from a pure theoretical perspective the reduction of the gap from 246 to 12 or 6 may not be a qualitatively significant advancement in this regard). More strict results have also been proven recently (see § 6.3).

in arithmetic progressions, but also certain arithmetic functions built from primes (such as weighted prime-counting functions and convolution-type correlations).

6.1.15 Feit-Thompson Conjecture

According to this conjecture, there are no distinct prime numbers p and q such that:

$$\frac{p^q - 1}{p - 1} \quad \text{divides} \quad \frac{q^p - 1}{q - 1} \tag{99}$$

It is reported that this conjecture has been verified for all primes $p, q < 1000$.[577]

It is worth noting that there was a famous stronger variant of the Feit-Thompson conjecture which proposed that these two quotients are always completely coprime. However, this stronger formulation was explicitly disproved by discovering a unique counterexample, that is: for the primes $p = 17$ and $q = 3313$, both expressions share a common prime divisor of 112643. Because the smaller fraction does not evenly divide the larger one, this discovery leaves the original Feit-Thompson conjecture completely intact.

6.1.16 Firoozbakht's Conjecture

This conjecture claims that the sequence $\sqrt[n]{p_n}$ is a strictly decreasing function of n, that is:

$$\sqrt[n+1]{p_{n+1}} < \sqrt[n]{p_n} \qquad \text{or equivalently} \qquad p_{n+1} < p_n^{1+(1/n)} \qquad (\text{for all } n \geq 1) \tag{100}$$

where p_n is the n^{th} prime number. The following list of $\sqrt[n]{p_n}$ for the first 15 primes should demonstrate how this sequence is strictly decreasing:

$$2.000, 1.732, 1.710, 1.627, 1.615, 1.533, 1.499, 1.445, 1.417, 1.400, 1.366, 1.351, 1.331, 1.308, 1.293$$

The conjecture has been verified computationally for all primes below 4×10^{18}, and later work using extended tables of maximal prime gaps has pushed the verification to all primes below $2^{64} \approx 1.84 \times 10^{19}$. In terms of restricting the size of prime gaps, this conjecture is stronger than most other similar conjectures like the Cramer and Shanks conjectures (see § 6.1.12 and § 6.1.33; also see § 6.3).

6.1.17 First Hardy-Littlewood Conjecture

The essence of this conjecture (which is about prime k-tuples and hence it may be called the *prime k-tuples conjecture*) is that the asymptotic number of prime k-tuples[578] can be computed explicitly by a given formula. This conjecture may be stated (loosely and partly) as: there are infinitely many primes that can form a specific k-tuple pattern where the numbers in the tuple differ by constants. More technically, the conjecture proposes that for any admissible[579] set of integers $\mathfrak{N} = \{n_1, n_2, \ldots, n_k\}$ the number of integers $n \leq x$ such that all members of the set $\{n + n_1, n + n_2, \ldots, n + n_k\}$ are prime is given asymptotically by:

$$\pi_{\mathfrak{N}}(x) \sim C_{\mathfrak{N}} \int_2^x \frac{dt}{(\ln\, t)^k} \tag{101}$$

[577] It is claimed that the search has been extended later to $p, q < 400000$, but this may concern the stronger variant (which is discussed in the next paragraph). So please check.

[578] Prime k-tuple is a finite set of primes with certain pattern and specific differences.

[579] For a pattern to be admissible, it must not consist of a complete set of residues modulo any prime p. For example, the tuple $(m, m + 2, m + 4)$ is not admissible because one of these numbers must always be divisible by 3 and hence it cannot produce infinitely many prime triplets.

where $\pi_{\mathfrak{N}}(x)$ is the count of such k-tuples up to x, $\sim$ is the asymptotic equivalence symbol, and $C_{\mathfrak{N}}$ is a constant that depends on the pattern of $\mathfrak{N}$.[580]

It is worth noting that the first Hardy-Littlewood conjecture is a massive generalization of the twin prime conjecture, and hence if the first Hardy-Littlewood conjecture is proven it will validate the twin prime conjecture (which represents the simplest case of the first Hardy-Littlewood conjecture). Also see § 6.1.6 (noting the similarity between the two asymptotic formulae, and the fact that the Bateman-Horn conjecture is a generalization of the first Hardy-Littlewood conjecture).

6.1.18 Fortunate Numbers Conjecture

According to this conjecture, all fortunate numbers are prime (see the Note in § 2.1.22). This conjecture has been verified computationally for at least the first 3000 fortunate numbers (which is extended very recently to 4600). Consequently, the conjecture is generally regarded as plausible.

There is another conjecture (similar to the fortunate numbers conjecture) which states: all *less-fortunate numbers* are prime (where "less-fortunate number" means $p_n\# - q$ where q is the largest prime less than $p_n\# - 1$). We note that less-fortunate numbers may also be called *lesser fortunate numbers* or *unfortunate numbers*.

6.1.19 Goldbach's Conjecture

This is one of the most famous, most simple, most challenging, and most traditional of open problems and conjectures related to prime numbers (and even beyond). In fact, it may be compared in these regards to Fermat's last theorem (which was proven in 1994). According to this conjecture, every even integer $n \geq 4$ can be written as the sum of two primes (whether different or not).

It is worth noting that this is the *strong Goldbach conjecture* as opposite to the *weak Goldbach conjecture* which states: every odd integer ≥ 7 can be written as the sum of three primes (not necessarily distinct).[581] This conjecture is *weak* because it can be obtained as a corollary of the *strong* conjecture since adding 3 to an even number (which is supposedly the sum of two primes) will produce an odd number (which is the sum of three primes).[582]

It is reported that the Goldbach conjecture is verified up to $n = 4 \times 10^{18}$ (with recent reports, yet to be independently validated, extending this bound even further). The conjecture is also supported by probabilistic models and analytic arguments. Also see Chen's theorem I (refer to § 5.1.8) which may also be regarded as a partial result or progress toward verifying or proving the Goldbach conjecture.

6.1.20 Hardy-Littlewood Conjecture F

This conjecture (which may also be labeled laxly as the *polynomial conjecture*) is essentially about the distribution of prime numbers (and is actually one of the most famous unsolved problems in number theory). The conjecture predicts how often prime numbers take the form of a quadratic polynomial, i.e. $f(n) = an^2 + bn + c$ where a is positive, $\gcd(a, b, c) = 1$, $a + b$ and c are not both even, and the discriminant $\Delta = b^2 - 4ac$ is not a perfect square. The conjecture provides an asymptotic formula for the count of

---

[580] More clearly, $\pi_{\mathfrak{N}}(x)$ represents the counting function for the number of integers $n \leq x$ for which the set $\{n + n_1, n + n_2, \ldots, n + n_k\}$ consists entirely of prime numbers, while $C_{\mathfrak{N}}$ (which is known as the *singular series* or the *Hardy-Littlewood constant*) is a correction factor that depends entirely on the specific pattern of offsets in the set $\mathfrak{N}$.

[581] As indicated earlier, the weak Goldbach conjecture has been proven (and hence it is a theorem; see § 5.1.16). We note that the weak Goldbach conjecture is related to the Vinogradov theorem and Waring's conjecture (see § 5.1.42).

[582] The choice of "3" is used to shift the even sequence directly into the odd sequence in equal steps, i.e.

$$4 + 3 = 7, \quad 6 + 3 = 9, \quad 8 + 3 = 11, \quad \cdots \quad \text{(and so on)}$$

these primes.[583]

6.1.21 Legendre's Conjecture

This conjecture is essentially about the distribution of primes in short intervals. It states that there exists at least one prime number between n^2 and $(n+1)^2$ for all $n \in \mathbb{N}$. This conjecture is verified for a wide range of values (reportedly up to $n = 3.33 \times 10^{13}$ or even $n = 7.05 \times 10^{13}$ where the latter comes from a verification of the stronger Oppermann conjecture). Moreover, proofs of partial or similar results do exist.[584] Legendre's conjecture is related to a number of other conjectures (such as the Brocard and Oppermann conjectures; see § 6.1.10 and § 6.1.25 as well as § 6.3) and even to some theorems (such as Bertrand's postulate and Ingham's theorem; see § 5.1.2 and § 6.4).

6.1.22 Lehmer's Totient Problem and Conjecture

The Lehmer totient problem (or the Lehmer conjecture) is a famous classical unsolved problem in number theory. The essence of this problem is the question of whether there is any composite number such that the Euler totient function $\phi(n)$ divides $n-1$. In fact, there are two (equivalent) formulations or approaches to this problem:

- Whether this divisibility property is a unique characterization of prime numbers.
- Whether composite solutions (known as *Lehmer numbers*) do exist.[585]

According to the Lehmer conjecture, if $\phi(n)$ divides $n-1$ then n must be a prime number. It has been proven that if a composite solution n to $\phi(n)|(n-1)$ does exist then it must be odd, square-free, and divisible by at least 15 distinct prime factors. Moreover, it must be a Carmichael number (see § 5.1.15, § 7.9.2 and § 9.7.1). It has been established that any composite counterexample must be extremely large (where the current results place the lower bound above 10^{30}).

6.1.23 Lemoine's Conjecture

Lemoine's conjecture states: any odd integer greater than 5 is the sum of an odd prime plus twice a prime (i.e. even semiprime; see § 9.5). In other words, for every $2 < n \in \mathbb{N}$ there exist primes p_1, p_2 (not necessarily distinct) such that $2n + 1 = p_1 + 2p_2$. This conjecture is stronger than (and hence implies) Goldbach's weak conjecture because $p_1 + 2p_2 = p_1 + p_2 + p_2$ (which is the essence of Goldbach's weak conjecture; see § 5.1.16) noting that Goldbach's weak conjecture is more relaxed about the form of the three primes.

Computational verification has established Lemoine's conjecture for all odd integers up to $n = 10^9$ (with recent reports raising this to $n = 10^{10}$ and beyond). In fact, Goldbach's weak conjecture (which is a proven theorem) may lend some support to Lemoine's conjecture (i.e. in an informal sense) since both conjectures represent odd integers as sums of three primes even though Lemoine's conjecture is more restrictive with regard to the nature of this sum.[586]

---

[583] The formula according to some references (which requires further checks) is:

$$\pi_f(x) \sim \frac{C_f}{\sqrt{a}} \int_2^x \frac{dt}{\sqrt{t} \ln t} \tag{102}$$

where $\pi_f(x)$ is the number of primes $p \leq x$ that are represented by $f(n)$, $\sim$ is the asymptotic equivalence symbol, and C_f is a correction factor that depends on the polynomial f (which depends on a, b, c). As indicated, this formula requires more rigorous checks.

[584] For example, it is proven that there is at least one prime between n^3 and $(n+1)^3$ for all sufficiently large n (Ingham's theorem or a consequence of it).

[585] "Lehmer numbers" may be used in a different meaning (i.e. a specific sequence of integers that generalize Lucas sequences).

[586] Also see `https://oeis.org/A046927`.

6.1.24 Mersenne Conjectures

Historically, "Mersenne's conjecture" refers to a certain statement about the primality of certain Mersenne numbers (i.e. integers of the form $2^n - 1$; see § 2.1.41). In short, Marin Mersenne (who is a seventeenth-century French mathematician) conjectured that for $n \leq 257$ (where $n \in \mathbb{N}$) the number $M_n = 2^n - 1$ is prime only for the values $n = 2$, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.[587] However, this conjecture contains a number of errors (i.e. the inclusion of $n = 67, 257$ and the exclusion of $n = 61, 89, 107$).[588] Recently, another (or "new") Mersenne's conjecture has emerged (seemingly motivated, in part, by a desire to understand the remarkable structure of Mersenne's original list and explain why Mersenne made his particular choices and mistakes), although the content of the new conjecture is very different from the content of the historical Mersenne conjecture.

Accordingly, there are currently more than one "Mersenne's conjecture", and hence we have "Mersenne's conjectures" (in accord with the title of this subsection). These Mersenne's conjectures (or possibly some of them) are:

• The old Mersenne conjecture (which we stated already; also see Point 4 of § 6.5).

• The new Mersenne conjecture, which commonly refers to the *Bateman-Selfridge-Wagstaff conjecture*, whose essence is establishing a link between Mersenne primes, Wagstaff primes and the form of their exponent p (as seen in § 6.1.7).

In fact, "Mersenne's conjecture" may even be used laxly to refer to the conjecture about the infinitude of Mersenne primes, i.e. the so-called *Lenstra-Pomerance-Wagstaff (or LPW) conjecture* which may also be called the *Mersenne primes conjecture* (see Point 1 of § 6.1.34).

6.1.25 Oppermann's Conjecture

This conjecture predicts that for all integers $n > 1$ there exists at least one prime between $(n^2 - n)$ and n^2, and at least another prime between n^2 and $(n^2 + n)$. This conjecture is obviously stronger than the Legendre conjecture (see § 6.1.21) because the gap between n^2 and $(n^2 + n)$ is smaller than the gap between n^2 and $(n + 1)^2$. Similarly, the gap between $(n^2 - n)$ and n^2 is smaller than the gap between $(n - 1)^2$ and n^2.

Roughly speaking $\big[$noting that $(n+1)^2 = n^2+2n+1\big]$, Oppermann's conjecture essentially breaks the gap in the Legendre conjecture into two gaps (i.e. a gap between n^2 and n^2+n and another gap between n^2+n and n^2+2n+1) where it puts a prime in each one of these gaps, and hence from Oppermann's conjecture we get two primes in the gap of Legendre's conjecture. Accordingly, if the Oppermann conjecture is established, the Legendre conjecture can be obtained as a corollary. Oppermann's conjecture has been verified computationally up to $n = 7.05 \times 10^{13}$.

6.1.26 Polignac's Conjecture

According to this conjecture, any even positive integer n can be written in infinitely many ways as the difference between two consecutive prime numbers. Alternatively, for every even positive integer n there are infinitely many pairs of consecutive primes whose difference is n. In fact, this conjecture is fundamentally related to the issue of prime gaps, i.e. it essentially predicts that prime gaps of any specific even size occur infinitely often. For $n = 2$, this conjecture reduces to the twin prime conjecture (see Point 1 of § 6.1.34), and hence this conjecture may be called the *generalized twin prime conjecture*.

The Polignac conjecture is mainly supported by some heuristic and analytic arguments. Although extensive computational searches may be able to provide some empirical support by finding many occurrences

[587] See `https://oeis.org/A109461`.
[588] See `https://oeis.org/A000043`.

of specified prime gaps and testing many even gap sizes, no finite computation can establish the conjecture or support it substantially. In short, the infinite scope of both the "every even positive integer" and "infinitely many ways" makes empirical computational verification, and even substantial support, virtually senseless.

6.1.27 Proth-Gilbreath Conjecture

The essence of this conjecture (which is also known as Gilbreath's conjecture) is that if the primes are arranged in a row and we repeatedly calculate the absolute differences between adjacent terms, the first number (i.e. the leftmost entry) in every resulting sequence will always be 1. The idea of this conjecture is illustrated in Figure 13. It is reported that the conjecture has been computationally verified for all primes up to 1.5×10^{15}.

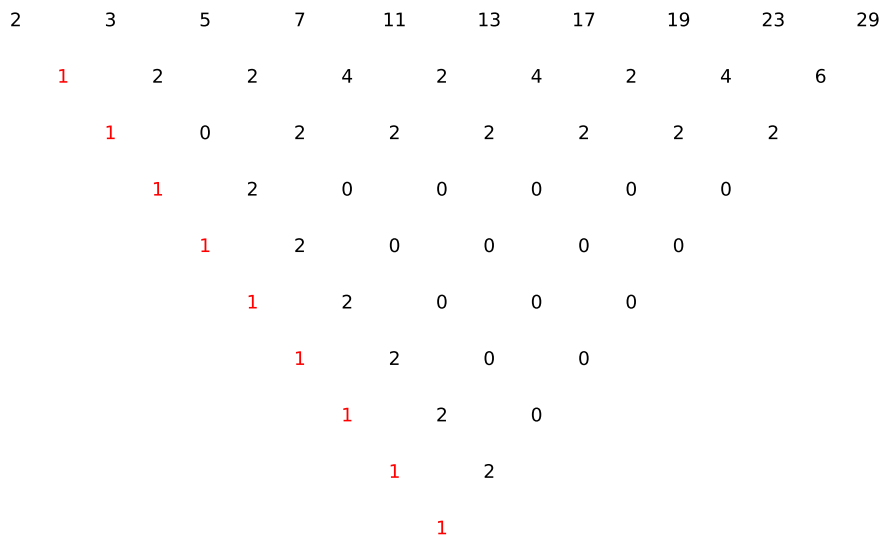


Figure 13: A "Proth-Gilbreath triangle" illustrating the Proth-Gilbreath conjecture for the first 10 prime numbers, i.e. 2 to 29 (see § 6.1.27).

6.1.28 Rassias' Conjecture

This conjecture predicts that for any odd prime p there exist two primes p_1, p_2 with $p_1 < p_2$ such that:

$$p = \frac{p_1 + p_2 + 1}{p_1} \tag{103}$$

It may also be stated as: for every odd prime p, there is at least one prime q where $q(p-1) - 1$ is also prime.[589] In fact, other formulations of this conjecture may be found in the literature (where their equivalence is demonstrated).

Rassias' conjecture is reportedly verified computationally for all odd primes $p < 10^9$. Within this range, empirical data demonstrates that a remarkably small prime q (specifically, $q \leq 1709$) always suffices to satisfy the condition. The conjecture may be viewed as a special case of Dickson's conjecture (see § 6.1.13) and is naturally generalized by Schinzel's hypothesis H (see § 6.1.30). Also see § 6.3.

[589] The condition $q < p$ may be imposed in computational searches, but it is not essential to the usual formulation of the conjecture.

6.1.29 Riemann's Hypothesis

This is one of the most famous and most important conjectures of number theory and complex analysis (if not all mathematics). The significance and fascination of this conjecture put it at the top of all mathematical problems (in the rank of famous problems like Fermat's last theorem and Goldbach's conjecture). Even though prime numbers are not mentioned in this hypothesis, the hypothesis is deeply connected to prime numbers.

The conjecture predicts that all the non-trivial zeros of the Riemann zeta function $\zeta(s)$ lie on the vertical line $\Re(s) = 1/2$ (known as "the critical line") in the complex plane, where $\Re(s)$ denotes the real part of the complex variable s.[590] This conjecture, if proven, would provide deeper insight into the distribution of prime numbers by giving much tighter control over the deviations of their distribution from its expected average behavior. It would also provide a sharper error bound in the prime number theorem (see § 5.1.31), yielding more precise estimates for the prime-counting function $\pi(x)$; see § 8.2.1.

It is noteworthy that Riemann's hypothesis has generalizations and modifications (such as the grand Riemann hypothesis and the modified grand Riemann hypothesis) as well as related conjectures. Moreover, Riemann's hypothesis (through the zeta function; see Eq. 48) indicates the deep connection between prime numbers (as discrete entities) and complex numbers (as continuous entities). A critical aspect of Riemann's hypothesis is that numerous proofs and theorems in mathematics are conditionally based on its validity, and hence if this conjecture is proved they will be fully validated (see for instance § 6.3). Such an advancement would represent a major leap in contemporary mathematics. In fact, Riemann's hypothesis, if proven, would have far-reaching implications and consequences even on some fully established results (as indicated already with regard to the prime number theorem; also see § 6.4).

Although Riemann's hypothesis is currently unproven, it is supported by many theoretical and probabilistic arguments as well as proven partial (or supporting) results, e.g. it is proven that there are infinitely many zeros on the critical line, and more than 40% of the non-trivial zeros lie on the critical line.[591] Moreover, it is computationally supported by (at least) the first 10^{13} zeros of the zeta function; all of which are verified to lie exactly on the aforementioned critical line.

6.1.30 Schinzel's Hypothesis H

This hypothesis (or conjecture) essentially predicts that a finite collection of non-constant irreducible polynomials with positive leading coefficients simultaneously takes prime values for infinitely many positive integers, provided they meet the local condition that no prime number divides the product of these polynomials for every integer. More technically, let $f_1(x), f_2(x), \ldots, f_k(x)$ be a finite set of non-constant polynomials that satisfy the following conditions:

- They have integer coefficients.
- They have positive leading coefficients.
- They are irreducible over $\mathbb{Q}$.
- There is no prime number p that divides $f_1(x) \times f_2(x) \times \cdots \times f_k(x)$ for every integer x.

Then there are infinitely many positive integers n such that all of $f_1(n), f_2(n), \ldots, f_k(n)$ are prime.

Schinzel's hypothesis H remains one of the most significant unproven conjectures in number theory because it encompasses many other famous open problems and conjectures (and even some proven theorems); for instance:

⋆ By taking a single polynomial $f(x) = ax + b$ with the given conditions we get Dirichlet's theorem on arithmetic progressions (see § 5.1.11).

[590] The trivial zeros of the zeta function are at the negative even integers.

[591] A recent AI investigation claims that more than two thirds of the zeros of the Riemann zeta function are simple and on the critical line.

⋆ By setting $f_1(x) = x$ and $f_2(x) = x + 2$ we get the twin prime conjecture (see Point 1 of § 6.1.34). Replacing 2 with 4 and 6 should similarly lead to the conjectured infinitude of cousin and sexy primes.
⋆ By setting $f_1(x) = x$ and $f_2(x) = x + c$ (where c is a positive even integer) we get a *weakened* form of Polignac's conjecture where the primes are not required to be consecutive (see § 6.1.26).
⋆ By taking a single polynomial $f(x) = x^2 + 1$ we get the $n^2 + 1$ primes conjecture (see Point 1 of § 6.1.34). This similarly applies to conjectures about the primality of polynomials of certain forms like the conjecture about the infinitude of n^4+1 primes and the infinitude of Euler primes (see Point 1 of § 6.1.34).
⋆ By taking a single polynomial $f(x)$ with the aforementioned conditions we get Bunyakovsky's conjecture (see § 6.1.11).
⋆ By setting $f_1(x) = a_1x + b_1$, $f_2(x) = a_2x + b_2$, $\ldots$, $f_k(x) = a_kx + b_k$ with the given conditions we get Dickson's conjecture (see § 6.1.13).

In fact, Schinzel's hypothesis H is commonly regarded as the "ultimate" conjecture for prime values of polynomials because of its incredible breadth and far-reaching implications in this regard. Despite this, Schinzel's hypothesis H may be seen as a consequence of the more comprehensive and more specific (and hence stronger) conjecture of Bateman-Horn (see § 6.1.6). This is because while Schinzel's hypothesis H is a rather qualitative statement (since it is about the existence of infinitely many primes), the Bateman-Horn conjecture is quantitative (since it provides a specific formula for the number of prime-generating integers as a function of $x \geq 1$ which logically implies the existence of infinitely many primes as $x \to \infty$).

One of the special cases of Schinzel's hypothesis H that is already proved is Dirichlet's theorem on arithmetic progressions (as indicated above). Beyond this, there are many theoretical and heuristic arguments, as well as computational evidence and partial results, that support the conjecture. In particular, the partial verifications and support of the conjectures encompassed by this hypothesis (as exemplified by the aforementioned list, e.g. the twin prime and Bunyakovsky conjectures) also provide support for Schinzel's hypothesis H, although the conjecture itself remains unproven.

6.1.31 Schinzel-Sierpinski Conjecture

This conjecture establishes a link between rational numbers $\mathbb{Q}$ and prime numbers $\mathbb{P}$. It simply predicts that any positive rational number q can be expressed as a quotient of shifted primes of the form $q = \frac{p_1+1}{p_2+1}$ where $p_1, p_2 \in \mathbb{P}$.[592] This conjecture is profoundly significant because it implies that the set of primes (in their specific shifted form $p + 1$) is sufficiently large and multiplicatively flexible that it can generate the entire set of positive rationals. As the set of rational numbers is infinite, this conjecture naturally implies the infinitude of prime numbers (which is a rather trivial, already proven result).

The Schinzel-Sierpinski conjecture may be supported by the theorem that for any positive rational number q, the power $q^{|G|}$ can be written as a product or quotient of shifted primes, that is:

$$q^{|G|} = \prod_{i=1}^{k} (p_i + 1)^{\varepsilon_i} \tag{104}$$

where G is the quotient group of order $|G| \leq 3$, $k \in \mathbb{N}$, $\varepsilon_i \in \{+1, -1\}$, and p_i are primes which may not be distinct. The Schinzel-Sierpinski conjecture is stronger and more specific than this theorem because it asserts that q itself, rather than a bounded power of q, can be represented using only two such primes with specific ε_i's. The conjecture may also be supported by other analytical, statistical and computational arguments and tests.

[592] A shifted prime is an integer obtained from a prime number p by adding a non-zero integer c, i.e. $p + c$. It is worth noting that if Schinzel's hypothesis H (see § 6.1.30) holds true, it guarantees that such a representation exists in an infinite number of ways for both the form $q = \frac{p_1+1}{p_2+1}$ and the form $q = \frac{p_1-1}{p_2-1}$.

6.1.32 Second Hardy-Littlewood Conjecture

According to this conjecture:

$$\pi(x+y) \leq \pi(x) + \pi(y) \tag{105}$$

where π denotes the prime-counting function (see § 8.2.1) and x, y are integers greater than 1. This relation means that the prime-counting function is subadditive on this domain.

The conjecture has a notable connection with the first Hardy-Littlewood conjecture (see § 6.1.17), where it has been proved that the two conjectures are incompatible. Specifically, it has been established that the first conjecture implies the existence of values of x, y for which $\pi(x+y) > \pi(x) + \pi(y)$. Nevertheless, no explicit numerical counterexample to the second conjecture is currently known.

The second conjecture therefore occupies an unusual position in the mathematical community. It has traditionally been regarded as probably false because of its incompatibility with the first conjecture (which is generally regarded as the more plausible of the two). At the same time, several works have established the inequality in increasingly broad ranges. While occasional claims of an unconditional proof have emerged in the literature, the second conjecture continues to be treated as an open problem in subsequent literature.

6.1.33 Shanks' Conjecture

This conjecture addresses the asymptotic growth rate of gaps between consecutive prime numbers. It simply claims that the maximum prime gap among primes not exceeding x is asymptotic to the square of the natural logarithm of x as x approaches infinity, that is:

$$g_{\max}(x) \sim (\ln x)^2 \qquad \text{as } x \to \infty \tag{106}$$

where $g_{\max}(x)$ is the maximum gap between any two consecutive primes (p_n and p_{n+1}) not exceeding x.

This conjecture arises from a probabilistic model for the distribution of prime gaps originally proposed by Cramer, and is therefore also known as the *Cramer-Shanks conjecture* (noting that Shanks independently arrived at this formulation using a different heuristic argument). Computational evidence across massive ranges of primes (including exhaustive searches up to 4×10^{18}) is broadly consistent with the predicted $(\ln x)^2$ growth rate. However, there are theoretical and heuristic indications that the leading constant in this asymptotic formula may be larger than 1. In particular, refinements of Cramer's model suggest that the maximal prime gap may asymptotically exceed $(\ln x)^2$ by a multiplicative factor, although the precise asymptotic behavior of the largest prime gaps remains unknown.

6.1.34 Conjectures on Infinitude of Certain Types of Primes

In the following list we outline the main open problems and conjectures about the infinitude of certain types of prime numbers:

1. It is conjectured that there are infinitely many primes of the following types: balanced, Bell, Carol, centered k-gonal ($k \neq 8, 9$),[593] cousin (also see § 6.1.26), cuban, Cullen, dihedral, emirp, Euler, factorial, Fibonacci, fortunate, full reptend, generalized Fermat, happy, harmonic, Higgs, highly cototient, Jacobsthal, Kynea, Leyland, Lucas, lucky, Mersenne,[594] Mersenne prime exponents,[595] Mirimanoff,

[593] According to this conjecture, there are infinitely many centered k-gonal primes for every $k \geq 3$ except for $k = 8$ and $k = 9$. The exclusion of $k = 8$ and $k = 9$ is because it is proven that there are no centered k-gonal primes for $k = 8$ and $k = 9$ (see § 2.1.5).

[594] This is also known as Lenstra-Pomerance-Wagstaff (or LPW) conjecture (see footnote [154]). We note that the infinitude (as well as finitude) of double Mersenne primes is also conjectured.

[595] Mersenne primes conjecture implies the infinitude of Mersenne prime exponents (and conversely), i.e. they are equivalent due to the one-to-one correspondence between the two types of primes.

$n^2 + 1$ ($n \in \mathbb{N}$),[596] $n^4 + 1$ ($n \in \mathbb{N}$), near-square, non-generous, NSW, Padovan,[597] palindromic (in base 10), palindromic wing (in base 10), partition, Pell, permutable, Perrin, Pierpont, primeval, primorial (and twin primorial),[598] Proth, quartan, regular (i.e. of Bernoulli, Euler and Genocchi types),[599] repunit,[600] safe, self (in even bases), sexy (also see § 6.1.26), Smarandache-Wellin, Sophie Germain, strobogrammatic, Thabit (of each kind), Tribonacci, twin, unique, Wagstaff, Wall-Sun-Sun,[601] Wieferich, Wilson, Wolstenholme,[602] and Woodall.

2. Chen primes conjecture: there are infinitely many Chen primes p for which $p + 2$ is composite (i.e. semiprime; see § 2.1.6 and § 9.5). It is worth noting that there are correlations between this conjecture and the twin prime conjecture. Specifically, if the twin prime conjecture is false, then this conjecture (i.e. about Chen primes with composite $p + 2$) must be true (because there are infinitely many Chen primes). Similarly, if this conjecture is false, then the twin prime conjecture must be true. On the other hand proving any one of these conjectures does not disprove the other conjecture (because there could be infinitely many of both types).
3. Home primes conjecture: every natural number greater than 1 has a home prime (i.e. every natural number greater than 1 will eventually reach a prime number through the successive process of prime factorization and concatenation). However, whether the set of distinct home primes generated specifically by composite numbers is infinite remains an open problem (see Point 4 of § 2.1.31).

We should finally note that many of the infinitude conjectures have counterparts (i.e. finitude conjectures). So, the above list of conjectures (and similar infinitude conjectures in other parts of this book) usually represent the common (or standard or mainstream) beliefs about infinitude. We may also say: many of the infinitude conjectures in this book should be understood as open problems with competing hypotheses and views, rather than as definitive consensus statements. This note should also apply broadly to the finitude conjectures (see for instance § 6.1.35), and even to conjectures in general (which is justified by the nature of conjectures as being about tentative open problems).

6.1.35 Conjectures on Finitude of Certain Types of Primes

In the following list we outline the main open problems and conjectures about the finitude of certain types of prime numbers:

1. Circular primes conjecture: there are only finitely many non-repunit circular primes (see § 2.1.7 and § 2.1.69; but also see footnote [58]).
2. Fermat primes conjecture: there are only finitely many Fermat primes. It is also conjectured that the known five Fermat primes are the only Fermat primes in existence (see § 2.1.20).
3. Stern primes conjecture: there are only finitely many Stern primes. In fact, it is conjectured that the eight known Stern primes are the only Stern primes in existence (see § 2.1.77).
4. Twin factorial primes conjecture: (5, 7) is the only twin factorial prime pair with the same n (i.e. $n = 3$; see § 2.1.19).

[596] This may also be called Landau's conjecture or Landau's problem (or one of Landau's conjectures or problems) and may also be called Landau's fourth problem and the fifth Hardy-Littlewood conjecture.

[597] There is seemingly an opposite conjecture, i.e. there are only finitely many Padovan primes.

[598] To be more clear: it is conjectured that there are infinitely many primorial primes, as well as composites (i.e. of the form $p_n\# \pm 1$), and twin primorial primes (see Point 10 of § 2.1.64).

[599] This may also be called Siegel's conjecture (noting that this seems to be part of Siegel's conjecture, with potential restriction to the Bernoulli regular). As indicated earlier, the infinitude of irregular primes (i.e. of Bernoulli, Euler and Genocchi types) is proven.

[600] It is worth noting that there are other conjectures related to repunit primes.

[601] It is also conjectured that there are only finitely many Wall-Sun-Sun primes (as well as none of them). See § 2.1.88.

[602] There is seemingly an opposite conjecture, i.e. there are only finitely many Wolstenholme primes. In fact, some mathematicians seem even to conjecture that the only Wolstenholme primes are the two currently known ones, i.e. 16843 and 2124679. See § 2.1.92.

5. Untouchable primes conjecture: 2 and 5 are the only untouchable primes in existence (see § 2.1.86).
6. Finitude (as well as infinitude) is conjectured for Wall-Sun-Sun primes (see footnote [601]).
7. Finitude (as well as infinitude) is seemingly conjectured for both Padovan and Wolstenholme primes (see footnotes [597] and [602]).

6.2 Classification of Open Problems and Conjectures

In this section we classify the open problems and conjectures about (or related to) prime numbers.

6.2.1 Foundations

In this subsection, we list a number of foundational open problems and conjectures about (or related to) prime numbers which are frequently encountered in the literature of number theory:
1. *abc* conjecture (see § 6.1.1).
2. Artin's conjecture on primitive roots (see § 6.1.5).
3. Beal's conjecture (see § 6.1.8).
4. Birch-Swinnerton-Dyer conjecture (see § 6.1.9).
5. Feit-Thompson conjecture (see § 6.1.15).
6. Goldbach's conjecture (see § 6.1.19).
7. Proth-Gilbreath conjecture (see § 6.1.27).
8. Riemann's hypothesis (and generalized Riemann hypotheses). See § 6.1.29.

6.2.2 Existence

There are many open problems and conjectures about the existence of prime numbers of certain types (or in particular situations or conditions) or mathematical entities (e.g. numbers or sequences) related to primes. We list in the following some examples of these open problems and conjectures:
1. Brocard's conjecture (see § 6.1.10).
2. Legendre's conjecture (see § 6.1.21).
3. Oppermann's conjecture (see § 6.1.25).
4. Rassias' conjecture (see § 6.1.28).
5. There exists an even integer $N < 246$ such that there are infinitely many pairs of primes that differ by N (an open problem related to Zhang's theorem and Polignac's conjecture; see § 5.1.44 and § 6.1.26).
6. There exists a counterexample to the Baillie-PSW primality test (see § 7.3.3). There is also an opposite conjecture (which belongs to § 6.2.3).
7. There exists at least one prime between n^3 and $(n+1)^3$ for *every* $n \in \mathbb{N}$ (noting that Ingham's theorem establishes this only for *all sufficiently large* n).
8. If an odd perfect number exists, then in its Eulerian form $N = q^k n^2$ we must have $k = 1$ (Descartes-Frenicle-Sorli conjecture).
9. Open problems and conjectures about infinitude (see § 6.2.4) are essentially about existence (i.e. of infinitely many). Similarly, some of the open problems and conjectures about finitude (see § 6.2.5) are essentially about existence (i.e. of only finitely many).

6.2.3 Non-Existence

In this subsection we list a number of conjectures and open problems about the non-existence of prime numbers of certain types or categories or under certain conditions (or non-existence of other mathematical objects related to prime numbers):

1. Agoh-Giuga conjecture (see § 6.1.2).[603]
2. Feit-Thompson conjecture (see § 6.1.15).
3. Goldbach's conjecture (i.e. there is no even integer > 2 that is not the sum of two primes; see § 6.1.19).
4. Lehmer's totient problem and conjecture (see § 6.1.22).[604]
5. There is no Fermat prime beyond F_4 (see § 2.1.20).
6. There is no Wall-Sun-Sun prime (noting that it is also conjectured that such primes do exist; see § 2.1.88).
7. There is no composite $n \in \mathbb{N}$ such that n^2 divides $2^{n-1} - 1$ (i.e. no Wieferich pseudoprimes to base 2 exist; see § 9.7.13).
8. There is no composite integer that is simultaneously a strong Fermat and strong Lucas pseudoprime (also see Point 41 of 6.2.4).
9. There is no odd prime p that divides the left factorial $!p = 0! + 1! + \cdots + (p-1)!$ (Kurepa's conjecture or the left factorial hypothesis).
10. Open problems and conjectures about finitude (see § 6.2.5) are essentially about the non-existence of further examples beyond a finite set.

6.2.4 Infinitude

In this subsection, we list a number of conjectures and open problems concerning the infinitude of certain types (or categories or sequences) of primes and prime-related objects. For brevity, we may list only the conventional names or labels of the conjectures that carry an infinitude implication:

1. See § 6.1.34 which is about the conjectures on the infinitude of certain types of primes.
2. Artin's conjecture on primitive roots (see § 6.1.5).
3. Bunyakovsky's conjecture (see § 6.1.11).
4. Cunningham chains conjecture (see § 9.1.3).
5. Dickson's conjecture (see § 6.1.13).
6. First Hardy-Littlewood conjecture (see § 6.1.17).
7. Fortunate numbers conjecture (see § 6.1.18).[605]
8. Hardy-Littlewood conjecture F (see § 6.1.20).
9. Polignac's conjecture (see § 6.1.26).[606]
10. Rassias' conjecture (see § 6.1.28).
11. Schinzel's hypothesis H (see § 6.1.30).
12. Schinzel-Sierpinski conjecture (see § 6.1.31).
13. There are infinitely many primes p such that $p! + 1$ is composite.
14. There are infinitely many primes p such that both $p - 1$ and $p + 1$ have a prime factor exceeding p^c for some constant $c > 1/2$.
15. There are infinitely many primes p such that the sum of digits of p is equal to a given value (with some restrictions, such as non-violation of basic divisibility rules, which generally depend on the base of numeric system). Also see Point 2 of § 6.6.
16. There are infinitely many primes of certain algebraic forms, e.g. n^2+1, n^2+2, n^2-2, $3n^2+1$, n^2+n+1, $n^2 + n + 41$, $2n^2 + 3n - 1$, $n^3 + 2$, $n^3 + 2n + 1$ (see for instance § 6.1.11).[607]

[603] This means: there is no composite number n that satisfies Eqs. 92 and 93.

[604] The essence of Lehmer's totient conjecture is that there is no composite number n such that $\phi(n)$ divides $n - 1$.

[605] It is worth remembering that the infinitude implied by the fortunate numbers conjecture is different from the infinitude of fortunate prime numbers (which is also conjectured; see § 2.1.22).

[606] We should mention here Kronecker's conjecture (a weaker version of Polignac's conjecture) which states: every even positive integer is the difference of infinitely many pairs of primes.

[607] The quadratic forms are related to the problem of "prime values of quadratic polynomials" which is a famous unsolved challenge in number theory. The essence of this problem is whether simple, single-variable quadratic polynomials with integer coefficients can generate infinitely many prime numbers as input values vary. Despite massive efforts not a single

17. There is an even integer $N < 246$ such that there are infinitely many pairs of primes that differ by N (an open problem related to Zhang's theorem and the Polignac conjecture; see § 5.1.44 and § 6.1.26).
18. There are infinitely many primes that can be written as the sum of two primes (i.e. the larger elements of twin prime pairs).[608]
19. There are infinitely many primes of the form $x^2 + y^6$ where x and y are integers.[609]
20. There are infinitely many primes of the form $\lfloor e^n \rfloor$ where $n \in \mathbb{N}$.[610]
21. There are infinitely many primes p such that p^2 does not divide $2^{p-1} - 1$.[611]
22. There are infinitely many primes p such that $p + 2$ is a semiprime.[612]
23. There are infinitely many primes p such that $p^3 + 2$ is also prime.
24. There are infinitely many primes p such that $p + 2$ is also prime or a prime power. Repeat for $p - 2$.
25. There are infinitely many primes p such that $2p - 1$ is also prime (similar to the Sophie Germain prime conjecture; see § 2.1.76). Also see § 9.1.3.
26. There are infinitely many primes p such that $(p+1)/2$ is also prime (similar to the safe prime conjecture; see § 2.1.72). Also see § 9.1.3.
27. There are infinitely many generalized Wieferich primes in every integer base ≥ 2 (see § 2.1.90 and Point 1 of § 2.7).
28. There are infinitely many primes in the Piatetski-Shapiro sequence $(\lfloor n^c \rfloor)_{n=1}^{\infty}$ for any non-integer $c \in (1, 2)$.[613]
29. There are infinitely many prime Catalan-Mersenne numbers (see § 9.1.2).[614]
30. There are infinitely many primes p such that the period (i.e. the Pisano period) of the Fibonacci sequence modulo p is exactly $p - 1$.
31. There are infinitely many primes p such that the order of 2 modulo p is $(p - 1)/2$.[615]
32. There are infinitely many primes that are the sum of two prime squares (i.e. of the form $p^2 + 4$ where $p \in \mathbb{P}$).
33. There are infinitely many primes of the form $p + 2^n$ (where $p \in \mathbb{P}$ and $1 \leq n \in \mathbb{N}$).[616]
34. There are infinitely many primes p such that $p + 2^n$ is prime for some $n \in \mathbb{N}$.[617]
35. There are infinitely many primes of the form $2^m + 3^n$ $(m, n \in \mathbb{N})$.
36. There are infinitely many primes whose digits are restricted to a small subset of possible digits (e.g. primes containing only the digits 0 and 1 or excludes the digits 3 and 7).[618]
37. For any fixed $\varepsilon > 0$, every interval of the form $(n, n + n^{\varepsilon})$ contains at least one prime for all sufficiently large integers n (and hence there are infinitely many primes in such intervals).[619]

---

quadratic polynomial has been unconditionally proven to yield infinitely many primes. The simplest of these is the famous Landau fourth problem on $n^2 + 1$ (see § 2.1.47). Another example is Euler primes of the form $n^2 + n + 41$ (see § 2.1.18). The problem actually extends to primes in non-linear polynomials in general (i.e. beyond quadratic).

[608] This is equivalent to the twin prime conjecture.

[609] Some sources seem to suggest that it is a proven theorem but we could not find a proof (so please check) noting that it may be proved conditionally. We should also note that the infinitude of $x^2 + y^6$ should imply the infinitude of $x^2 + y^3$.

[610] See `https://oeis.org/A000149`.

[611] This is the conjecture that there are infinitely many non-Wieferich primes (noting that this has been proven conditionally, i.e. if the *abc* conjecture holds true). See § 2.1.90 and § 6.1.1.

[612] This may be generalized by replacing 2 with h (where h is a positive even integer), which may be viewed as a semiprime analogue of Polignac's conjecture (especially if h is restricted to be a prime gap between consecutive primes). Also see § 5.1.9 and § 6.1.26.

[613] A recent study seems to prove this for $1 < c < 10318869/8886224$.

[614] In fact, it is conjectured that every Catalan-Mersenne number is prime.

[615] This is a direct analogue and variation of Artin's conjecture on primitive roots (see § 6.1.5).

[616] This is equivalent to the conjecture that there are infinitely many pairs of primes whose difference is a power of 2.

[617] This is stronger than the conjecture of Point 33.

[618] This conjecture is the "restricted digit" or (sparse set) version of the theorem about the infinitude of primes omitting a single digit (see Point 23 in § 5.2.4). In fact, this conjecture is a sort of generalization or extension to that theorem.

[619] The conjectural content of this statement is actually for $0 < \varepsilon < 1$. For $\varepsilon \geq 1$ it is already proven (see § 5.1.2).

38. The Euclid-Mullin sequence includes all primes (see § 9.1.4).[620]
39. It is unknown (and hence it is an open problem) whether there are infinitely many primes p for which the Mersenne number $2^p - 1$ is composite (see § 2.1.41).
40. There are infinitely many Catalan pseudoprimes (see § 9.7.2).
41. There are infinitely many composite integers that are strong Fermat and strong Lucas pseudoprimes simultaneously (also see Point 8 of 6.2.3).
42. Many other conjectures (especially in the categories of prime distribution and prime gaps, such as Bateman-Horn and Legendre's) have infinitude implications and consequences.
43. As indicated earlier, many of the finitude conjectures (see for instance § 6.2.5) have counterparts (i.e. corresponding infinitude conjectures).

6.2.5 Finitude

In this subsection we list some of the conjectures and open problems about the finitude of certain types and categories of prime numbers:

1. See § 6.1.35 which is about the conjectures on the finitude of certain types of primes.
2. There are only finitely many (possibly only four) double Mersenne primes (noting that their infinitude is also conjectured).
3. There are only finitely many (possibly none) primes p such that p^3 divides $2^{p-1} - 1$.
4. There are only finitely many primes p such that $p! + 1$ is a perfect square (Brocard's problem applied to prime numbers).[621]
5. There are only finitely many primes of certain truncatable types in certain numeral bases. For many standard types, this finiteness has been proved (often by exhaustive computation), while other variants remain open.
6. As indicated earlier, many of the infinitude conjectures have counterparts (i.e. corresponding finitude conjectures). See for instance § 6.1.34.
7. It is unknown whether there are finitely or infinitely many primes of certain forms. Examples of such forms are: $2^p + p$ ($p \in \mathbb{P}$), $n! + n + 1$ ($n \in \mathbb{N}$), and $n^n + n + 1$, among many others.

6.2.6 Distribution

In this subsection we list some of the common conjectures and open problems about the distribution of prime numbers (or related to their distribution) in various senses and contexts:

1. Andrica's conjecture (see § 6.1.4).
2. Artin's conjecture on primitive roots (see § 6.1.5).
3. Bateman-Horn conjecture (see § 6.1.6).
4. Brocard's conjecture (see § 6.1.10).
5. Bunyakovsky's conjecture (see § 6.1.11).
6. Cramer's conjecture (see § 6.1.12).
7. Cunningham chains conjecture (see § 9.1.3).
8. Dickson's conjecture (see § 6.1.13).
9. Elliott-Halberstam conjecture (see § 6.1.14).
10. Euclid-Mullin sequence conjecture (see § 9.1.4).
11. Firoozbakht's conjecture (see § 6.1.16).
12. First Hardy-Littlewood conjecture (see § 6.1.17).
13. Hardy-Littlewood conjecture F (see § 6.1.20).

[620] The Euclid-Mullin sequence is an infinite sequence of primes, so the conjectural content is in "includes all primes".
[621] The only known solutions of Brocard's problem (i.e. $n! + 1 = m^2$) are $n = 4$, 5, and 7.

14. Legendre's conjecture (see § 6.1.21).
15. Oppermann's conjecture (see § 6.1.25).
16. Polignac's conjecture (see § 6.1.26).
17. Rassias' conjecture (see § 6.1.28).
18. Riemann's hypothesis (and generalized Riemann hypotheses; see § 6.1.29).
19. Schinzel's hypothesis H (see § 6.1.30).
20. Second Hardy-Littlewood conjecture (see § 6.1.32).
21. Shanks' conjecture (see § 6.1.33).
22. We may also broadly classify conjectures concerning the infinitude and finitude of specific prime types and families (see for instance § 6.2.4 and § 6.2.5) under the "Distribution" category (or at least as closely related to it), since questions of infinitude and finitude concern the long-term distribution of these prime families, including their asymptotic behavior and whether they persist indefinitely. Even when such conjectures do not explicitly predict an asymptotic density, they nevertheless address the global occurrence and long-term behavior of these prime families.
23. We may also refer in this context to the Lemke Oliver and Soundararajan bias (which we indicated earlier; see Point M of § 5.2.6).[622]

Also see chapter 8 (and § 8.5 in particular).

6.2.7 Algebraic Forms

In this subsection we list some of the common conjectures and open problems about the algebraic forms of prime numbers and related issues:

1. Bateman-Horn conjecture (see § 6.1.6).
2. Bateman-Selfridge-Wagstaff conjecture (see § 6.1.7).
3. Bunyakovsky's conjecture (see § 6.1.11).
4. Dickson's conjecture (see § 6.1.13).
5. Hardy-Littlewood conjecture F (see § 6.1.20).
6. Mersenne conjectures (see § 6.1.24).
7. Rassias' conjecture (see § 6.1.28).
8. Schinzel's hypothesis H (see § 6.1.30).
9. Also see § 6.2.4 and § 6.2.5 for open problems and conjectures about the infinitude and finitude of certain algebraic forms of prime numbers (e.g. $n^2 + 1$ and $2^p + p$).
10. Since primes are positive integers, open problems and conjectures about algebraic forms of integers (or natural numbers) often apply to primes as a special case. For example, it is conjectured that every integer (and hence every prime) not of the form $9n \pm 4$ is a sum of three cubes.

6.2.8 Numeric Forms

In this subsection we list some of the conjectures and open problems about the numeric forms of prime numbers and related issues (which are mostly related to digit and string format of prime numbers and are normally base-dependent):

1. See § 6.2.4 and § 6.2.5 for open problems and conjectures about the infinitude and finitude of certain numeric forms of prime numbers (and related issues).
2. While the Copeland-Erdos constant is proven to be normal in base 10, its normality in every base $b \geq 2$ other than $b = 10$ remains an open problem (see Point 27 of § 5.2.8). It is widely conjectured to be normal in every base $b \geq 2$ (meaning it is absolutely normal), though a formal proof for any base other

[622] This phenomenon was initially observed computationally and its explanation involves conjectural results. Hence, it may fit within the classification of conjectures (at least in its explanation).

than 10 remains unknown.
3. It is an open problem whether the real number formed by concatenating the values of the prime-counting function $\pi(n)$ [that is: $0.\pi(1)\pi(2)\ldots = 0.0122334444\ldots$] is a normal number (see § 8.2.1 and § 9.1.6).[623]
4. We may also refer in this context to the Lemke Oliver and Soundararajan bias (see Point 23 of § 6.2.6; also see Point 29 of § 5.2.8).

6.2.9 Role of Primes in the Number System

In this subsection we list some of the conjectures and open problems regarding the role of prime numbers in the structure of the number system (mainly the integers) and related issues:
1. Beal's conjecture (see § 6.1.8).
2. Fortunate numbers conjecture (see § 6.1.18).
3. Goldbach's conjecture (see § 6.1.19).
4. Lemoine's conjecture (see § 6.1.23).
5. Polignac's conjecture (see § 6.1.26).
6. Proth-Gilbreath conjecture (see § 6.1.27).
7. Schinzel-Sierpinski conjecture (see § 6.1.31).
8. Every even positive integer can be written as the difference between at least one pair of primes (Maillet's conjecture which is weaker than Polignac's conjecture).
9. Every even positive integer is the difference of infinitely many pairs of primes (Kronecker's conjecture which is weaker than Polignac's conjecture but stronger than Maillet's conjecture).
10. If an odd perfect number exists, then in its Eulerian form $N = q^k n^2$ we must have $k = 1$ (Descartes-Frenicle-Sorli conjecture).
11. Every integer $n > 1$ has a home prime.
12. There are no three consecutive powerful numbers (Erdos-Mollin-Walsh conjecture).[624]
13. Also see Catalan-Dickson conjecture (and the opposing Guy-Selfridge conjecture) in § 9.1.1.

6.2.10 Primality Testing and Sieving

In this subsection we list a number of conjectures and open problems about primality testing and/or prime sieving (or have some relation to primality testing and sieving):
1. Agoh-Giuga conjecture (see § 6.1.2).
2. Agrawal's conjecture (and the modified version; see § 6.1.3).
3. There exists a counterexample to the Baillie-PSW primality test (see § 7.3.3). There is also an opposite conjecture.
4. The smallest Riesel number is 509203 (see § 7.9.3).
5. The smallest Sierpinski number is 78557 (see § 7.9.4).
6. Artin's conjecture on primitive roots (see § 6.1.5) predicts the infinitude and, in suitable cases, the density of primes for which a given integer is a primitive root. Consequently, it has potential applications to questions concerning the distribution of primes and hence to certain prime-sieving problems.
7. For some primality tests (see for instance § 7.3.12 and § 7.3.18), deterministic variants or deterministic bounds are available under the assumption that the generalized (or extended) Riemann hypothesis holds (see § 6.1.29).
8. Lehmer's totient conjecture (see § 6.1.22) is closely related to primality testing through the characterization of primes by the condition $\phi(n)|(n-1)$.

[623] It seems that a recent conditional proof shows that its normality follows from Cramer's conjecture.

[624] A powerful number is a positive integer n where for every prime p that divides n, p^2 also divides n (see `https://oeis.org/A001694`). It should be obvious that perfect powers are a proper subset of powerful numbers.

9. A longstanding open problem concerning deterministic polynomial-time primality testing without assuming the generalized (or extended) Riemann hypothesis (see § 6.1.29) was resolved by the development of the AKS primality test (see § 7.3.1).

We should finally note that although conjectures about primality testing and sieving cannot currently provide unconditional primality tests or sieves, extensive computational evidence in their favor may occasionally qualify them to offer heuristic support for primality determinations obtained by other methods, without constituting a proof of primality (see § 7.3.22).

6.2.11 Subsets

In this subsection we list a number of conjectures and open problems regarding the subset relationships among prime types and categories (and related issues):
1. Catalan-Mersenne numbers are a proper subset of prime numbers (see § 9.1.2).
2. Fermat primes are a proper subset of regular primes (noting that all five known Fermat primes are regular; see § 2.1.20).
3. Fortunate numbers are a proper subset of prime numbers (see § 6.1.18).
4. The numbers in the Euclid-Mullin sequence are an improper subset of the prime numbers (see § 9.1.4).

6.2.12 Divisibility and Modularity

In this subsection we list a number of conjectures and open problems about divisibility and modularity connected to prime numbers (and related issues):
1. Agoh-Giuga conjecture (see § 6.1.2).
2. Artin's conjecture on primitive roots (see § 6.1.5).
3. Feit-Thompson conjecture (see § 6.1.15).
4. Lehmer's totient problem and conjecture (see § 6.1.22).
5. Rassias' conjecture (see § 6.1.28).
6. Schinzel-Sierpinski conjecture (see § 6.1.31).
7. There is no odd prime that divides the left factorial $!p = 0! + 1! + \cdots + (p-1)!$ (Kurepa's conjecture or left factorial hypothesis).
8. There are infinitely many primes p such that p^3 does not divide $2^{p-1} - 1$.
9. There are only finitely many (possibly none) primes p such that p^3 divides $2^{p-1} - 1$.
10. There is no composite $n \in \mathbb{N}$ such that n^2 divides $2^{n-1} - 1$ (see § 9.7.13).

6.2.13 Calculation of Primes

In this subsection (which is about conjectures and open problems on the calculation of the n^{th} prime number exactly) we only include the following "broad conjecture": there is no closed-form formula in "elementary terms" for the n^{th} prime number p_n. Conjectures and open problems beyond this "conjecture" (and its scope) should be investigated in the future.

6.2.14 Estimation of p_n

In this subsection we list a number of conjectures and open problems about (or related to) the estimates and approximations of the n^{th} prime number (where "Estimation" includes imposing bounds and restrictions on its size, e.g. by inequalities):[625]
1. Andrica's conjecture: $\sqrt{p_{n+1}} < \sqrt{p_n} + 1$. See § 6.1.4.
2. Cramer's conjecture: $p_{n+1} = p_n + O(\ln^2 p_n)$. See § 6.1.12.

[625] For simplicity (and consistency with the commonly used forms) the focus of the following relations is p_{n+1}.

3. Cramer-Granville conjecture: $p_{n+1} < p_n + K(\ln^2 p_n)$ for some constant $K > 1$.
4. Farhadian's conjecture: $p_{n+1} < p_n \sqrt[n]{\frac{p_n \ln n}{\ln p_n}}$ (for $n \geq 5$).
5. Firoozbakht's conjecture: $p_{n+1} < p_n^{1+(1/n)}$. See § 6.1.16.
6. Nicholson's conjecture: $p_{n+1} \leq p_n \sqrt[n]{n \ln n}$ (for $n \geq 5$).

6.3 Relationships between Conjectures

In this section we briefly discuss relationships between conjectures and open problems in number theory about (or related to) prime numbers. The following list represents examples of such relationships:[626]

1. The *abc* conjecture implies the finiteness of solutions to Brocard's problem (see § 6.1.1).[627]
2. The *abc* conjecture implies the finiteness of solutions to the Fermat-Catalan conjecture (see § 6.1.1).[628]
3. Andrica's conjecture is relatively weak compared with stronger prime-gap conjectures (such as Cramer's and Oppermann's conjectures) although it is still stronger than other conjectures (like Legendre's conjecture).
4. Artin's conjecture on primitive roots was proved conditionally assuming the validity of the generalized Riemann hypothesis (see § 6.1.5 and § 6.1.29).
5. The Bateman-Horn conjecture is stronger than (and hence implies) Schinzel's hypothesis H (see § 6.1.6 and § 6.1.30).
6. Bunyakovsky's conjecture may be regarded as a special case of the Bateman-Horn conjecture (see § 6.1.11 and § 6.1.6).[629]
7. Bunyakovsky's conjecture is a special case (i.e. the $k = 1$ case) of Schinzel's hypothesis H (see § 6.1.11 and § 6.1.30).
8. Cramer's conjecture is stronger than (and hence implies) Legendre's conjecture (for large n). See § 6.1.12 and § 6.1.21.
9. Dickson's conjecture is a special case (i.e. the linear case) of the Bateman-Horn conjecture (see § 6.1.6 and § 6.1.13).
10. Dickson's conjecture is a special case (i.e. the linear case) of Schinzel's hypothesis H (see § 6.1.13 and § 6.1.30).
11. Dubner's conjecture is stronger than (and hence implies) Goldbach's conjecture for even integers greater than 4208 (see § 6.1.19).[630]
12. Dubner's conjecture implies the twin prime conjecture (see § 2.1.84).
13. Under the Elliott-Halberstam conjecture, it can be proven that there are infinitely many pairs of consecutive primes differing by at most 12 (see § 6.1.14).
14. Under the generalized Elliott-Halberstam conjecture, it can be proven that there are infinitely many pairs of consecutive primes differing by at most 6 (see § 6.1.14).[631]
15. Firoozbakht's conjecture is stronger than Cramer's conjecture (in terms of restricting the size of prime gaps). See § 6.1.12 and § 6.1.16.

---

[626] We note that some of these statements may be controversial (possibly because of different considerations and perspectives).

[627] Brocard's problem (which is different from Brocard's conjecture) asks for all integer solutions to the equation: $n! + 1 = m^2$, i.e. when adding 1 to a factorial results in a perfect square. The only known solutions (known as Brown numbers) are (4, 5), (5, 11), and (7, 71).

[628] Fermat-Catalan conjecture claims that there are only finitely many solutions to the equation $x^p + y^q = z^r$ using pairwise coprime positive integers (x, y, z), where the exponents satisfy the inequality $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$.

[629] I.e. the Bunyakovsky conjecture is essentially the qualitative single-polynomial version of the quantitative (broader and stronger) Bateman-Horn conjecture.

[630] Dubner's conjecture states that every even integer greater than 4208 can be expressed as the sum of two t-primes, i.e. primes that belong to a twin prime pair. Also see `https://oeis.org/A007534`.

[631] This guarantees that at least one of the twin, cousin, and sexy prime conjectures must be true.

16. Firoozbakht's conjecture is stronger than Shanks' conjecture (in terms of restricting the size of prime gaps). See § 6.1.16 and § 6.1.33.
17. The first Hardy-Littlewood conjecture is a quantitative upgrade (or refinement) to Dickson's conjecture (see § 6.1.13 and § 6.1.17).
18. The first Hardy-Littlewood conjecture implies that the second Hardy-Littlewood conjecture is false (see § 6.1.17 and § 6.1.32).
19. Kronecker's conjecture is weaker than Polignac's conjecture but stronger than Maillet's conjecture (see § 6.1.26).[632]
20. Oppermann's conjecture is stronger than (and hence implies) each of Andrica's, Brocard's and Legendre's conjectures (see § 6.1.4, § 6.1.10, § 6.1.21 and § 6.1.25).
21. Polignac's conjecture is a special case of the first Hardy-Littlewood conjecture (see § 6.1.17 and § 6.1.26).
22. Rassias' conjecture (with some reformulation) may be regarded as a special case of Dickson's conjecture (see § 6.1.13 and § 6.1.28). Consequently, it may also be regarded as a special case of Schinzel's hypothesis H (see § 6.1.30).
23. The bound on prime gaps derived from the Riemann hypothesis is weaker than the bound predicted by Cramer's conjecture (see § 6.1.12 and § 6.1.29).
24. Schinzel's hypothesis H implies the infinitude of Sophie Germain primes, and hence the infinitude of safe primes (see § 2.1.72, § 2.1.76 and § 6.1.30).
25. The infinitude of primes represented by suitable irreducible polynomials (such as $n^2 + 1$) follows conditionally from Schinzel's hypothesis H (see § 6.1.30).
26. Shanks' conjecture is stronger than Cramer's conjecture (see § 6.1.12 and § 6.1.33).
27. The conjecture that "there exists an even integer $N < 246$ such that there are infinitely many pairs of primes that differ by N" follows from the Polignac conjecture (see § 6.1.26; also see § 5.1.44).
28. The twin, cousin, and sexy prime conjectures (on infinitude) are special cases of Dickson's conjecture, corresponding respectively to the pairs of linear forms $(n, n+2)$, $(n, n+4)$, and $(n, n+6)$. The Bateman-Horn, first Hardy-Littlewood, Polignac, and Schinzel hypothesis H conjectures are like Dickson's in this regard, serving as generalized frameworks that imply these specific cases (with appropriate consideration of what and how "special case" means and applies in each case).
29. The conjecture that "there are infinitely many composite numbers of the form $2^p - 1$ where p is a prime" can be proved conditionally based on the first Hardy-Littlewood conjecture (see § 2.1.41 and § 6.1.17).
30. The conjectured infinitude of non-Wieferich primes is conditionally implied by the *abc* conjecture (see § 2.1.90 and § 6.1.1).
31. Summaries: the following are examples of summaries of relationships between conjectures (where $\Rightarrow$ means "implies", $>$ means "is stronger than", and $\supset$ means "is more general than"):[633]
    - Bateman-Horn $\supset$ Bunyakovsky.
    - Bateman-Horn $\supset$ Dickson.
    - Bateman-Horn $\Rightarrow$ First Hardy-Littlewood (and, more generally, the corresponding polynomial prime-value conjectures).
    - Bateman-Horn $\Rightarrow$ Schinzel H.
    - {Bateman-Horn, Dickson, First Hardy-Littlewood, Polignac, Schinzel H} $\Rightarrow$ {Twin, Cousin, Sexy}.[634]
    - Dubner $>$ Goldbach (for integers > 4208).
    - Dubner $\Rightarrow$ Twin.

[632] Kronecker's conjecture states: every even positive integer is the difference of infinitely many pairs of primes. Maillet's conjecture states: every even positive integer can be written as the difference between at least one pair of primes.

[633] As indicated earlier, there are many other examples of such summaries; moreover these examples generally provide broad and loose ideas. In fact, many other relationships can be derived from these relationships (and similar relationships) by combination. We should also note that some of these relationships may be disputed (based, potentially, on different considerations and perspectives).

[634] I.e. each of the conjectures on the left implies the infinitude of twin, cousin, and sexy primes on the right.

- Firoozbakht > Shanks > Cramer > Oppermann > Andrica > Legendre (regarding prime gaps).[635]
- First Hardy-Littlewood ⇒ Dickson ⇒ Polignac ⇒ {Twin, Cousin, Sexy}.
- GRH ⇒ RH.
- Oppermann ⇒ {Andrica, Brocard, Legendre}.
- Polignac > Kronecker > Maillet.
- Schinzel H ⊃ Bunyakovsky.
- Schinzel H ⊃ Dickson ⊃ {Twin, Cousin, Sexy}.
- Schinzel H ⇒ {Sophie Germain, Safe}.

6.4 Relationships between Theorems and Conjectures

In this section we briefly discuss relationships between theorems and conjectures about (or related to) prime numbers. The following list represents examples of such relationships:[636]

1. Bertrand's postulate provides a classical upper bound on the gaps between consecutive primes. Consequently, any conjecture proposing an upper bound for prime gaps must be compatible with the bound implied by Bertrand's postulate (see § 5.1.2).
2. The Bombieri-Vinogradov theorem may be regarded as an unconditional averaged substitute for the generalized Riemann hypothesis in certain applications concerning the distribution of primes in arithmetic progressions (see § 5.1.4 and § 6.1.29).
3. Brun's theorem establishes an upper bound on the density of twin primes, proving they are sparse enough to have a convergent reciprocal sum whether the twin prime conjecture is true or false (see § 2.1.84 and § 5.1.5).
4. The Brun-Titchmarsh theorem imposes a bound on the density of primes in arithmetic progressions, preventing the Elliott-Halberstam conjecture from extending to full level $\vartheta = 1$ (see § 5.1.6 and § 6.1.14).[637]
5. Catalan's *conjecture* can be proven assuming the *abc* conjecture (noting that Catalan's *conjecture* has already been proven unconditionally; see § 6.1.1).[638]
6. Dirichlet's theorem is a special case (specifically, the degree-1 case) of Bunyakovsky's conjecture (see § 5.1.11 and § 6.1.11).
7. Dirichlet's theorem is a special case (specifically, the $k = 1$ case) of Dickson's conjecture (see § 5.1.11 and § 6.1.13).
8. Dirichlet's theorem is a special case (specifically, the $k = 1$, degree-1 case) of Schinzel's hypothesis H (see § 5.1.11 and § 6.1.30).
9. The first Hardy-Littlewood conjecture is stronger than (and hence implies) the Green-Tao theorem (see § 5.1.17 and § 6.1.17).
10. Goldbach's conjecture is stronger than (and hence implies) Chen's theorem I (see § 5.1.8 and § 6.1.19).
11. Goldbach's conjecture is stronger than (and hence implies) Goldbach's ternary conjecture (see § 5.1.16 and § 6.1.19).
12. Legendre's conjecture is stronger than (and hence implies) Ingham's theorem (see § 6.1.21).[639]
13. Lemoine's conjecture is stronger than (and hence implies) Goldbach's ternary conjecture (see § 5.1.16

[635] We note that the strength of a prime gap conjecture is determined by how small an upper bound it places on the gap (i.e. $g_n = p_{n+1} - p_n$). Accordingly, a stronger conjecture provides a smaller bound than what a weaker conjecture provides.

[636] We note that some of these statements may be controversial (possibly because of different considerations and perspectives).

[637] The parameter ϑ represents the level of distribution of primes in arithmetic progressions (according to the formulation of Elliott-Halberstam conjecture).

[638] Catalan's conjecture (now known as Mihailescu's theorem) states that the only solution in integers $x, y, a, b > 1$ to the equation $x^a - y^b = 1$ is $3^2 - 2^3 = 1$.

[639] Ingham's theorem states that there is at least one prime between n^3 and $(n+1)^3$ for all sufficiently large n.

and § 6.1.23).

14. Riemann's hypothesis (if proved) would imply a stronger version of the prime number theorem (with a much tighter error term) than what is currently proved unconditionally (see § 5.1.31 and § 6.1.29).[640]
15. Distribution theorems for prime numbers in arithmetic progressions can be significantly strengthened conditionally under the assumption of the generalized Riemann hypothesis, yielding substantially sharper error bounds than those known unconditionally (see § 6.1.29).
16. For $h = 2$, the twin prime conjecture is stronger than (and hence implies) the corresponding case of Chen's theorem II (see § 2.1.84 and § 5.1.9). However, the scope of Chen's theorem II is considerably wider than that of the twin prime conjecture, as it applies to all positive (or non-zero) even shifts h, rather than only to the shift $h = 2$.[641]
17. The twin prime conjecture is stronger than (and hence implies) Zhang's theorem, including all the subsequent improvements introduced unconditionally and conditionally on its prime gap bound c (see § 2.1.84 and § 5.1.44).[642]
18. Zhang's theorem proves a weak existential form of Polignac's conjecture, demonstrating that there exists at least one even integer h below a fixed bounded threshold such that h occurs infinitely often as a gap between consecutive primes (see § 5.1.44 and § 6.1.26).
19. Summaries: the following are examples of summaries of relationships between theorems and conjectures (where $\Rightarrow$ means "implies", and $>$ means "is stronger than"):[643]
    - Bateman-Horn $\Rightarrow$ {Green-Tao, PNT}.
    - {Bateman-Horn, Bunyakovsky, Dickson, Elliott-Halberstam, Schinzel H} $\Rightarrow$ Dirichlet.
    - Elliott-Halberstam $>$ Bombieri-Vinogradov.
    - Elliott-Halberstam $\Rightarrow$ Zhang (including its improvements, and bounded gaps theorems in general).
    - First Hardy-Littlewood $\Rightarrow$ {Dirichlet, Green-Tao, PNT}.
    - Goldbach $\Rightarrow$ {Chen I, Vinogradov, Ternary Goldbach}.
    - GRH $\Rightarrow$ {PNTAP, Vinogradov}.
    - GRH $\Rightarrow$ Ternary Goldbach (for sufficiently large numbers).
    - GRH $\Rightarrow$ Siegel-Walfisz $\Rightarrow$ Dirichlet.
    - GRH $\Rightarrow$ Strong PNT $\Rightarrow$ PNT $\Rightarrow$ {Bertrand, Chebyshev}.
    - Legendre $\Rightarrow$ Ingham.
    - Lemoine $\Rightarrow$ Ternary Goldbach.
    - Polignac $\Rightarrow$ Zhang.
    - Twin $\Rightarrow$ Zhang.
    - {Twin, Cousin, Sexy} $\Rightarrow$ Chen II (for $h = 2, 4, 6$ respectively).

6.5 Falsified Conjectures

In this section we give some examples of historical conjectures about (or related to) prime numbers which were eventually falsified and proved to be wrong. The importance and usefulness of this topic are

[640] More specifically, the Riemann hypothesis, that all non-trivial zeros of $\zeta(s)$ lie on the critical line $\Re(s) = 1/2$, implies the prime number theorem with the explicit error estimate $\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x)$.

[641] In fact, this statement similarly applies to the cousin and sexy prime conjectures in their relation to the corresponding cases of Chen's theorem II.

[642] Again, this statement similarly applies to the cousin and sexy prime conjectures in their relation to the bounds established by Zhang's framework.

[643] "Implies" and "is stronger than" are broad and loose (and generally case-dependent). As indicated earlier, there are many other examples (noting that these examples generally provide broad and loose ideas). In fact, many other relationships can be derived from these relationships (as well as relationships from § 5.3 and § 6.3 and the like) by combination. We should also note that the indicated theorems are proved unconditionally (and hence the implications are purely theoretical with no practical consequences). We should also note that some of these relationships may be disputed (based, potentially, on different considerations and perspectives, noting as well the lax meaning of $\Rightarrow$ and $>$).

not restricted to historical awareness, but they also highlight the need for caution when formulating or accepting conjectures, even when they appear to be supported by strong indications and evidence, such as analytic or heuristic arguments or computational trends.[644]

1. Fermat primes conjecture: according to this conjecture, all numbers of the form

$$F_k = 2^{2^k} + 1 \qquad (k \in \mathbb{N}_0) \tag{107}$$

   which are nowadays known as Fermat numbers, are prime. A counterexample that falsifies this conjecture is $F_5 = 2^{2^5} + 1$ (see § 2.1.20). To date, no Fermat number F_k with $k \geq 5$ is known to be prime, despite extensive computational searches. This has led to the modern conjecture that there are only finitely many Fermat primes; in particular, it is conjectured that the five known Fermat primes are the only prime Fermat numbers.
2. Goldbach's other conjecture: according to this conjecture, every odd composite number can be written in the form $p+2k^2$ where p is a prime number and k is a non-zero integer. A counterexample that falsifies this conjecture is 5777, which is an odd composite number but cannot be written in this form.[645]
3. Golomb's conjecture on prime gaps: according to this conjecture, there is an increasing sequence $\{a_k\}$ of positive integers and a constant $B > 0$ with the property that $\{a_k + n\}$ contains no more than B prime numbers for every integer n. This conjecture was recently disproved using new results in the study of small gaps between primes, showing that no such uniformly bounded sequence exists.
4. Marin Mersenne's conjecture: according to this conjecture, the numbers of the form $M_n = 2^n - 1$ (where $\mathbb{N} \ni n \leq 257$) are prime only for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$.[646] However, this list includes $n = 67, 257$ (which do not produce primes) and excludes $n = 61, 89, 107$ (which do produce primes), and hence the conjecture was falsified.[647] Also see § 6.1.24.
5. Mertens' conjecture: this conjecture (which is highly significant because its truth would imply the Riemann hypothesis) is related indirectly to the distribution of primes through the Mobius function $\mu(n)$. The conjecture states that the sum of the Mobius function would always be bounded by $\pm\sqrt{n}$, that is:

$$|M(n)| < \sqrt{n} \qquad (\text{for all integers } n > 1) \tag{108}$$

   where $M(n)$ is Mertens' function defined as:

$$M(n) = \sum_{k=1}^{n} \mu(k) \tag{109}$$

   The conjecture was falsified by proving that counterexamples must exist at very large values of n, though no explicit counterexample has ever been individually identified.
6. Polya's conjecture:[648] this conjecture is about the parity of the number of prime factors of integers (counted with multiplicity). It predicts that for any integer $n > 1$, the number of integers up to n

[644] For example, the polynomial $n^2 + n + 41$ has a high density of prime values (see for instance `https://oeis.org/A056561` noting that it produces primes for all $0 \leq n \leq 39$). It is therefore tempting, after quick and limited computational tests, to conjecture that numbers of the form $n^2 + n + 41$ are prime for all $n \in \mathbb{N}_0$. However, a slightly more extensive computation disproves this conjecture as it fails immediately after 39 (e.g. $n = 40, 41, 44$ do not produce prime values).

[645] Also see `https://oeis.org/A060003` and `https://oeis.org/A046921`. We note that since 5777 and 5993 are the only known exceptions among odd composite numbers, Goldbach's other conjecture may be revived or modified to account for these specific exceptions. It is also worth noting that Goldbach's other conjecture in its original form (which includes prime numbers by allowing $k = 0$) has a link to Stern primes (see § 2.1.77) and their emergence. This is an issue that we plan to investigate in future volumes.

[646] See `https://oeis.org/A109461`.

[647] See `https://oeis.org/A000043`.

[648] This was not proposed originally as a definitive conjecture but rather as a claim whose truth implies the Riemann hypothesis (see § 6.1.29), and hence it is more appropriately referred to as the Polya problem.

with an odd number of prime factors is at least as large as the number with an even number. The conjecture seems intuitively true for small numbers, but it was found that this is untrue (where some counterexamples were found at sufficiently large n).

7. Skewes' conjecture:[649] this conjecture is about the belief (for over a century) that $\pi(x) < \mathrm{Li}(x)$ for all $x > 1$, where $\pi(x)$ is the prime-counting function and $\mathrm{Li}(x)$ is the logarithmic integral function (see § 8.2.1 and § 8.2.2). However, it was proved later that $\pi(x) - \mathrm{Li}(x)$ changes sign infinitely many times (a result known as Littlewood's theorem; see § 5.1.25 and § 5.1.31).
8. The stronger variant of the Feit-Thompson conjecture: see § 6.1.15.

6.6 Potential Open Problems and Conjectures

There are many potentially novel open problems and conjectures concerning primes (or related to primes) that, to the best of our knowledge, have not been explicitly formulated or discussed in the existing literature. Indeed, we have referred in several places in this book to examples of such potentially novel open problems and conjectures. The following remarks outline a collection of broad proposals and examples of such prime-related open problems, conjectures, and issues that may deserve further attention and discussion to clarify their situation from this perspective (as they, for instance, have received insufficient attention in the literature, or their status remains unclear or controversial):

1. There is no simple recurrence relation that generates an infinite sequence consisting entirely of distinct primes.

   The status of this statement is unclear because the term "simple" has no generally accepted mathematical definition in this context. Under some interpretations of "simple" and "recurrence relation", such sequences can be generated, whereas under more restrictive interpretations the question may become non-trivial. Thus, a prerequisite for treating this as a well-defined open problem is to specify precisely what constitutes a "simple recurrence relation". A potentially interesting problem is to formulate precise notion or notions of such simplicity under which the existence or nonexistence of such a recurrence relation can be investigated. Also see § 9.1.
2. Are there infinitely many prime numbers with a fixed digit sum $k \in \mathbb{N}$ (noting that this issue is base-dependent)? The literature seems inconsistent in this regard where different suggestions based on varying heuristic perspectives can be found:

   • For specific small fixed sums in large bases, there are only finitely many such primes.[650]

   • For any valid digit sum, there are typically infinitely many such primes, especially as the base becomes large.[651]

   Apparently, it was recently proved that the digit sum of primes is well-distributed in residue classes. However, this does not directly imply that for every base b and every fixed digit sum k there are infinitely many primes with digit sum k. The existence of infinitely many such primes for general k remains a delicate and largely open question. This issue is seemingly the subject of ongoing research and hence we should wait more upcoming results and breakthroughs to clarify the situation further. Also see Point 15 of § 6.2.4.
3. Is there an elementary non-tautological function that produces primes and composites alternately, e.g. $f(n)$ is prime and $f(n+1)$ is composites for all n even (or odd)?[652]
4. Is it possible to find or construct an exact mathematical formula that efficiently and practically generates all prime numbers (either sequentially or non-sequentially) without relying on prior data, tautological

[649] We label this as "Skewes' conjecture" for the purpose of identification even though Skewes is not the originator of this conjecture.

[650] A more conservative phrasing is that for fixed small digit sums, primes become extremely sparse, but finitude is not known in general.

[651] Even though this sounds heuristically reasonable, it may be too strong as a general statement.

[652] The main purpose of "non-tautological" is to exclude tricks and gimmicks like those indicated in § 5.2.14.

tricks, or vacuous gimmicks? The question may be strengthened by imposing additional conditions such as "generating *precisely* all prime numbers" (thereby excluding formulae that produce extraneous non-prime outputs or only partial subsets of the primes).

5. Are the digit frequencies of prime numbers in different numeral systems governed by the same or similar statistical distributions, or are these distributions wholly or partially dependent on the base? The question may be elaborated, for instance, by distinguishing between leading, internal, and terminating digits (where such issues could be investigated in future volumes).
6. Is there a numeral system in which all prime numbers (with at most finitely many exceptions) can be represented using only a proper subset of the set of digits in that system?

We also provide in the following points some observations and remarks about prime-related areas where open problems and conjectures can be easily found:

A. One of the richest areas of open problems and conjectures about primes is the issue of infinitude and finitude of certain types or categories of primes or related entities. In fact, one of the main categories of prime conjectures is about this issue. So, conjecture-seeking individuals can start with this area due to its richness and relative ease.[653] However, it should be noted that there are many "giant" conjectures in this area that make many such specific conjectures special cases or immediate consequences (and hence trivial).
B. Another rich area of open problems and conjectures about primes is the issue of existence and non-existence of certain types or categories of primes or related entities. What has been said about infinitude and finitude in the previous point partly applies to existence and non-existence.[654]
C. Another rich area of open problems and conjectures about primes, related to the previous two points, concerns the simultaneous satisfaction of multiple properties or membership in multiple classes. For example, one may ask whether there exist, or whether there are infinitely many, primes that simultaneously belong to two or more specified types or classes (e.g. primes that are both of type 1 and type 2, or simultaneously of types 1, 2, 3, etc.). Conversely, one may ask whether certain types or classes of primes are mutually exclusive, i.e. whether their defining properties can or cannot be satisfied simultaneously by the same prime. Similar questions of compatibility and exclusion can also arise for other prime-related mathematical entities and structures, including numbers and functions.
D. Another rich area of open problems and conjectures concerning prime numbers involves the issue of base dependency of various prime types and categories (including related entities) which are base-dependent. Investigations of such base-dependent properties and phenomena have often focused on the decimal system or on a relatively small number of specific numeral systems (usually low-value base systems such as binary, octal, and hexadecimal). This raises the possibility of exploring such questions systematically in other bases, including high-value bases (e.g. base 100). Such bases may reveal novel phenomena and patterns, or may give rise to new problems, technical obstacles, and hence conjectures that are less apparent in commonly studied low-value bases.
E. Recreational mathematics, particularly in number theory, can generate an enormous number of elementary prime-related open problems and conjectures with relatively little effort. Many of these questions may be mathematically interesting in a recreational or pedagogical sense without making a substantial contribution to mathematical knowledge. Consequently, one should distinguish between problems that might be valuable as recreational or educational mathematics and those that deserve significant investment as research problems.[655]

[653] Relative ease in proposing and formulating a conjecture does not imply ease in resolving it. In fact, conjectures on infinitude and finitude could be extremely difficult to resolve, as illustrated by some long-standing conjectures in this category, such as Landau's fourth problem and the twin prime conjecture.

[654] In fact, there is a close relationship between existence/non-existence and infinitude/finitude.

[655] It seems to me that large parts of recreational mathematics are trivial and pointless (in the sense that they do not serve serious research that improves our understanding and makes real progress in our knowledge). Some types of

F. We should finally note that proposing a conjecture, in itself, is a relatively easy task. However, for such a proposal to constitute a worthwhile contribution, it should be based on thorough investigation (for example, by identifying certain patterns, developing theoretical or heuristic arguments in its support, or conducting extensive computational verification). Without such supporting efforts, a conjecture may be of limited value and may not warrant further consideration or investigation. Accordingly, conjectures should ideally be proposed by researchers whose expertise and intuition in the relevant area enable them to formulate conjectures that are worthy of consideration and further investigation.

recreational mathematics may even be contrived, frivolous and silly. Consequently, I would question whether this aspect of mathematics should be actively encouraged within serious academic and research circles, particularly when doing so might divert valuable time and resources from research with greater potential for substantive mathematical progress. The mathematical community should therefore establish criteria to distinguish between worthy mathematical activities (or at least those of higher priority) and unworthy (or less important) activities. This is especially useful for novice and young mathematicians who lack sufficient knowledge to make such judgments.

Chapter 7
Tests and Sieves of Primes

Primality tests are tests (usually in the form of algorithms) used to identify if a given integer is prime or composite, while prime sieves are algorithms that find all primes up to a specified limit (or within a specified range) by systematically eliminating composite integers. In this chapter, we investigate primality tests (and occasionally compositeness tests) as well as sieves used to identify and enumerate prime numbers. We also devote a section of this chapter to integer factorization, which is closely related to both primality testing and sieving (see § 7.10).

7.1 Introductory Remarks

Before we go through the core investigation of primality testing and sieving, it is worth noting the following remarks:

1. While primality tests evaluate candidates in isolation, sieving operations exploit structural patterns over intervals to eliminate composites collectively. So, primality tests target structural properties of individual integers, while primality sieves target structural properties of ranges of integers (which are largely determined by divisibility patterns and regularities among composites rather than direct identification of primes or composites). In other words, primality tests exploit the mathematical properties of individual integers, whereas primality sieves exploit the structural distribution of numbers across an entire range of integers.
2. The difficulty and computational complexity of primality testing (and, in some cases, specialized sieving methods) is strongly dependent on the algebraic structure of the candidate integers under consideration. Certain prime families, such as Mersenne primes, admit very efficient specialized primality tests, making candidates in these families easier to identify and verify than arbitrary integers.
3. In general, the computational cost of primality testing (and integer factorization; see § 7.10) increases as the size of the integers under consideration grows, with complexity typically measured in terms of their bit-length. Prime sieving likewise requires increasing computational resources as the search bound or interval being sieved expands. The precise growth depends on the sieving algorithm and implementation, but sieve methods generally exploit systematic divisibility patterns to eliminate composites collectively rather than testing each integer independently, meaning that their resource scaling is largely governed by the size of the target interval and the deterministic divisibility structure being exploited.
4. The practical performance of a primality test often differs substantially from what its theoretical asymptotic complexity alone would suggest, due to factors such as implementation overheads, memory access requirements, and hardware constraints. Similar considerations apply to prime sieves, where memory access patterns, cache locality, and memory bandwidth can be particularly important. In general, a better asymptotic complexity does not necessarily imply better practical performance, especially for finite input sizes and particular hardware architectures.
5. Sieving algorithms excel at eliminating multiples of small primes across large ranges simultaneously, but traditional implementations become increasingly constrained by memory requirements as the search range grows. To handle larger intervals efficiently, modern sieving approaches employ techniques such as segmentation, deliberately balancing memory consumption against computational overhead and, where appropriate, choosing segment sizes that promote efficient use of the processor cache.

6. From a methodological perspective, the effectiveness of a primality sieve depends heavily on how efficiently it identifies and eliminates composite candidates. Ultimately, its overall utility depends not only on its elimination efficiency but also on its computational complexity and memory requirements.
7. From a computational perspective, sieving algorithms can benefit from processing the search space in contiguous segments. In segmented sieving, these segments may be sized to fit within the available cache memory, improving data locality and potentially reducing memory-access costs and overall processing time.
8. The memory consumed by primality sieves is often a more binding constraint than the required CPU time. In fact, the memory bottleneck of primality sieves is a classic computational constraint that often overshadows execution time.
9. The term "probable prime" (as opposed to terms like "proven prime" or "confirmed prime" or "certain prime" or "deterministic prime") is technically used to mean an integer that passes a specific primality test that all prime numbers pass but which most composite numbers fail to pass. In other words, it is an integer that meets a necessary, but not sufficient, primality condition.[656]
10. In many practical applications, the distinction between a probable prime and a proven prime is negligible, given the high confidence provided by well-designed probabilistic primality tests. However, establishing a rigorous proof of primality can entail substantially greater computational cost and practical effort than what is required by probabilistic testing. So, while the practical gap between a probable prime and a proven prime is narrow in many applications and contexts, it can be almost unbridgeable in others.
11. In large-scale applications, primality testing relies almost exclusively on probabilistic methods rather than deterministic algorithms due to severe computational constraints. Although general deterministic testing is theoretically tractable, it remains practically infeasible for large arbitrary inputs (hence leaving deterministic approaches viable primarily for numbers of specific mathematical forms and particular properties that facilitate special deterministic tests).
12. Primality testing and integer factorization are distinct computational problems, although they are closely related. For large integers, particularly those formed as products of large primes, determining whether an integer is prime is generally much more computationally efficient than finding its prime factorization. A test that establishes that an integer is composite does not, by itself, identify its prime factors or make factorization straightforward. Consequently, although primality can often be established efficiently, factoring certain large composite integers can remain computationally infeasible with currently known classical algorithms.
13. According to the prime number theorem (see § 5.1.31), primes become less frequent among larger integers, with their density near x being approximately $1/\ln x$. Consequently, a search that tests successive integers for primality will, on average, need to examine more candidates to find a prime as the search moves to larger numbers. This increasing scarcity can contribute to the computational cost of prime discovery, although the overall cost also depends on the search strategy and the efficiency of the primality testing algorithm.
14. Referring to the previous points, the computational cost of searching for large primes typically increases for two main reasons: primality testing generally becomes more expensive as candidate integers grow in size, and primes become less frequent among larger integers. Together, these factors typically increase the expected cost of prime discovery, although the magnitude of the increase depends on the search strategy and the primality testing algorithm employed.
15. In general, record-breaking primes are not found by testing random integers uniformly, but by searching within special algebraic families where efficient primality tests and other computational advantages are

[656] As indicated previously (see § 1.3), primality is an absolute, intrinsic and deterministic property, and hence it is independent, for instance, of base and any other casual contexts and extrinsic attributes let alone our state of knowledge.

available. This largely explains why most known record primes are of Mersenne type (and a few other specially-structured types).

16. Strictly speaking, the definition of a particular prime type (which includes a characteristic property of that type) cannot be considered as a test (or a basis for a test) for that prime type because it usually assumes primality already, and hence the characteristic property is just to identify the type not if the given number is a prime of that type (see for instance the definition of balanced, Bell and Carol primes in § 2.1.1, § 2.1.2 and § 2.1.3). This is unlike, for instance, Lucas-Lehmer test (see § 7.3.10) which determines in one go if an integer (which is unknown to be prime) is a Mersenne prime or not. In fact, even if such a presumption of primality is not implied by the definition, the concept of "test" does not fit well with such definition-based characteristics (and related procedures). However, we may tolerate such use of "definition-based tests" especially for tests for specific prime types (see § 7.3.20).
17. The management of pseudoprimes (see § 9.7) is central to primality testing. Consequently, efficient and reliable methods for filtering out these composites substantially improve the performance of probabilistic primality tests by reducing false positives and computational overheads.
18. Many modern prime sieves differ more in engineering optimizations than in underlying mathematical principles. As for primality tests, the situation is more complicated (although this definitely applies in some cases and instances). Further details will be provided in subsequent volumes.
19. Finally, we note that the terminology used in the literature on primality testing and sieving is not entirely consistent. For example, a given test or sieve may be known by several names, while a single name may be used for multiple versions or variants. Some names may also be derived from associated theorems or researchers, or may be introduced informally or used provisionally.[657] Readers should therefore exercise care when consulting the literature on primality testing and sieving, paying particular attention to the definitions, specifications, and references associated with each named method.

7.2 Simple Tests

Simple tests are basic signs and instantaneous checks used to show that a given integer is composite. These tests are so simple and trivial that they do not require significant time or effort or computational capabilities to perform. Some of these tests may not even qualify as "tests" because they are no more than simple observations. In general, these may be considered as preliminary "primality tests" in the sense of representing necessary but not sufficient conditions for primality (i.e. a number failing these tests is definitely composite). We outline in the following points examples of such quick tests (or signs or rules or ... etc.):[658]

1. Any integer greater than 5 whose last digit is 0, 2, 4, 5, 6, or 8 is composite (i.e. prime numbers greater than 5 must end in 1, 3, 7, or 9).
2. Simple divisibility rules can be used as quick tests for compositeness. For example, the number 1308981471 is obviously composite because the sum of its digits is divisible by 3. Similarly, the number 10389517574843 can be immediately seen to be composite because it is divisible by 11 (according to the alternating sum rule for divisibility by 11).
3. Simple modularity rules can be used as quick tests for compositeness. For example, if we divide an integer greater than 3 by 6 and get a remainder of 0, 2, 3, or 4, it is definitely composite (because all primes greater than 3 are of the form $6k \pm 1$ where $k \in \mathbb{N}$; see § 5.1.34).[659]

[657] These issues are not unique to primality testing and sieving; similar terminological inconsistencies occur throughout mathematics, including number theory and computational mathematics, as well as in science more generally. The degree of inconsistency varies across topics, and some areas may exhibit greater ambiguity than others.

[658] In fact, some items in this list (especially among those in the end) may not be trivial (as stated) but they can be so in certain circumstances and contexts. Also, some items may not be practically useful as primality tests but they are included for potential benefit in some cases. We note that we assume decimal notation unless stated otherwise.

[659] More elaborate modularity rules may also be used, e.g. $p \overset{30}{=} 1, 7, 11, 13, 17, 19, 23$, or 29 (for any prime $p > 5$).

4. No two consecutive integers (except 2 and 3) can be both prime. So, if we know (or assume) that $m > 3$ is prime then $m - 1$ and $m + 1$ must be composite.
5. All even integers greater than 2 are composite (noting that this is included already).
6. All factorials ($n!$ for $n \geq 3$) and primorials ($p_n\#$ for $n \geq 2$, and $n\#$ for $n \geq 3$) are composite.
7. All repunit numbers (in any base $b \geq 2$) with a composite number of digits are composite.
8. All repunit numbers in odd perfect square bases (e.g. base 9) are composite.
9. All multi-digit non-repunit repdigits (or monodigits) are composite.
10. All perfect numbers are composite.[660]
11. All abundant numbers (including weird numbers) are composite.[661]
12. All triangular numbers greater than 3 are composite.[662]
13. All integers of the form $2^n + 1$ with n not a power of 2 are composite (see § 2.1.20).
14. All integers of the form $2^n - 1$ with composite n are composite (see § 2.1.41).
15. All Catalan numbers greater than 5 are composite.
16. All Fibonacci numbers greater than 3 with composite index are composite.
17. All Jacobsthal numbers greater than 5 with composite index are composite.
18. All Pell numbers greater than 1 with composite index are composite.
19. All decimal palindromic numbers greater than 11 with even number of digits are composite.
20. All integers greater than 5 which the decimal representation of their reciprocals is terminating are composite.
21. All binomial coefficients greater than 1 (excluding those of the form $C_1^p = C_{p-1}^p$ where p is prime) are composite.
22. All centered 8-gonal and 9-gonal numbers greater than 1 are composite.
23. All strict pandigital integers in base 10 are composite.[663]
24. All $n! + 1$ are composite when $n + 1$ is prime ($n \geq 3$).
25. Any Cullen number whose index n (> 1) is of the form $6k + 1$ or $6k + 2$ is composite.
26. Any Lucas number L_n ($n > 1$) whose index n is neither a power of 2 nor a prime is composite.
27. Any Woodall number whose index n is of the form $6k + 4$ or $6k + 5$ is composite.
28. Any integer n whose square divides the central binomial coefficient C_n^{2n} is not prime.
29. Any integer $n > 5$ for which the period of $1/n$ in base 10 is not a divisor of $n - 1$ is composite.
30. Any integer $n > 1$ that does not divide the n^{th} Perrin number P_n is composite.
31. Any integer $n > 1$ that divides $(n - 1)!$ is composite.[664]
32. Many algebraic forms are necessarily composite because they are (non-trivially) factorable, e.g. $n^2 \pm n$ and $a^n \pm b^n$ (with proper conditions on the variables; see for example § 5.2.3 and § 5.2.7).[665]
33. We may even include simple primality tests (like Fermat and Wilson tests which are based on Fermat and Wilson theorems; see § 5.1.15, 5.1.43, 7.3.6, and 7.3.19) in some simple cases where the test can be trivially done.
34. Also see § 7.3.20 for some simple type-specific primality tests (or signs).

[660] A perfect number is a positive integer that is equal to the sum of its proper divisors.

[661] An abundant number is a positive integer that is smaller than the sum of its proper divisors. Weird number is an abundant number that cannot be expressed as a sum of any subset of its proper divisors.

[662] Triangular numbers are integers of the form $(n^2 + n)/2$ where $n \in \mathbb{N}$.

[663] Strict pandigital integer in base 10 is an integer that uses each digit from 0 to 9 exactly once.

[664] The converse is also true for $n > 4$.

[665] As a specific example: for all $a > 2$ and $n > 1$ (where $a, n \in \mathbb{N}$) the expression $a^n - 1$ is always composite. Similarly: for all $m, n \in \mathbb{N}$, $(2m)^{2n+1} + 1$ is composite. We should also consider forms like $n! + k$ (for $2 \leq k \leq n$) and $p_n\# + k$ (for $2 \leq k \leq p_n$).

7.3 Primality Tests

A primality test is a process for determining whether a given natural number is prime or composite. There are many tests (or algorithms) designed for this purpose, each with varying levels of generality (i.e. by being applicable to all primes or being limited to certain types of primes), complexity and efficiency. In fact, their variations are not limited to these characteristics and attributes but they extend to many other characteristics and attributes. For example, they differ in being deterministic or probabilistic (where the probabilistic methods also vary in the degree of certainty or confidence in their results). Similarly, they may vary in being conditional (whose outcome depends on unproven assumptions or results) or unconditional. The algorithms of these tests also vary in their asymptotic computational complexity (e.g. some run in polynomial time while others run in exponential time).

In fact, the variations extend even to the variants and flavors of the individual methods and algorithms where some of these methods and algorithms represent categories and classes rather than being single and specific ones (although they are labeled with identical or similar labels). In short, the topic of primality tests is vast and diverse from many aspects and perspectives. The interested readers should refer to the extensive literature of this subject, although we will touch on some of these issues in this volume (see for instance § 7.5) and provide more details in subsequent volumes.

In the following subsections, we outline some of the most notable primality tests, which range from relatively-basic ones to advanced ones (where we order them alphabetically). In fact, there are many other tests although most of these tests are either integrated or embedded within more advanced (or general or robust) tests or they are of limited validity and applicability (e.g. by being specific to certain types of numbers or they require certain assumptions and conditions).

7.3.1 AKS Test

The AKS test (where AKS stands for Agrawal-Kayal-Saxena) is distinguished by being general, deterministic, unconditionally correct[666] and polynomial-time at the same time, and hence it has an exceptional theoretical importance although its practical usefulness is rather limited. The basic idea of the test is that: n is prime *iff* the following congruence relation is identically true:

$$(X + a)^n \equiv X^n + a \pmod{X^r - 1, n} \tag{110}$$

where $a \in \mathbb{Z}$, $n \in \mathbb{N}$, r is an integer used to bound the degree of the polynomials during the test, and X is the indeterminate of polynomial ring.[667] The remaining technicalities of this test are mostly about reducing the complexity (and hence the time) of the computations required to verify this relation and benefit from this basic idea.

It is worth noting that the emergence of this algorithm resolved a historical open problem (and conjecture) about deterministic polynomial-time primality testing without the assumption of generalized Riemann hypothesis. Before this breakthrough, determining whether a number was prime in polynomial time required choosing between a randomized guess or assuming unproven complex analysis hypotheses. Also see § 6.1.3.

7.3.2 APR Test

Historically, the APR test (where APR stands for Adleman-Pomerance-Rumely) was the first deterministic general-purpose primality test that could efficiently handle massive numbers without relying on unproven

[666] "Unconditionally correct" means its correctness does not depend on unproven assumptions or conjectures (unlike some other primality tests whose correctness depends on unproven results like the generalized Riemann hypothesis).

[667] A polynomial $f(X)$ belongs to the ring $R[X]$ if the coefficients of $f(X)$ belong to R (where X is the indeterminate of the ring R).

hypotheses (such as the generalized Riemann hypothesis which, for instance, the deterministic Miller test requires; see § 7.3.12). Another important feature of the test is that it does not require prior knowledge of the factors of $n \pm 1$ (unlike for example the Lucas and Morrison tests; see § 7.3.9 and § 7.3.13), while running in quasi-polynomial time (or almost so).

The theoretical foundation of this test uses the arithmetic of cyclotomic fields and Jacobi sums (which make it possible to prove primality by verifying certain congruences in suitable cyclotomic rings). Broadly speaking, the foundational theorem of this test asserts that if certain algebraic congruences hold in carefully chosen cyclotomic structures, then the tested integer must be prime. Subsequent research led to refined variants of the algorithm, most notably the APR-CL test, which improved its practical performance and computational efficiency.

7.3.3 Baillie-PSW Test

This is a combined primality test in the sense that it combines two strong probabilistic primality tests: a Miller-Rabin test to base 2, and a Lucas sequence test. The key idea of the Baillie-PSW test is that the sets of numbers that can fool each test are extremely unlikely (and potentially impossible) to overlap, and hence combining these two tests gives very strong practical reliability (even though it is theoretically unproven). So, the Baillie-PSW test is probabilistic in nature although it is practically deterministic (at least up to very large numbers) thanks to its reliance on two consecutive strong tests and hence the result is almost certain.[668] The test is commended for being fast and efficient (as well as being effectively deterministic).

Formally (but broadly and briefly) speaking, the Baillie-PSW test declares that an odd integer $n > 1$ is a probable prime *iff* the following conditions are satisfied simultaneously:

- n is not a perfect power.
- n passes a base-2 strong probable prime Miller-Rabin test.
- Choosing the first integer $D \in \{5, -7, 9, -11, 13, -15, \ldots\}$ such that the Jacobi symbol $\left(\frac{D}{n}\right) = -1$, and setting the Lucas sequence parameters $P = 1$ and $Q = \frac{1-D}{4}$, n passes the corresponding strong Lucas probable prime test.

If any of these conditions fails, the test definitively declares n as composite. Also see Point 1 of § 7.9.5.

7.3.4 Division Test

This test (commonly known as the trial division test) checks whether an integer $n > 1$ has any divisor between 2 and $\sqrt{n}$. If n is divisible by any integer in this range then n is composite; otherwise it is prime. The key mathematical fact behind the test is: if n is composite then $n = ab$ for some integers $a, b > 1$ where one of the factors a and b is less than or equal to $\sqrt{n}$.

Since every even integer greater than 2 is composite, after checking divisibility by 2 (which is trivial), the test only needs to examine odd divisors up to and including $\sqrt{n}$. This reduces the number of divisibility checks by about half. In fact, this test can be optimized further by exploiting (for instance) the $6k \pm 1$ rule (see Point 3 of § 7.2), which reduces the search space even more than just eliminating even integers.

The trial division is the simplest and most direct primality test. It is practical for relatively small numbers but becomes inefficient (and possibly practically impossible) for large numbers because its running time grows on the order of $\sqrt{n}$. Consequently, it is not suitable for testing very large integers. This test is obviously deterministic. Also see § 7.10.12.

[668] In fact, it is probabilistic within our current knowledge (noting that no counterexample to the Baillie-PSW test is currently known).

7.3.5 Elliptic Curve Primality Proving

This (commonly abbreviated as ECPP) may be described as a category of primality testing methods and algorithms (rather than being a single and entirely-specific method). It is widely used in primality testing and may be praised for its generality, efficiency and practicality (as well as being deterministic and hence conclusive) and therefore it is widely used in number theory and cryptography. The basic idea of ECPP is that for a prime p the number of points on an elliptic curve[669] modulo p is close to $p+1$ and it follows certain distribution patterns which can be exploited to determine the primality (or otherwise) of integers (mainly very large integers).

Formally speaking, the ECPP can be outlined as follows: suppose

- $N > 1$ is an integer such that $\gcd(N, 6) = 1$.
- E is an elliptic curve over the ring $\mathbb{Z}/N\mathbb{Z}$ defined by the congruence relation: $y^2 \equiv x^3 + Ax + B \pmod N$ where $A, B \in \mathbb{Z}/N\mathbb{Z}$ and $\gcd(\Delta, N) = 1$ where $\Delta = 4A^3 + 27B^2$ is the discriminant.
- There is an integer m and a prime q dividing m such that $q > \left(\sqrt[4]{N} + 1\right)^2$.
- There is a point P on E such that $mP = \mathcal{O}$ (where $\mathcal{O}$ represents the neutral element on E).
- The point $(m/q)P$ is well-defined in projective coordinates and its z-coordinate satisfies $\gcd(z_q, N) = 1$.

If all these conditions are met then N is prime.

7.3.6 Fermat Test

This test is based on Fermat's little theorem which states: if $p \nmid a$ (where p is prime) then $a^{p-1} \overset{p}{=} 1$ (see § 5.1.15). So by contraposition, if $a^{n-1} \overset{n}{\neq} 1$ (where n is a suspected prime and $n \nmid a$) then n is *definitely* composite (otherwise, n is a probable prime to base a). In this sense, the test is deterministic for compositeness (i.e. when the test fails as indicated already) but probabilistic for primality. Passing the test for additional bases may increase confidence in primality, but does not prove primality, since Carmichael numbers pass the test for every base coprime to n (see for instance § 5.1.15, § 7.9.2 and § 9.7.1). This means that this test can be categorically fooled by Carmichael numbers, and hence it remains a probabilistic primality test regardless of the number of bases used (unlike some other tests). We note that the Fermat test is generally considered to be the simplest probabilistic primality test (or at least one of the simplest).

The Fermat test (as underlined by Fermat's little theorem) is a basis for many other tests in the sense that these tests are elaborations of the Fermat test or they employ it in some form within their testing mechanism. For example, Miller-Rabin and Solovay-Strassen tests (see § 7.3.12 and § 7.3.18) can be viewed as strengthened versions of the Fermat test that impose additional conditions to detect pseudoprimes, while Lucas and Pepin tests (see § 7.3.9 and § 7.3.15) are based on different primality criteria but are closely related in spirit and they are often used alongside Fermat-type methods. In fact, Fermat-type probabilistic tests are frequently combined with complementary Lucas-type tests to create highly reliable hybrid verification systems (see for instance § 7.3.3). So, the Fermat test as stated above may be rarely used directly, but it is widely used within other tests and primality testing mechanisms. Overall, the Fermat test is one of the most important primality tests despite its limitations. Also see § 9.7.6.

7.3.7 Fibonacci Test

Fibonacci primality test is a method used to determine if an integer is prime by exploiting the properties of the Fibonacci sequence (see the Note in § 2.1.21). Although there is no single Fibonacci test, the term typically refers to checking a number against specific congruence relations and properties that all prime

[669] "The number of points on an elliptic curve" means the total count of (x, y) points that satisfies the equation of the curve.

numbers must satisfy. The most common Fibonacci test seems to be based on the theorem that states: if n is a prime number ($\neq 2, 5$) then it must satisfy $n|\mathcal{F}_{n-\left(\frac{5}{n}\right)}$ where $\mathcal{F}_k$ is the k^{th} Fibonacci number and $\left(\frac{5}{n}\right)$ is the Jacobi (or Legendre) symbol.[670] Like the Fermat primality test (see § 7.3.6), the Fibonacci test is probabilistic, and hence a number that fails this test is definitely composite, but if it passes, it is a probable prime. Also see § 9.7.7.

The Fibonacci test is embedded (in some shape or form) in several other primality tests, and serves as the inspiration or motivation for some other tests. A prominent example is the Pell test (see § 7.3.14) which mimics the Fibonacci test. Another example is the Lucas probabilistic primality test and its variants (see § 7.3.9) which use recurrence sequences closely related in spirit to the Fibonacci sequence. Similar statements can be made about other sequence-based primality tests (such as the Frobenius test; see § 7.3.8). More sophisticated algorithms, such as the Baillie-PSW primality test (see § 7.3.3), combine a base-2 strong probable prime test with a Lucas sequence test, thereby incorporating ideas that originate from the Fibonacci (and Lucas) sequence properties. While these methods are distinct tests with different conditions and guarantees, they are fundamentally unified by their use of recurrence relations, modular arithmetic, and the properties of sequences modulo an integer. Overall, the Fibonacci primality test is closely linked to a broader class of sequence-based primality criteria and probabilistic tests.

7.3.8 Frobenius Test

The Frobenius test (which most commonly refers to the quadratic Frobenius test or QFT) is a highly efficient probabilistic primality test that is used to determine if an integer is a probable prime or composite. It expands on simpler tests (like the Fermat and Lucas tests; see § 7.3.6 and § 7.3.9) by utilizing the algebraic properties of the Frobenius automorphism over quadratic fields. This test has a significantly lower probability of error than most other similar tests and hence it is highly reliable. For example, it is considered more powerful than the Miller-Rabin test (see § 7.3.12) for identifying composite numbers. Also see Point 5 of § 7.9.5, and § 9.7.8.

Broadly speaking, the test selects parameters to build a specific quadratic polynomial extension ring modulo n, and then verifies whether the algebraic elements obey specific identities that are strictly true for all prime numbers. The following is an outline of the algorithm of one variant of this test: let $n > 1$ be an odd integer, $b, c \in \mathbb{Z}$, the Jacobi symbol $\left(\frac{-c}{n}\right) = 1$, the Jacobi symbol $\left(\frac{b^2+4c}{n}\right) = -1$, B is a large positive integer (say 50000), then:

• If n is divisible by a prime less than or equal to $\min\{B, \sqrt{n}\}$, or n is a perfect square, then n is composite (and hence exit).

• Calculate $x^{(n+1)/2}$ modulo $(n, x^2 - bx - c)$. If $x^{(n+1)/2} \notin \mathbb{Z}/n\mathbb{Z}$, then n is composite (and hence exit).

• Calculate x^{n+1} modulo $(n, x^2 - bx - c)$. If $x^{n+1} \not\equiv -c$, then n is composite (and hence exit).

• Let $n^2 - 1 = 2^r s$ where s is odd. If $x^s \not\equiv 1$ modulo $(n, x^2 - bx - c)$ and $x^{2^j s} \not\equiv -1$ modulo $(n, x^2 - bx - c)$ for all $0 \leq j \leq (r - 2)$, then n is composite (and hence exit).

If n is not found composite (in the previous steps) then n is a probable prime. Repeating the test with distinct, appropriately selected parameters can reduce the probability that a composite integer passes, subject to the error bounds established for the specific variant.

7.3.9 Lucas Test

The Lucas test is a deterministic primality testing algorithm.[671] Unlike probabilistic tests (such as Frobenius and Miller-Rabin tests; see § 7.3.8 and § 7.3.12), it provides a rigorous and definitive proof for

[670] It is worth noting that the divisibility requirement $n|\mathcal{F}_{n-\left(\frac{5}{n}\right)}$ may be called the *Lucas-Fibonacci condition.*

[671] We note that "Lucas test" may refer to other tests (created by Lucas or attributed to him).

primality by verifying a stronger condition related to Fermat's little theorem (see § 5.1.15).[672] However, it requires knowing the complete prime factorization of $n-1$ (which can make the test computationally demanding).[673] This test is based on the following theorem (i.e. Lucas primality test theorem): a natural number $n > 1$ is prime *iff* there exists an integer a $(1 < a < n)$ where $a^{n-1} \overset{n}{=} 1$ and for every prime factor p of $n-1$ we have $a^{(n-1)/p} \overset{n}{\neq} 1$.

It is worth noting that there is another "Lucas test", i.e. the *strong Lucas test* which is an advanced and rigorous "variant" of the standard Lucas test. It is a probabilistic test acting as a powerful mathematical tool for identifying composite numbers, i.e. if an odd integer fails the strict modular sequence conditions of this test then it is definitely composite, but an integer that passes the test is a probable prime. The strong Lucas test may be described as the algebraic counterpart to the Miller-Rabin (strong Fermat) test (by virtually substituting standard exponentiation with Lucas sequences).

7.3.10 Lucas-Lehmer Test

This test is specific to Mersenne primes, determining whether a given Mersenne number $M_p = 2^p - 1$ is prime or not (see § 2.1.41). It is fast, simple and deterministic, making it the standard method for finding and testing large Mersenne primes. Unlike general-purpose primality tests which must work with arbitrary integers, the Lucas-Lehmer test exploits the special structure of Mersenne numbers and requires only repeated squaring, subtraction, and modular reduction (as will be seen). So, while these general-purpose tests take considerable time and resources on testing massive numbers (due to their general nature and reliance on sophisticated operations), the Lucas-Lehmer test relies entirely on fast and simple operations (as stated), which makes it extremely fast and efficient.

Moreover, in modern computing architectures, arithmetic modulo $2^p - 1$ can be implemented very efficiently in binary (since multiples of 2^p can be folded back into lower-order bits using simple and fast addition operations, rather than expensive and slow division algorithms), and this ensures extra speed and efficiency. As a result, Mersenne numbers can be tested for primality far more quickly and efficiently than most other numbers of comparable size thanks to the Lucas-Lehmer test. These computational advantages are the primary reason that the largest known prime numbers discovered to date have all been Mersenne primes.

Formally speaking, the Lucas-Lehmer test starts by defining the following recurrence sequence:

$$S_{i+1} \equiv S_i^2 - 2 \pmod{M_p} \tag{111}$$

where $i = 0, 1, \ldots, p-3$ with $S_0 = 4$. The suspected Mersenne prime ($M_p = 2^p - 1$ where p is an odd prime) is then prime *iff*

$$S_{p-2} \equiv 0 \pmod{M_p} \tag{112}$$

7.3.11 Lucas-Lehmer-Riesel Test

This is a fast deterministic primality test specifically designed for numbers of the form $N = 2^n k - 1$ with odd $k < 2^n$ (see § 2.1.71). In fact, this test generalizes the Lucas-Lehmer test for Mersenne primes (see § 7.3.10) noting that numbers of this form are a generalization of Mersenne numbers. Hence, this test (like the Lucas-Lehmer test) enjoys certain computational advantages over general-purpose primality tests for

[672] We note that the Lucas primality test may be considered as a more complex version of the Fermat primality test (see § 7.3.6). In fact, in a broad mathematical sense the Lucas primality test may be viewed as a practical converse to Fermat's little theorem since it provides a sufficient condition for primality based on modular exponentiation and multiplicative order properties.

[673] In general, primality tests that rely on the (complete or partial) factorization of $n-1$ or $n+1$ are limited by this requirement, which restricts their applicability.

the numbers of that form, making it the fastest (or at least one of the fastest) deterministic test known for those numbers.

The Lucas-Lehmer-Riesel algorithm generates a finite sequence where each term is calculated from the previous one using a recurrence relation. The test is concluded with the final term of the sequence which determines if the tested number is prime or not. The algorithm can be outlined as follows: choose an appropriate starting value u_0 for the sequence, then generate the sequence as follows:

$$u_{i+1} \equiv u_i^2 - 2 \pmod{N} \tag{113}$$

where $0 \leq i \leq n-3$. The number N is then prime *iff* $u_{n-2} \equiv 0 \pmod{N}$. As for the starting value u_0, its determination represents the main challenge in this algorithm. The following are rules (or examples) for determining u_0 in some cases:

- For $k = 1$ and odd n: select $u_0 = 4$ (i.e. Mersenne prime test by Lucas-Lehmer algorithm; see § 7.3.10).
- For $k = 3$ and $n \overset{4}{=} 0$ or $n \overset{4}{=} 3$: select $u_0 = 5778$.
- For $k \overset{6}{=} 1$ or $k \overset{6}{=} 5$: select $u_0 \equiv (2+\sqrt{3})^k + (2-\sqrt{3})^k \pmod{N}$.

We should finally note that the Lucas-Lehmer-Riesel test (including the special case of the Lucas-Lehmer test) has a main disadvantage of being specific to a certain type of integers (i.e. those of the form $2^n k - 1$ with odd $k < 2^n$), unlike the general-purpose primality tests which are valid (at least in principle) for all types of integers.

7.3.12 Miller-Rabin Test

This test is based on the properties of modular arithmetic (where Fermat's little theorem is exploited in the process). The test is probabilistic where the probability of error can be arbitrarily minimized by repeating the test with different bases (noting that the test is fast and hence high confidence in the result can be obtained with speed and efficiency).

The objective of this test is to determine if an odd integer $n > 3$ is composite or probable prime. The test can be outlined as follows:

- Express $n-1$ as $2^s d$ (i.e. $n - 1 = 2^s d$) where $s \geq 1$ and d is odd.
- For a chosen base $a \in \{2, \ldots, n-2\}$, n passes the test if either:
  $a^d \overset{n}{=} 1$ or
  $a^{2^r d} \overset{n}{=} -1$ for some $r = 0, \ldots, s-1$.

If n violates both conditions then n is definitively composite, while if n satisfies either condition then n is a strong probable prime to base a. Also see Point 3 of § 7.9.5, and § 9.7.12.

In this context we should refer to the deterministic Miller test under the generalized Riemann hypothesis which is a conditional version of the Miller-Rabin test (although Miller test historically precedes Miller-Rabin test). In essence, the test translates the probabilistic Miller-Rabin algorithm into a conditional, rigorous and deterministic framework by setting a strict upper bound on the search space for a mathematical witness of compositeness.

7.3.13 Morrison Test

This test is a deterministic algorithm that proves a natural number n is prime by exploiting the factorization of $n+1$ (when much of this factorization is known or can be easily obtained), and hence it is unlike some other tests that use the factorization of $n-1$ (see for instance § 7.3.9 and § 7.3.16). The theorem behind this test states (noting that F is the fully factored part of $n+1$, while R is the remaining part, i.e. $n + 1 = F \cdot R$):

- if we can find a Lucas sequence L_k with a discriminant $D = P^2 - 4Q$ such that the Jacobi symbol

$\left(\frac{D}{n}\right) = -1$, and
• if the sequence satisfies $L_{n+1} \stackrel{n}{=} 0$ while observing $\gcd(L_{(n+1)/q}, n) = 1$ for all prime factors q of F,
then every prime divisor p of n must satisfy $p \stackrel{F}{=} \pm 1$. Accordingly, if F exceeds $\sqrt{n} + 1$, the symmetry of the conditions forces n to be prime.

This approach is mathematically significant because it generalizes the Lucas-Lehmer test (see § 7.3.10) which is specific to Mersenne numbers, providing a robust theoretical background for certifying primality when $n + 1$ can be easily factorized.

7.3.14 Pell Test

This primality test is similar to the Fibonacci test (see § 7.3.7) as it replaces the Fibonacci sequence with the Pell sequence (see the Note in § 2.1.57). According to this test, if n is an odd prime then it must satisfy $n | \mathcal{P}_{n-\left(\frac{2}{n}\right)}$ where $\mathcal{P}_k$ is the k^{th} Pell number and $\left(\frac{2}{n}\right)$ is the Jacobi (or Legendre) symbol. This is a probabilistic primality test (in the sense of providing a necessary but not sufficient condition for primality), and hence a number that fails this test is definitely composite, but if it passes it is a probable prime. Composites that pass this test are "Pell pseudoprimes" (see § 9.7).

7.3.15 Pepin Test

This test is specific to Fermat primes, i.e. whether a Fermat number is prime or not (see § 2.1.20). The test is based on the following theorem (i.e. Pepin's primality test theorem): the k^{th} Fermat number $F_k = 2^{2^k} + 1$ is prime *iff*:

$$3^{(F_k-1)/2} \equiv -1 \pmod{F_k} \tag{114}$$

where $k \geq 1$. This test is obviously simple and deterministic, but its applicability is limited because Fermat numbers increase extremely rapidly, making modular exponentiation modulo F_k computationally expensive for large k (so that only few of these numbers can be tested by this method in reasonable time).

7.3.16 Pocklington Test

This test (which may also be called Pocklington-Lehmer test) is based on partial factorization of $n - 1$ (where n is the suspected prime to be tested). It is deterministic, unconditionally correct and general although it is mostly used with certain types of numbers and with favorable conditions (e.g. when some factors of $n - 1$ are already known or can be easily obtained). This test is based on the following theorem (i.e. Pocklington's primality test theorem):
Let $n > 1$ be an integer, and let F be a known factor of $n - 1$. Suppose that for every prime factor p of F, there exists an integer a such that $a^{n-1} \equiv 1 \pmod{n}$ and $\gcd(a^{(n-1)/p} - 1, n) = 1$. If $F > \sqrt{n} - 1$, then n is prime.

7.3.17 Proth Test

According to Proth's theorem (or rather a variant of it), a Proth number b is prime *iff* there is an integer a with the Jacobi symbol condition $\left(\frac{a}{b}\right) = -1$ such that b divides $a^{(b-1)/2} + 1$. Proth's theorem provides a deterministic and computationally-efficient primality test for Proth numbers (see § 2.1.65), and this should explain why very large Proth primes are relatively easy to find compared to large primes of most other types (as well as arbitrary large primes).

7.3.18 Solovay-Strassen Test

This test is based on Euler's criterion (see § 5.1.13) and the law of quadratic reciprocity and it involves the use of Legendre (or Jacobi) symbol. The basic idea of this test is the following modular equation:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} \tag{115}$$

where $a \in \mathbb{Z}$ is a given base, p is an odd prime coprime to a, and $\left(\frac{a}{p}\right)$ is the Legendre symbol. So, if $m > 1$ is an odd natural number coprime to a and we consider the congruence equation (where the Jacobi symbol is used here):

$$\left(\frac{a}{m}\right) \equiv a^{(m-1)/2} \pmod{m} \tag{116}$$

then m is definitely composite if this congruence fails for some values of a, while m is probably prime as long as this congruence holds with certain values of a (where this probability increases as more values of a pass the test of this congruence). This test is obviously probabilistic (but it can be made deterministic under the assumption of the generalized Riemann hypothesis; see § 6.1.29). Also see Point 4 of § 7.9.5 and § 9.7.4.

7.3.19 Wilson Test

Because Wilson's theorem provides a necessary and sufficient condition for primality in general (see § 5.1.43), it provides (in principle) a deterministic primality test for arbitrary integers (unlike some other tests which provide probabilistic tests or tests that apply only to special forms of numbers). However, the direct computational implementation of Wilson's theorem is inefficient because evaluating $(n-1)!$ modulo n requires $O(n)$ modular multiplications using the straightforward approach. Consequently, the test is generally impractical for large integers compared with more efficient primality testing algorithms. From this standpoint, Wilson's theorem is primarily of theoretical interest, i.e. it is used in proving other theorems or for educational purposes rather than as a basis for a practical method in actual computational primality testing.

7.3.20 Tests for Specific Prime Types

In the previous subsections (as well as § 7.2) we were mostly talking about tests for primality (i.e. whether an integer is prime or not). In this subsection we briefly investigate tests for specific types of primes, i.e. whether an integer (or prime number) is a prime of a specific type or not.[674] The following are some examples of such tests (and related theorems):[675]

1. An integer > 5 that contains digits other than 1, 3, 7, and 9 cannot be a circular prime (see § 2.1.7).
2. An integer > 5 that contains digits other than 0, 1, 2, 5, and 8 cannot be a dihedral prime (see § 2.1.16).
3. An integer > 5 whose last digit is not 7 cannot be a Fermat prime (see § 2.1.20).
4. An integer that is not of the form $c^2 + 1$ ($c \in \mathbb{Z}$) cannot be a generalized Fermat prime with $n > 0$ (see § 2.1.24).
5. An integer that is not of the form $4k + 1$ ($k \in \mathbb{N}$) cannot be a generalized Fermat prime with $n > 0$ (see § 2.1.24).
6. An integer > 5 that is not of the form $4k - 1$ cannot be a Jacobsthal prime (see § 2.1.36).

[674] Actually, these tests are mostly probable primality tests (or rather compositeness tests), and they are largely useful in sieving operations for specific prime types. We should also note that some of these are trivial or non-practical as primality tests (but we include them for relative completeness and potential utility in some cases).

[675] The statements related to base-dependent types (usually characterized by digits constraints) are in base 10 (unless stated otherwise here or elsewhere).

7. In binary numeral system, a non-repunit integer cannot be a Mersenne prime (i.e. every Mersenne prime is a binary repunit). See § 2.1.41.
8. An integer q that is not of the form $q = 2kp + 1$ (where $k \in \mathbb{N}$ and p is an odd prime) cannot be a prime divisor of Mersenne number $2^p - 1$ (see § 2.1.42).
9. An integer q that does not satisfy $q \overset{2p}{=} 1$ and $q \overset{8}{=} \pm 1$ (where p is an odd prime) cannot be a prime divisor of Mersenne number $2^p - 1$ (see § 2.1.42).
10. A multi-digit integer that contains any of the digits 2, 3, 5, and 7 cannot be a minimal prime (see § 2.1.45).
11. An integer > 2 that is not of the form $4k + 1$ cannot be an $n^2 + 1$ prime (see § 2.1.47).
12. An integer > 11 with an even number of digits cannot be a palindromic prime (see § 2.1.53).
13. A multi-digit integer that is neither a repunit nor a permutation of a number of the form $a \ldots ab$ (where a and b are distinct digits from the set $\{1, 3, 7, 9\}$) cannot be a permutable prime (see § 2.1.58).
14. A prime p for which $p - 1$ has a prime divisor other than 2 and 3 cannot be a Pierpont prime (see § 2.1.60).
15. An odd prime that is neither a Fermat prime nor of the form $6k + 1$ cannot be a Pierpont prime (see § 2.1.60).
16. An integer that is not of the form $4k + 1$ (or equivalently $a^2 + b^2$) cannot be a Pythagorean prime ($k, a, b \in \mathbb{N}$; see § 2.1.66).[676]
17. An integer > 2 that is not of the form $16k + 1$ cannot be a quartan prime (see § 2.1.67).[677]
18. An integer $q = 2p + 1$ that does not divide the Mersenne number $2^p - 1$ (where $p \overset{4}{=} 3$ is prime) cannot be a safe prime (see § 2.1.41 and § 2.1.72).
19. An integer > 7 that is not of the form $12k - 1$ cannot be a safe prime (see § 2.1.72).
20. An integer > 3 that is not of the form $6k - 1$ cannot be a Sophie Germain prime (see § 2.1.76).[678]
21. If q is prime and $n = 2q + 1$ with $2^{n-1} \overset{n}{=} 1$ and $2^q \overset{n}{\neq} 1$ then n is prime (i.e. n is a safe prime and q is a Sophie Germain prime). See § 2.1.72 and § 2.1.76.
22. An integer that contains digits other than 0, 1, 6, 8, and 9 cannot be a strobogrammatic prime (see § 2.1.78).
23. A pair of integers $(n, n+2)$ that is not of the form $(6k-1, 6k+1)$ cannot be a twin prime pair ($n > 3$). See § 2.1.84.
24. A pair of integers $(n, n + 2)$ not satisfying $n(n + 2) \overset{9}{=} 8$ cannot be a twin prime pair ($n > 3$). See § 2.1.84.
25. An integer that is not of the form $4k - 1$ cannot be a Wagstaff prime (see § 2.1.87).
26. We should also include the following type-specific tests that we discussed earlier in the subsections of this section (i.e. § 7.3): Lucas-Lehmer test which is specific to Mersenne primes (see § 7.3.10), Lucas-Lehmer-Riesel test which is specific to Riesel primes (or numbers of the form $2^n k - 1$; see § 7.3.11), Pepin's test which is specific to Fermat primes (see § 7.3.15), and Proth's test which is specific to Proth primes (see § 7.3.17).
27. Subset relationships (see § 5.2.12) can be useful as tests for specific prime types (or replacement of such tests) when the test for the superset type is easy compared to the subset test (or easier than the subset test). For example, if prime type 1 is a superset of prime type 2 and it is easy to verify that a given integer n is not of prime type 1 then we can use the subset relationship to establish that n is not of prime type 2.
28. We should also note that the definitions of prime types (see the subsections of § 2.1) usually provide

[676] We may also say: an odd prime of the form $4k + 1$ (or equivalently $a^2 + b^2$ where $a, b \in \mathbb{N}$) is Pythagorean; otherwise it is non-Pythagorean.

[677] The primes of the form $n^4 + 1$ are a proper subset of the quartan primes and hence the statement similarly applies to the $n^4 + 1$ primes (see § 2.1.48).

[678] We may replace $6k - 1$ with $3k - 1$ (although the latter condition is weaker because it excludes fewer integers).

"definition-based tests" for those specific prime types (where we are tolerating the use of "test" here; see Point 16 of § 7.1). For example, the equation $p_n = (p_{n-1} + p_{n+1})/2$ provides a "test" for balanced primes (see § 2.1.1). Similarly, the divisibility requirement $p^2|(2^{p-1} - 1)$ provides a "test" for Wieferich primes (see § 2.1.90).

29. Also see § 7.2 for some simple type-specific primality tests.
30. Also see § 7.3.21 for some hypothetical type-specific primality tests (such as those in Points 10 and 11 of § 7.3.21).

7.3.21 Hypothetical Tests

There are many theorems and results in prime number theory that can (in principle) lay the foundation for primality tests even though such tests are trivial or non-practical (due for instance to their high computational cost with the availability of better alternatives). Such tests (or potential tests) can be aptly described as hypothetical due to their purely theoretical nature. In fact, we met many examples of such tests in the past (e.g. in § 5.2.10, § 5.2.13, § 7.2 and § 7.3.20). Even some of the tests discussed in section 7.3 are not practical for various reasons. For instance, the trial division test (see § 7.3.4) is not practical for large numbers because it requires checking many potential divisors (up to $\sqrt{n}$). Similarly, Wilson's test (see § 7.3.19) in its straightforward form is not practical even for relatively small n because it involves evaluating $(n-1)!$ modulo n which requires $O(n)$ modular multiplications, making the required arithmetic very expensive or prohibitive.

Such hypothetical tests (whether for primality in general or for specific types of primality) are not entirely useless even when they are impractical, because (for instance) they can be useful in some cases and circumstances, and hence it is useful to be aware of such tests. In any case, such tests are theoretically useful (e.g. by improving our understanding of primality and related mathematical structures) regardless of practicality or any other direct benefit. The following are some examples of such hypothetical primality tests (or their theoretical foundations):

1. Any integer $n > 3$ that divides $2^n + 1$ is composite.
2. If an odd integer > 1 can be expressed as a sum of two perfect squares in more than one way (ignoring the sign and order of the squares) then n is composite.
3. If an odd integer > 1 can be expressed as a difference of two perfect squares in more than one way (ignoring the sign and order of the squares) then n is composite.
4. If an integer $n \geq 5$ is such that n^2 does not divide the numerator of the harmonic number $H_{n-1} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1}$ when written in reduced form, then n is composite (by the contrapositive of Wolstenholme's theorem).
5. For any integer $n \geq 2$, n is prime *iff* for every integer k with $1 \leq k \leq (n-1)$ the following congruence holds: $C_k^n \stackrel{n}{=} 0$.[679]
6. For any integer $n \geq 2$, n is prime *iff* for every integer k with $0 \leq k \leq (n-1)$ the following congruence holds: $C_k^{n+k} \stackrel{n}{=} 1$ (a variant of Babbage's theorem).
7. For any integer $n \geq 3$, n is prime *iff* for every integer k with $1 \leq k \leq (n-1)$ the following congruence holds: $(k-1)!(n-k)! \stackrel{n}{=} (-1)^k$.[680]
8. For any integer $n \geq 3$, n is prime *iff* for every integer k with $1 \leq k \leq (n-1)$ the following congruence holds: $C_{k-1}^{n-1} \stackrel{n}{=} (-1)^{k-1}$.[681]
9. For any integer $n \geq 2$, n is prime *iff* the non-zero residue classes modulo n (i.e. $\{1, 2, \ldots, n-1\}$) form

[679] This is the binomial coefficient divisibility property of primes (which means that a prime number n divides all the internal binomial coefficients in the n^{th} row of Pascal's triangle). By the symmetry $C_k^n = C_{n-k}^n$, the range $1 \leq k \leq (n-1)$ can equivalently be replaced by $1 \leq k \leq \lfloor n/2 \rfloor$.

[680] This is Simionov's theorem which is based on Wilson's theorem (and is supposedly a generalization of Wilson's theorem).

[681] This is the binomial coefficient formulation of Simionov's theorem, equivalent to the factorial formulation in Point 7.

a cyclic multiplicative group of order $n-1$.

10. Any prime $p > 5$ for which 10 is not a primitive root (modulo p) is not a full reptend prime.
11. Clement's theorem (see § 5.1.10) can be a basis for a hypothetical primality test for twin primes.
12. The theorem: "n is prime *iff* $\sigma(n) = 1 + n$" can provide a hypothetical deterministic primality test. However, to be sensible the calculation of $\sigma(n)$ must not require knowing the factors of n. This can be achieved, for instance, by using the recursive formula $\sigma(n) = \sigma(n-1)+\sigma(n-2)-\sigma(n-5)-\sigma(n-7)+\cdots$, where the indices subtracted from n are the generalized pentagonal numbers (i.e. 1, 2, 5, 7, 12, 15, 22, 26, 35, 40, 51, 57, 70, 77, ...) and the signs alternate in pairs.[682] Although this method avoids factoring n, its computational cost makes it impractical for large inputs when complexity is measured in the bit-length of n.
13. Referring to the previous point, we may get similar hypothetical tests from the theorems: "n is prime *iff* $s(n) = 1$", "n is prime *iff* $\tau(n) = 2$", and "n is prime *iff* $\phi(n) = n-1$". In fact, similar theorems may also provide theoretical foundations for similar hypothetical tests (i.e. deterministic, but impractical, primality tests).
14. A deterministic version of the Fermat primality test (i.e. by testing all bases $2 \leq a < n$) should also be classified in this category (since it is impractical due to its high or prohibitive computational cost). In fact, even the standard probabilistic Fermat primality test (see § 7.3.6) can be of little practical value in most situations due to lack of reliability (and hence it may also be classified in this category).[683]
15. Cyclotomic polynomial properties (and related theorems) may also provide theoretical foundations for a primality test (or tests) even though such tests are not expected to be practical within the current mathematical knowledge (but this may change with upcoming research developments).[684]
16. The Riemann zeta function (see Eq. 48) may also provide a theoretical basis for testing (or rather identifying) primes, i.e. in principle if we identify the exact non-trivial zeros of the Riemann zeta function then we can recover all prime numbers and therefore determine whether a given integer n is prime.[685] However, this is entirely impractical.
17. Some of the theorems and formulae for calculating and generating prime numbers (e.g. Willans' formula; see § 5.2.14) may be regarded as potential theoretical bases for hypothetical primality tests by considering if a suspected prime meets the conditions of the theorem or satisfy the formula (although this is very unlikely or impractical). Such theorems and formulae (under certain conditions) may be regarded as primality test algorithms disguised behind mathematical formulation. However, these hypothetical tests are generally vacuous (e.g. because they are tautological) or impractical (e.g. because they rely on highly theoretical conditions or computationally prohibitive foundations). Nevertheless, it is useful to keep this perspective in mind as this can be useful in some special circumstances or can be activated in the future due to favorable developments in forthcoming research.

7.3.22 Primality Testing and Conjectures

There are some "hypothetical primality tests" but in a different sense to what we were talking about in § 7.3.21, although they may also by "hypothetical" in the sense of § 7.3.21 by being, for instance, impractical. These tests are represented or implied by conjectures about (or related to) primality testing (see for instance § 6.2.10). A prominent example is the Agoh-Giuga conjecture (see § 6.1.2) which should

[682] We note that the expansion stops when $(n - i)$ drops below zero, while a correction term of magnitude n (with its sign following the same paired pattern) is added when n itself is a generalized pentagonal number. Also see `https://oeis.org/A001318`.

[683] The reliability of the standard probabilistic Fermat primality test is limited by the existence of Carmichael numbers (see § 5.1.15, § 7.9.2 and § 9.7.1).

[684] In fact, refined variants of cyclotomic-based tests (not based on naive and direct approaches) of practical value are seemingly emerging recently (although caution may be required regarding some claims and results in the literature due, for instance, to reliance on artificial intelligence or lack of sufficient testing and verification).

[685] This sounds more like a sieve than a test.

directly provide a deterministic primality test if it is proven. We should also remember in this context that the validity or determinism of some primality tests relies on the supposed validity of certain conjectures, such as the generalized Riemann hypothesis.

Overall, we have at least three types of conjecture-related "primality tests":

1. Primality tests provided directly and explicitly by conjectures (like Agoh-Giuga-based test; see § 6.1.2).
2. Primality tests provided indirectly and implicitly by conjectures (like Agrawal-based optimized test; see § 6.1.3).
3. Primality tests whose validity or determinism is conditioned by the validity of certain conjectures (like the deterministic Miller test; see § 7.3.12).[686]

We should also note that in one case at least, the emergence of a primality test (i.e. the AKS test; see § 7.3.1) resolved a historical open problem and proved a conjecture. This case represents another example of the intimate relationship between primality testing and conjectures. In fact, this represents a relationship of different type to those outlined already (and hence we may claim that we have at least four types of conjecture-related primality tests).

In any case, well tested conjectures may provide "probable primality tests" in the sense that they can be used in some cases to support other tests or to obtain a certain degree of probability or confidence about the primality status of certain numbers. In other words, while highly tested conjectures cannot provide a true probabilistic test (with mathematically bounded error rates) they can increase our empirical confidence in the primality of a number or serve as secondary validation alongside well established probabilistic primality tests (in the conventional sense). In short, this kind of testing should be distinguished from the rigorous notion of conventional probabilistic primality testing, which comes with mathematically established error bounds.

The following table outlines common examples of conjecture-related (which are mostly conjecture-conditioned) primality tests where we indicate the beneficial effects of the conjectures (or test):[687]

Primality Test	**Related Conjecture**	**Benefit of Conjecture (or Test)**
Agoh-Giuga	Agoh-Giuga	Conj yields fully deterministic test
AKS	Agrawal	Conj optimizes run time of AKS test
AKS	Prime testing in P time	Test proved conjecture
Baillie-PSW	No BPSW pseudoprimes	Conj yields ultra-fast flawless deterministic test
ECPP	Lenstra's distribution	Conj imply fast polynomial-time execution
Lucas Test Variants	GRH	Conj restricts necessary trial bases to small bound
Miller Test	GRH	Conj makes test fully deterministic in P time

We should finally refer to the relationships between prime distribution conjectures (see for example § 6.2.6) and primality testing and sieving, e.g. potential utilization of Legendre's conjecture (see § 6.1.21) in the search and verification of primes. Many conjectures (like Legendre's) directly imply constraints on where primes must exist, which can theoretically optimize primality testing searches (as well as sieving ranges). Accordingly, well tested conjectures may provide sufficient confidence to be exploited probabilistically in primality testing and sieving; an issue that should be handled on a case-by-case basis. The issue of relationships between prime distribution and primality testing and sieving will be investigated further in § 8.7.4.

[686] A deterministic version of the Solovay-Strassen test can also be obtained under the generalized Riemann hypothesis (see § 7.3.18).

[687] For the Baillie-PSW test, see Point 1 of § 7.9.5. Due to the restriction on the table width, some entries are loosely phrased.

7.4 Prime Sieves

"Prime sieves" (or "primality sieves") primarily means algorithms for finding all prime numbers within a given range of natural numbers (e.g. up to 100000) by systematic elimination of composites in that range, and hence leaving only the prime numbers within that range. Primality sieves (in this sense) are usually implemented computationally although in theory most of them can be conducted even manually (noting that this may be difficult or prohibitive for practical reasons). These sieves are of deterministic nature as they produce a list of all prime numbers (with nothing else) in the given range with absolute certainty.

However, "prime sieves" may be used in an analytic or combinatorial sense, which is different from its algorithmic sense that we already defined. So, we should distinguish between "prime-generating sieves" (or "prime-finding sieves" or "algorithmic sieves") which is the standard and primary meaning of "prime sieves", and the "analytic/combinatorial sieves". The fundamental difference between them is in their nature and ultimate objective, that is: prime-generating sieves are discrete *algorithms* used by computer scientists to physically *construct* list tables of prime numbers, while analytic/combinatorial sieves are *theoretical* mathematical tools used by number theorists to *calculate* bounds, approximations, and density estimations of prime sets without listing the elements (or not necessarily so).

We outline in the following subsections of this section some of the common prime sieves. Ideally, the algorithmic sieves and the analytic/combinatorial sieves should be investigated and categorized into two different sections. However, for factors related to the size and structure of this book we put both these categories in one section (i.e. § 7.4). Nevertheless, to distinguish the two categories we grouped the algorithmic sieves in the first five subsections (ordered alphabetically), and grouped the analytic/combinatorial sieves in the next six subsections (also ordered alphabetically). But it is important to note that in some cases the distinction between algorithmic and analytic sieves is not clear-cut as some sieves have algorithmic variants (or versions or flavors) and analytic ones.[688] In fact, this can be another reason or justification for mixing the two categories in one section rather than separating them in two sections.

Anyway, there is an intimate relationship between the algorithmic and analytic sieves from historical, theoretical and practical perspectives. Analytic sieves theory actually evolved directly from an attempt to turn the sieve of Eratosthenes (and possibly some of its variants) into an algebraic counting formula, and hence "analytic sieves" are natural descendants of algorithmic sieves. This should add an extra justification for mixing them up. We should finally refer to some integer factorization algorithms which can also be described as sieves (see § 7.10.5, § 7.10.9 and § 7.10.11). Also see § 7.6.1.

7.4.1 Atkin's Sieve

The sieve of Atkin is a modern prime sieve that improves upon the asymptotic efficiency of the classical sieve of Eratosthenes by using properties of certain quadratic forms together with modular arithmetic. Although it has better theoretical complexity, it is considerably more complicated to understand and implement, and for moderate ranges the sieve of Eratosthenes is often faster in practice. The basic idea of this sieve is to exploit certain quadratic forms (of integers involving algebraic sums of squares and their multiples) with modular arithmetic to filter out the composites in that range and hence obtain the primes in that range.

The algorithm of this sieve can be outlined as follows:

• Obtain an initial list of natural numbers (in the given range) where these numbers are potentially prime.[689]

[688] As we will see in § 7.4.9, Legendre's sieve may be an example of a bridge between the two categories (or even having an algorithmic variant and an analytic/combinatorial variant) although it is seemingly more appropriate to be identified and classified as an analytic/combinatorial sieve (and that is what we did by listing it in the last six subsections).

[689] This is essentially done through creating a Boolean array for the integers in the specified range, initially marking the relevant candidates as false (the base primes 2, 3, and 5 are handled separately).

• For suitable $x, y \in \mathbb{N}$ check the numbers n (in the obtained list) of the following three quadratic forms:

$$n = 4x^2 + y^2 \qquad n = 3x^2 + y^2 \qquad n = 3x^2 - y^2 \tag{117}$$

• If a number n (in the given list) of one of these forms meets certain congruence conditions modulo 60 (or modulo 12 in some variants), its candidate-prime status is toggled.
• More tests are conducted on the obtained list of likely primes to remove multiples of the squares of known primes and hence a final list of all (confirmed) primes in that range is obtained, i.e. the remaining numbers (together with the primes 2, 3, and 5) are exactly the primes in the specified range.

7.4.2 Eratosthenes' Sieve

The sieve of Eratosthenes is an ancient algorithm for finding all the prime numbers up to a given number $n \in \mathbb{N}$ by marking the multiples of each prime starting from 2. The algorithm can be outlined as follows (assuming $n > 2$):
• List all the natural numbers greater than 1 and less than or equal to n.
• Remove all the multiples of 2 from the list.[690]
• If the next remaining number in the list is $\leq \sqrt{n}$ remove all its multiples from the list.[691]
• Repeat the process in the previous point until the next remaining number is $> \sqrt{n}$.
• The remaining numbers in the list are the required primes.

It is noteworthy that these days the sieve of Eratosthenes is largely of historical and educational value (rather than practical value) due to the emergence of more efficient algorithms for searching for primes (especially the very large ones) and sieving them. However, the basic principles of this sieve remain embedded in some of the modern sieves and algorithms which can be regarded as improved versions of this sieve.

7.4.3 Euler's Sieve

Euler's sieve (also known as the linear sieve) is a classic prime sieving algorithm. It can be regarded as a refinement of the sieve of Eratosthenes. The main distinction between them is that Euler's sieve, unlike the sieve of Eratosthenes, generates every composite number exactly once. This eliminates the redundant work found in the sieve of Eratosthenes, where a number such as 60 is visited and crossed out multiple times (by 2, 3, and 5). Consequently, Euler's sieve achieves a true linear running time, $O(n)$. However, despite its superior asymptotic complexity, Euler's sieve is often slower than the sieve of Eratosthenes for large ranges in practical implementations because of larger constant factors and less favorable memory-access patterns (see § 7.6.3).

The algorithm of Euler's sieve can be outlined as follows (where $n > 2$, I is the list of candidate numbers, and P is the list of discovered primes):
• List all integers from 2 up to n to form $I = [2, 3, 4, 5, \ldots, n]$, with all numbers initially unmarked, and initialize an empty list of primes P.
• Examine the elements of I sequentially. Let the current number under evaluation be i. If i remains unmarked (indicating it is prime), add it to P as a newly discovered prime.
• For the current number i, regardless of whether it is marked or unmarked, process the primes p currently stored in P in increasing order. For each prime p, calculate the product pi. If $pi > n$, stop processing further primes for this i. Otherwise, mark pi as composite in I. Then, if i is divisible by p, stop processing

[690] "Multiple" here does not include the number itself, i.e. the multiples of m are km where $1 < k \in \mathbb{N}$.
[691] Whether the consideration of $\sqrt{n}$ belongs to the original sieve or not seems controversial, and may be an added improvement to the original sieve.

further primes for this i. This termination condition ensures that each composite is generated exactly once, using its smallest prime factor p.
• Repeat this evaluation sequentially for every integer i from 2 up to n.

7.4.4 Sundaram's Sieve

This sieve is similar to the sieve of Eratosthenes but it works by eliminating integers of the form $i+j+2ij$ from the list $1, 2, \ldots, n$ (where $i, j \in \mathbb{N}$). The algorithm of this sieve can be outlined as follows:
• Eliminate all the integers of the form:

$$i + j + 2ij \qquad \text{where} \quad 1 \leq i \leq j \quad \text{and} \quad (i + j + 2ij) \leq n \tag{118}$$

• The remaining integers k are mapped to $2k + 1$ to obtain all odd primes $\leq (2n + 1)$.
• The number 2 is added to the list to obtain all primes $\leq (2n + 1)$.

As we see, Sundaram's sieve is an elegant algorithm that removes all integers of the form $i+j+2ij$ from the set $\{1, \ldots, n\}$, and hence it generates all odd primes up to $2n+1$ through the mapping of k to $2k+1$. This means that it eliminates half of the composite search space (by bypassing even numbers and tracking indices only up to n to find primes up to $2n + 1$) which reduces the memory requirement substantially. However, its time performance is typically worse than comparative sieves (like Eratosthenes and Atkin) because multiple (i, j) pairs can generate identical values which leads to redundancies.[692] Accordingly, its simple arithmetic structure and elegance make it highly educational and memory efficient for small limits, but its inefficient performance for large scale operations makes it inferior to competitive sieves.

7.4.5 Wheel Sieve

This is a prime-generating sieve that uses "wheel factorization" to skip integers that are divisible by small primes such as 2, 3, 5, and 7. The basic idea of the algorithm of this sieve is to use "wheels" (i.e. patterns of numbers which are indivisible by small primes like 2, 3, 5, 7) to eliminate from the beginning (and hence avoid going through) multiples of these small primes. A wheel is constructed from the repeating pattern of integers that are coprime to the product of these small primes. By excluding obvious composites from the outset, the sieve operates on a reduced set of candidate integers, thereby decreasing the amount of work required during sieving. This "intrinsic elimination" substantially reduces the number of integers (i.e. in the range or search space) that must be processed during the sieving procedure, and enhances the efficiency and speed of this sieve significantly (which supposedly gives the wheel sieve an advantage in comparison to competitive sieves).

Wheel factorization is often used as an optimization of the classical sieve of Eratosthenes, although wheel sieves constitute a broader class of algorithms and are not necessarily identical to an optimized Eratosthenes sieve. In practice, wheel sieves can offer performance improvements by reducing the volume of numbers that must be processed, although the magnitude of the improvement depends on the wheel size and implementation details. Accordingly, in real world computing, the wheel sieve can be slower than a highly optimized sieve of Eratosthenes.

We should finally note that the term "wheel sieve" is sometimes used interchangeably with the sieve of Pritchard in broader discussions. However, "wheel sieve" serves as a general paradigm for any sieve utilizing a fixed (static) wheel to skip small primes. In contrast, the sieve of Pritchard represents a highly specific advanced realization of this concept. It utilizes a dynamically growing wheel and has an asymptotic running time of $O(N/\log\log N)$, making it a theoretically distinct algorithm rather than just

[692] In fact, these performance variations normally depend on the particular implementations and variants of these algorithms.

a typical instance of the static wheel paradigm. Nevertheless, the use of these terms in the literature should be examined on a case-by-case basis to determine the exact intent of the authors.

7.4.6 Brun's Sieve

This sieve (which may also be called *Brun's pure sieve*) is a combinatorial sifting method designed to estimate the size of sets of integers by filtering out those belonging to specific congruence classes (or, equivalently, satisfy certain divisibility conditions). Unlike the sieve of Eratosthenes (see § 7.4.2) which seeks exact prime identification, Brun's sieve utilizes a sophisticated truncation of the inclusion-exclusion principle to provide manageable upper and lower bounds. Its primary application is in providing statistical estimates and theoretical bounds for sets of "almost-primes" (see § 9.6). So, Brun's sieve is a "prime sieve" in the sense that it is used for studying the distribution and existence of prime numbers (rather than for testing or determining if a specific number is prime or not).

In short, Brun's sieve (unlike the sieve of Eratosthenes) is an analytic or combinatorial tool rather than a computational algorithm, even though in principle it can be implemented as an algorithmic sieve. The theoretical power of the Brun sieve has been demonstrated in numerous fields and applications; most prominently in proving the convergence of the sum of the reciprocals of twin primes (see § 5.1.5). From a historical perspective, Brun's sieve is widely regarded as marking the birth of modern sieve theory (or at least as a foundational contribution to this theory).

7.4.7 Harman's Sieve

This is a rather sophisticated method in analytic number theory designed to study the distribution of prime numbers, particularly in settings where classical sieve methods alone are insufficient. Unlike more traditional sieves (such as the Brun and Selberg sieves; see § 7.4.6 and § 7.4.10), Harman's method combines sieve techniques with estimates for exponential sums and related tools from harmonic analysis. This makes it especially effective for detecting primes in sparse or thin sequences, as well as in short intervals (where traditional sieving methods are bottlenecked by the parity problem).[693]

A distinguishing feature of Harman's sieve is its ability to transform prime-counting problems into estimates for bilinear forms and exponential sums, allowing information about primes to be extracted from sequences with relatively low density. The method has been applied successfully to problems involving primes in short intervals, primes represented by special forms, and other sequences defined by arithmetic or analytic constraints. As a result, it has led to significant advances in understanding the distribution of primes in structured and sparse sets.

7.4.8 Large Sieve

This is a family of analytic methods, in the form of inequalities, used to study the distribution of a set of integers, and hence being a sieve in the technical sense may be questioned by some. The main property (and actually strength) of the large sieve, which justifies its "large" label, is that it "excludes" considerably more congruence classes (modulo a prime p) than other "small" sieves, such as Brun and Selberg sieves (see § 7.4.6 and § 7.4.10). So, while "small" sieves usually exclude a few residue classes (say two), the large sieve can "exclude" a large part of the residue classes (modulo p).[694]

Another characteristic feature of the large sieve, in addition to its "analytic" nature and being "large", is its link (at least in some of its variants) to the duality principle in functional analysis. The large sieve also

[693] In fact, Harman's method can overcome certain limitations of classical sieves in particular applications, but it should not be regarded as a general solution to that fundamental problem.

[694] More precisely, the large sieve (unlike combinatorial sieves, like Brun, which construct upper/lower bounds by removing residue classes in a structured way) does not explicitly remove residue classes but instead bounds how evenly a set distributes across residue classes.

provides powerful upper bounds for the size of a set of integers that avoids specified residue classes modulo many primes, which is one of the standard formulations of the large sieve inequality. One of the major applications and achievements of the large sieve is its contribution to the proof of the Bombieri-Vinogradov theorem (see § 5.1.4).

7.4.9 Legendre's Sieve

This sieve is commonly associated with the sieve of Eratosthenes (see § 7.4.2), by regarding it as an extension (or improvement or inspiration or ...) of the Eratosthenes sieve and its fundamental idea. However, the literature is generally confusing about the actual nature of Legendre's sieve as if there are seemingly various versions or understandings of this sieve and its nature. For example:

• Some sources identify Legendre's sieve as a formula for counting prime numbers (rather than finding them as it is the case with the sieve of Eratosthenes). Accordingly, the difference between the Legendre and Eratosthenes sieves is in their nature and purpose, that is: Eratosthenes' is a computational algorithm for sieving and listing primes, while Legendre's is an analytical formula for counting and estimating their numbers (by applying the same inclusion-exclusion principle). In simple words, the output of Eratosthenes' is a list of primes and hence it is an algorithmic sieve, while the output of Legendre's is a numerical estimate or exact count (represented by lower and upper bounds or by a single number) and hence it is an analytic or combinatorial sieve.

• Other sources consider Legendre's sieve as an improved version of the Eratosthenes sieve, and hence both are algorithms for finding and listing primes. Some sources seem to suggest that the difference between the two algorithms is that while the Eratosthenes sieve eliminates multiples of primes starting from $2p$ (see § 7.4.2), the Legendre sieve eliminates multiples of primes starting from p^2 (to avoid redundant marking of smaller multiples). However, this is more likely to be a misuse of "Legendre's sieve" or misconception based on confusion with some suggested improvements of the Eratosthenes sieve.

In fact, even the naming of this sieve may suggest such various "versions" where some call it "Legendre's sieve" while others call it "Eratosthenes-Legendre sieve" (noting as well the extra terminology in some sources of the "Legendre's sieve principle" which provides a theoretical framework for the traditional Eratosthenes sieve and similar sieves). The interested readers should therefore inspect the literature carefully about these details.

7.4.10 Selberg's Sieve

This is a powerful and mathematically elegant (but rather complicated) technique in analytic number theory developed in the late 1940s (as a refinement of earlier sieve methods used to study primes and their distribution) to estimate the size of "sifted sets" (i.e. integers that satisfy specific conditions defined by congruence relations). Unlike traditional and more elementary sieves, it introduces carefully chosen weight functions to estimate the size of sifted sets with greater flexibility and precision (and thus avoiding a naive use of the inclusion-exclusion principle which can lead to substantial errors). This approach allows mathematicians to derive upper bounds for quantities, such as the number of primes in certain sequences or patterns, and usually yields results that are difficult to obtain with classical and more elementary tools (like the sieve of Eratosthenes; see § 7.4.2). In fact, it is particularly effective for providing upper bounds for the distribution of primes and prime-related sequences.

The Selberg sieve has played a central role in modern developments of prime number theory, influencing results related to twin primes, gaps between primes, and other fundamental problems in the field. It has also contributed to the developments of modern sieve methods, and potentially influenced some major breakthroughs such as Selberg's work on the distribution of primes and recent advancements in proving

bounded gaps between prime numbers.[695]

However, the Selberg sieve, like other standard sieve methods, is subject to the "parity barrier" which limits its ability to distinguish between integers with an even and an odd number of prime factors. This fundamental limitation arises because standard sieve methods generally lack sufficient information to distinguish primes from certain sequences of composite numbers, as they cannot adequately detect the parity of the number of prime factors on their own.

7.4.11 Turan's Sieve

This is a mathematical technique in analytic number theory used to estimate the size of "sifted sets" (i.e. sets of integers that avoid specified arithmetic properties, often related to congruence conditions or divisibility by primes). More explicitly, it establishes an upper bound on the number of integers that escape the sifting process, such as those remaining after elements divisible by small primes or other structured subsets are removed.

Unlike classical inclusion-exclusion sieves, Turan's method is based on a second-moment (variance) argument and is therefore probabilistic in nature. In fact, it is one of the foundational tools in probabilistic number theory. Moreover, it is generally simpler, but potentially less precise, than more sophisticated and refined sieves (such as the Selberg sieve; see § 7.4.10) although it is still powerful and reliable for solving many problems. Its most famous application is in providing a simplified proof of the Hardy-Ramanujan theorem on the normal order of the number of prime factors of an integer (see § 5.1.18).

7.4.12 Sieves for Specific Prime Types

In the previous subsections we were largely talking about sieves for primes in general. In this subsection we briefly investigate sieves for specific types of primes (as well as sieve-related issues and theorems linked to specific types of primes). Historically, prime sieving is about searching for primes in general rather than specific prime types (unlike prime testing which can equally be general and specific, as seen in § 7.3). However, this is not an issue of principles but an issue of historical development. In other words, there is nothing wrong with the concept of "type-specific prime sieves" but they were not investigated and developed in the past with the same level of interest.

Anyway, there are various aspects to the issue of "type-specific prime sieving" which deserve our attention and hence will be discussed in the following points (noting that our intent here is to highlight such issues rather than diving deep in their investigation which will be deferred to the future):

1. The weak interest in "type-specific prime sieving" may be justified by the fact that most prime types are sufficiently characterized to eliminate almost all integers from the beginning (excluding a very tiny fraction of them) which makes the size of the search space very restricted at the outset, and hence any general sieving operation would be very inefficient (if not senseless). For example, if we want to find all the Fibonacci primes within a given range then all is needed is to identify all the Fibonacci numbers in that range and test them individually (after eliminating the composite-indexed ones; see Point 16 in § 7.2).

   However, in certain prime types (e.g. twin primes) the specification is rather generic and vague (mainly for the other primes in the pairs) because the candidate numbers are not explicitly parameterized independent of their primality status, and hence type-specific sieving operations can be sensible (see the upcoming Point 5). We may also include in this category of potentially sensible type-specific prime sieving (i.e. like twin primes) other prime types such as safe primes, Sophie Germain primes, cousin primes and sexy primes.

[695] Some seem to suggest that it may even have influenced Selberg's elementary proof of the prime number theorem (see § 5.1.31).

2. In principle, general sieve frameworks can be adapted to search for specific types of prime numbers. However, this is unlike (for instance) the Lucas-Lehmer primality test which is designed from the beginning for Mersenne primes specifically (see § 7.3.10).
3. Certain theorems (which may be classified as type-specific primality test theorems) have direct sieving implications and hence they can benefit type-specific prime sieves in searching for those specific types of primes. For example, the following theorem imposes limits on any sieving operation that search for factorial primes: $n! \pm 1$ (where $n \geq 1$ for $n! + 1$, and $n \geq 3$ for $n! - 1$) is prime *iff* it has no prime divisor p in the range $n < p \leq (n! \pm 1)^{1/2}$ (see § 2.1.19). Similarly, the following theorem imposes limits on any sieving operation that search for primorial primes: $p_n\# \pm 1$ (where $n \geq 1$ for $p_n\# + 1$, and $n \geq 2$ for $p_n\# - 1$) is prime *iff* it has no prime divisor p in the range $p_n < p \leq (p_n\# \pm 1)^{1/2}$ (see § 2.1.64).
4. Many simple and type-specific primality tests along with their related theorems (see for example § 7.2 and § 7.3.20) can benefit type-specific sieving operations by imposing algebraic or parity rules of exclusion, even if those tests and theorems lack direct sieving implications and sifting mechanisms. For instance, because $n^2 + 1$ is strictly even (and thus composite) for all odd $n > 1$, a type-specific sieve for $n^2 + 1$ primes can systematically exclude all odd values of n from the candidate generator. This optimization immediately reduces the initial search space by half, restricting the sieve to even values of n.
5. We should finally note that there are proposals of type-specific prime sieves in recent research (e.g. proposals of sieves for twin primes) which reveal a growing interest in this topic.

Also see § 7.6.4.

7.5 Classifications of Primality Tests

There are many classifications of primality tests. Some of these classifications (and related issues) are outlined in the following subsections. However, before that we note the following remarks:

1. These classifications are based on different criteria; consequently, a single test often belongs to multiple categories under different classification schemes.
2. Some classifications are not clear-cut, depending on the particular test or the context in which it is considered.
3. Some classifications may not be comprehensive or mutually exclusive.
4. Unless stated otherwise, classifications of primality tests refer to their standard or commonly used implementations, noting that the classifications may differ for alternative implementations (e.g. in the selection of bases and parameters, the use of randomization, and the nature of the resulting primality guarantee).
5. Primality testing (and their classification in particular) is very difficult to summarize and present in the form of concise generalizations. This is because it is a rather messy subject where there are many variations in opinions, implementations, versions, and so on. Hence, the following subsections (or at least some of them) should be regarded as broad, and sometimes loose, outlines whose more accurate details will be provided in future volumes.

7.5.1 Analytical vs Computational

Primality tests may be classified as analytical (theoretical) or computational (algorithmic). While basic tests rely purely on theory and can often be carried out by hand, complex evaluations of large integers usually require algorithmic implementation. However, the distinction between the two types frequently blurs, making the classification dependent on the situation. Simple analytical tests are commonly implemented algorithmically, even though they can be easily performed manually. Conversely, advanced computational tests are deeply rooted in theoretical foundations, making their classification highly depen-

dent on the circumstances and choice. Consequently, whether a primality test is regarded as analytical or computational often depends on the context in which it is being used and discussed.

7.5.2 Computational Complexity

Primality tests may be classified according to their asymptotic computational complexity (independently of whether they are deterministic or stochastic, and independently of their error probability) as follows, ordered from asymptotically fastest to slowest:

1. Polynomial time (class P) whose running time scales as a polynomial function of the bit-length n, i.e. $O(n^k)$ where $n = \log_2 N$ (noting that N is the tested number and k is a constant).
2. Quasi-polynomial time whose running time grows slightly faster than a polynomial but much slower than sub-exponential.
3. Sub-exponential time whose running time grows faster than quasi-polynomial but slower than pure exponential.
4. Exponential time whose running time grows exponentially with the bit-length of the input.

However, we should note that the classification of certain primality tests can be highly subtle and problematic, as their proven asymptotic bounds often depend on whether the analysis relies on unproven mathematical heuristics or rigorous unconditional proofs (as well as other factors and considerations). Furthermore, practical performance for everyday input sizes depends heavily on hidden constant factors, such as the size of k in $O(n^k)$, meaning an asymptotically slower algorithm may be faster in reality for smaller numbers. We therefore abstain from going through more details and classifying specific primality tests (mainly those of § 7.3), leaving this discussion to the future.

We should also note that quasi-polynomial time may be regarded as a special case of sub-exponential time. Consequently, these categories can be combined into three main classes (i.e. polynomial, sub-exponential, and exponential), ordered from asymptotically fastest to slowest.

7.5.3 Deterministic vs Probabilistic

Primality tests can be classified from the perspective of their results (strictly, exhaustively and disjointly) into deterministic and probabilistic. The output of deterministic tests is a definitive mathematically certain answer regarding whether a number is prime or composite, while the output of probabilistic tests is not absolutely certain. In this sense, "deterministic" (or "probabilistic") in this classification refers to the certainty of the result rather than to the computational procedure used to obtain it (see § 7.5.4). We note the following about this classification:

1. This classification may be labeled as "Definitive vs Probable" (or "Proven vs Probable") to avoid confusion with the "Deterministic vs Stochastic" classification of § 7.5.4. However, the word "definitive" is commonly used as a general adjective and hence it is not as strong in its technical impression and impact as "deterministic". We therefore preferred the "Deterministic vs Probabilistic" label which should be sufficiently clear (noting the label "Deterministic vs Stochastic" of the other classification). To make the situation more clear, in Point 10 of this subsection and Point 2 of subsection 7.5.4 we identified the status of the main primality tests from the perspectives of these classifications. Anyway, contextual clues should clarify the situation in most cases and contexts.
2. Typically, if the probabilistic test declares an integer composite, the conclusion is certain, but if it declares the integer prime, the conclusion is only that the integer is a probable prime, with a quantifiable probability of error. However, the probability of primality in the latter case must be sufficiently high for the test to be useful for practical purposes (and even for some theoretical purposes).
3. Referring to the previous point, a probabilistic test usually attempts to find a "witness" to composite-

ness.[696] If a witness is found, the tested number is declared definitely composite. If no witness is found, the tested number is declared probable prime. A composite number that passes such a test is called a pseudoprime (with respect to that test or its parameters; see § 9.7).

4. Unlike deterministic tests, it is sensible and useful to repeat a probabilistic test (usually with different conditions and parameters) to increase the confidence in the result. Moreover, a probabilistic test can become deterministic if all possible bases (up to a specific mathematical limit) are tested. Also see § 7.9.5.
5. Error reduction in probabilistic tests is exponential in the number of independent bases tested.
6. A primality test can be probabilistic unconditionally and deterministic conditionally (e.g. by assuming Riemann's hypothesis). See for instance § 7.3.12.
7. Typically, deterministic tests have high computational cost and slower execution speed, while probabilistic tests are significantly faster, making them highly useful for large numbers.
8. Deterministic and probabilistic tests can be used complementarily and integrally to optimize efficiency. For example, fast probabilistic tests can be used to sieve out obvious composites quickly, while slow deterministic tests run subsequently on the remaining candidates to guarantee absolute primality.
9. All deterministic tests produce the same final output (i.e. whether the tested number is prime or composite), while probabilistic tests can differ in their final output (i.e. in their quantitative error probability, and whether the tested number is composite or probable prime).
10. We may categorize the primality tests investigated previously (mainly in § 7.3) as follows:[697]
    Deterministic: AKS, APR, Division, ECPP, Lucas (but see § 7.3.9), Lucas-Lehmer, Lucas-Lehmer-Riesel, Morrison, Pepin, Pocklington, Proth, and Wilson.
    Probabilistic: Baillie-PSW (but see § 7.3.3 and § 7.9.5), Fermat, Fibonacci, Frobenius, Miller-Rabin (but see the last paragraph of § 7.3.12), Pell, and Solovay-Strassen.
11. The principal advantage of deterministic tests is their certainty, whereas the principal advantage of probabilistic tests is typically their greater speed and practical efficiency. Accordingly, probabilistic tests dominate practical computer science due to their speed, while deterministic tests remain fundamental for pure mathematical proofs and specialized large primes. In short, probabilistic tests are typically the natural choice in practical applications, while deterministic tests are the natural choice in theoretical settings and contexts.

7.5.4 Deterministic vs Stochastic

Primality tests can be classified (from the perspective of their algorithmic procedure) into deterministic and stochastic. Deterministic tests follow a fixed procedure for a given input, while stochastic tests use probabilistic choices (or random sampling) during their procedure. In this sense, "deterministic" (or "stochastic") in this classification refers to the computational procedure used to obtain the result rather than whether the result is certain or not (see § 7.5.3). We note the following about this classification:

1. Considering the classification of this subsection with that of subsection 7.5.3, primality tests may be divided into four categories (noting that the examples may depend on their particular implementation):
   - Deterministic-deterministic (i.e. definitive-deterministic) like AKS (see § 7.3.1).
   - Deterministic-stochastic (i.e. definitive-stochastic) like ECPP (see § 7.3.5).
   - Probabilistic-deterministic like Fibonacci (see § 7.3.7).
   - Probabilistic-stochastic like Miller-Rabin (see § 7.3.12).
2. We may categorize the primality tests investigated previously (mainly in § 7.3) as follows:[698]

[696] A witness (in primality tests) means an auxiliary number that mathematically proves that the tested number is composite.
[697] The categorization may depend on their particular implementation, which is usually taken as the standard one.
[698] The categorization may depend on their particular implementation, which is usually taken as the standard one.

Deterministic: AKS, APR, Baillie-PSW, Division, Fibonacci, Lucas, Lucas-Lehmer, Lucas-Lehmer-Riesel, Morrison, Pell, Pepin, Pocklington, Proth, and Wilson.
Stochastic: ECPP, Fermat, Frobenius, Miller-Rabin, Solovay-Strassen.[699]

3. Stochastic algorithms use a degree of randomness in their procedure to improve execution efficiency over traditional deterministic approaches, and hence they are typically (but not necessarily) faster than their deterministic counterparts.
4. Stochastic primality tests fall into two main branches: Monte Carlo and Las Vegas. Monte Carlo tests run in a fixed, predictable time but carry a small probability of incorrectly labeling a composite number as prime. In contrast, Las Vegas tests always produce a 100% accurate result, but their execution time is variable and depends entirely on randomness to find a definitive proof. In short, Monte Carlo tests risk error to guarantee speed, while Las Vegas tests risk speed to guarantee absolute correctness. An example of Monte Carlo test is Miller-Rabin, while an example of Las Vegas is ECPP. The most widely used stochastic tests in practical applications (e.g. cryptography) are Monte Carlo methods due to their exceptional speed and minimal resource usage.
5. Unlike being deterministic (i.e. definitive) or probabilistic, being deterministic or stochastic is not very clear cut, neither conceptually nor practically. Conceptually, there are various types and amounts of randomness, which in some cases blur the difference between deterministic and stochastic. Practically, some stochastic primality tests can be derandomized and made deterministic under suitable assumptions and implementations (and vice versa). This is reflected in the fact that many primality tests have deterministic versions (or variants or flavors or inspirations etc.) and stochastic ones.

7.5.5 General vs Specific

General (or general-purpose) primality tests apply to prime numbers in general, while specific (or special-purpose) tests apply to specific types of prime numbers. We note the following about this classification:

1. The input of a general test is an integer and the output is whether it is prime or not, while the input of a specific test is an integer or prime and the output is whether it is prime of that specific type or not (i.e. composite or prime of different type).
2. We may categorize the primality tests investigated previously (mainly in § 7.3) as follows:
   General: AKS, APR, Baillie-PSW, Division, ECPP, Fermat, Fibonacci, Frobenius, Lucas, Miller-Rabin, Morrison, Pell, Pocklington, Solovay-Strassen, and Wilson.
   Specific: Lucas-Lehmer (for Mersenne), Lucas-Lehmer-Riesel (for Riesel), Pepin (for Fermat), Proth (for Proth).
   In fact, there are many other general and specific primality tests which are "small" (or elementary or unnamed) and hence they are not listed here (see for instance § 7.2 and § 7.3.20).
3. The main advantage of special primality tests is their efficiency in testing the specific prime type (as compared to the corresponding general tests), while their main disadvantage is restriction to that prime type (unlike general tests which work for all primes). In short, special tests trade generality for extreme efficiency.
4. "Specific (or special-purpose) test" may be used to mean a test that applies to a certain type of integers (e.g. by having a certain algebraic form or subject to a given condition) even though the output of the test is a conclusion about primality in general (i.e. whether the tested number is prime or not). Accordingly, tests like the following (for example) are specific: Lucas (requires knowing full prime factorization of $n-1$), Morrison (requires substantial factorization of $n+1$), and Pocklington (requires substantial factorization of $n-1$). Other examples can be easily found.

[699] For most of these tests, we are assuming their implementation with random bases and/or parameters.

7.5.6 Primality vs Compositeness

While "primality tests" nominally determine whether an integer is prime, several methods focus inherently on establishing non-primality, hence functioning strictly as "compositeness tests" (see for instance § 7.2). Rather than serving merely as indirect routes to eliminate primality, compositeness tests can operate as standalone procedures to identify composite numbers (when such identification is required).

Because primality and compositeness are complementary attributes (for integers greater than 1), proving or disproving one property directly implies the status of the other. Accordingly, these methods can be used interchangeably (mainly logically rather than procedurally). As a result, classifying a procedure strictly as a primality test or compositeness test can become artificial and largely dependent on the specific context and objectives (even though in practice these procedures are usually used to detect primality which is the rarer and highly sought-after attribute).

7.5.7 Nature of Tests from Input-Output Perspective

In this subsection we investigate briefly the nature of primality tests from the perspective of their input and output (where "primality tests" here is taken in a very broad sense). In theory, we can identify and classify the main types of primality tests from this perspective as follows:

1. A test whose input is a general integer (i.e. not a specific type of integer) and its output is the general primality (or compositeness) of that integer (i.e. not a specific type of primality). Examples of this include the division and Wilson tests (see § 7.3.4 and § 7.3.19).
2. A test whose input is a specific type of integer and its output is a specific type of primality (or compositeness). Examples of this include the Lucas-Lehmer, Pepin and Proth's tests (see § 7.3.10, § 7.3.15 and § 7.3.17).
3. A test whose input is a general integer and its output is a specific type of primality (or compositeness or negation of that specific type of primality). Examples of this can be found in § 7.3.20 (see for instance Points 1 and 2 of § 7.3.20).
4. A test whose input is a specific type of integer and its output is general primality (or compositeness). Examples of this can be found in § 7.2 (see for instance Points 18 and 19 of § 7.2).
5. A test whose input is a prime number and its output is a specific type of primality (or negation of this type of primality). Examples of this include:
   - Tests like those given in Points 14 and 15 of § 7.3.20.
   - Definition-based tests (if we tolerate such tests; see Point 16 of § 7.1 and Point 28 of § 7.3.20).

7.6 Classifications of Prime Sieves

Like primality tests, prime sieves have several classifications based on their nature or behavior. In the following subsections we outline some of these classifications (subject to the scope and size of this introductory volume).[700]

7.6.1 Algorithmic vs Analytic/Combinatorial

We have briefly discussed this already in the preamble of § 7.4 and hence we focus our attention here on characterizing these two categories. The main characteristics of algorithmic sieves are:

- They are usually deterministic.
- They produce an explicit list of primes up to a given bound (say n).
- They are used heavily in computational number theory and computer science.
- They typically have complexity analyses involving time and memory consumption.

[700] We note that the remarks given in the preamble of § 7.5 broadly apply to classifications of prime sieves as well.

• Their output is the actual set of primes, not information about their density or count (although such information may be derived subsequently).

The main characteristics of analytic/combinatorial sieves are:

⋆ They are primarily theoretical rather than algorithmic.
⋆ They usually estimate the size of sets rather than enumerate their members.
⋆ They often provide upper and lower bounds.
⋆ They are central tools in analytic number theory.
⋆ They are used in problems concerning prime distribution, twin primes, almost-primes, and related topics.

As hinted previously, some analytic/combinatorial sieves originate from the same basic idea as algorithmic sieves by repeatedly and systematically removing multiples of primes. In fact, the combinatorial sieve framework can be viewed as an abstraction of the logic underlying this kind of algorithmic sieves (like the sieve of Eratosthenes; see § 7.4.2). On the other hand, some analytic sieves can be implemented computationally, and some prime-generating algorithms can be analyzed using sieve-theoretic ideas. So we can loosely say: there are algorithmic-based analytic sieves and vice versa (i.e. analytic-based algorithmic sieves). To put it in a different way, ideas frequently move in both directions where analytic sieve methods can formalize and generalize principles and concepts that originated in explicit sieving algorithms, while algorithmic sieves can be developed, refined and optimized using insights and inspirations obtained from analytic sieve theory. This should assert our previous claim that the two categories are intimately linked historically, conceptually and practically, even though their nature and goals are different.

7.6.2 Analytic vs Combinatorial

Analytic and combinatorial prime sieves are two broad approaches in number theory for estimating or detecting primes (or almost-primes) within a set of integers. They share a common goal (which is "sifting out" integers with small prime factors) but differ in philosophy, tools, and typical strength of results. So far we put analytic and combinatorial sieves in one category (against the category of algorithmic sieves) to outline their broad nature as "analytical sieves" versus "computational sieves" (i.e. algorithmic sieves). However, analytic and combinatorial sieves have sufficiently distinct characteristic features to justify treating them as two different categories (or at least sub-categories).

Broadly speaking, analytic sieves use analytic tools to estimate the distribution of integers free of small prime factors (typically producing asymptotic or averaged results), while combinatorial sieves use purely discrete algebraic counting principles (like the principle of inclusion-exclusion) to estimate the size of sets after removing specific arithmetic progressions. An example of analytic sieves is the large sieve (see § 7.4.8), while an example of combinatorial sieves is Brun's sieve (see § 7.4.6).

In fact, the distinction between analytic and combinatorial sieves is not always clear, and hence Selberg's sieve (for instance) may be classified as analytic from certain perspectives and as combinatorial from other perspectives (see § 7.4.10). Similarly, the large sieve (see § 7.4.8) may be classified as analytic by some and as combinatorial by others. This sort of inherent uncertainty can be met in many fields and topics (in mathematics, science, general knowledge, etc.) due to the involvement of many factors and considerations that blur the distinctions.

The main characteristics of analytic sieves (as opposed to combinatorial, rather than algorithmic, sieves) are:

• They use techniques from analysis (e.g. complex analysis, harmonic analysis, L-functions, and integral transforms).
• They estimate counts of primes and show existence of primes in sets (and potentially control almost-primes).
• They focus on average behavior of arithmetic functions rather than combinatorial structure.

• They play a central role in modern results on the distribution of primes and almost-primes.

The main characteristics of combinatorial sieves are:

⋆ They rely on inclusion-exclusion principles, combinatorial identities, arithmetic functions, bounding techniques, and discrete counting arguments.

⋆ They typically produce upper and lower bounds for sifted sets rather than finding sharp asymptotics.

⋆ They focus on counting formulae and inequalities derived from combinatorics.

⋆ They are useful for producing upper bounds and partial results related to problems such as twin primes and primes in arithmetic progressions.

We should finally note that (standard versions of) both analytic and combinatorial sieves suffer from the "parity problem" which is an inherent limitation that prevents them from distinguishing between numbers with an odd or even number of prime factors. Consequently, they cannot detect exact primes without being combined with extra (independent) analytic input.

7.6.3 Computational Complexity

Algorithmic sieves may be classified according to their computational complexity as follows, ordered by asymptotic running time (from slower to faster in theory):

1. Near-linear sieves (mainly traditional sieves like the standard sieve of Eratosthenes; see § 7.4.2) which eliminate composite numbers by marking multiples of known primes. Their time complexities are close to linear, with the standard sieve of Eratosthenes having a complexity of $O(N \log \log N)$ where N is the upper limit of the sieve range.
2. Linear sieves (like the Euler sieve; see § 7.4.3) which optimize the process by ensuring that every composite number is crossed out exactly once. This eliminates the redundant work found in the standard sieve of Eratosthenes and achieves $O(N)$ time complexity.
3. Sub-linear sieves (like an enhanced variant of the sieve of Atkin; see § 7.4.1) which achieve a theoretical time complexity of $O(N/\log \log N)$ by utilizing techniques such as wheel factorization and counting solutions to quadratic forms.

As indicated already, the above order is about theoretical time complexity. However, the practical speed on modern computing facilities often violates this order. For example, in the real world the (segmented) sieve of Eratosthenes regularly beats both Euler's sieve and Atkin's sieve for most reasonable ranges of N. This happens because the sieve of Eratosthenes has remarkable cache locality (i.e. it accesses memory sequentially), whereas Euler's sieve and Atkin's sieve require more complex array indexing, bookkeeping, and data structures that slow down the operation. In conclusion, the gap between theoretical and practical efficiency is one of the defining factors when evaluating prime sieves.

7.6.4 General vs Special

General (or general-purpose) prime sieves are designed to target all prime numbers unconditionally within a continuous range of integers (normally 2 to N), while special (or special-purpose) prime sieves are designed to target primes that fit a highly specific mathematical structure, form, or algebraic sequence.

The main characteristics of general sieves are:

• They scan the entire dense sequence of natural numbers (2, 3,..., N).

• Their purpose is to find every single prime number up to the chosen upper limit N.

• They do not care about the unique properties or algebraic form of individual numbers.

• They typically begin with a broad list of integers and systematically rule out composite numbers by marking multiples of primes.

• Examples of general sieves are: the sieves of Eratosthenes, Atkin and Sundaram (see § 7.4.1, § 7.4.2 and § 7.4.4).

The main characteristics of special sieves are:
⋆ Instead of sifting through all consecutive integers, they adjust the sieving mechanism to exclusively find or isolate numbers that fit a precise algebraic identity or pattern (i.e. they target restricted, sparse subsets of numbers).
⋆ Because they only check numbers belonging to a specific sequence, they can skip vast blocks of integers that a general sieve would waste memory and time processing.
⋆ They exploit structural mathematical shortcuts (benefiting mainly from the properties and forms of numbers).
⋆ Their typical use is in searching for massive primes of certain types and factoring very big integers.
⋆ Examples of special sieves are: the "Lucas-Lehmer Sieve Frameworks", and the "Arithmetic Progression Sieves".[701] We also refer to § 7.4.12 especially with regard to the proposals of type-specific prime sieves in recent research (e.g. those related to twin primes; see Point 5 in § 7.4.12).

Also see § 7.10 with regard to the intimate relationship between prime sieving and integer factorization, and the sieving characteristics of some integer factorization algorithms (refer for instance to § 7.10.5 and § 7.10.11).

7.7 Theorems and Conjectures on Testing and Sieving

Theorems on primality testing and sieving were briefly investigated in § 5.2.10, while open problems and conjectures on testing and sieving were briefly investigated in § 6.2.10. More details about these topics should follow in the upcoming volumes of this book.

7.8 Relationships between Tests and Sieves

In this section we outline common relationships and comparisons between primality tests and sieves,[702] including comparisons among tests, among sieves, and between the two. Some contents also address related issues that inform these relationships and comparisons (rather than focusing directly on them).

7.8.1 Relationships and Comparisons among Tests

The following is a sample of statements about (or related to) relationships and comparisons among primality tests:

1. The detection power of a primality test is its mathematical capability to correctly identify composite numbers. Primality tests vary considerably in their detection power. As an example, the following tests are ordered according to their detection power from weaker to stronger:[703]

   $$\text{Fermat} < \text{Solovay-Strassen} < \text{Miller-Rabin}.$$

   For instance, Carmichael numbers (i.e. absolute pseudoprimes; see § 9.7.1) defeat the Fermat test completely but cannot fool Miller-Rabin test indefinitely. This is because every Carmichael number is a Fermat pseudoprime to every base relatively prime to it, but no composite number is a strong pseudoprime to all such bases.

[701] We use "Lucas-Lehmer Sieve Frameworks" here to refer to the combined use of initial sieving algorithms and advanced primality tests (namely the Lucas-Lehmer test) to efficiently search for Mersenne primes, while we use "Arithmetic Progression Sieves" to refer to sieves deliberately configured to only search for primes hidden inside a specific linear pattern (like $p = kx + 1$). We should note that these (and even "special-purpose sieves") are not really standard sieves in a strict technical sense (even though they incorporate sieving processes). However, our intention of this classification should be justifiable and understandable.

[702] This should be understood more broadly to include testing and sieving (i.e. not only tests and sieves).

[703] This should be justified by the fact that for a fixed base a, the mathematical subset relation among the pseudoprimes (or "liars" which are the composite numbers that fool the test) is:
Fermat pseudoprimes $\supset$ Solovay-Strassen (i.e. Euler) pseudoprimes $\supset$ Miller-Rabin (i.e. strong) pseudoprimes.

2. The relationships between various types of pseudoprimes strongly impact the relationships between probabilistic primality tests. An example of this is already seen in Point 1. Another example (but of different nature) is that the relationship between Miller-Rabin and Lucas pseudoprimes (i.e. being disjoint sets or almost so) is what motivates the Baillie-PSW tests and gives it its extra strength (see § 7.3.3 and Point 1 of § 7.9.5). This example demonstrates that the relationship between pseudoprime categories directly determines the algorithmic strength of combined probabilistic tests (as well as the relative strength of probabilistic tests of the previous point).
3. Multiple probabilistic tests can be combined to form an exceptionally strong hybrid test, as demonstrated by the Baillie-PSW test (see § 7.3.3 and Point 1 of § 7.9.5). However, combining tests does not automatically yield a substantial improvement in detection power. The strength of a hybrid test crucially relies on utilizing individual tests whose mathematical weaknesses are independent or complementary. To be more specific, the effectiveness of a hybrid test depends, in part, on the overlap between the sets of composite numbers that pass its component tests. If two tests have identical sets of pseudoprimes under the specified testing procedures, combining them provides no additional composite-detection power. Conversely, if their pseudoprime sets overlap only partially, the combination can improve detection by eliminating composites that pass one test but fail the other. If the sets are entirely disjoint over the relevant domain, no composite number can pass both tests. The extent of any probabilistic improvement depends on the structure of the overlap and, where randomized tests are involved, on the relevant probability bounds and dependence between test outcomes. Exponential reductions in error probability require additional assumptions, such as suitable independence or conditional error bounds across repeated rounds.
4. Special-purpose (or special-form) primality tests can outperform general-purpose tests when the structure of the number is known and matches the assumptions of the test. However, their applicability is restricted to numbers of the required type (or form). For example, the Lucas-Lehmer and Pepin tests (see § 7.3.10 and § 7.3.15) are substantially more efficient than general-purpose primality tests on Mersenne and Fermat numbers respectively, but cannot be applied to arbitrary integers.
5. In practice, deterministic primality verification over a bounded range can be achieved by establishing rigorous bounds for fixed-base primality tests. Specifically, a probabilistic primality test can be made deterministic (see § 7.5.3) for all integers below a specified threshold if a fixed set of bases or parameters has been proved sufficient to distinguish every prime from every composite number in that range. For example, the Miller-Rabin test (see § 7.3.12) is deterministic for all integers $n < 318665857834031151167461$ when applied to the fixed set of twelve prime bases 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, and 37.[704] This means that the bound 318665857834031151167461 is the smallest composite number that is a strong pseudoprime to all twelve listed prime bases. Consequently, the fixed-base procedure correctly and deterministically identifies every prime and every composite strictly below this bound, assuming a correct implementation.
6. A primality test can be probabilistic unconditionally and deterministic conditionally (i.e. under certain assumptions or conditions). For example, the Miller-Rabin test becomes deterministic under the generalized Riemann hypothesis or by testing a specific finite set of published fixed bases below a certain bound (see § 7.3.12, Point 5 of the present subsection, and Point 3 of § 7.9.5). Similarly, the Solovay-Strassen test is unconditionally probabilistic but becomes deterministic under the generalized Riemann hypothesis with some additional conditions (see § 7.3.18 and Point 4 of § 7.9.5).
7. Although combining multiple probabilistic tests typically yields a more reliable hybrid procedure (see Point 3), it does not inherently produce a deterministic primality test. Determinism requires additional mathematical guarantees, such as a proof that the combined tests reject every composite number in the relevant domain. The same limitation applies to repeated applications of a single probabilistic

[704] See `https://oeis.org/A014233`.

test: under suitable assumptions, independent randomized rounds can reduce the probability of error exponentially, but any finite number of rounds may leave a non-zero error probability unless additional guarantees establish correctness. Also see § 7.9.5.

8. Most modern primality tests essentially try to detect a "witness of compositeness" (i.e. a piece of evidence that the number is not prime). Rather than searching directly for factors, they test mathematical properties that every prime number must satisfy. If one of these properties fails, the failure serves as a witness that the number is composite. For deterministic tests, the absence of a witness implies that the number is definitively prime. For probabilistic tests, the absence of a witness implies only that the number is a probable prime.
9. As indicated previously, the actual computational complexity of prime tests is highly dependent on their individual characteristics and their implementation. Their theoretical computational complexity is just one factor in determining their actual performance. For example, the AKS test (see § 7.3.1) is polynomial-time in theory but it is slower than the ECPP or Miller-Rabin tests for almost all practical n (see § 7.3.5 and § 7.3.12).
10. The reliability of probabilistic primality tests can be quantified by their error bounds. For instance, the Miller-Rabin and Solovay-Strassen tests (see § 7.3.12 and § 7.3.18) achieve guaranteed per-round error probabilities of at most $1/4$ and $1/2$ respectively (showing that Miller-Rabin is stronger than Solovay-Strassen in this sense, as seen earlier in Point 1). In contrast, the Fermat test (see § 7.3.6) has no non-trivial uniform per-round error bound for all composite numbers, confirming its status as the weakest of the three tests.[705] Also see Points 3 and 4 of § 7.9.5.
11. Repeating a probabilistic primality test or increasing the number of rounds to improve confidence can be preferable to using a deterministic algorithm when speed is important and a very small residual error probability is acceptable. For suitable probabilistic tests, such as Miller-Rabin (see § 7.3.12), each additional independent round reduces the upper bound on the probability of incorrectly identifying a composite number as probably prime. Consequently, the error probability can be made arbitrarily small with a computational cost that grows approximately linearly with the number of rounds, although a finite number of rounds does not generally establish primality with mathematical certainty.
12. As indicated already, repeating a probabilistic primality test can increase confidence in the result. If a test has a per-round error probability of at most r, and the rounds are performed independently, then the probability that all k rounds fail to detect a given composite number is at most r^k (i.e. the error probability decreases exponentially with the number of rounds). For example, since the Miller-Rabin test (see § 7.3.12) has a per-round error probability of at most $1/4$ for any odd composite number when the bases are chosen independently and uniformly at random from the standard admissible range, after k independent rounds the probability that the number passes all rounds is at most $(1/4)^k$.
13. Probabilistic tests are often asymmetric (or one-sided), i.e. they are deterministic (or definitive) about compositeness but probabilistic (or uncertain) about primality.[706] In contrast, deterministic tests are definitive about both, i.e. when correctly implemented, they determine whether an integer is prime or composite without probabilistic error.
14. As indicated previously, probabilistic primality tests are typically faster than deterministic alternatives, although the practical performance difference varies with the application, input size, implementation, and required error probability. Furthermore, advances in deterministic algorithms can narrow this gap and, in certain settings, make deterministic methods equally efficient or preferable.

[705] This is because of Carmichael numbers (see § 7.9.2), for which every base coprime to the number is a Fermat liar. Because the error probability for these numbers in this case is 1, rather than being securely bounded below 1, the Fermat test cannot guarantee a non-trivial uniform per-round error bound across all composite numbers.

[706] "Often" accounts for rare exceptions, i.e. while the most famous probabilistic tests (like Miller-Rabin and Solovay-Strassen) are asymmetric, there are rare probabilistic tests that can be symmetric or have two-sided errors (i.e. they are probabilistic about both).

15. Also see the subsections of § 7.5 which contain substantial contents related to relationships and comparisons among tests.

7.8.2 Relationships and Comparisons among Sieves

The following is a sample of statements about (or related to) relationships and comparisons among prime sieves:

1. Algorithmic prime sieves vary in their architecture; the following are the common architectures (which may overlap in design and implementation):
   • Traditional filtering: eliminates composites by marking multiples of known primes sequentially.
   • Structural wheel factorization: skips multiples of small primes (e.g. 2, 3, 5) entirely during initialization to reduce the search space.
   • Segmented processing: divides the range $[2, N]$ into smaller blocks to fit data entirely into the CPU cache.
   • Quadratic forms: uses number-theoretic properties of quadratic forms and modular arithmetic to identify primes by toggling candidate states (rather than explicit division-based primality testing).
2. Referring to Point 1 (also see § 7.6.3), segmented algorithmic prime sieves (most commonly the segmented sieve of Eratosthenes) are a memory-optimized extension of the classic sieves that trade a small amount of extra algorithmic complexity for much better scalability. By dividing the range $[2, N]$ into smaller local blocks (segments) that fit entirely within a computer's high-speed cache memory, it overcomes the severe hardware limitations of the non-segmented versions.[707] For example, the segmented sieve of Eratosthenes can slash memory requirement from linear (or near-linear) to sub-linear (see § 7.6.3).
3. Algorithmic prime sieves vary in their time complexity theoretically and practically. However, it is difficult to order them in a definitive way due to the involvement of various factors.[708] Nevertheless, among the algorithmic sieves of § 7.4 (i.e. Atkin, Eratosthenes, Euler, Sundaram, and wheel) the wheel and Atkin are on the faster side while Sundaram is on the slower side. In any case, the relative performance of these algorithms depends strongly on the implementation and the range of integers being sieved.[709]
4. Algorithmic sieves vary in their space complexity theoretically and practically. However, with reference to the algorithmic sieves of § 7.4, the space complexities are actually much less differentiated than the time complexities. With the potential exception of Atkin, the baseline implementations of these sieves share a linear space complexity of $O(N)$.[710] Consequently, in their comparable forms, these algorithms cannot be meaningfully distinguished asymptotically by memory usage, i.e. differences arise primarily in constant factors and lower-level implementation details.
5. Segmentation and wheel factorization are among the most effective strategies to improve sieving performance. Most practical high-performance sieves use these techniques (frequently in combination).[711]

[707] It is noteworthy that cache-optimized memory behavior can be more important than asymptotic complexity for large-scale prime sieving.

[708] The computational performance of prime sieves depends on both asymptotic complexity and implementation-specific factors such as memory access patterns, cache efficiency, and constant factors.

[709] Generally speaking, for small ranges simple architectures win, while for massive ranges cache-optimization (segmentation) and memory configuration matter more than theoretical big O notation.

[710] With segmentation, space complexity can drop substantially from $O(N)$ to $O(\sqrt{N})$. However, segmentation is essentially an implementation-level factor.

[711] It is worth noting that segmentation fundamentally alters memory usage rather than asymptotic time complexity, which remains essentially unchanged. In other words, it is primarily an optimization of space rather than time, although it can substantially improve practical running time by enhancing cache locality and reducing cache misses. Conversely, wheel factorization is primarily a time-optimization strategy that improves practical performance by reducing the candidate search space. While this optimization does not alter the core asymptotic time complexity of standard sieves, it drastically reduces the constant factor by slashing the absolute number of operations required.

6. Algorithmic sieves are primarily compared in terms of strategy, hardware and software architecture, arithmetic operations, memory layout, cache behavior, and auxiliary outputs. We note that "auxiliary outputs" are additional data structures generated alongside the prime list to support further computations. For example, a *smallest prime factor* (SPF) array enables efficient integer factorization by allowing the prime factors of an integer to be determined through repeated division by its recorded values.
7. Many modern prime-sieving algorithms can be viewed as extensions, refinements, or optimizations of the classical sieve of Eratosthenes. This characterization also applies, to varying degrees, to certain analytic and combinatorial sieving methods, although these may rely on fundamentally different mathematical principles. Despite its ancient origins, the sieve of Eratosthenes remains a fundamental reference algorithm against which many contemporary sieve implementations are theoretically analyzed and practically compared.
8. The following is a sample of comparative examples among specific sieves (both algorithmic and analytic/combinatorial):[712]

   • Atkin is a fast algorithm using modular arithmetic shortcuts, whereas Eratosthenes is conceptually simpler but less optimized (in its standard version). So, Atkin is asymptotically faster than Eratosthenes, although in reality it is often slower for moderate input sizes because its heavier arithmetic and control overhead outweigh its theoretical advantages (unless carefully optimized).

   • While Atkin uses quadratic-residue congruences and modular conditions to toggle primality in a more complex but asymptotically efficient way, Euler (linear sieve) builds primes by ensuring each composite is marked exactly once by its smallest prime factor for a simpler strictly linear-time process.

   • Both Atkin and Sundaram generate primes by excluding composite numbers, but Sundaram achieves this by removing numbers that match the simple algebraic form $i + j + 2ij$, while Atkin uses complex binary quadratic forms and modular arithmetic to optimize performance (trading Sundaram's simplicity for superior asymptotic speed).

   • Both Atkin and Wheel reduce the set of candidate integers using modular arithmetic and residue classes, but Wheel is a simpler pre-sieving technique that removes multiples of small primes via repeating modular patterns, whereas Atkin is a more sophisticated full prime-finding algorithm that uses quadratic residue conditions to classify remaining candidates as prime or composite.

   • Eratosthenes is a straightforward elimination procedure for marking composites, whereas Euler (linear sieve) is an optimized algorithm that processes each composite exactly once using smallest prime factor structure.

   • Both Eratosthenes and Sundaram are systematic elimination processes, but Sundaram identifies odd primes indirectly by removing numbers of the form $i + j + 2ij$, rather than eliminating multiples as in Eratosthenes. Accordingly, Sundaram requires no prime multiplication, unlike Eratosthenes which strictly steps through prime multiples.

   • Standard Eratosthenes initializes a candidate list of all integers (2 to N), while Wheel improves efficiency by constructing a wheel from small primes and considering only numbers coprime to their product. This eliminates all numbers divisible by those small primes before sieving begins, reducing the size of candidate pool and the amount of required work.

   • Brun yields upper (and sometimes lower) bounds for prime patterns, while Eratosthenes deterministically enumerates all primes up to a given limit without approximation.

   • Brun is a classical combinatorial sieve that primarily produces upper bounds for sets of integers with prescribed prime restrictions (famously applied to twin primes), while Harman is a more modern analytic technique that combines sieve ideas with harmonic analysis to obtain fine distribution results for

[712] There are many such comparative examples among specific sieves (i.e. listing them is not practical within our scope and space). This sample should provide a taste of the kind of relationships and comparisons among sieves.

primes (particularly in short intervals and related settings).

• Selberg directly refines and generalizes the core concept of Brun while sharpening its error terms and resulting bounds. Selberg is widely recognized for producing cleaner, more precise upper bounds than Brun's pure combinatorial method.

• Legendre applies the inclusion-exclusion principle to count primes by subtracting multiples of small prime factors, but it fails for large limits due to accumulation of error terms. Selberg resolves this issue by substituting exact inclusion-exclusion weights with optimized quadratic weights.

• Legendre is based on exact inclusion-exclusion to count integers avoiding small prime factors, but the number of inclusion-exclusion terms grows rapidly, making the method computationally unwieldy and difficult to adapt with controlled errors. Turan instead replaces exact counting with averaging and second-moment estimates, yielding more manageable bounds for average behavior.

• Turan emphasizes average-case bounds via probabilistic methods, whereas Selberg is variational in nature and optimizes a quadratic form.

9. Also see the subsections of § 7.6 which contain substantial contents related to relationships and comparisons among sieves.

7.8.3 Relationships and Comparisons between Tests and Sieves

The following is a sample of statements about (or related to) relationships and comparisons between primality tests (on one hand) and sieves (on the other):[713]

1. Prime sieves are inherently bulk-processing (or batch) algorithms, computing primality information for many integers simultaneously. On the other hand, primality tests are inherently single-instance algorithms, evaluating one candidate integer at a time.
2. The intimate relationship between primality testing and sieving can be seen both conceptually and practically. Sieves determine the primality status of many integers simultaneously by exploiting shared divisibility information, which may be viewed as implicitly carrying out a large number of primality determinations (i.e. "tests") in a single operation. Conversely, one can generate (or "sieve") the primes in a range such as $[2, N]$ by applying a primality test to each integer individually and collecting those that are prime, although this is generally a much less efficient approach than dedicated sieving algorithms.
3. Hybrid approaches further illustrate the close relationship between primality testing and sieving. For example, wheel factorization and small-prime sieving are frequently integrated directly into primality testing algorithms to eliminate obvious composites efficiently, while pre-computed sieves are often used as a pre-processing step to accelerate the primality testing process. In practice, many modern number-theoretic algorithms combine both paradigms: sieves to exploit small-scale arithmetic structure, and dedicated primality tests to verify individual large candidates.
4. The choice between primality testing and sieving depends on the application. Tests are generally preferable for isolated or sparse primality queries, very large integers (such as those encountered in cryptography), and memory-constrained environments, whereas sieves are typically more efficient when many queries must be answered within a bounded range, when a complete list of primes or factorization data is required, or when conducting computational number-theoretic experiments.[714]
5. Probabilistic primality tests and prime sieves serve complementary (rather than competing) roles in practice: sieves are typically used to efficiently enumerate all primes up to a moderate bound, while probabilistic tests are used to quickly determine the primality of individual large integers. Together, they form distinct but often combined tools for handling primes across different computational regimes.
6. Nearly all prime sieves exploit the fact that every composite number has a prime factor $p \leq \sqrt{N}$.

[713] As indicated previously, "tests and sieves" includes "testing and sieving".

[714] Computational investigations of prime gaps, twin-prime distributions, and problems such as Goldbach's conjecture often employ high-performance sieving, particularly when examining large intervals.

By marking multiples of such small primes, they can eliminate all composites up to N. In contrast, primality tests need not rely on explicitly searching for small factors. Some tests (like AKS) determine primality using algebraic properties that characterize primes. Thus, while the "small prime factor" principle (i.e. $p \leq \sqrt{N}$) underlies most sieve algorithms, it is not a necessary ingredient of primality testing in general.

7. Despite their distinction, tests and sieves can be interdependent. For example, sieving algorithms may use primality tests to verify boundary cases or handle numbers outside the main sieve structure, while primality tests may use sieving techniques to quickly eliminate small prime factors before performing more complicated checks.
8. Primality tests are optimized for checking individual large numbers efficiently, while sieves trade extra memory for speed when generating many primes up to a limit.[715] For a large contiguous range of integers, a sieve is typically much faster than applying individual primality tests to each number.
9. A probabilistic primality test may "incorrectly" classify a composite number as a probable prime, but a correctly implemented conventional prime sieve will never include a composite number in its final output. In this sense, sieves are deterministic (or definitive) algorithms.
10. Primality tests scale primarily with the size (bit-length) of the numbers being tested, whereas sieves scale primarily with the size of the range over which primes are being generated.
11. Sieves achieve low average computational cost per integer when generating primes over intervals, whereas isolated large-number primality queries are generally better handled by dedicated primality tests.
12. Sieves exploit arithmetic structure shared across many integers in a range, whereas primality tests analyze the arithmetic structure of a single candidate integer.
13. Loosely speaking, the trial division technique sits at the intersection of both worlds (i.e. tests and sieves), acting as the most basic primality test while functionally operating like a miniature inverted sieving mechanism. Also see § 7.3.4 and § 7.10.12.

7.9 Topics Related to Primality Testing and Sieving

We outline in this section some common topics in number theory related to primality testing and/or sieving.

7.9.1 Almost-Primes in Testing and Sieving

Almost-primes (see § 9.6) play an important role in sieve methods (and computational number theory in general). In sieve theory, sets of almost-primes appear naturally as the near misses left after removing multiples of small primes, and this makes them central objects in certain sieving techniques (like the Brun and Selberg sieves; see § 7.4.6 and § 7.4.10) to approximate the distribution of primes. They are also important in primality testing, where composite numbers with no small prime factors (often including almost-primes with large factors) are among the most challenging cases for algorithms to distinguish from true primes.

7.9.2 Carmichael Numbers

We briefly discussed or mentioned Carmichael numbers in several places of this book (see for instance § 5.1.15 and § 9.7.1). Carmichael numbers represent a key obstruction to Fermat-based primality testing methods because they are composite numbers that mimic primes by satisfying Fermat's little theorem for all coprime bases. Their existence explains why simple Fermat-based testing and sieving procedures fail to reliably distinguish primes from composites. Regarding the abundance and distribution of Carmichael

[715] In simple words, tests avoid memory cost of sieves, while sieves reduce need for repeated tests.

numbers (which are related to sieving as well as testing), although there are infinitely many Carmichael numbers, they are extremely rare compared to prime numbers as counted by $\pi(x)$.[716] Furthermore, Carmichael numbers form a subset of the Fermat pseudoprimes to any fixed base (see § 9.7.6), and are therefore less numerous than the pseudoprimes to that base.

7.9.3 Riesel Problem and Number

The Riesel problem (which is a famous open problem in number theory) is a quest to find the smallest Riesel number where "Riesel number" is defined as an odd positive integer k for which $2^n k - 1$ is composite for all $n \in \mathbb{N}$. It is conjectured that the smallest Riesel number is 509203 (which is currently the smallest known Riesel number). The Riesel problem is closely related to primality testing and sieving. In short, the Riesel problem relies on sieving to eliminate composite candidates in sequences of $2^n k - 1$ and on specialized primality testing (such as Lucas-Lehmer-Riesel test; see § 7.3.11) to determine whether any remaining terms are prime. It is proven that there are infinitely many Riesel numbers. More specifically, it is proven that every integer of the form $509203 + 11184810m$, where m is a non-negative integer, is a Riesel number.

7.9.4 Sierpinski Problem and Number

This is a famous challenge in number theory that asks for the smallest Sierpinski number where "Sierpinski number" is defined as an odd positive integer k for which $2^n k + 1$ is composite for all $n \in \mathbb{N}$. It is conjectured that the smallest Sierpinski number is 78557 (which is currently the smallest known Sierpinski number). While the Sierpinski problem does not superficially appear to be about the testing and sieving of primes, it is deeply interconnected with both. In short, massive-scale sieves are used to exploit algebraic covering sets and eliminate bulk composite candidates, while specialized single-instance primality tests (such as Proth's test; see § 7.3.17) are used to search for the elusive counterexample primes that disqualify the remaining k values. It is proven that there are infinitely many Sierpinski numbers. More specifically, it is proven that every integer of the form $78557 + 140100870m$, where m is a non-negative integer, is a Sierpinski number. It is obvious that the Sierpinski problem is a twin to the Riesel problem, i.e. these problems are about the smallest odd positive integers k for which $2^n k \pm 1$ are composite for all $n \in \mathbb{N}$.

7.9.5 Pseudoprimes in Testing and Sieving

In primality testing, pseudoprimes (see § 9.7) represent the main cause of failure of probabilistic algorithms like the Fermat test (see § 7.3.6). Because these numbers fool basic primality checks, elaborate algorithms that use multiple bases or stronger variants are required to filter them out. In sieving processes, basic sieving techniques are employed first to eliminate obvious composite numbers before more advanced testing and sieving methods are applied to remove pseudoprimes.

In the following remarks we briefly discuss (within specific examples) an important aspect of pseudoprimes in their relation to primality testing and sieving; specifically, how mathematicians use the unique structural properties of specific pseudoprimes to create highly accurate primality tests (and potentially sieving procedures):

1. The Baillie-PSW test (see § 7.3.3) may be the ultimate application of using pseudoprime properties as a primality sign by combining two strong probabilistic primality tests that largely have mutually exclusive pseudoprime properties (i.e. a Miller-Rabin test to base 2, and a Lucas sequence test). Strong pseudoprimes to base 2 and strong Lucas pseudoprimes have fundamentally different structural requirements to fool these tests, and hence there are no known composite numbers that possess the

[716] For example, below 10^{22}, there are more than 2.0×10^{20} prime numbers, but only about 5.0×10^7 Carmichael numbers. See `https://oeis.org/A006880` and `https://oeis.org/A055553`.

properties required to be a pseudoprime for both tests simultaneously. Therefore, an integer that simultaneously passes both tests is almost certainly prime (even though it is not proven theoretically). In short, although the Baillie-PSW test is theoretically unproven to be a definitive test for all integers, it serves as a highly reliable primality test for numbers up to thousands of digits. Also see Point 8 of 6.2.3 and Point 41 of 6.2.4.

2. Carmichael numbers are possibly the most prominent example of pseudoprimes (see for instance § 5.1.15, § 7.9.2 and § 9.7.1). According to Korselt's criterion, a composite number n is a Carmichael number *iff* it is square-free and, for every prime divisor p of n, the number $p-1$ divides $n-1$. Although checking this structural property directly is computationally expensive (because it requires factorization), understanding this algebraic structure allows us to construct (or identify) large Carmichael numbers. This should help identify the worst failures of the Fermat primality test (and hence guide the development of more robust primality testing algorithms that successfully avoid the trap of these exceptional composites).
3. Strong pseudoprimes are odd composite integers that pass the Miller-Rabin primality test for a specific base a (see § 7.3.12 and § 9.7.12). It is proven that an odd composite number $n \neq 9$ can be a strong pseudoprime for at most 25% of all possible bases $1 \leq a < n$ coprime to n. So, by choosing k random bases independently the probability that a composite number is a strong pseudoprime for all of these bases drops exponentially to (at most) 0.25^k. Accordingly, running this test sufficiently many times reduces the chance of accidentally accepting a pseudoprime to virtually zero (which is safe enough for many practical applications like cryptographic key generation). This means that the structural property of strong pseudoprimes (represented by the 25% rule) is crucial for determining the reliability of the Miller-Rabin test theoretically and practically. In fact, some implementations use a fixed set of carefully chosen bases (rather than random ones), and hence for bounded ranges this can make the test completely deterministic.
4. Euler-Jacobi pseudoprimes are odd composite integers that pass the Solovay-Strassen primality test for a specific base a (see § 7.3.18 and § 9.7.4). It is proven that an odd composite number n can be an Euler-Jacobi pseudoprime for at most 50% of all possible bases $1 \leq a < n$ coprime to n. So, by choosing k random bases independently the probability that a composite number is an Euler-Jacobi pseudoprime for all of these bases drops exponentially to (at most) 0.5^k. Much like the Miller-Rabin test discussed in Point 3, executing this check sufficiently many times reduces the probability of accepting a pseudoprime to virtually zero, and employing a fixed set of carefully chosen bases similarly allows for a completely deterministic test within bounded ranges.
5. Frobenius pseudoprimes in their relation to the Frobenius test (see § 7.3.8 and § 9.7.8) are similar to strong/Euler-Jacobi pseudoprimes in their relation to the Miller-Rabin/Solovay-Strassen tests (see Points 3 and 4). However, the error probability (per test) of the Frobenius test (or rather a variant of this test) is much smaller than that in these tests (i.e. 1/7710 for Frobenius versus 1/4 for Miller-Rabin and 1/2 for Solovay-Strassen), and hence it is harder for a composite number to be a Frobenius pseudoprime (i.e. to pass the Frobenius test). So, this is a case where a stricter pseudoprime structural property directly yields a stronger primality test.

7.9.6 Prime Factorization of Large Numbers

One of the central problems in computational number theory is the efficient factorization of very large integers into their prime factors. Integer factorization is closely connected with primality testing and with sieving techniques used in many factorization algorithms. This problem also has major implications in cryptography, particularly in public-key encryption systems such as RSA (see § 10.1). Although sophisticated algorithms exist for factoring very large integers, such as the general number field sieve (commonly known as GNFS; see § 7.10.5), no classical general-purpose algorithm is currently known that can perform

integer factorization in polynomial time. The complexity of factorization remains an important open question, with ongoing research producing improved algorithms and partial results. Also see § 7.10.

7.10 Factorization Algorithms

Primality testing and sieving and integer factorization represent distinct but deeply interconnected pillars of computational number theory. Primality tests (like Miller-Rabin; see § 7.3.12) and sieving methods (like the sieve of Eratosthenes; see § 7.4.2) function as filters, where sieves efficiently isolate all prime numbers within a broad range (through eliminating composites in that range), while primality tests determine whether a single isolated integer is prime or not without revealing its factors. On the other side, prime factorization algorithms (like the general number field sieve; see § 7.10.5) solve the inherently harder problem of breaking a composite number down into its constituent prime building blocks. The relationship between them is generally interdependent and mutually beneficial. For example, factorization algorithms rely on primality testing as a termination condition to verify when an extracted factor cannot be broken down further, while factorization techniques frequently employ optimized trial division using sieved prime lists in their initial stages to quickly find out small prime factors before using more complex techniques to complete the factorization task.

Overall, primality testing, sieving and factorization share a considerable amount of theoretical and practical frameworks (represented mostly by theorems and techniques) to achieve their objectives and benefit each other. Accordingly, in modern computational number theory these areas are intertwined through shared reliance on common mathematical and computational tools (such as modular arithmetic and prime distribution insights) as well as through their common goals. This intimate relationship can also be found in practical areas (like cryptography; see § 10.1) which benefit from all these areas to achieve their objectives.

Based on this introduction, it is natural for us to investigate integer factorization algorithms within this chapter (which is primarily about primality testing and sieving). In the following subsections we will investigate, rather briefly, common examples of factorization algorithms. However, before we go through these details we should note the following remarks:

1. In line with what we said already about the close relationship between primality testing, sieving and factorization, some of the following integer factorization algorithms may also be classified as sieving algorithms (and some are even labeled as such; see for instance § 7.10.5 and § 7.10.9). So, these algorithms may also be listed within the sieves of § 7.4.
2. Integer factorization algorithms are commonly divided into two broad categories: general-purpose algorithms and special-purpose algorithms. The running time of a general-purpose algorithm depends primarily on the size of the integer being factored and does not rely on any special properties of its factors. In contrast, the running time of a special-purpose algorithm depends on specific properties of the integer or of one of its (initially unknown) factors, such as factor size, smoothness, or special algebraic form. The particular properties that influence the running time vary from one algorithm to another.
3. Among the integer factorization algorithms that we listed here we may classify the following algorithms as general-purpose: the continued fraction factorization, Dixon's factorization method, the general number field sieve, the multiple polynomial quadratic sieve, the quadratic sieve, and Shanks' square forms factorization. Similarly, we may classify the following algorithms as special-purpose: the elliptic curve method, Fermat's factorization method, Pollard's rho algorithm, Pollard's $p-1$ algorithm, the special number field sieve, the trial division, and Williams' $p+1$ algorithm.[717]

[717] Some authors describe Pollard's rho as a general-purpose algorithm because it does not require any special algebraic structure in the input number. However, in the standard factorization literature it is more often grouped with special-purpose algorithms because its running time is governed by the size of the smallest factor rather than the total size

4. Integer factorization algorithms can be categorized as deterministic or randomized. Deterministic algorithms follow a fixed sequence of operations for a given input and parameters, while randomized algorithms incorporate random choices that can affect the execution path and running time. Deterministic algorithms include: the continued fraction factorization (but can be randomized), Fermat's factorization, Pollard's $p-1$ (but can be randomized), the quadratic sieve (but can be randomized), Shanks' square forms factorization, the trial division, and Williams' $p+1$ (but can be randomized). Randomized algorithms include: the elliptic curve factorization, Dixon's factorization, the general number field sieve, the multiple polynomial quadratic sieve, Pollard's rho, and the special number field sieve.[718]
5. Our discussion here of integer factorization is within the framework of classical computing (not quantum computing) and hence all the listed algorithms and their details (such as their classification into general-purpose and special-purpose) should be understood within this context. In short, we are interested here only in classical factorization algorithms (noting that non-classical algorithms, such as Shor's algorithm, fall outside the scope of this chapter and may be considered in future volumes).
6. Most factorization algorithms are mathematically sophisticated and often require substantial background material to be presented in full. Since such a treatment would be inconsistent with the intended scope and length of this introductory volume, we limit ourselves here to brief outlines with only minimal explanations. Detailed discussions of these algorithms, together with additional factorization methods, will be presented in subsequent volumes.

7.10.1 Continued Fraction Factorization

This (commonly abbreviated as CFRAC) is a general-purpose integer factorization algorithm that can be viewed conceptually as a refinement of the approach underlying Dixon's method (see § 7.10.2), although it predates Dixon's method historically. The algorithm is based on finding certain congruent squares modulo n (where n is the composite integer to be factored) by using the continued fraction expansion of $\sqrt{n}$. CFRAC was one of the fastest general-purpose factoring methods until it was superseded by the emergence of other more efficient factorization methods (such as the quadratic sieve and the general number field sieve; see § 7.10.9 and § 7.10.5).

In more formal terms, the primary goal of CFRAC is to find two integers x and y such that $x^2 \overset{n}{=} y^2$ where $x \overset{n}{\neq} \pm y$. This search is conducted by generating many intermediate congruences of the form $A_k^2 \overset{n}{=} r_k$ via the continued fraction expansion of $\sqrt{n}$, which are then combined using linear algebra to form perfect squares. Once x and y are constructed from these combined relations, then computing $\gcd(x-y,n)$ or $\gcd(x+y,n)$ often yields a non-trivial factor of n. The theoretical justification of this is the identity $x^2-y^2=(x-y)(x+y)$ and hence $n|(x-y)(x+y)$.

The algorithm of CFRAC may be outlined as follows:

1. Generate the continued fraction expansion of $\sqrt{n}$.
2. Form convergents and residues: for each convergent, compute the numerator A_k and the associated residue r_k satisfying $A_k^2 \overset{n}{=} r_k$.
3. Collect smooth relations: search for residues r_k that are B-smooth (i.e. factor completely over a chosen factor base of small primes). Track the sign of each residue separately or include -1 in the factor base.

---

of the integer. A similar disparity may be encountered in the classification of Shanks' square forms factorization. In general, being general-purpose or special-purpose is not a very clear-cut issue (at least in some cases and instances) due to the involvement of various factors and considerations, and hence this classification should be understood broadly.

[718] In some cases, the classifications are not clear-cut due to conceptual and/or algorithmic disparities and variations (both during formulation and implementation) which can also be reflected in personal viewpoints and interpretations. For example, the multiple polynomial quadratic sieve and the quadratic sieve may be classified as deterministic algorithms implemented with randomized heuristics. We should also note that in practice, many modern implementations of factorization algorithms introduce randomization to improve performance, even when the underlying algorithm is essentially deterministic.

4. Construct exponent vectors: express each smooth residue as $r_k = \prod_{p_i \in B} p_i^{e_{i,k}}$ (including the sign factor if -1 is in the factor base) and record the exponent vector $(e_{1,k}, e_{2,k}, \ldots)$ modulo 2.
5. Assemble the exponent vectors into a matrix (over the finite field $\mathbb{F}_2$).
6. Use linear algebra (e.g. Gaussian elimination modulo 2) to find a non-trivial linear dependency among the exponent vectors modulo 2.
7. Combine the corresponding relations $\prod A_k^2 \overset{n}{=} \prod r_k$ (which essentially represents $x^2 \overset{n}{=} y^2$ with $x \overset{n}{=} \prod A_k$ and $y \overset{n}{=} \sqrt{\prod r_k}$, provided that the product of the selected residues is a non-negative perfect square). If the condition $x \overset{n}{\neq} \pm y$ is not satisfied, the resulting congruence of squares yields only trivial gcd and another dependency must be tried.
8. Calculate $\gcd(x - y, n)$ and/or $\gcd(x + y, n)$
9. If either gcd is strictly between 1 and n, then it is a non-trivial factor of n.

7.10.2 Dixon's Factorization Method

This method belongs to the family of *congruence of squares* factorization algorithms, extending the idea underlying Fermat's factorization method (see § 7.10.4) and may be regarded as a precursor to the modern quadratic sieve (see § 7.10.9). It uses a "factor base" of small primes to find a combination of relations that form a perfect square. Historically, it was the first factorization algorithm with a rigorous sub-exponential expected running-time bound.

The basic strategy of this method is to find a congruence of squares modulo n (i.e. the integer to be factored), aiming to identify two integers X and Y such that $X^2 \overset{n}{=} Y^2$ where $X \overset{n}{\neq} \pm Y$. Once found, the greatest common divisor $\gcd(X - Y, n)$ or $\gcd(X + Y, n)$ yields a non-trivial factor of n with a considerable success rate.[719] As we see, this strategy is similar to that of CFRAC and ultimately to Fermat's (see § 7.10.1 and § 7.10.4).

The algorithm of Dixon's factorization method may be outlined as follows (where we are supposed to factorize a composite integer n):

1. Choose a factor base $B = \{p_1, p_2, \ldots, p_k\}$ consisting of all small primes up to a chosen smoothness bound.[720]
2. Find smooth values by choosing integers x_i uniformly at random modulo n and compute $r_i \overset{n}{=} x_i^2$, retaining only those r_i values that are B-smooth (noting that r_i denotes the least non-negative residue modulo n).
3. Express each r_i as a factorization over B, and form the corresponding exponent vectors modulo 2.
4. Use Gaussian elimination modulo 2 to find a non-trivial linear dependency.
5. Construct the congruence of squares by letting $X = \prod_{i \in S} x_i$ and $Y^2 = \prod_{i \in S} r_i$ where S is the selected dependent subset. The dependency ensures that the product of the selected residues is a perfect square, so Y is an integer and $X^2 \overset{n}{=} Y^2$.
6. Compute the greatest common divisors $d_1 = \gcd(X - Y, n)$ and $d_2 = \gcd(X + Y, n)$.
7. If $1 < d_j < n$ ($j = 1$ or 2), then d_j is a non-trivial factor of n. Otherwise, try another dependency or collect additional smooth relations.

7.10.3 Elliptic Curve Method

This (commonly abbreviated as ECM and developed by Lenstra) is a fast (sub-exponential) algorithm used to find small prime factors of large composite integers. Its running time depends primarily on the

[719] For semiprimes with two distinct prime factors, a randomly generated congruence of squares has a probability of approximately 1/2 of being non-trivial under the usual assumptions. Once such a congruence is obtained, at least one of $\gcd(X - Y, n)$ and $\gcd(X + Y, n)$ yields a non-trivial factor of n.

[720] We note that basic Dixon's method does not restrict the base only to primes where n is a quadratic residue modulo p_i.

size of the prime factor being sought, rather than the size of the composite number itself. It serves as a powerful generalization of Pollard's $p-1$ algorithm (see § 7.10.8) by replacing the multiplicative group used in Pollard's algorithm with the group of points on an elliptic curve. As one of the most effective special-purpose factoring methods, ECM is typically capable of finding prime factors in the range of about 50-60 digits (depending on computational resources and the probability of success).

The algorithm can be outlined as follows (where n is the composite integer to be factored):

1. Choose a random elliptic curve E over $\mathbb{Z}/n\mathbb{Z}$ $\left[\text{i.e. } E : y^2 \equiv x^3 + ax + b \pmod{n}\right]$ with a point P on it (i.e. $P \in E$) where the discriminant $\Delta = 4a^3 + 27b^2 \not\equiv 0 \pmod{n}$.
2. Pick a smoothness bound B.
3. Compute a large multiplier $k = \prod_{q \leq B} q^{\lfloor \log_q B \rfloor}$, where the product is over primes q.
4. Compute point multiplication $Q = kP$.[721]
5. Check modular inverses: during the elliptic-curve addition steps, a modular inverse of a denominator d modulo n may be required.[722]
6. Whenever an inverse is required: calculate $g = \gcd(d, n)$. If:
   $1 < g < n$: g is a non-trivial factor of n.
   $g = n$: the computation fails for this curve and point. Choose a new curve or point and restart.
   $g = 1$: continue the double-and-add computation.
7. If the entire point multiplication (i.e. $Q = kP$) completes and every required denominator is coprime to n (so that every corresponding gcd equals 1), the curve has failed to find a factor. Choose a new curve or point and restart.

7.10.4 Fermat's Factorization Method

This method factorizes an odd composite integer n by expressing it as the difference of two squares (i.e. $n = x^2 - y^2$) which immediately yields the algebraic factors $n = (x - y)(x + y)$. This method is based on the fact that every odd integer can be represented as a difference of two squares (noting that for an odd prime n, this representation yields only the trivial factorization $1 \times n$), and hence the method searches for values x and y such that $y^2 = x^2 - n$ (which is just reordering of $n = x^2 - y^2$). Once found, the aforementioned factorization is achieved. This technique is highly efficient when n is a semiprime whose two prime factors are positioned close to each other, as the value of x will be just above the square root of n, which requires very few attempts to find.

The algorithm of this method may be outlined as follows:

1. Set $x = \lceil \sqrt{n} \rceil$.
2. Compute $x^2 - n$.
3. If $x^2 - n$ is a perfect square y^2 then $n = (x - y)(x + y)$ which is the required factorization.
4. Otherwise, increase x by 1 and repeat.

It is worth noting that if n is a prime number, the algorithm will not find a perfect square until $x = (n + 1)/2$, resulting in a trivial factorization of $1 \times n$. For large integers, this creates a massive loop that is highly inefficient. In practical implementations, a termination threshold (such as a maximum number of iterations or a check against other trial division methods) should be added to prevent excessive computation. We also note that if n is even, then one may first factor out all powers of 2, writing $n = 2^k m$ with m odd. Fermat's factorization method can then be applied to the odd component m. Since extracting powers of 2 is trivial, the method can thus be used indirectly for even composite integers.

Finally, it is worth noting that CFRAC (see § 7.10.1) is conceptually related to Fermat's factorization

[721] This step is typically executed using the standard double-and-add algorithm for elliptic curve point addition.

[722] In elliptic curve arithmetic, adding or doubling points involves computing a fraction. The denominator d represents the bottom of this fraction. Dividing by d modulo n requires finding its modular inverse, which motivates the $\gcd(d, n)$ check.

method because both methods exploit the idea of representing information about n through squares. In Fermat's method we directly search for integers x and y such that $x^2 - y^2 = n$ which immediately yields the factorization $n = (x - y)(x + y)$, while in CFRAC we elaborate and generalize this idea by using the continued fraction expansion of $\sqrt{n}$ to generate relations that can be combined to obtain a congruence of squares modulo n, from which non-trivial factors can be extracted using $\gcd(x - y, n)$. More broadly, conceptual connections of this kind are common among integer factorization methods, which often adapt, refine, or extend mathematical ideas underlying earlier techniques. Further examples of these similarities and conceptual connections will be encountered in the future.

7.10.5 General Number Field Sieve

This (abbreviated as GNFS) is the fastest known general-purpose classical algorithm for factoring very large integers (especially those with no special structure or form). It is widely used in computational number theory and cryptography (particularly when analyzing the security of cryptosystems like RSA which rely on the difficulty of factoring large composite numbers). Thanks to its efficiency, this algorithm is regarded as the primary threat to the RSA keys of insufficient size. Generally speaking, this algorithm takes a large composite number (often hundreds of digits long) and finds its prime factors through a series of mathematical and computational processes (mainly: polynomial selection, sieving, filtering, applying linear algebra operations, and square rooting).[723]

Unlike the special number field sieve (see § 7.10.11), which exploits the special algebraic structure of certain integers to achieve improved factoring performance, the general number field sieve can be applied to large composite integers in general without requiring such a special form. It is also worth emphasizing that, despite the word "sieve" in its name, GNFS is fundamentally an integer factorization algorithm rather than a sieve for generating or identifying prime numbers. Nevertheless, classifying it as a sieve (in the sense of sieve-based factorization method) is entirely appropriate because sieving is a central stage of its procedure (as indicated already).

The algorithm of GNFS may be outlined (broadly and loosely) as follows (where n is the integer to be factored):

1. Polynomial selection: choose a linear polynomial and a nonlinear irreducible polynomial with a common root modulo n to define the rational and algebraic number fields.
2. Factor base construction: define rational and algebraic factor bases using small primes and prime ideals to test for smoothness.
3. Sieving/Relation collection: find coprime pairs (a, b) where both the rational value $a - bm$ and the algebraic norm are smooth (recording each successful pair as a relation).
4. Relation accumulation: collect sufficiently many relations to obtain a non-trivial linear dependency among their exponent vectors modulo 2.
5. Linear algebra stage: build a large sparse matrix over the finite field $\mathbb{F}_2$ from exponent vectors and solve for non-trivial dependencies.
6. Square construction: combine the found dependencies to generate congruent squares across the rational and algebraic domains.
7. Square root stage: compute the corresponding square roots in both number fields and translate them into a congruence of squares modulo n, i.e. $x^2 \overset{n}{=} y^2$.
8. Factor extraction: compute $\gcd(x - y, n)$ and $\gcd(x + y, n)$. If either gcd is strictly between 1 and n, it is a non-trivial factor of n.

[723] It is reported that GNFS has been used in practice to factor integers of up to approximately 270 decimal digits in large-scale record computations. While there is no strict cutoff limit, the computational cost grows extremely rapidly, making significantly larger factorizations infeasible with current classical hardware and resources. This is why sufficiently large RSA keys remain secure under present classical attacks.

9. Iteration: if both gcd yield only trivial values (i.e. 1 or n), repeat the process using a different dependency.

7.10.6 Multiple Polynomial Quadratic Sieve

This (usually abbreviated as MPQS) is an advanced algorithm used to factor large composite integers, typically ranging between 40 to 100 decimal digits. It was developed as an improved version of the quadratic sieve (see § 7.10.9). While both algorithms share the same underlying mathematical foundation, MPQS improves on the QS by dynamically switching between multiple quadratic polynomials (instead of relying on a single one) to keep numerical values small, and this greatly increases the efficiency of the sieving stage. Historically, MPQS demonstrated substantial improvements over the basic QS, with published results reporting more than an order of magnitude reduction in sieving effort under particular implementations and conditions. However, its practical performance depends on the implementation, input size, and computing environment.

The basic idea of MPQS is to search for (x, y) values satisfying $x^2 \overset{n}{=} y^2$ with $x \overset{n}{\neq} \pm y$ (or rather constructing such a congruence of squares) where n is the integer to be factored. If found then a factor of n can be obtained using $\gcd(x - y, n)$ or $\gcd(x + y, n)$. In practice, MPQS constructs such congruences by collecting and combining relations obtained from values of multiple quadratic polynomials. The use of multiple polynomials (instead of one as in QS) allows the sieve to generate values that remain small in magnitude over the sieving interval, making them more likely to be smooth and thereby significantly increasing the rate at which useful relations are found.[724]

The algorithm of MPQS can be outlined as follows:

1. Select small primes p (as factor base) such that $\left(\frac{n}{p}\right) = 1$ where $\left(\frac{n}{p}\right)$ is the Legendre symbol and p is an odd prime not dividing n. The factor base also accounts for the prime 2, when appropriate, and negative values through the factor -1.
2. Choose A and B such that $B^2 \overset{A}{=} n$ and define the polynomial $Q(s) = As^2 + 2Bs + C$, where $C = \frac{B^2 - n}{A}$ (noting that the congruence condition ensures that C is an integer). This satisfies the congruence $(As + B)^2 \overset{n}{=} AQ(s)$.
3. Search for values of s for which $Q(s)$ factors completely over the factor base, accounting for signs and any special cases. These factorizations yield (smooth) relations for the factorization process.
4. Gather sufficiently many smooth relations, typically more than the number of primes in the factor base, to obtain linear dependencies among their exponent-parity vectors.
5. Represent the prime exponents modulo 2 and solve the resulting homogeneous linear system over Galois field 2 to identify subsets of relations whose combined prime exponents are all even.
6. Construct $x^2 \overset{n}{=} y^2$ and calculate $\gcd(x - y, n)$ and $\gcd(x + y, n)$.
7. If either gcd is strictly between 1 and n, it gives a non-trivial factor of n. Otherwise, try another dependency.

Finally, although the multiple polynomial quadratic sieve is an integer factorization algorithm, its core computational phase is a sieving process. The sieve is used to identify smooth polynomial values, from which relations are collected and combined to construct a congruence of squares, ultimately enabling the factorization of the composite integer into its prime factors. Thus, the "sieve" label in its name appropriately depicts its nature, i.e. it is a sieve that factorizes composite integers (or more precisely: a sieve-based factorization method).

[724] Smooth in this context means all their prime factors are less than or equal to a chosen bound.

7.10.7 Pollard's Rho Algorithm

This is a probabilistic algorithm for integer factorization. It is particularly effective at finding relatively small prime factors of large composite integers n. Under standard theoretical assumptions, its expected running time is proportional to the square root of the smallest prime factor being sought. The algorithm also requires very little auxiliary memory compared with factorization methods such as GNFS and QS, which involve collecting relations and performing substantial linear algebra computations. The algorithm's practical efficiency depends primarily on the size of the factor being sought, rather than on the number of digits in n. Consequently, it can factor integers with many digits when they have sufficiently small prime factors, although it is generally ineffective for factoring large semiprimes whose prime factors are both large.

The algorithm is named after the Greek letter ρ because the sequence generated by its iteration function eventually enters a cycle, producing a tail-and-cycle structure that resembles the letter when diagrammed. The sequence is deterministic for a given choice of starting value and iteration function, but the algorithm uses randomized choices and is therefore probabilistic in its operation. Several variants and implementation improvements exist, including Brent's variant, which can reduce computational overhead.

The algorithm of this method may be outlined as follows:[725]

1. Choose a simple polynomial function, typically $f(x) = x^2 + c \pmod n$ where c is a random constant (usually $c = 1$).
2. Pick a random starting seed value x_0 (usually $x_0 = 2$).
3. Set both x and y equal to x_0 (say $x = 2$ and $y = 2$).
4. Do repeatedly:
   $x = f(x)$
   $y = f(f(y))$
   $d = \gcd(|x - y|, n)$
5. If:
   $d = 1$: no factor is found yet. Continue repeating.
   $1 < d < n$: d is a non-trivial factor of n.
   $d = n$: restart the algorithm with different parameters (using different c and/or different x_0).

It is worth noting that Pollard's rho algorithm requires running a primality test first (e.g. a quick Miller-Rabin primality test) if n is unknown to be composite. If n happens to be a prime number, the step $d = \gcd(|x-y|, n)$ will almost always return 1, and hence it will eventually cycle and return $d = n$, forcing a reset. In short, prime n leads to repeated failure to find non-trivial factor.

7.10.8 Pollard's $p - 1$ Algorithm

This method is designed to find a prime factor p of a composite number n where $p - 1$ is smooth.[726] Accordingly, the speed of finding a prime factor p depends on whether $p - 1$ is smooth. The algorithm relies on Fermat's little theorem (see § 5.1.15) and allows for the extraction of a prime factor using simple modular exponentiation and greatest common divisor calculations.

The idea of this algorithm is: suppose p divides n, and we pick a bound B and compute an exponent M that acts as a multiple of many small prime powers up to B, e.g. $M = B!$ or $M = \operatorname{lcm}(1, 2, \ldots, B)$. If $p - 1$ is B-smooth, then $p - 1$ will cleanly divide M. This yields (where we are appealing to Fermat's little theorem assuming a and p are coprime):

$$M = k(p-1) \quad \Rightarrow \quad a^M = a^{k(p-1)} = \left(a^{p-1}\right)^k \equiv 1^k = 1 \pmod p \tag{119}$$

[725] This is a simple "Floyd Cycle Detection" version of this algorithm.
[726] Smooth (or power smooth) integer in this context means all of its prime factors are relatively small.

i.e. p divides $a^M - 1$. Since p also divides n, p must divide their gcd, i.e. $\gcd(a^M - 1, n)$. As long as this gcd is not equal to n or 1, a non-trivial factor of n is found.

The algorithm of this method may be outlined as follows (representing one variant of this algorithm):

1. Choose a smoothness bound B (say 20).
2. Compute $M = \text{lcm}(1, 2, \ldots, B)$.
3. Pick a base a such that $1 < a < n$ (say $a = 2$).
4. Starting with the picked a, for each prime $q \leq B$, keep calculating and updating:

$$a \leftarrow a^{q^{\lfloor \log_q B \rfloor}} \pmod{n} \tag{120}$$

   where $\leftarrow$ means assignment.
5. Calculate $g = \gcd(a - 1, n)$.[727]
6. If:
   $1 < g < n$: g is a non-trivial factor of n.
   $g = 1$: increase B and try again.
   $g = n$: the algorithm fails. Choose a different a (or use a different method).

7.10.9 Quadratic Sieve

This (abbreviated as QS) is a powerful integer factorization algorithm used to break down large integers into their prime factors. The main advantages of this algorithm are its speed and simplicity. In fact, it is the fastest integer factorization algorithm (among general-purpose factorization algorithms) for relatively small integers, and the second fastest in general (i.e. second only to the general number field sieve; see § 7.10.5). Moreover, it is significantly simpler to implement than comparable general-purpose factorization methods. The algorithm is developed as a modification of Dixon's factorization method (see § 7.10.2), which itself is based on the Fermat factorization method (see § 7.10.4).

A historical achievement of the quadratic sieve was the factorization of RSA-129 (a 129-digit integer) in 1994 using a large distributed computation. Despite the "sieve" label attached to this algorithm, it is more appropriately classified as an integer factorization method rather than a sieve method (even though the "sieve" label is still technically applicable because the data collection stage uses a sieving process). In this regard, it is like GNFS, MPQS and SNFS (see § 7.10.5, § 7.10.6 and § 7.10.11).

The algorithm of the quadratic sieve may be outlined as follows (where n is the integer to be factored):[728]

1. Choose a factor base by selecting a set of small primes $p \leq B$ (typically including -1) for which n is a quadratic residue modulo p (noting that B is a bound based on the size of n).
2. Define the quadratic polynomial by letting $x \approx \lceil \sqrt{n} \rceil$ and computing values of $Q(x) = x^2 - n$.[729]
3. Search for smooth values: find values of x such that $Q(x)$ factors completely over the factor base, i.e. $Q(x)$ is B-smooth. Use a sieving process to efficiently identify likely smooth values.
4. Record exponent vectors: for each smooth $Q(x)$, express it as a product of factor-base primes. Store the exponents modulo 2, producing a binary exponent vector.
5. Collect enough relations: continue sieving until more smooth relations have been gathered than there are primes in the factor base.
6. Solve a linear system modulo 2: use Gaussian elimination (or a similar method) on the exponent vectors to find a non-trivial dependency among the vectors.

[727] By the time the loop ends, the final value stored in a is already equal to the original $a^M \pmod{n}$. We note that $\text{lcm}(1, 2, \ldots, B) = \prod_{q \leq B} q^{\lfloor \log_q B \rfloor}$.

[728] In fact, this is a simplified description of the basic QS. Practical implementations may use optimizations such as sieving over intervals, partial relations, and more advanced linear algebra techniques.

[729] This represents the standard single-polynomial quadratic sieve (noting that it may be formulated differently).

7. Construct a congruence of squares: combine the corresponding relations to obtain $X^2 \stackrel{n}{=} Y^2$. The dependency ensures that the product of the selected $Q(x)$ values is a perfect square.
8. Calculate $\gcd(X - Y, n)$ and/or $\gcd(X + Y, n)$. If the gcd yields a non-trivial value, then it is a factor of n.
9. If the gcd yields a trivial factor (i.e. 1 or n), gather additional relations and try another dependency (from your existing matrix first).
10. Apply the same process to any composite factors until the complete prime factorization of n is obtained.

As indicated already, the quadratic sieve can be viewed as a modification (or generalization) of Fermat's factorization method (see § 7.10.4). Instead of searching for a single identity $y^2 = x^2 - n$ (as in Fermat), it searches for a combination of many values $x^2 - n$ whose product becomes a square, yielding a congruence of squares modulo n from which factors can be extracted. In its approach to collecting and combining suitable relations, the quadratic sieve builds on Dixon's factorization method (see § 7.10.2).

7.10.10 Shanks' Square Forms Factorization

This (commonly abbreviated as SQUFOF) is an integer factorization algorithm based on the properties of binary quadratic forms and the continued-fraction expansion of quadratic irrationals ($\sqrt{n}$ or $\sqrt{kn}$ where n is the integer to be factored). SQUFOF is exceptionally fast for factoring integers up to about 2^{64} and is often regarded as one of the fastest general-purpose factorization algorithms in this range. Moreover, it requires very little memory (unlike, for instance, CFRAC or QS which require the storage and processing of large matrices and other relational data). Consequently, SQUFOF is commonly used in factorization software as a first-stage method before more powerful algorithms are applied. It is noteworthy that SQUFOF is practically designed to factor odd composite integers that are not perfect squares. However, stripping the power of 2 from an even composite is trivial and hence SQUFOF can be used for factoring the odd part of even composites (which are not powers of 2).

The algorithm of SQUFOF may be outlined as follows (where n is the integer to be factored):[730]

1. Start with an odd composite integer n, optionally scaling by a small multiplier k.
2. Compute the continued fraction expansion of $\sqrt{kn}$, tracking the sequences P_i, Q_i associated with the reduction of quadratic forms in the principal cycle.
3. Search for an index where Q_i is a perfect square (ignoring trivial early occurrences).
4. When found, let $r = \sqrt{Q_i}$ and construct a corresponding unreduced ambiguous form derived from the continued fraction data.
5. Use this form to initialize a reverse reduction recurrence that traverses a non-principal ambiguous cycle of forms.
6. Continue until reaching an ambiguous (symmetric) reduced form at the cycle's midpoint.
7. From this form's parameters, compute $\gcd(\cdot, n)$ to obtain a non-trivial factor.[731]
8. If the result is trivial, restart with a different multiplier k.

7.10.11 Special Number Field Sieve

This (abbreviated as SNFS) is a highly efficient integer factorization algorithm used for numbers of a specific form. As its name suggests, it is a special-purpose variant of the general number field sieve (see § 7.10.5). While the general number field sieve (GNFS) can factor any large integer, the special number field sieve only works for numbers that can be represented as a polynomial with small coefficients (usually

[730] SQUFOF is rather messy and lengthy to explain in full (considering the scope and space of this introductory volume). The following is a very brief (essentially qualitative) outline to give a general idea about SQUFOF rather than an accurate technical account. A full technical account will be provided in the future.

[731] The dot in the gcd is a placeholder for a specific coefficient obtained from the previous operations.

small relative to the number being factored). The SNFS is most effective for integers of the form $r^e \pm s$ where r and s are small integers. Common examples include Mersenne numbers $(2^m - 1)$ and Fermat numbers $(2^{2^k} + 1)$.

Similar to the GNFS, the SNFS factorization is performed through a series of mathematical and computational processes (mainly: polynomial selection, sieving, applying linear algebra operations, and square rooting). The SNFS is significantly faster than the GNFS, and hence the SNFS is the fastest known algorithm for these specific types of large integers. A historic achievement of the SNFS was its successful factorization of the ninth Fermat number (F_9) in 1990. Like the GNFS, the SNFS algorithm is an *integer factorization* method more than a *sieve* method although it is still technically appropriate to classify it as a sieve (as justified previously; see for instance § 7.10.5).

The algorithm of SNFS may be outlined as follows (where n is the integer to be factored):[732]

1. Express n in a form like $r^e \pm s$ where r and s are relatively small integers.
2. Choose a base $x = r^k$ for a small integer k.[733]
3. Define a low-degree polynomial f with small coefficients such that $f(x) \stackrel{n}{=} 0$ (often $f(x) = n$ or a small multiple of n).
4. Construct a rational side (using a simple linear polynomial with a root modulo n) and an algebraic side (using the number field generated by a root of $f(x)$).
5. Select factor bases (sets of small primes) on both the rational and algebraic sides to be used to test smoothness.
6. Search over many integer pairs (a, b) and compute the corresponding rational and algebraic norms. Record a relation whenever both norms factor completely over the chosen factor bases (i.e. they are smooth).
7. Continue collecting relations until there are more relations than factor-base elements. Store the exponent vectors of the prime factorizations modulo 2.
8. Form a large sparse matrix over the finite field $\mathbb{F}_2$ from the collected relations. Solve for non-trivial dependencies among rows.
9. Use a dependency to combine relations so that the product of rational side values is a square, and the product of algebraic side values is also a square in the number field.[734]
10. Compute the corresponding square roots on both sides, and convert the algebraic square root back into a congruence of squares modulo n.
11. Obtain a congruence of squares $X^2 \stackrel{n}{=} Y^2$ and calculate $\gcd(X - Y, n)$ and/or $\gcd(X + Y, n)$. If the gcd yields a non-trivial value, then it is a factor of n.
12. If the dependency gives only trivial factors (i.e. 1 or n) use another dependency from the linear algebra stage (until a non-trivial factorization is obtained).

7.10.12 Trial Division Algorithm

This is the most basic and direct integer factorization algorithm. It simply factorizes an integer n by checking its potential prime divisors (and their powers by repeatedly dividing out any factor that is found) between 2 and $\sqrt{n}$. The speed of this algorithm depends primarily on the size of its smallest prime factor. The algorithm is effective when n has small prime factors, but in the worst case (e.g. when n is prime or the product of two large primes) it may need to test all potential divisors up to $\sqrt{n}$, making it inefficient for large integers.

Accordingly, the trial division algorithm is mainly suitable for small integers (say up to about 10 digits

[732] This outline is essentially a qualitative high-level conceptual sketch of SNFS which lacks essential technical details and rigor, as its primary purpose is to give a broad idea about SNFS.

[733] While choosing a power of r is a standard construction, it is not the universal choice in SNFS.

[734] Strictly speaking, additional considerations (such as analyzing the unit group) are needed to ensure and compute a true square root of the corresponding algebraic element.

long) or for stripping away tiny factors before running heavier algorithms. For example, it is a common practice in cryptography to use the trial division first to strip away small prime factors (which are easy to find) before employing more sophisticated algorithms (like the general number field sieve or the elliptic curve method; see § 7.10.5 and § 7.10.3) to complete the factorization. Also see § 7.3.4.

7.10.13 Williams' $p+1$ Algorithm

This algorithm extracts a prime factor p from a composite number n when $p+1$ is smooth (i.e. it consists entirely of small prime factors), and hence it is particularly effective when n has such a prime factor p. It serves as a direct algebraic counterpart to Pollard's $p-1$ algorithm (see § 7.10.8), and thus it can be seen as a variant of it. However, rather than using ordinary modular exponentiation as in Pollard's $p-1$ algorithm, Williams' method uses Lucas sequences to carry out analogous calculations associated with a quadratic field extension.

The algorithm of this method may be outlined as follows (representing one variant of this algorithm):

1. Choose a suitable integer parameter A.
2. Choose a smoothness bound B.
3. Compute the exponent $M = \prod_{q \leq B} q^{\lfloor \log_q B \rfloor}$.
4. Compute the Lucas sequence term $V_M \pmod n$ using the initial conditions $V_0 = 2$ and $V_1 = A$.[735]
5. Calculate $g = \gcd(V_M - 2, n)$.
6. If:

   $1 < g < n$: g is a non-trivial factor of n.

   $g = 1$: the algorithm failed to find a factor. Change the parameter A or increase the bound B, then try again.

   $g = n$: the algorithm fails to find a proper factor with the current parameters. Restart the algorithm with different initial parameters, e.g. by changing A or adjusting B (or use a different method).

We should finally note that the algorithm only works as intended if the discriminant $\Delta = A^2 - 4$ is a quadratic non-residue modulo p (as indicated in Point 4). If Δ is a quadratic residue modulo p, the algorithm effectively searches for a smooth $p-1$ factor instead. Since p is unknown beforehand, there is an approximate 50% chance that a randomly chosen parameter A will cause the algorithm to behave like Pollard's $p-1$ algorithm rather than Williams' $p+1$ algorithm.

[735] The Lucas sequence is defined here by the recurrence relation: $V_0 = 2$, $V_1 = A$ and $V_k = AV_{k-1} - V_{k-2}$ where all arithmetic operations are performed modulo n. The choice of A must be suitable for exploiting the $p+1$ group order modulo the prime factor being sought (in particular, $A^2 - 4$ should be a quadratic non-residue modulo that prime factor).

Chapter 8
Distribution of Primes

In this chapter we investigate the distribution of prime numbers and related topics. The distribution of prime numbers concerns the study of how primes are spread among the positive integers. Although prime numbers appear irregular and unpredictable individually, they exhibit well-defined statistical patterns and structures when viewed collectively and at large scale. This area of analytic number theory investigates crucial questions such as how many primes exist below a given number (the prime-counting function; see § 8.2.1), how the density of primes decreases as integers grow larger, how far apart consecutive primes tend to be (prime gaps), and how primes are distributed within regular structures like arithmetic progressions. Understanding these patterns and structures has led to fundamental results, such as the prime number theorem (see § 5.1.31), which describes the asymptotic frequency of primes, and continues to motivate research into many unresolved problems concerning the behavior of prime numbers.

8.1 General Facts about Distribution of Primes

The following is a collection of basic statements about the distribution of prime numbers, intended to provide a solid general overview for readers who are unfamiliar with the subject:

1. Although prime numbers appear scattered randomly among the integers, their collective distribution follows predictable statistical patterns over large ranges of integers.
2. Although the primality of integers is deterministic (see Point 5 of § 1.3) and the global distribution of primes follows predictable statistical patterns, the primality of individual numbers remains unpredictable, behaving much like random numbers on a local scale.
3. Although it is relatively easy to estimate the number of primes below a certain bound by using the prime number theorem (see § 5.1.31), it is generally much more difficult to identify the specific primes below that bound, and this computational difficulty increases as the magnitude of the integers grows.
4. Although there is a lower limit on the size of the gap between two successive primes (i.e. 2 in the case of twin primes noting the exception of the pair 2, 3) there is no upper limit on the size of this gap.[736]
5. As indicated already, the gap between two successive prime numbers can be arbitrarily large, that is: for any $n \in \mathbb{N}$ there are n consecutive composite numbers.[737]
6. Primes become sparser (i.e. less frequent) as we move higher up the number line. However, the gaps between successive primes vary unpredictably.
7. The average gap between prime numbers keeps growing as integers get larger, but primes never stop appearing.
8. The distribution of prime numbers (i.e. the number of primes less than or equal to $x \in \mathbb{R}$ as a function of x) follows a logarithmic pattern. This is demonstrated in Figure 14 where the prime-counting function $\pi(x)$ (which counts the number of primes $\leq x$; see § 8.2.1) appears approximately linear with a slope of about 1 on this log-log plot (up to $x \leq 10^{20}$, noting that the slope approaches 1 as $x \to \infty$).
9. For any integer $n > 1$ there is at least one prime number between n and $2n$ (see § 5.1.2). There are other theorems (as well as many conjectures) of a similar nature (see for instance § 5.2.6 and § 6.2.6).

[736] *Prime gap* is the difference between successive prime numbers, that is: $g_n = p_{n+1} - p_n$ where g_n is the n^{th} prime gap.
[737] More precisely, for every $n \in \mathbb{N}$, there exist consecutive primes $p < q$ such that $q - p > n$.

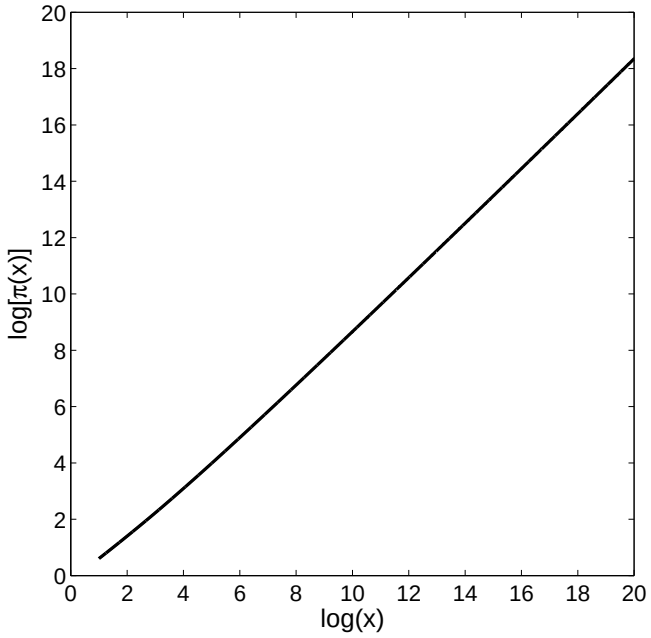


Figure 14: The plot of $\log\left[\pi(x)\right]$ versus $\log(x)$ for $x \leq 10^{20}$. See Point 8 of § 8.1.

8.2 Prime Counting and Distribution Functions

We investigate in this section the main prime counting and distribution functions (as well as some functions related to the topic of prime counting and distribution).

8.2.1 The π Function

The function $\pi(x)$ (which is known as the prime-counting function) is defined as the number of primes that do not exceed a given real number x (noting that it is completely unrelated to the mathematical constant $\pi \approx 3.14159$). This function may be given formally by the following sum:

$$\pi(x) = \sum_{p \leq x} 1 \tag{121}$$

For example, $\pi(1) = 0$ because there is no prime ≤ 1, $\pi(2) = 1$ because there is only 1 prime number ≤ 2 which is 2, and $\pi(20) = 8$ because there are 8 prime numbers ≤ 20 which are 2, 3, 5, 7, 11, 13, 17, 19.[738] This function is of "step" or "staircase" nature because it increases by 1 at every prime number and remains constant between primes. The behavior of this function is largely described by the prime number theorem which predicts its asymptotic growth at large x (see § 5.1.31).

8.2.2 The li and Li Functions

As we saw in § 5.1.31, the ratio $x/\ln x$ is used in the prime number theorem to describe the asymptotic behavior of the prime-counting function $\pi(x)$. However, a more accurate description of this behavior than this ratio is given by the *logarithmic integral function* $\mathrm{li}(x)$, and this is more often used by number theorists. Accordingly, the function $\mathrm{li}(x)$ is commonly used as a good approximation to the $\pi(x)$ function.

[738] See `https://oeis.org/A000720` and `https://oeis.org/A006880`.

It is worth noting that the logarithmic integral function is defined (via the Cauchy principal value) as:

$$\mathrm{li}(x) = \int_0^x (\ln t)^{-1} dt \tag{122}$$

In number theory, the *offset logarithmic integral function*:

$$\mathrm{Li}(x) = \int_2^x (\ln t)^{-1} dt \tag{123}$$

is usually preferred to avoid the singularity at $t = 1$.

8.2.3 Riemann's Prime-Power Counting Function

This is a step function, usually denoted as $J(x)$ or $\Pi(x)$ and may also be called (laxly) the *Riemann prime-counting function*. It counts the number of primes and prime powers less than or equal to x, weighing each prime power p^n by $1/n$ (where $n \in \mathbb{N}$). For example, $J(5) = 3.5$ because we have three p^1 primes (i.e. 2, 3, 5) and only one p^2 (i.e. 2^2) which are less than or equal to 5 and hence we have $3/1 + 1/2 = 3.5$ (noting that there is no p^n for $n > 2$ that is less than or equal to 5). Similarly, $J(9) = 16/3$ because we have four p^1 primes (i.e. 2, 3, 5, 7), two p^2 (i.e. 2^2 and 3^2) and only one p^3 (i.e. 2^3) which are less than or equal to 9 and hence we have $4/1 + 2/2 + 1/3 = 16/3$ (noting that there is no p^n for $n > 3$ that is less than or equal to 9).

Accordingly, this function is calculated, through the use of the standard prime-counting function $\pi(x)$, by the following sum:

$$J(x) = \sum_{n \geq 1} \frac{\pi(x^{1/n})}{n} \tag{124}$$

Although this sum seems infinite (since $n \geq 1$ means $n = 1, 2, 3, \ldots$) the non-zero terms are finite and hence the sum is finite. This is because all the terms become zero once $x^{1/n}$ falls below 2 (i.e. the first prime) since there is no prime below 2 and hence $\pi(x^{1/n}) = 0$ for all subsequent terms. Accordingly, this sum may be written as:

$$J(x) = \sum_{n=1}^{N} \frac{\pi(x^{1/n})}{n} \tag{125}$$

where $N = \lfloor \log_2(x) \rfloor$. The values of the Riemann prime-power counting function for the first 10 natural numbers (i.e. corresponding to $x = 1, 2, \ldots, 10$) are: 0, 1, 2, 5/2, 7/2, 7/2, 9/2, 29/6, 16/3, 16/3.[739]

The Riemann prime-power counting function is given (analytically or explicitly) by a number of formulae such as:

$$J(x) = \mathrm{li}(x) - \sum_{\rho} \mathrm{li}(x^{\rho}) - \ln 2 + \int_x^{\infty} \frac{dt}{t(t^2 - 1) \ln t} \tag{126}$$

where li is the logarithmic integral function (see § 8.2.2) and ρ are the non-trivial zeros of the Riemann zeta function (see Eq. 48 and § 6.1.29). In fact, this formula (and similar formulae) actually reveals the profound nature of this function and its theoretical connections to other theoretical and mathematical entities (e.g. its link to the Riemann zeta function). This is unlike the above sum formula of Eq. 124 which is a "practical" tool for calculating this function.[740]

The Riemann prime-power counting function $J(x)$ is also related to the standard prime-counting function

[739] See `https://oeis.org/A096624` and `https://oeis.org/A096625`.

[740] In fact, this $J(x)$ (as given by Eq. 126) is an analytic representation of the step function $J(x)$ of Eq. 124.

$\pi(x)$, through the Mobius function $\mu(n)$, by the following formula:

$$\pi(x) = \sum_{n \geq 1} \frac{\mu(n)}{n} J(x^{1/n}) \tag{127}$$

As seen, this formula is an algebraic inversion device that uses the Mobius function to restore (or extract) the standard prime-counting function from the Riemann prime-power counting function (and hence it is aptly called the *Mobius inversion formula* since it reverses the effect of the formula of Eq. 124).

8.2.4 Riemann's *R*-Function

This function provides a smooth approximation for the prime-counting function $\pi(x)$ which is more accurate than the approximation of the logarithmic integral $\text{li}(x)$ (see § 8.2.1 and § 8.2.2; also see § 5.1.31). It is given by the formula:

$$R(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \text{li}(x^{1/n}) \tag{128}$$

where $R(x)$ is the Riemann R-function, $\mu(n)$ is the Mobius function, and $\text{li}(x)$ is the logarithmic integral function (see § 8.2.2). On comparing the formulae of Eqs. 127 and 128 we can see that the Riemann R-function uses the same Mobius inversion structure but it replaces the step-function $J(x)$ with the smooth analytic function $\text{li}(x)$.

The Riemann R-function is also given by the following power series:

$$R(x) = 1 + \sum_{k=1}^{\infty} \frac{(\ln x)^k}{k \cdot k! \cdot \zeta(k+1)} \tag{129}$$

where ζ is the Riemann zeta function (see Eq. 48). This series (which is called the *Gram series*) is rapidly converging and provides a very good fit for $\pi(x)$ and hence it is widely used in actual calculations.

8.2.5 Chebyshev's Functions

Chebyshev (prime-counting) functions, which are usually denoted $\theta(x)$ and $\psi(x)$, are closely related functions that weight primes and prime powers by their logarithms. They are often easier to work with than the standard prime-counting function $\pi(x)$ and hence they are commonly used to simplify the study of the distribution of prime numbers and to prove the prime number theorem (see § 5.1.31).

The $\theta(x)$ function is a sum of the logarithms of all primes up to x, while the $\psi(x)$ function is also a sum of such logarithms but instead of only counting over the primes it counts over their powers as well (i.e. $p, p^2, p^3, \ldots$) for all prime powers up to x. Accordingly, these functions are given by:

$$\theta(x) = \sum_{p \leq x} \ln p \qquad\qquad \psi(x) = \sum_{p^k \leq x} \ln p \tag{130}$$

For example:

$$\theta(14) = \ln 2 + \ln 3 + \ln 5 + \ln 7 + \ln 11 + \ln 13 = \ln 30030 \approx 10.30995 \tag{131}$$

Similarly:

$$\psi(14) = \ln 2 + \ln 3 + \ln 5 + \ln 7 + \ln 11 + \ln 13 + [\ln 2 + \ln 2] + [\ln 3] = \ln 360360 \approx 12.79486 \tag{132}$$

where $[\ln 2 + \ln 2]$ corresponds to 2^2 and 2^3, while $[\ln 3]$ corresponds to 3^2 (all of which are ≤ 14).

The following table lists the (approximate) values of the $\theta(x)$ and $\psi(x)$ functions for $x = 1, 2, ..., 14$:[741]

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\theta(x)$	0	0.69	1.79	1.79	3.40	3.40	5.35	5.35	5.35	5.35	7.75	7.75	10.31	10.31
$\psi(x)$	0	0.69	1.79	2.48	4.09	4.09	6.04	6.73	7.83	7.83	10.23	10.23	12.79	12.79

It is shown that if Riemann's hypothesis holds then:

$$|\theta(x) - x| < \frac{1}{8\pi}\sqrt{x}\,(\ln x)^2 \qquad \text{(for all } x \geq 599) \tag{133}$$

$$|\psi(x) - x| < \frac{1}{8\pi}\sqrt{x}\,(\ln x)^2 \qquad \text{(for all } x \geq 73.2) \tag{134}$$

8.3 Relationships among Prime Counting and Distribution Functions

The prime counting and distribution functions (see § 8.2) are intimately related. Examples of these relationships are presented in the following points:

1. The $\pi(x)$ and $\mathrm{li}(x)$ functions are related by the following formula:

$$\pi(x) = \mathrm{li}(x) + O(X) \qquad (x \to \infty) \tag{135}$$

where O is the big O notation, and X (which is a function of x) has various estimates which vary in their accuracy, e.g.

$$X = xe^{-a\sqrt{\ln x}} \qquad \text{or} \qquad X = xe^{-0.2098(\ln x)^{0.6}(\ln\ln x)^{-0.2}} \qquad \text{or} \qquad X = \sqrt{x}\ln x \tag{136}$$

where a is a positive constant that depends on the zeros of the Riemann zeta function (noting that the first two estimates hold unconditionally, while the last estimate, which is the best, is conditioned by the validity of the Riemann hypothesis; see § 6.1.29).

2. The $\pi(x)$ and $\mathrm{li}(x)$ functions are also related by the following formulae:

$$|\pi(x) - \mathrm{li}(x)| \leq \frac{0.2593x}{(\ln x)^{0.75}}e^{-\sqrt{(\ln x)/6.315}} \qquad (x \geq 229) \tag{137}$$

$$|\pi(x) - \mathrm{li}(x)| < \frac{\sqrt{x}\ln x}{8\pi} \qquad (x \geq 2657) \tag{138}$$

noting that the first formula holds unconditionally, while the last formula, which provides a stronger asymptotic error bound, is conditioned by the validity of the Riemann hypothesis (see § 6.1.29).

3. The $\pi(x)$ [or rather $\pi(x^{1/n})$] and $J(x)$ functions are related by the formula of Eq. 124.
4. The $\pi(x)$ and $J(x)$ [or rather $J(x^{1/n})$] functions are related by the formula of Eq. 127.
5. The $\pi(x)$ and $\theta(x)$ functions are related by the following formulae:

$$\pi(x) = \frac{\theta(x)}{\ln x} + \int_2^x \frac{\theta(t)}{t\,(\ln t)^2}dt \qquad \theta(x) = \pi(x)\ln x - \int_2^x \frac{\pi(t)}{t}dt \qquad (x \geq 2) \tag{139}$$

6. The $\mathrm{li}(x)$ and $J(x)$ functions are related by the formula of Eq. 126.
7. The $\mathrm{li}(x)$ and $R(x)$ functions are related by the formula of Eq. 128.
8. The $\theta(x)$ and $\psi(x)$ functions are related by the formula:

$$\psi(x) = \sum_{k\geq 1}\theta(x^{1/k}) \tag{140}$$

[741] Also see `https://oeis.org/A035158` regarding $\theta(x)$.

Finally, it is worth noting the following points:
• The $\psi(x)$ function has a direct link to the non-trivial zeros (ρ) of the Riemann zeta function (see Eq. 48) through the following formula:

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \ln(2\pi) - \frac{\ln(1 - x^{-2})}{2} \tag{141}$$

• The following asymptotic statements (which are related to the prime-counting functions) are mathematically equivalent (where $x \to \infty$, see § 5.1.31):

$$\pi(x) \sim \frac{x}{\ln x} \qquad \pi(x) \sim \mathrm{li}(x) \qquad \theta(x) \sim x \qquad \psi(x) \sim x \tag{142}$$

8.4 Theorems about Distribution of Primes

This issue was briefly introduced in § 5.2.6. While we originally planned to discuss it here in greater detail, the manuscript has already reached the maximum length intended for an introductory volume.[742] In contrast, the section on conjectures about the distribution of primes (see § 8.5) was retained because it was already fully prepared. Furthermore, whereas established theorems are well-documented and historically settled, open problems and conjectures remain under active evolving research. In the context of prime distribution, these unresolved questions arguably offer a richer ground for immediate discussion. A comprehensive examination of the theorems related to the distribution of primes will instead be a primary focus of upcoming volumes. For this introductory volume, the foundation laid in § 5.2.6 should provide sufficient background.

8.5 Conjectures about Distribution of Primes

There are many conjectures about (or related to) the counting and distribution of prime numbers. In fact, the number of conjectures in the topic of counting and distribution of primes is disproportionately larger than the number of conjectures in most other topics of prime numbers (and possibly number theory in general). This prominence is reflected in the immense volume of literature and the high academic profile of historical and contemporary investigations on the subject. Consequently, the distribution of primes remains one of the most active and densely populated areas for theoretical conjectures in modern mathematics.

The exceptionally large number of conjectures about counting and distribution of primes may be explained by a number of factors; some of which are outlined in the following points:
• Even though prime numbers appear randomly distributed on a local scale, they follow rather strict patterns on a global scale (as formulated, for instance, by the prime number theorem; see § 5.1.31). So, it is exceptionally important for understanding prime numbers to bridge this gap between the local and global behaviors, and this should justify the high density of these conjectures as they deal with one of the most important issues in number theory (and primes in particular). In short, many ideas (formulated as conjectures) emerge to address this exceptionally important issue and characterize the global behavior of primes and its relation to their local behavior.
• The exceptionally important hypothesis of Riemann (see § 6.1.29) in number theory has a profound link to the issue of counting and distribution of primes (through the zeros of the zeta function). The "obsession" of number theorists with this hypothesis (due to its importance) naturally and continually

[742] In fact, this reason affects other parts of this book which were unfortunate to be left late in the queue.

generates conjectures about counting and distribution of primes. In fact, the Riemann hypothesis is (historically and theoretically) the birth place and breeding ground for many of these conjectures.

• The fascination of infinity (which leads to obsession with the infinitude of types of primes) should also be considered as an important factor for the large number of conjectures about counting and distribution of primes since infinitude/finitude is a counting issue (noting that there is a big number of conjectures about, or related to, the in/finitude of certain types and categories of primes).

We present in the following list a sample of common examples of such conjectures (ordered alphabetically):[743]

1. Andrica's conjecture (see § 6.1.4). This conjecture is essentially about prime gaps and hence it is directly related to the counting and distribution of primes. Being about prime gaps (and hence prime distribution) can be demonstrated by the following chain of relations:

$$g_n = p_{n+1} - p_n = \left(\sqrt{p_{n+1}} - \sqrt{p_n}\right)\left(\sqrt{p_{n+1}} + \sqrt{p_n}\right) < \left(\sqrt{p_{n+1}} + \sqrt{p_n}\right) \tag{143}$$

   where the last step is justified by the inequality $\left(\sqrt{p_{n+1}} - \sqrt{p_n}\right) < 1$ which is asserted by Andrica's conjecture (assuming its validity). Now, if we note that asymptotically we have:

$$\left(\sqrt{p_{n+1}} + \sqrt{p_n}\right) \simeq 2\sqrt{p_n} \tag{144}$$

   then we get:

$$g_n \lesssim 2\sqrt{p_n} \tag{145}$$

   i.e. Andrica's conjecture implies that, as primes become larger, the gaps between consecutive primes are bounded above asymptotically by approximately $2\sqrt{p_n}$. This means that the conjecture puts an upper bound on the size of prime gaps that depends on the size of prime and hence on the location on the number line. Anyway, Andrica's conjecture is a rather weak statement as compared to some other conjectures related to prime gaps (like the Cramer and Oppermann conjectures; see Points 5 and 11), even though it is stronger than some other conjectures (like the Legendre conjecture; see Point 10). Stronger conjectures (supported by analytic, heuristic and computational evidence) suggest that the actual prime gaps are asymptotically much smaller than $2\sqrt{p_n}$ for large p_n.
2. Bateman-Horn conjecture (see § 6.1.6). This conjecture predicts how often polynomials (satisfying specific criteria) take prime values. More specifically, it predicts the asymptotic frequency with which one or several non-constant irreducible polynomials (with integer coefficients, positive leading coefficients, and with no local obstruction) simultaneously take prime values as their integer argument tends to infinity. Hence, the conjecture is about the counting and distribution of primes within certain algebraic structures (i.e. polynomial sequences).
3. Brocard's conjecture (see § 6.1.10). This conjecture is about the counting and distribution of prime numbers but in terms of their squares, and hence it establishes a link between prime numbers and their squares. While the prime number theorem (see § 5.1.31) indicates that primes become sparser as we move up on the number line, Brocard's conjecture suggests that the interval between p_n^2 and p_{n+1}^2 grows sufficiently fast to always embrace at least four primes. This should impose a kind of regulation on the gaps between primes as well as their density in general. It is worth noting the similarity between Brocard's conjecture and Oppermann's conjecture (see Point 11) since both are formulated in terms of squares (i.e. of primes or integers). This similarly (and broadly) applies to Legendre's conjecture (see Point 10) noting that Legendre's conjecture (like Brocard's conjecture) is weaker than Oppermann's

[743] In § 6.2.6 we listed a number of open problems and conjectures related to the distribution of primes (in the broad sense of distribution). Most of these conjectures were also presented and discussed in § 6.1. So, in the following list we want to dive rather deeper by inspecting and analyzing some of these conjectures specifically from the perspective of distribution (which is the subject of this chapter).

conjecture.

4. Bunyakovsky's conjecture (see § 6.1.11). What has been said about the Bateman-Horn conjecture (see Point 2) generally applies to the Bunyakovsky conjecture due to their structural similarities. Specifically, the Bunyakovsky conjecture is a special case of the broader, stronger Bateman-Horn conjecture; it serves as the qualitative, single-polynomial version of the quantitative Bateman-Horn conjecture.
5. Cramer's conjecture (see § 6.1.12). This conjecture provides a probabilistic model for the distribution of prime numbers among the integers by predicting the growth of the maximum gaps between consecutive primes. Specifically, it suggests that primes behave like random points scattered on the number line with a density of $1/\ln x$, yielding a maximal gap near x of $\sim (\ln x)^2$. This bound is significantly more precise and restrictive than those of other hypotheses, such as Legendre's conjecture (see Point 10), which only predicts a gap size of order $O(\sqrt{x})$.
6. Elliott-Halberstam conjecture (see § 6.1.14). This conjecture is about how evenly primes are distributed in arithmetic progressions. In fact, it suggests that prime numbers are distributed (on average) "optimally" across arithmetic progressions, and hence it is a significant advancement on a number of issues related, for instance, to the Dirichlet theorem and the prime number theorem for arithmetic progressions (see § 5.1.11 and § 5.1.32). The conjecture has (direct and indirect) impact on a number of important topics in number theory such as the size of gaps between consecutive primes and the parity problem in sieve theory.
7. Firoozbakht's conjecture (see § 6.1.16). This is one of the strongest gap regulating conjectures in number theory as it imposes one of the tightest bounds on the size of prime gaps. For example, it is stronger than the Cramer conjecture (see Point 5), and hence if it is true then Cramer's conjecture would also be true.[744] However, because it is so restrictive it seems inconsistent with the (largely supported) Cramer-Granville heuristic model, which means that it could be false even though its potential violation would only occur at extremely large values (noting that it is currently verified up to 4×10^{18} or 2^{64} and possibly higher; see § 6.1.16). We note that what has been said about the Cramer conjecture (with regard to its relation to the Firoozbakht conjecture) largely applies to the Shanks conjecture (see Point 15).[745]
8. First Hardy-Littlewood conjecture (see § 6.1.17). This conjecture predicts an asymptotic formula for the number of occurrences of prime constellations, represented by admissible k-tuples of integers whose simultaneous shifts take prime values. More specifically, it predicts the frequency with which all the elements of such a tuple simultaneously yield primes as the integer parameter tends to infinity, thereby providing a quantitative model for the distribution of prime constellations.
9. Goldbach's conjecture (see § 6.1.19). This conjecture predicts that every even integer greater than 2 can be written as the sum of two primes, and hence it does not seem to be about the counting and distribution of prime numbers. However, it is closely related (even though indirectly) to the issue of counting and distribution of primes because it implies that primes are so dense that they can represent any even integer as the sum of two primes. In fact, the conjecture implies not only that primes are "sufficiently dense", but also that primes are "sufficiently well-distributed" among integers (i.e. they are not clumped together in a way that would leave gaps in the sequence of even integers).[746]
10. Legendre's conjecture (see § 6.1.21). By predicting regularity in prime distribution and providing an implicit bound on prime gaps, this conjecture strongly impacts our understanding of prime counting and distribution. In fact, Legendre's conjecture predicts a strong form of regularity in the local distribution

[744] For the Cramer conjecture we have $g_n \lesssim (\ln p_n)^2$ while for the Firoozbakht conjecture we have $g_n \lesssim (\ln p_n)^2 - \ln p_n$.

[745] But note the difference in nature between the Cramer conjecture (which is about all gaps) and the Shanks conjecture (which is about maximal gaps).

[746] It is worth noting that what has been said already about the (strong) Goldbach conjecture largely applies to the weak (or ternary) Goldbach conjecture, but because the weak conjecture was proven recently, it does not belong to the present section (which is about conjectures rather than proven theorems; see § 5.1.16).

of primes by asserting that prime gaps are of order $O(\sqrt{x})$. Therefore, even though the conjecture may not affect our view of the global behavior of primes (as formulated by results like the prime number theorem and the Chebyshev bias; see § 5.1.31 and § 8.7.1), it would significantly improve our insight into their local behavior (as represented by prime spacing), thereby enhancing our overall understanding of how primes are counted and distributed. Also see Points 3 and 11.

11. Oppermann's conjecture (see § 6.1.25). This conjecture (which is stronger than Legendre's conjecture; see Point 10) predicts that primes are sufficiently dense and well-distributed such that each of the intervals (n^2-n, n^2) and (n^2, n^2+n) contains at least one prime. In other words, the conjecture asserts that primes occur within both intervals, imposing a specific constraint on the gaps between consecutive primes. Also see Point 3.
12. Polignac's conjecture (see § 6.1.26). As a generalization of the twin prime conjecture (see Point 16), Polignac's conjecture has direct significance for the distribution of primes, since it predicts the infinitude of prime pairs separated by every even gap. It is also closely connected to the first Hardy-Littlewood conjecture (see Point 8). Whereas Polignac's conjecture provides a qualitative framework for the occurrence of prime gaps, the first Hardy-Littlewood conjecture provides quantitative asymptotic predictions for their frequency and for the local distribution of primes. Together, these conjectures illustrate the central role of prime gaps in understanding the distribution of prime numbers.
13. Riemann's hypothesis (see § 6.1.29). Even though this hypothesis (which is one of the most famous and important conjectures in all of mathematics) is about the non-trivial zeros of the Riemann zeta function $\zeta(s)$, it is deeply linked to the issue of counting and distribution of prime numbers. If proven, it would provide a much sharper estimate for the error term of the prime-counting function $\pi(x)$, and significantly refine our understanding of the counting of primes and the regularity of their distribution among integers.[747] This issue was briefly indicated previously (see for instance § 8.3). It is worth noting that the extensions and generalizations of the Riemann hypothesis (see § 6.1.29) also have a direct beneficial impact on the issue of prime counting and distribution and our understanding of it (e.g. they provide a better error bound for how primes are distributed in arithmetic progressions and imply precise control over how primes are distributed in general; see for instance § 6.4).
14. Schinzel's hypothesis H (see § 6.1.30). The discussion of the Bateman-Horn conjecture (see Point 2) broadly applies to Schinzel's hypothesis H, since the two conjectures have essentially the same hypotheses concerning the polynomials and the absence of local obstructions. However, their conclusions differ in specificity, i.e. while Schinzel's hypothesis H predicts the existence of infinitely many integers at which all the specified polynomials take prime values, the Bateman-Horn conjecture predicts an asymptotic formula for the number of such integers up to a given bound.
15. Shanks' conjecture (see § 6.1.33). This conjecture provides a precise estimate for the maximal gap between consecutive prime numbers and may be regarded as a refinement of Cramer's conjecture (see Point 5). Its essence is that as $x \to \infty$, the largest gap between consecutive primes up to x becomes asymptotically equivalent to the square of the natural logarithm of x. The significance of this estimate is that it characterizes the smoothness of the prime distribution in the asymptotic limit. Specifically, while the prime number theorem (see § 5.1.31) describes the expected (or average) size of the gaps between primes near x (which is approximately $\ln x$), Shanks' conjecture specifies the magnitude of the extreme upper outliers of these gaps (which is approximately $\ln^2 x$). This implies that although substantial fluctuations in gap sizes occur for large x, they remain vanishingly small compared to x (noting that at large x, $\ln^2 x$ is extremely small in comparison to x).[748] Consequently, this bound reflects a strong form of global asymptotic regularity in the distribution of primes. Also see Point 7.

[747] In fact, if proven, the Riemann hypothesis would validate many conditional theorems and conjectures (some of which are linked to the issue of counting and distribution of primes), and hence it would, from this perspective, improve our understanding of this issue, as well as many other issues related and unrelated to prime numbers.

[748] This may be quantified as $\lim_{x\to\infty} \frac{\ln^2 x}{x} = 0$.

16. Twin prime conjecture (see Point 1 of § 6.1.34). As a special case of the first Hardy-Littlewood conjecture (noting that twin prime pairs are 2-tuples), the twin prime conjecture is intimately related to the issue of counting and distribution of prime numbers (see § 6.1.17 as well as Point 8 of the present section). This similarly applies to the Polignac conjecture (noting that the twin prime conjecture is a special case of the Polignac conjecture; see Point 12).
17. We should finally note that the conjectures about the infinitude (as well as finitude) of certain types and categories of primes (see § 6.1.34, § 6.1.35, § 6.2.4 and § 6.2.5) should also be included in this list because the issue of in/finitude is essentially a counting problem.

8.6 Prime Gaps

The investigation of prime gaps (i.e. the intervals between consecutive prime numbers) is an important aspect of the study of prime distribution, since the two subjects are fundamentally connected. Formally, if p_n denotes the n^{th} prime, then the n^{th} prime gap is given by:

$$g_n = p_{n+1} - p_n \tag{146}$$

Many of the principal questions concerning prime gaps have already been addressed, either directly or indirectly, in the previous sections through our discussion of prime distribution. Nevertheless, for completeness, it is appropriate to include a separate section devoted specifically to prime gaps within a chapter on the distribution of prime numbers.

Although the study of prime gaps is not always formulated in terms of theorems or conjectures about the counting and distribution of prime numbers, it nevertheless provides an important perspective on the distribution of primes. The behavior of prime gaps reveals much about the structure of the sequence of prime numbers, and many central questions concerning prime distribution can be reformulated in terms of the size, frequency, and patterns of these gaps. The following subsections briefly discuss some of the principal properties and phenomena associated with prime gaps.

8.6.1 Size and Distribution of Prime Gaps

We outline the main issues about the size and distribution of prime gaps in the following points (where we mostly benefit from our previous investigations):

1. The size of gaps between consecutive primes tend to grow as we go up on the number line. This is logical because as the integers grow in size the chance of them having a factor among the smaller integers increases, and hence primes become less frequent as numbers get larger. However, prime gaps do not grow at a steady rate as we can still find very small gaps (e.g. of size 2) between very big primes.
2. A fundamental theorem in the study of prime gaps is the prime number theorem (see § 5.1.31) which provides an approximation for the density of prime numbers as a function of prime size (i.e. asymptotic density of primes). This theorem implies that as n becomes large, the average gap between consecutive primes grows roughly as $\ln n$. In Figures 15 (linear) and 16 (logarithmic) we plot the actual average prime gap for n between 1 and 10^7 alongside the theoretical $\ln n$ prediction.[749]
3. While the prime number theorem (see § 5.1.31) provides an estimate of an average gap size of $\ln n$ between primes near n, the actual size and distribution of prime gaps are rather erratic, i.e. their size and distribution can vary dramatically as we go up on the number line. In other words, while this theorem gives an overall trend for the behavior of prime gaps, it does not provide precise answers for the size and location of individual prime gaps. In short, prime gaps are predictable in aggregate and

[749] In fact, the "actual" in these figures is the moving average in windows of 1000 consecutive prime gaps plotted at the start of each window. This is done for a better visual and more informative outcome.

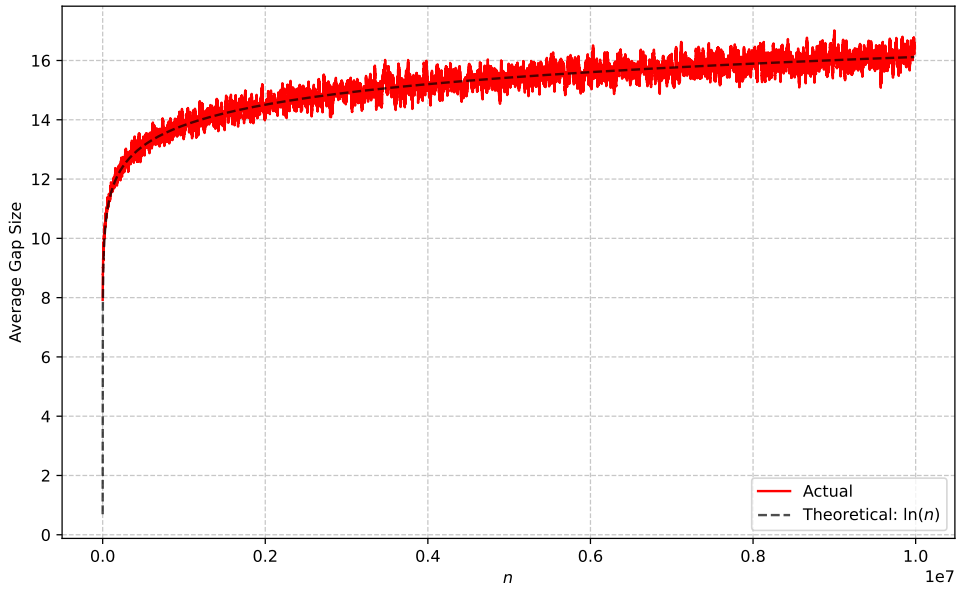


Figure 15: Linear plot of the actual average prime gap for n between 1 and 10^7 alongside the theoretical $\ln n$ prediction (see Point 2 of § 8.6.1).

chaotic in detail.

4. Regarding the lower bound on the size of prime gaps, the smallest possible prime gap is 2 (excluding the exceptional case of 2 and 3 which have a gap of 1). In this regard, the twin prime conjecture hypothesizes that there are infinitely many prime pairs $(p, p+2)$ and hence there are infinitely many prime gaps of size 2. The infinitude of gaps of size ≤ 246 (i.e. there are infinitely many pairs of primes whose difference is at most 246) has been proven (see § 5.1.44). Also see footnote [576].
5. Regarding the upper bound on the size of prime gaps, there is no such bound (i.e. arbitrarily large gaps between primes occur). A famous construction that proves this claim is:

$$(n!+2), (n!+3), \ldots, (n!+n) \tag{147}$$

which is a sequence of $n-1$ consecutive composite integers (and hence we have a gap consisting of at least $n-1$ consecutive composite numbers noting that we can choose n to be as large as we wish). A similar construction with primorials $n\#$ (see the Note in § 2.1.64) replacing factorials $n!$ also works (and is more efficient).
6. There are many theorems and conjectures that deal directly or indirectly with issues related to the size and distribution of prime gaps. Examples of such theorems and conjectures (from what we investigated in this book) are: the prime number theorem (see § 5.1.31), Bertrand's postulate (see § 5.1.2), Andrica's conjecture (see § 6.1.4), Cramer's conjecture (see § 6.1.12), Legendre's conjecture (see § 6.1.21), and Oppermann's conjecture (see § 6.1.25). Also see § 8.5.

8.6.2 Patterns of Prime Gaps

Some patterns (related to the size and distribution of prime gaps) have already been indicated in the previous subsection (e.g. an average gap size of $\ln n$ between primes near n; see § 8.6.1). In fact, there are many other gap patterns indicated (mostly indirectly) by proven theorems or open problems and conjectures. An example of such patterns is the fact indicated by the Polignac conjecture (see § 6.1.26

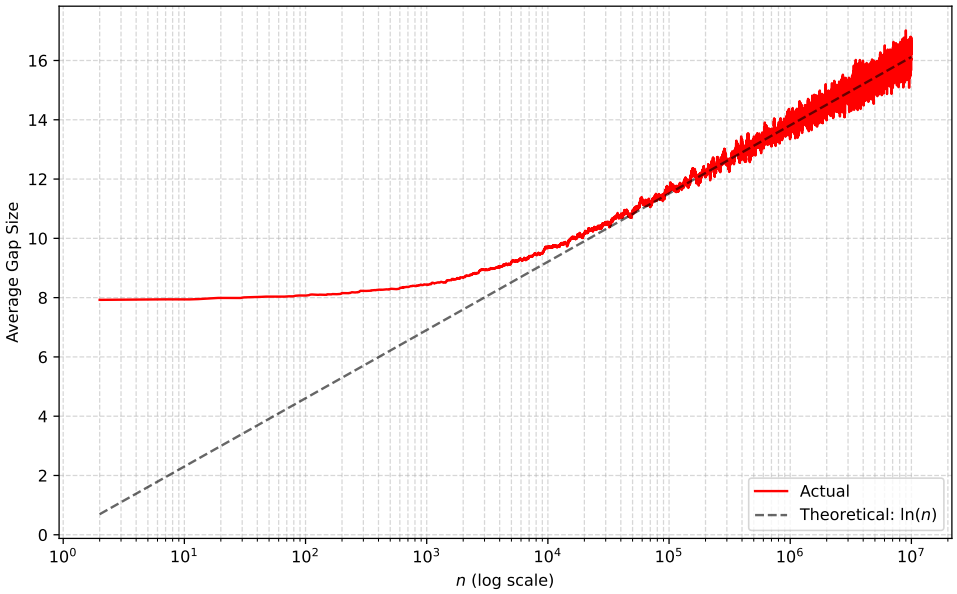


Figure 16: Logarithmic plot of the actual average prime gap for n between 1 and 10^7 alongside the theoretical $\ln n$ prediction (see Point 2 of § 8.6.1).

and Point 12 of § 8.5) which suggests that every positive even integer occurs as a prime gap infinitely many times.

The first Hardy-Littlewood conjecture related to prime k-tuples (see § 6.1.17) may provide another example of such pattern (although the "gap" in this case may have a loose sense since it may not be between consecutive primes).[750] In fact, within this loose sense even theorems like Dirichlet's theorem (see § 5.1.11) and the Green-Tao theorem (see § 5.1.17) may provide examples of such pattern.

Anyway, recent studies indicate that prime gaps are not equally likely to follow one another, which suggests that even within the supposed chaos of prime gaps at the local (or "microscopic") level, there may still be a deep underlying structural order and subtle patterns (such as frequent appearance of gaps of certain size) that may be formally established and rationalized in future research.

8.6.3 Known Prime Gaps

The following records have been reported as of June 2026:[751]

1. The largest known prime gap with proven-prime endpoints is 1113106. Here, "proven-prime endpoints" means that the primality of both endpoint numbers has been rigorously established, and all intervening integers have been verified to be composite.
2. The largest known prime gap with probable-prime endpoints is 16045848. Here, "probable-prime endpoints" means that the endpoints have passed appropriate probable-prime tests but their primality has not been rigorously proved. Such tests provide strong evidence of primality, but their precise guarantees depend on the tests and assumptions used.

[750] We should distinguish between strict prime gaps (i.e. differences between consecutive primes) and the more general notion of "gaps" representing distances in sequences of primes regardless of being consecutive or not (as in k-tuples for instance). So, "loose sense" refers to the latter where such gaps may be labeled as "generalized gaps".

[751] We note that record values may change as new computational results become available, and reported figures may differ according to the definitions, primality-certification standards, and conventions used. Also refer to `https://primegap-list-project.github.io/` as a useful source of information and data on prime gaps.

3. The largest known maximal prime gap is 1854 (which follows the prime 1014123199963633090 69).[752] A maximal prime gap is a difference between two consecutive primes that is strictly larger than every preceding prime gap. This record is distinct from the largest known prime gap overall, that is: a gap can be much larger than 1854 without being maximal, provided an even larger gap has already occurred at a smaller prime.
4. The smallest prime gap is 1, occurring only between 2 and 3. It is also the only odd prime gap, since every prime other than 2 is odd, and the difference between two odd integers is even.

8.7 Topics Related to the Distribution of Primes

We outline in this section some topics in number theory related to the distribution of primes. In fact, there are many such topics and hence the following topics are just a sample.

8.7.1 Chebyshev's Bias

Chebyshev's bias, also known as a prime number race, refers to the phenomenon that certain classes of primes appear more frequently than others up to a given limit, even when the classes have the same asymptotic relative density among all primes. More specifically, for most cutoffs x, the number of non-Pythagorean primes is greater than the number of Pythagorean primes (see § 2.1.66). For example, the count of non-Pythagorean primes is greater than or equal to the count of Pythagorean primes for every cutoff $x < 26861$. At $x = 26861$, the latter count first exceeds the former.[753]

Although it is proven unconditionally that the lead switches infinitely many times as $x \to \infty$, the non-Pythagorean primes dominate the race the vast majority of the time. Under the generalized Riemann hypothesis for the relevant Dirichlet L-functions, together with the linear-independence hypothesis on their zero ordinates, the logarithmic density of the set of cutoffs where the non-Pythagorean primes lead the race has been calculated to be about 0.9959.

8.7.2 Ulam Spiral

The Ulam spiral (also known as the *prime spiral*) is a graphical representation of prime numbers that reveals unexpected non-random patterns in their distribution. It shows that primes tend to cluster along diagonal, horizontal, and vertical lines. The spiral is created by arranging positive integers in a square grid, starting from the center and moving outwards in a spiral pattern, usually counter-clockwise (see the left hand side frame of Figure 17). The non-primes are then removed (or the prime numbers are highlighted) to show the final pattern of the distribution of primes within this two-dimensional construction (see the right hand side frame of Figure 17).

Figure 18 shows the pattern of the distribution of primes in this construction for the first 10^4 positive integers. As we see, the plot shows that the distribution of primes exhibits a considerable degree of structural regularity. So, while the distribution of primes is often considered irregular and random, the Ulam spiral suggests that primes have a deeper underlying order within the sequence of positive integers.

8.7.3 Number of Primes vs Number of Their Digits

In this subsection we briefly investigate the number of prime numbers as a function of the number of their digits. This function is obviously base-dependent and hence we use base 10 (i.e. decimal representation)

[752] See `https://pzktupel.de/RecordGaps/GAP01.php` and `https://primegap-list-project.github.io/lists/prime-gaps-high-watermarks/`.
[753] See `https://oeis.org/A007350`.

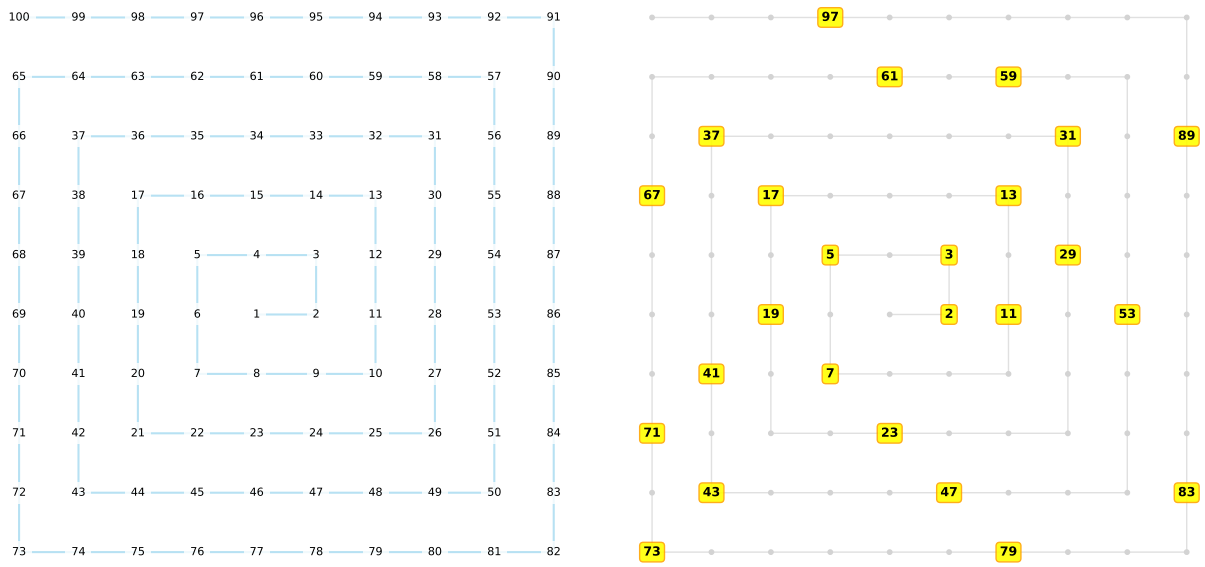


Figure 17: A plot showing how to construct the Ulam spiral. See § 8.7.2.

because it is the conventional base for representing numbers in mathematics. In fact, this issue can be elaborated (such as investigating the issue considering various base systems) but in this volume we limit our attention to a simple plot (i.e. number of primes versus number of digits) in base 10.

In Figure 19 we present a plot of the number of primes versus the number of digits n for $1 \leq n \leq 10$ on a semi-logarithmic scale. The plot shows a clear upward trend, indicating that as the number of digits increases, the total number of prime numbers grows in a highly predictable manner. The nearly linear trend on this log-scaled axis demonstrates that the growth rate is roughly exponential. This behavior is a direct consequence of the prime-counting function $\pi(x)$ and its asymptotic distribution as described by the prime number theorem (see § 5.1.31 and § 8.2.1). Specifically, the number of primes grows approximately exponentially with the number of digits, but the factor $1/n$ moderates this growth. Correspondingly, the proportion of n-digit integers that are prime decreases asymptotically as $1/(n \ln 10)$.

8.7.4 Relations between Prime Distribution and Primality Testing and Sieving

There are broad relationships between prime distribution and primality testing and sieving. Theorems and conjectures that handle the distribution of primes can provide theoretical guidance for testing and sieving, e.g. in optimizing sieving ranges and primality testing searches. In the following points we provide a glimpse on this issue:

1. Distribution theorems estimate the density of primes around a given number, and this can provide guiding expectations about how many candidates a search may need to examine (which is useful for designing efficient testing and sieving strategies). As a specific example, the prime number theorem (see § 5.1.31) states that the number of primes less than x is approximately $x/\ln x$. This means the density of primes near a large integer n is roughly $1/\ln n$. Accordingly, this can be exploited as an algorithmic guide to accurately predict how many integers must be tested on average before hitting a prime. For instance, if searching for a 100-digit prime, one must sample roughly $\ln(10^{100}) \approx 230$ random candidates (or about 115 odd candidates). This directly informs the design, time-complexity estimates, and optimization of primality testing and sieving software.
2. Existence theorems can provide rigorous bounds for searches for prime numbers. For example, Bertrand's

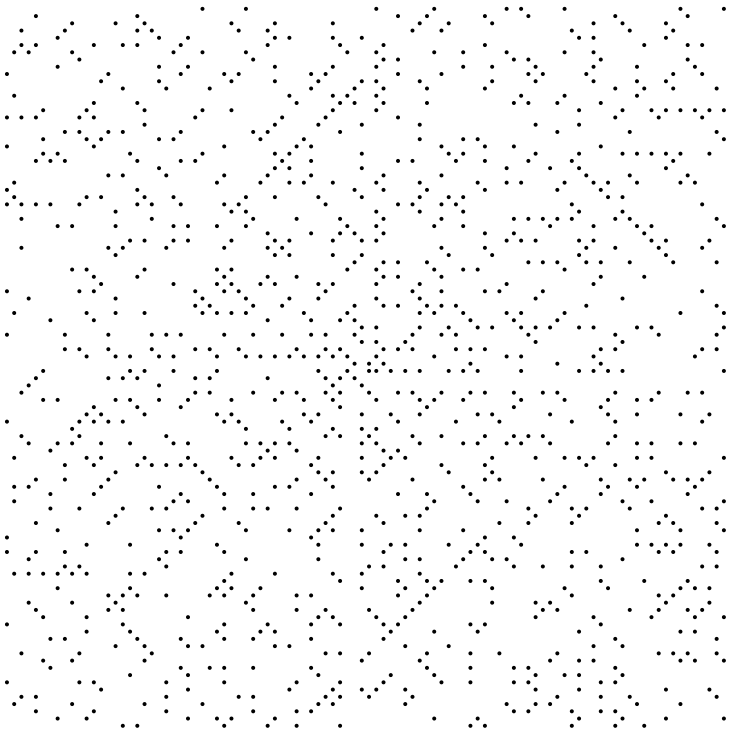


Figure 18: The Ulam spiral for the first 10^4 positive integers. See § 8.7.2.

postulate (see § 5.1.2) asserts that for every integer $n > 1$, there exists at least one prime p satisfying $n < p < 2n$. This guarantees that a prime larger than n can be found by searching the finite interval $(n, 2n)$. In an algorithm that examines candidates systematically and correctly tests their primality, this result provides an explicit upper bound on the search range and a mathematically justified stopping condition. Although the postulate does not itself dictate a specific search algorithm, it supports formal proofs of termination and establishes a strict bound on the maximum number of candidates an algorithm must examine.

3. The preceding discussion of distribution theorems can be extended, with appropriate caution, to conjectures about prime distribution. Conjectures supported by extensive computational evidence may provide useful heuristic guidance for estimating prime density and expected search effort, and may inform the design of probabilistic search and sieving strategies. However, empirical verification does not establish their universal validity, and their practical use must depend on the specific conjecture, the available evidence, and the algorithmic context. Each application should therefore be assessed on a case-by-case basis. As an example, Cramer's conjecture (see § 6.1.12) asserts that the maximum gap between consecutive primes up to x is $O(\ln^2 x)$ as $x \to \infty$. Although unproved, this conjecture provides a heuristic indication of the scale of large prime gaps. It may therefore inform the analysis of prime-search strategies, but it does not establish rigorously accurate probabilistic limits on maximum search intervals. Decisions concerning memory allocation and segment sizes in parallel sieving implementations may therefore benefit from this heuristic, but they require additional algorithmic analysis and empirical performance evaluation.

Overall, results on prime distribution, whether established theorems or well-supported conjectures, can contribute to the analysis and design of primality testing and sieving algorithms. Rigorous theorems can

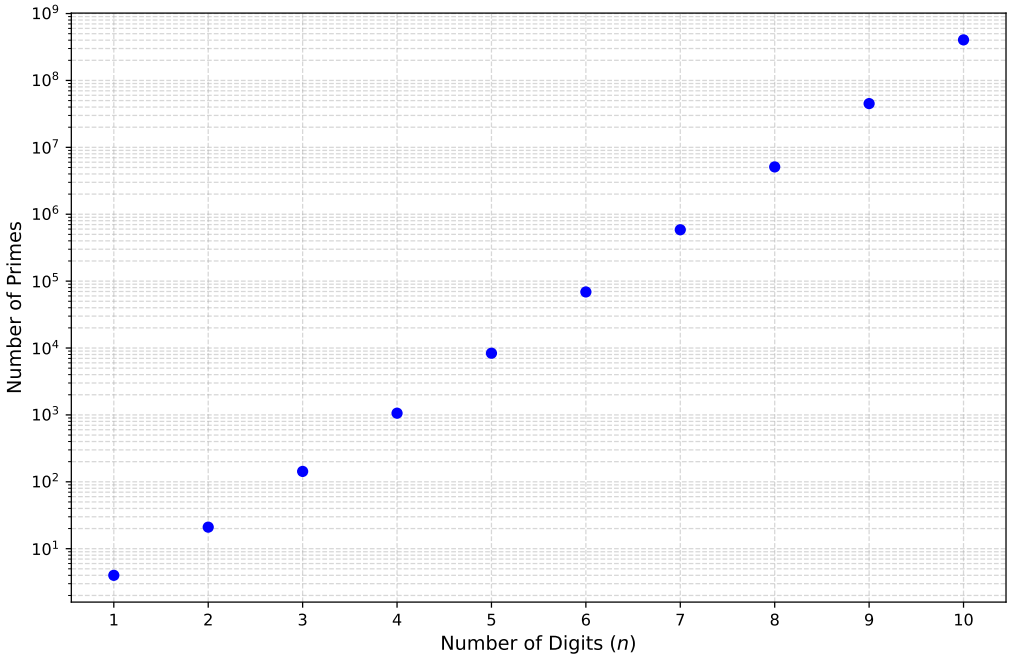


Figure 19: Plot of the number of primes versus the number of their digits n for $1 \leq n \leq 10$ on a semi-logarithmic scale. The points represent the exact number of primes calculated within each digit interval using the prime-counting function difference $\pi(10^n) - \pi(10^{n-1})$. See § 8.7.3.

establish the existence of primes within specified intervals, while distribution estimates and conjectural results can provide guidance on prime density and expected search effort. These insights can help assess computational costs, plan search strategies and inform algorithmic decisions. However, their practical implications depend on the strength of the underlying results and the specific algorithms being considered.

Chapter 9
Miscellaneous Topics

In this chapter we discuss, rather briefly, miscellaneous topics related to prime numbers.

9.1 Sequences Related to Primes

In this section we briefly investigate a number of sequences that have a connection to the investigation of prime numbers.[754]

9.1.1 Aliquot Sequence

The aliquot sequence is a sequence of natural numbers where each term of it is the sum of the proper divisors of the previous term. The sequence ends when it reaches 1 because the sum of the proper divisors of 1 is 0. According to the Catalan-Dickson conjecture, every aliquot sequence is bounded and will ultimately terminate in either one of three predictable ways: ending with a prime number (which leads to 1, and then terminates at 0), ending with a perfect number, or ending with a set of amicable or sociable numbers (and hence falling into a repeating cycle). An opposite conjecture (by Guy and Selfridge) is that some aliquot sequences are unbounded above (i.e. they diverge) and hence the Catalan-Dickson conjecture is false.

9.1.2 Catalan-Mersenne Sequence

The Catalan-Mersenne sequence (which may also be referred to as Catalan-Mersenne chain or numbers) is defined recursively as follows:

$$a_0 = 2 \qquad\qquad a_n = 2^{a_{n-1}} - 1 \quad (n > 0) \tag{148}$$

The first five terms of this sequence (i.e. a_0 through a_4) are:

$$2, 3, 7, 127, 170141183460469231731687303715884105727$$

noting that they are all prime.[755] According to the Catalan-Mersenne conjecture, all terms of this sequence are prime numbers. The primality of a_n for all $n \geq 5$ is currently unknown.[756]

9.1.3 Cunningham Chains

A Cunningham chain is a finite sequence of prime numbers in which each term is related to the preceding term by a specified recurrence. More specifically, a Cunningham chain of the first kind of length k (often referred to as being of Sophie Germain type; see § 2.1.76) is a sequence of precisely k prime numbers

[754] We note that the sequences here are mostly supposed to be related to primes in their definition, construction, or properties (unlike, for instance, the Fibonacci sequence whose relation to primes is "casual", i.e. by having prime terms).

[755] See `https://oeis.org/A007013`.

[756] It is worth noting that a_5 is a colossal number with about $10^{37.70942}$ decimal digits. It is so large that proving its primality is intractable using currently known practical methods, though computational searches have verified it has no prime factors below 10^{51}.

$(p_1, \ldots, p_k)$ where $p_{i+1} = 2p_i + 1$ (for all $1 \leq i < k$). This means that all terms of this sequence except the first are safe primes, and all terms except the last are Sophie Germain primes. Similarly, a Cunningham chain of the second kind of length k is a sequence of precisely k prime numbers $(p_1, \ldots, p_k)$ where $p_{i+1} = 2p_i - 1$ (for all $1 \leq i < k$).

As an example, (2, 5, 11, 23, 47) is a Cunningham chain of the first kind of length 5 (noting that the next number in the sequence, 95, is composite). Similarly, (19, 37, 73) is a Cunningham chain of the second kind of length 3 (noting that the next number in the sequence, 145, is composite). It is conjectured that there are infinitely many Cunningham chains of every given finite length k, for both the first and second kinds.[757] It is worth noting that Cunningham chains may be generalized to sequences of prime numbers $(p_1, \ldots, p_k)$ such that $p_{i+1} = ap_i + b$ or $p_{i+1} = ap_i - b$ (for all $1 \leq i < k$) where a and b are fixed positive coprime integers.

9.1.4 Euclid-Mullin Sequence

The Euclid-Mullin sequence is an infinite sequence of distinct prime numbers derived from the constructive method used in Euclid's proof that there are infinitely many primes. The sequence is generated by starting with the prime 2 and iteratively selecting the least prime factor of $(p_1 \times p_2 \times \cdots \times p_k) + 1$ to find the next term p_{k+1}. In other words, each term in the sequence is the least prime factor of one plus the product of all earlier terms. The first 20 terms of this sequence are: 2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, 52662739, 23003, 30693651606209, 37, 1741, 1313797957.[758] As we see, the Euclid-Mullin sequence is not monotonic. An open problem in number theory is whether every prime number eventually appears in this sequence. It is conjectured (supported by heuristic arguments) that they actually do.

9.1.5 Pillai Sequence

The Pillai sequence consists of integers whose greedy representations as sums of primes (and the number 1) establish successive records for the number of summands required. The greedy algorithm repeatedly subtracts the largest prime not exceeding the current remainder, stopping when the remainder reaches 0 or 1. If the remainder reaches 1, it is included as the final summand, even though 1 is not prime. The sequence therefore records the smallest non-negative integer whose greedy representation requires exactly n summands, for each $n \geq 0$. The first six terms in this sequence are: 0, 1, 4, 27, 1354, 401429925999155061.[759] For clarity, we note:

- 0 requires 0 terms.
- 1 requires 1 term (1).
- 4 requires 2 terms ($4 - 3 = 1 \quad \rightarrow \quad 3 + 1$).
- 27 requires 3 terms ($27 - 23 = 4 \quad \rightarrow \quad 4 - 3 = 1 \quad \rightarrow \quad 23 + 3 + 1$).

9.1.6 Prime-Counting Sequence

This sequence represents the number of prime numbers less than or equal to n [i.e. $\pi(n)$; see § 8.2.1] where $n = 1, 2, \ldots$. The first 20 terms of this sequence are: 0, 1, 2, 2, 3, 3, 4, 4, 4, 4, 5, 5, 6, 6, 6, 6, 7, 7, 8, 8.[760] The sequence steps up by 1 every time it hits a prime (i.e. $n \in \mathbb{P}$) and stays the same when n is not prime.

[757] No Cunningham chain can have infinite length, since every such chain must eventually contain a composite number. For $k = 2$, the first kind conjecture is equivalent to the conjecture that there are infinitely many Sophie Germain primes, or equivalently, infinitely many safe primes.

[758] See `https://oeis.org/A000945`.

[759] See `https://oeis.org/A066352`.

[760] See `https://oeis.org/A000720`.

9.1.7 Prime Gaps Sequence

This sequence represents the differences between consecutive prime numbers, i.e, $g_n = p_{n+1} - p_n$ where $n = 1, 2, \ldots$. The first 20 terms of this sequence are: 1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2.[761] All terms of this sequence are even except the first.

9.1.8 Sequences of Prime-Generating Constants

A prime-generating constant is a real number that can be plugged into a specific mathematical function to output prime numbers. The following are prominent examples of sequences of prime numbers generated by certain constant-based formulae:

1. Mills' sequence: this is a sequence of prime numbers generated by taking the floor of A^{3^n} (for $n = 1, 2, \ldots$) where $A \approx 1.306377883863080690468$6 is the Mills constant (see § 5.1.30). Also see § 2.1.44 and § 9.3.
2. Wright's sequence: this is a sequence of prime numbers generated by taking the floor of iterated exponentiation starting from a specific real-valued constant (whose existence is proven). The sequence is built using the following recursive rule:

$$g_0 = \alpha \qquad\qquad g_{n+1} = 2^{g_n} \quad (\text{for } n \geq 0) \tag{149}$$

   where $\lfloor g_n \rfloor$ is prime for all $n \geq 1$. The parameter α is known as the Wright constant which is ≈ 1.92878.[762] The first three primes of this sequence are: 3, 13, 16381.[763] Also see § 9.3.

It is noteworthy that despite their mathematical elegance, prime-generating constants and their associated formulae have very limited practical usefulness for generating large primes. Although these formulae guarantee the primality of the integers they generate under the appropriate mathematical assumptions, calculating their terms efficiently can be difficult. In particular, obtaining sufficient precision in a prime-generating constant may require substantial information about the primes in its associated sequence, depending on how the constant is defined and constructed. Consequently, such constants are primarily of theoretical and illustrative interest, demonstrating the power of mathematics to encode an infinite sequence in a single real number and a simple formula. They can be viewed as mathematical forms of information encoding, although extracting that information may be computationally expensive. In practical applications, especially cryptography, established prime-generation algorithms are far more suitable because they allow primes to be generated and tested efficiently.

9.2 Series Related to Primes

In this section we briefly investigate common examples of series that have connection to the investigation of prime numbers.

9.2.1 Harmonic Series of Primes

The harmonic series of prime numbers is the sum of reciprocals of all primes, that is:

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots = \left(\sum_{p \in \mathbb{P}} \frac{1}{p} \right) \quad \to \quad \infty \tag{150}$$

[761] See `https://oeis.org/A001223`.
[762] See `https://oeis.org/A086238`.
[763] See `https://oeis.org/A016104`.

This series is divergent (as indicated in the equation) noting that its divergence is used to prove the infinitude of prime numbers (see § 1.6). Also see Figure 11 in § 5.1.28.

9.2.2 Alternating Harmonic Series of Primes

This is the same as the harmonic series of prime numbers (see § 9.2.1) but with an alternating sign, that is:

$$\frac{1}{2}-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{11}-\cdots=\left(\sum_{n=1}^{\infty}(-1)^{n-1}\frac{1}{p_n}\right)\approx 0.26960635 \tag{151}$$

i.e. it is convergent (noting that it satisfies the conditions of the alternating series test).

9.2.3 Series of Reciprocal Squares of Primes

This series is the sum of the reciprocals of squares of all prime numbers, that is:

$$\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\frac{1}{11^2}+\cdots=\left(\sum_{p\,\in\,\mathbb{P}}\frac{1}{p^2}\right)\approx 0.45224742 \tag{152}$$

i.e. it is convergent (which follows directly from the fact that the series of reciprocal squares of all positive integers converges to $\pi^2/6$).

9.2.4 Twin Prime Series

This series represents the sum of the reciprocals of all twin primes, that is:

$$\sum_{\substack{p\in\mathbb{P}\\ p+2\in\mathbb{P}}}\left(\frac{1}{p}+\frac{1}{p+2}\right)=\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\cdots=\mathcal{B}_2\approx 1.90216058 \tag{153}$$

where $\mathcal{B}_2$ is Brun's constant.[764] So, this series is convergent (see § 5.1.5).

9.3 Constants Related to Primes

The following are some examples of common constants closely-related to (or associated with) prime numbers and they are frequently met in the literature of prime number theory:

1. Artin's constant (denoted by C_A): this constant appears in Artin's conjecture on primitive root (see § 6.1.5). Broadly speaking, the constant represents the asymptotic density of prime numbers p for which a fixed integer a is a primitive root modulo p (up to a correction factor depending on a). It is expressed as an infinite product over all prime numbers p, that is:[765]

$$C_A=\prod_{p\text{ prime}}\left(1-\frac{1}{p(p-1)}\right)\approx 0.3739558136 \tag{154}$$

2. Brun's (twin primes) constant (denoted by $\mathcal{B}_2$): this is a series-defined constant obtained by summing the reciprocals of all twin primes (see § 5.1.5 and § 9.2.4). Its numerical value is approximately 1.90216058.[766]

[764] See `https://oeis.org/A065421`.
[765] See `https://oeis.org/A005596`.
[766] See `https://oeis.org/A065421`.

3. Copeland-Erdos constant (denoted by C_{CE}): this is a prime-built irrational number formed by concatenating the decimal digits of the prime numbers (i.e. $C_{\text{CE}} = 0.2357111317\ldots$).[767] Its name originates from the Copeland-Erdos theorem which states that this constant is a normal number in base 10 (see for instance Point 27 of § 5.2.8).
4. Euler-Mascheroni (or Euler) constant (denoted by γ): this constant appears frequently in analysis and number theory (including in topics related to prime numbers even though there is no reference to prime numbers in its definition; see for instance § 5.1.29 and § 5.1.37). It is defined as the limiting difference between the harmonic series and the natural logarithm, that is:[768]

$$\gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \ln n\right) \approx 0.5772156649 \tag{155}$$

5. Hardy-Littlewood (twin primes) constant (denoted by C_2 or Π): this is related to the density and distribution of twin primes and is defined and estimated as:[769]

$$C_2 = \prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right) \approx 0.6601618158 \tag{156}$$

6. Linnik's constant (denoted by L): this is a fundamental constant in analytic number theory that appears in Linnik's theorem which establishes an upper bound on the least prime in an arithmetic progression. The details are given in § 5.1.24.
7. Meissel-Mertens (or Mertens) constant (denoted by M): this is defined as the limiting difference between the harmonic series of primes (see § 9.2.1) and the double logarithm, that is:[770]

$$M = \lim_{x\to\infty}\left(\sum_{p\leq x}\frac{1}{p} - \ln(\ln x)\right) \approx 0.2614972128 \tag{157}$$

   Also see § 5.1.28 and Eq. 58 in particular.
8. Mills' constant (denoted by A):[771] this is a prime-generating constant (see § 5.1.30 and Point 1 of § 9.1.8).
9. Prime constant (denoted by ρ): this is a prime-encoding constant obtained by concatenating the values of the characteristic function of primes $\big[$i.e. $f(n) = 1$ if n is prime and $f(n) = 0$ if n is not prime$\big]$, that is: $\rho = 0.0110101000101\ldots$.[772] By extracting the n^{th} digit (after the decimal point) of this constant the output will tell whether n is prime or not. As a constant of a specific magnitude, $\rho \approx 0.0110101000101$ in binary which is equivalent to $\rho \approx 0.41468250985$ in decimal.[773]
10. The prime-encoding number in the Sierpinski formula (i.e. $C = 0.020300050000000700\ldots$): this is given by the formula in Point 5 of § 5.2.14.
11. Wright's constant (denoted by α): this is a prime-generating constant (see Point 19 of § 5.2.2 and Point 2 of § 9.1.8).[774]

---

[767] See `https://oeis.org/A033308`.
[768] See `https://oeis.org/A001620`.
[769] See `https://oeis.org/A005597`.
[770] See `https://oeis.org/A077761`.
[771] It may be more common to denote this constant by θ but we avoid this because it may cause confusion since θ is used to denote the first Chebyshev prime-counting function (see § 8.2.5). Also see `https://oeis.org/A051021`.
[772] See `https://oeis.org/A010051`.
[773] See `https://oeis.org/A051006`.
[774] See `https://oeis.org/A086238`.

9.4 Generalization of Primality into Higher Dimensions

There are generalizations and extensions to the concepts of *prime numbers* and *primality* beyond their ordinary meanings, which are linked to positive integers greater than 1 that are divisible only by themselves and 1. Some of these generalizations and extensions will be investigated in the following subsections. However, we should insist that this book (and the types of primes that we investigated in the previous chapters, and chapter 2 in particular) is all about ordinary prime numbers, and hence the discussion in the present section can be regarded as a digression.

In the present section we briefly investigate the generalization of the concept of *prime numbers* (and *primality*) into "higher-dimensional spaces" noting that the ordinary meaning of prime numbers is defined over the set of "one-dimensional" positive integers. Examples of such generalizations are: Gaussian primes, Gaussian Mersenne primes, Eisenstein primes, and Hurwitz primes (which are covered in the next subsections).[775]

9.4.1 Gaussian Primes

In the ring of Gaussian integers, a *Gaussian prime* is a Gaussian integer that cannot be factorized into simpler Gaussian integers (where in this context some ordinary prime numbers remain prime while others do not).[776] More technically, a Gaussian prime is a non-unit (and non-zero) Gaussian integer that cannot be factored as a product of two non-unit Gaussian integers. We note:

1. Considering the basic form of complex numbers, we have three main types of Gaussian primes:
   - Real Gaussian primes, i.e. Gaussian primes of the form $\pm p$ where p is an ordinary prime number (noting that only a subset of these numbers are Gaussian primes, i.e. those with $p \overset{4}{=} 3$). Examples of this type are: $\pm 3, \pm 7, \pm 11$.
   - Imaginary Gaussian primes, i.e. Gaussian primes of the form $\pm \mathrm{i}p$ where p is an ordinary prime number (noting again that only a subset of these numbers are Gaussian primes, i.e. those with $p \overset{4}{=} 3$). Examples of this type are: $\pm \mathrm{i}3, \pm \mathrm{i}7, \pm \mathrm{i}11$.
   - Strictly complex Gaussian primes, i.e. Gaussian primes of the form $a + \mathrm{i}b$ where $\mathbb{Z} \ni a, b \neq 0$ (noting again that only a subset of these numbers are Gaussian primes, i.e. those with $a^2 + b^2$ being an ordinary prime number). Examples of this type are: $\pm 1 \pm \mathrm{i}$ (considering all 4 possibilities).
2. From the above definitions we can see that Gaussian primes (within the Gaussian integer system) are the equivalent of prime numbers (within the ordinary integer system), that is:
   - The Gaussian integers (complex) correspond to the ordinary integers (real).
   - The unit Gaussian integers ± 1, $\pm \mathrm{i}$ (complex) correspond to the ordinary unit integer ± 1 (real).
   - The zero Gaussian integer $0 + 0\mathrm{i}$ (complex) corresponds to the ordinary zero integer 0 (real), and both are excluded from the definitions of primes.
   - "Gaussian prime cannot be factored as a product of two non-unit Gaussian integers" (complex) corresponds to "prime number cannot be factored as a product of two non-unit integers" (real).
3. If the norm of a Gaussian integer is an ordinary prime number, then the Gaussian integer is a Gaussian prime.[777] However, the converse is not always true: a Gaussian prime may have a composite norm. For example, 3 is a Gaussian prime because $3 \overset{4}{=} 3$, but its norm is $N(3) = 9$ which is composite.

---

[775] Strictly speaking, these examples concern generalizations of primality to other algebraic structures, rather than generalizations into higher spatial dimensions. Gaussian and Eisenstein primes arise from rings of integers in quadratic number fields, whereas Hurwitz primes belong to the Hurwitz quaternion ring. Nevertheless, in this section we use the language of higher dimensions as an informal means of motivating these generalizations, thereby simplifying the presentation and avoiding technical details that would distract from the main discussion. More precise and rigorous algebraic accounts will be provided in upcoming volumes.

[776] A Gaussian integer is a complex number (z) whose real and imaginary parts are integers, i.e. $z = a + \mathrm{i}b$ where $a, b \in \mathbb{Z}$ and i is the imaginary unit (i.e. $\mathrm{i}^2 = -1$). Unit Gaussian integers are ± 1, $\pm \mathrm{i}$.

[777] "Norm" here means algebraic norm, i.e. $N(z) = a^2 + b^2$.

4. Gaussian primes exhibit, when plotted in the complex plane, interesting geometric patterns arising from the symmetries of the Gaussian integer lattice as well as complex distribution patterns. Readers interested in visualizations of Gaussian primes can find many examples of such plots in the literature and online.

9.4.2 Gaussian Mersenne Primes

Gaussian Mersenne primes are Gaussian integers analogous to Mersenne primes (see § 2.1.41), and hence they may be referred to as Mersenne primes in Gaussian integers. So, they are a specialized proper subset of the Gaussian primes (see § 9.4.1). Formally, a Gaussian Mersenne prime is a Gaussian prime of the form $\mathscr{M}_p = (1+\mathrm{i})^p - 1$ where i is the imaginary unit and p is an ordinary prime. This should reveal the close similarity between the real (or ordinary) and complex (or Gaussian) Mersenne primes, and hence justify the labeling of Gaussian Mersenne primes, that is:
• Just as ordinary Mersenne primes are built from powers of 2, Gaussian Mersenne primes are built from powers of $(1+\mathrm{i})$ which is a Gaussian prime factor of 2, since $2 = (1+\mathrm{i})(1-\mathrm{i})$.
• As with ordinary Mersenne primes, the primality of the index p is a necessary but not sufficient condition for the primality of $\mathscr{M}_p$.

9.4.3 Eisenstein Primes

These are primes in $\mathbb{Z}[\omega]$ where ω is a primitive complex cube root of 1. An Eisenstein prime is an Eisenstein integer z (see the upcoming Note) that is non-zero, non-unit, and cannot be factored as a product of two non-unit Eisenstein integers. There are two types of Eisenstein prime:
• Ordinary prime numbers which are congruent to 2 (modulo 3) such as 2, 5, 11, 17.[778] All unit multiples of these primes (e.g. $-2, 2\omega$) are also Eisenstein primes (although only one associate is an ordinary prime number). The largest known ordinary Eisenstein prime is apparently $10223 \times 2^{31172165} + 1$ (with about 9.38 million decimal digits).
• The Eisenstein integers whose norm is an ordinary prime such as $1-\omega$ and $2+\omega$ (both of norm 3), or $3+\omega$ and $2-\omega$ (both of norm 7).

Note: *Eisenstein integers* are complex numbers of the form $z = a + b\omega$ where $a, b \in \mathbb{Z}$ and ω is a primitive complex cube root of 1, specifically:

$$\omega = e^{2\pi \mathrm{i}/3} = \frac{-1 + \mathrm{i}\sqrt{3}}{2} \tag{158}$$

The units (i.e. numbers with norm 1) in Eisenstein integers are: $\pm 1, \pm\omega, \pm\omega^2$. The (algebraic) norm $N(z)$ of an Eisenstein integer $z = a + b\omega$ is defined as:

$$N(z) = N(a + b\omega) = a^2 - ab + b^2 \tag{159}$$

The norm is always a non-negative integer. The norm is also multiplicative, i.e. $N(z_1 z_2) = N(z_1)N(z_2)$ where z_1, z_2 are Eisenstein integers.

9.4.4 Hurwitz Primes

These are a special type of numbers in the ring of Hurwitz quaternions (see the upcoming Note). While Hurwitz primes are not prime numbers in the ordinary sense (i.e. in $\mathbb{N}$), they are analogous to prime numbers in that they cannot be factored into the product of two non-unit elements in the ring of Hurwitz

[778] See `https://oeis.org/A003627`.

quaternions. A Hurwitz quaternion is prime if its norm (i.e. $a^2+b^2+c^2+d^2$) is an ordinary prime number (i.e. in $\mathbb{N}$).

Note: A *quaternion* is a four-dimensional number system that extends the concept of complex numbers (which are two-dimensional) by adding two additional imaginary parts (i.e. it consists of a real part and three imaginary parts). A quaternion is typically represented in the form $a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}$, where a, b, c, d are real numbers while $\mathrm{i}, \mathrm{j}, \mathrm{k}$ are imaginary units, i.e. $\mathrm{i}^2=\mathrm{j}^2=\mathrm{k}^2=\mathrm{ijk}=-1$ with the cross-multiplication relations $\mathrm{ij}=\mathrm{k}$, $\mathrm{jk}=\mathrm{i}$, $\mathrm{ki}=\mathrm{j}$ and with sign reversal for reverse multiplication (since multiplication is non-commutative).

Hurwitz quaternions (or *Hurwitz integers*) are a proper subset of the set of quaternions, which are of the form: $a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}$ where a, b, c, d are integers or half-odd integers (i.e. either all integers or all half-odd integers). The units in the Hurwitz quaternions are the invertible elements (i.e. those with a norm of 1), which include $\pm 1, \pm\mathrm{i}, \pm\mathrm{j}, \pm\mathrm{k}$ (as well as the 16 variations of $\pm\frac{1}{2}\pm\frac{1}{2}\mathrm{i}\pm\frac{1}{2}\mathrm{j}\pm\frac{1}{2}\mathrm{k}$). The (algebraic) norm $N(z)$ of a Hurwitz integer $z=a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}$ is defined as:

$$N(z)=N(a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k})=a^2+b^2+c^2+d^2 \tag{160}$$

The norm is always a non-negative integer (i.e. even when the coefficients a, b, c, d are half-odd integers). The norm is also multiplicative, i.e. $N(z_1 z_2)=N(z_1)N(z_2)$ where z_1, z_2 are Hurwitz integers.

9.5 Semiprimes

A semiprime (also known as *biprime*, and *2-almost-prime*) is a natural number which is the product of exactly two prime numbers (whether different like $21=3\times 7$ or identical like $25=5\times 5$). They are highly significant in cryptography (particularly in the RSA cryptosystem) as the security of the system relies on the difficulty of factoring a very large semiprime into its two constituent primes.

In the following points we briefly investigate some issues about semiprimes:

1. As indicated already, semiprimes are partitioned into two categories: square-free semiprimes (which are products of two distinct prime numbers), and square semiprimes (which are the squares of prime numbers). The former have exactly four positive divisors while the latter have exactly three positive divisors.
2. "Strong semiprimes" is a term used in cryptography to refer to square-free semiprimes whose factors are roughly the same size.[779] These are "strong" because they are much harder to factorize using common algorithms (and hence they are strong from a cryptographic viewpoint).
3. Semiprimes are almost as frequent as primes for very small integers, but as the integers grow larger semiprimes become more frequent than primes.[780] The distribution of semiprimes is governed by the counting function $\pi_2(x)$, which represents the number of semiprimes less than or equal to x. The asymptotic behavior of $\pi_2(x)$ may be given by:

$$\pi_2(x)\sim\frac{x\ln(\ln x)}{\ln x}\qquad\qquad(x\to\infty) \tag{161}$$

On comparing this to the prime-counting function $\pi(x)$ as given by the prime number theorem (see § 5.1.31 and Eq. 62 in particular) we can see that the ratio of semiprimes to primes is roughly $\ln(\ln x)$. Now, since $\ln(\ln x)$ grows to infinity (even though very slowly), semiprimes become increasingly more common than primes. Figure 20 gives a rough idea about the count of primes and semiprimes up to

[779] However, if the factors are extremely close, Fermat's factorization method (see § 7.10.4) may trivially break the system, while if one factor is too small, the elliptic curve method (see § 7.10.3) or the trial division algorithm (see § 7.10.12) may easily tear it apart.

[780] See `https://oeis.org/A001358` and `https://oeis.org/A000040` as well as Figure 20.

$x = 10^6$ and indicates their comparative asymptotic behavior as x increases towards infinity.

4. Notable theorems related to semiprimes are Chen's theorems I and II (see § 5.1.8 and § 5.1.9) and Iwaniec's theorem (see § 5.1.21).
5. Another notable theorem related to semiprimes is: there are infinitely many pairs of consecutive square-free semiprimes whose difference is at most 26. Subsequent improvements have reduced the bound to 6.

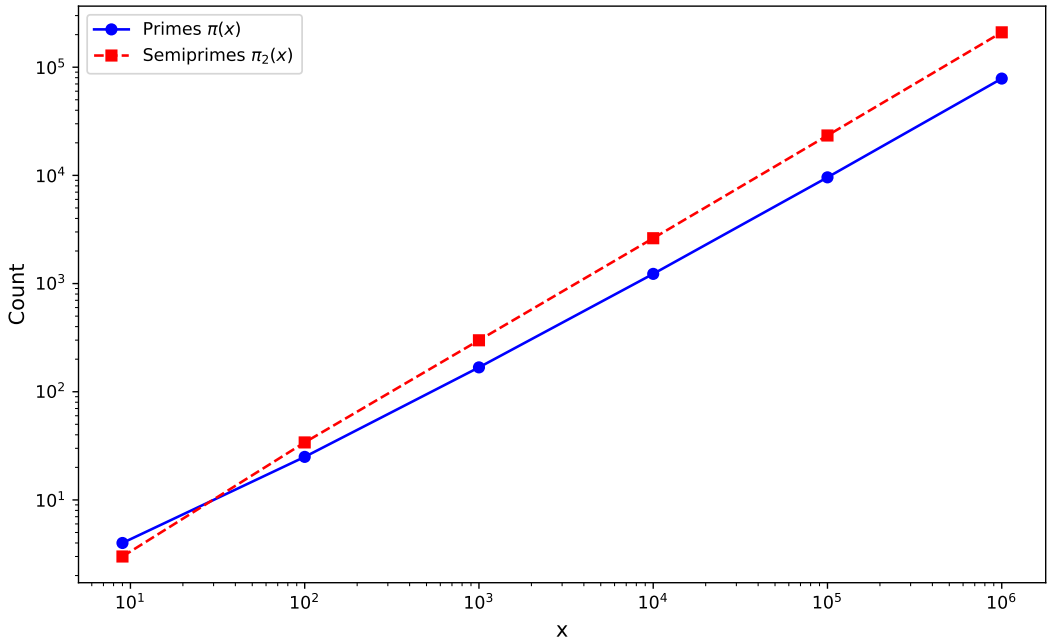


Figure 20: Logarithmic plot of $\pi(x)$ and $\pi_2(x)$ versus x. See § 9.5.

9.6 Almost-Primes

Almost-prime is a positive integer that has a given number of prime factors (counted with multiplicity). More specifically, $n \in \mathbb{N}$ is a k-almost-prime *iff* it is the product of exactly k prime numbers (whether different or not). For example, prime numbers are 1-almost-primes, semiprimes are 2-almost-primes (see § 9.5), and 8, 12, 18 are 3-almost-primes.[781]

It is worth noting the following:

1. Although the formal mathematical definition of k-almost-prime includes (in principle) any $k \in \mathbb{N}$, for the "almost-prime" terminology to be sensible and useful k should be a small natural number greater than 1 (say $k = 2, 3, 4$).
2. "k-almost-prime" may be used to mean: a number with at most k prime factors (counted with multiplicity). However, such use may depend on the context rather than convention.
3. Notable theorems related to k-almost-primes (i.e. 2-almost-primes or semiprimes) are indicated in Points 4 and 5 of § 9.5.

[781] Also see `https://oeis.org/A001358`, `https://oeis.org/A014612`, and `https://oeis.org/A014613`.

9.7 Pseudoprimes

A pseudoprime (also known as *false prime*) is a composite number that satisfies a primality condition normally expected to hold for prime numbers, and therefore can deceive certain primality tests into identifying it as prime. The term is usually associated with a specific primality test, since a number may be a pseudoprime with respect to one test but not another. Some authors use the term *pseudoprime* more broadly to refer to *probable primes*, including both genuine primes and composite numbers that pass the test. Pseudoprimes are commonly classified according to the prime property they imitate and the corresponding primality test they satisfy. In the following subsections, we briefly examine the most common types of pseudoprimes.

9.7.1 Absolute Pseudoprimes

An absolute pseudoprime (also known as *absolute Fermat pseudoprime*) is a composite integer n that is a Fermat pseudoprime to every base a coprime to it (see § 9.7.6). Consequently, an absolute pseudoprime cannot be detected as composite by Fermat's primality test using any coprime base (see § 7.3.6). In fact, absolute pseudoprimes are the same as Carmichael numbers (see § 5.1.15 and § 7.9.2). The first 10 absolute Fermat pseudoprimes are: 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341.[782] It has been proven that there are infinitely many Carmichael numbers.

9.7.2 Catalan Pseudoprimes

A Catalan pseudoprime is a composite integer that satisfies a specific congruence relation involving Catalan numbers that is otherwise true for all odd primes. More specifically, a composite number n is a Catalan pseudoprime if it satisfies the following congruence relation:

$$C_{(n-1)/2} \equiv (-1)^{(n-1)/2} \cdot 2 \pmod{n} \tag{162}$$

where C_k is the k^{th} Catalan number (see the Note in § 2.1.4). This congruence relation is satisfied by any odd prime n and hence composite numbers that satisfy it are pseudoprimes. There are only 3 known Catalan pseudoprimes which are: 5907, 1194649, 12327121.[783] However, it is conjectured that there are infinitely many Catalan pseudoprimes.

9.7.3 Elliptic Pseudoprimes

An elliptic pseudoprime is a composite integer that satisfies a primality condition derived from the theory of elliptic curves. Just as a Fermat pseudoprime (see § 9.7.6) resembles prime behavior in modular exponentiation, an elliptic pseudoprime resembles prime behavior in the group of points on an elliptic curve. In other words, an elliptic pseudoprime is a composite number that evades detection by a primality test that is based on elliptic curve groups (see for instance § 7.3.5), much like a Fermat pseudoprime evades detection by Fermat's primality test (see § 7.3.6). There are infinitely many elliptic pseudoprimes.

9.7.4 Euler-Jacobi Pseudoprimes

An Euler-Jacobi pseudoprime is a composite integer that satisfies the Euler criterion for a specific base (see § 5.1.13). More specifically, an odd composite integer n is an Euler-Jacobi pseudoprime to base $a \in \mathbb{N}$

[782] See `https://oeis.org/A002997`.

[783] See `https://oeis.org/A163209`. It is worth noting that the two largest known Catalan pseudoprimes are the squares of the only two known Wieferich primes (i.e. 1093 and 3511; see § 2.1.90).

if

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n} \tag{163}$$

where a and n are coprime and $\left(\frac{a}{n}\right)$ is the Jacobi symbol. The first 10 Euler-Jacobi pseudoprimes (for $a = 2$) are: 561, 1105, 1729, 1905, 2047, 2465, 3277, 4033, 4681, 6601.[784] There are infinitely many Euler-Jacobi pseudoprimes for any fixed base $a > 1$. It is worth noting that Euler-Jacobi pseudoprimes are a proper subset of Fermat pseudoprimes for a common base a (see § 9.7.6). Also see § 7.3.18 and Point 4 of § 7.9.5.

9.7.5 Euler Pseudoprimes

An Euler pseudoprime is an odd composite integer n that satisfies the following congruence relation:

$$a^{(n-1)/2} \equiv \pm 1 \pmod{n} \tag{164}$$

where a and n are coprime. As we see, the condition of Euler pseudoprime is weaker (or less restrictive) than the condition of Euler-Jacobi pseudoprime (see § 9.7.4) because the Jacobi symbol is more specific than ± 1 (i.e. the Jacobi symbol is specifically $+1$ or -1). So, every Euler-Jacobi pseudoprime is an Euler pseudoprime, but not every Euler pseudoprime is an Euler-Jacobi pseudoprime.

It is noteworthy that many (and possibly most) authors use the terms "Euler pseudoprime" and "Euler-Jacobi pseudoprime" interchangeably to refer to the stronger Jacobi symbol condition (i.e. what we call specifically Euler-Jacobi pseudoprime). The weaker (or looser) condition ± 1 may be identified as a basic Euler pseudoprime requirement to establish a distinction between the two or avoid a potential confusion. There are infinitely many Euler pseudoprimes for any fixed base $a > 1$.

9.7.6 Fermat Pseudoprimes

A Fermat pseudoprime (also known as *Poulet number* and *Sarrus number*)[785] is a composite number n that satisfies $a^{n-1} \overset{n}{=} 1$ for some base a coprime to n (and hence it mimics the result of Fermat's little theorem and passes the Fermat primality test for a specific base a; see § 5.1.15 and § 7.3.6). The first 10 Fermat pseudoprimes (to base 2) are: 341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701.[786] There are infinitely many Fermat pseudoprimes for any given base $a > 1$. It is worth noting that absolute pseudoprimes (see § 9.7.1) are a proper subset of Fermat pseudoprimes.

9.7.7 Fibonacci Pseudoprimes

A Fibonacci pseudoprime is a composite integer that satisfies specific congruence relations (or divisibility requirements) related to the Fibonacci sequence, and hence it behaves like a prime number under Fibonacci-based tests (see for instance § 7.3.7). More specifically, a Fibonacci pseudoprime is a composite integer n coprime to 5 that divides $\mathcal{F}_{n-\left(\frac{5}{n}\right)}$ where $\mathcal{F}_k$ is the k^{th} Fibonacci number and $\left(\frac{5}{n}\right)$ is the Jacobi symbol. This is based on the Fibonacci primality theorem which states: if $n \neq 5$ is a prime number then it must satisfy $n|\mathcal{F}_{n-\left(\frac{5}{n}\right)}$, and hence a composite number that mimics this prime property is a pseudoprime.[787] There are infinitely many Fibonacci pseudoprimes.

[784] See `https://oeis.org/A047713`.
[785] "Poulet numbers" may refer specifically to Fermat pseudoprimes to base 2.
[786] See `https://oeis.org/A001567`.
[787] See `https://oeis.org/A141137` and `https://oeis.org/A081264`.

9.7.8 Frobenius Pseudoprimes

A Frobenius pseudoprime is an odd composite integer that passes the Frobenius probable primality test (noting that this type of pseudoprimes is defined with respect to a specific monic polynomial which is usually a quadratic; see § 7.3.8).[788] So, such a composite integer resembles a prime in this property which makes it a pseudoprime. There are infinitely many Frobenius pseudoprimes for every fixed monic, square-free polynomial under the standard definition of the Frobenius test. Also see Point 5 of § 7.9.5.

9.7.9 Lucas Pseudoprimes

A Lucas pseudoprime is an odd composite integer that satisfies the Lucas probabilistic primality test (which may be seen as a more complex version of the Fermat primality test). The first 10 Lucas pseudoprimes are: 323, 377, 1159, 1829, 3827, 5459, 5777, 9071, 9179, 10877.[789] There are infinitely many Lucas pseudoprimes.

9.7.10 Perrin Pseudoprimes

A Perrin pseudoprime is a composite integer n that divides the n^{th} term of the Perrin sequence (see the Note in § 2.1.59). This division requirement is a necessary, but not sufficient, condition for primality and hence a composite integer that mimics this prime property is a pseudoprime. Perrin pseudoprimes are among the rarest known types of pseudoprime (noting that there are only two such numbers less than one million, i.e. 271441 and 904631).[790] However, it is proven that there are infinitely many Perrin pseudoprimes.

9.7.11 Somer-Lucas Pseudoprimes

A Somer-Lucas pseudoprime (also known as *Somer-Lucas d-pseudoprime* and *Lucas d-pseudoprime*) is an odd composite integer that mimics a primality property related to the Lucas sequences, and may be regarded as a specific generalization of the Fermat d-pseudoprime (see the upcoming Note). Under certain restrictions on d and the parameters of the Lucas sequence, the set of Somer-Lucas d-pseudoprimes may be finite, although the generality (or otherwise) of this claim should be checked in the literature.

Note: While a standard Fermat pseudoprime n to base a satisfies the congruence relation $a^{n-1} \stackrel{n}{=} 1$, a Fermat d-pseudoprime is a composite integer that satisfies the congruence relation:

$$a^{(n-1)/d} \stackrel{n}{=} 1 \tag{165}$$

for some positive integer d that divides $n-1$. This paradigm is usually explored within the context of broadening primality tests or identifying composite numbers that behave like primes under more specific conditions.

9.7.12 Strong Pseudoprimes

A strong pseudoprime is an odd composite integer that passes the Miller-Rabin primality test for a specific base a (see § 7.3.12). The first 10 strong pseudoprimes (to base 2) are: 2047, 3277, 4033, 4681, 8321, 15841, 29341, 42799, 49141, 52633.[791] Strong pseudoprimes are much rarer than the standard Fermat

[788] See for instance `https://oeis.org/A212424`. We note that monic polynomial is a polynomial whose leading coefficient is 1.
[789] See `https://oeis.org/A217120`.
[790] See `https://oeis.org/A013998`. Also see `https://oeis.org/A018187`.
[791] See `https://oeis.org/A001262`.

pseudoprimes (see § 9.7.6). However, it is proven that there are infinitely many strong pseudoprimes for any specific base $a > 1$. It is worth noting that strong pseudoprimes to a given base are a proper subset of Euler-Jacobi pseudoprimes to that base, and hence it is also a subset of Fermat pseudoprimes since Euler-Jacobi pseudoprimes are a proper subset of Fermat pseudoprimes (see § 9.7.4 and § 9.7.6). Also, there is no composite number that is a strong pseudoprime to every base coprime to it (unlike Carmichael numbers which are "Fermat pseudoprimes" to all coprime bases; see § 9.7.1). Also see Point 3 of § 7.9.5.

9.7.13 Wieferich Pseudoprimes

A Wieferich pseudoprime is a composite integer n that satisfies the congruence relation $v^{n-1} \overset{n^2}{=} 1$ where $\mathbb{N} \ni v \geq 2$ is a given base and $\gcd(n, v) = 1$. In other words, they are the composite analogues of Wieferich primes (see § 2.1.90).[792] It is not known whether there are infinitely many Wieferich pseudoprimes for any fixed base $v \geq 2$.

9.8 Methods and Algorithms

Mathematical methods and computational algorithms in prime number theory (and related topics) are broad subjects, and hence detailed treatment is deferred to future volumes. Therefore, in this section we provide a sample of these techniques alongside some illuminating examples. In fact, we have already encountered such methods and algorithms (mainly in chapter 7) represented by primality tests, sieves, and integer factorization algorithms, and hence we refer the reader to that chapter (see in particular § 7.3, § 7.4 and § 7.10). We may also refer to § 5.2.14 and § 5.2.15 which provide more examples of such methods and algorithms (related to the calculation of primes and estimation of p_n) and their theoretical background.

9.8.1 Evaluation of $\pi(x)$

Specialized algorithms are required to calculate the prime-counting function $\pi(x)$ (see § 8.2.1) because counting primes individually becomes impractical as numbers get larger. To calculate the precise value of $\pi(x)$, we cannot use the prime number theorem (see § 5.1.31) because it gives an asymptotic estimate rather than an exact counting formula.[793] The following are two examples of such methods and algorithms with brief explanations:

1. Meissel-Lehmer algorithm: this is a highly efficient combinatorial method for computing exact values of the prime-counting function $\pi(x)$. The method uses an inclusion-exclusion approach to count integers not divisible by any prime $p \leq \sqrt{x}$.[794] Instead of checking every number up to x (which would be slow), the algorithm uses optimized recursion and inclusion-exclusion ideas to count primes without the need to find every prime number individually. Hence, it is much faster than naive prime counting or standard linear sieves.
2. Lagarias-Miller-Odlyzko algorithm: this is a combinatorial algorithm for computing the exact value of the prime-counting function $\pi(x)$ more efficiently than earlier methods, including earlier formulations of the Meissel-Lehmer algorithm (see Point 1). The theoretical analysis of this algorithm establishes upper bounds on its computational complexity, expressed in terms of the number of arithmetic operations required and the amount of storage needed as functions of x. These are complexity bounds, concerning

[792] See for instance `https://oeis.org/A353175`.

[793] In practice, even a straightforward algorithm like the sieve of Eratosthenes can compute $\pi(x)$ exactly for moderately large values of x, but specialized prime-counting algorithms become necessary when x is so large that generating all primes up to x is no longer efficient or feasible.

[794] The actual Meissel-Lehmer algorithm uses a different threshold to optimize the recursive calls and improve performance. The above threshold (i.e. $p \leq \sqrt{x}$) is to indicate the fundamental limit of divisibility by primes rather than stating the actual threshold in the Meissel-Lehmer algorithm.

the algorithm's running time and space requirements, rather than upper or lower bounds on the value of $\pi(x)$ itself, as in the estimates associated with the prime number theorem (see § 5.1.31). The analysis demonstrates significant improvements in asymptotic running time and storage requirements compared to earlier methods.

We should finally note that the methods and algorithms for evaluating $\pi(x)$ may be regarded as prime sieves (see § 7.4) but in a different sense from that of ordinary sieves, i.e. while ordinary sieves (such as the sieve of Eratosthenes; see § 7.4.2) are about finding and listing primes within given sets of integers, these algorithms are about counting primes within such sets of integers. Thus, the output of ordinary sieves is a list of prime numbers, whereas the output of these algorithms is a single non-negative integer (representing the number of primes). We should also refer to footnote [793], which indicates the possibility of using prime sieves as prime-counting algorithms. Overall, prime-counting algorithms are closely related to prime sieves, and some employ sieving techniques as part of their computations.

9.8.2 Prime Calculation and Generation

Examples of analytic or theoretical methods for calculating and generating primes have already been encountered (see for instance § 5.2.14). In this subsection we provide another example, but this time of computational (or algorithmic) nature, namely Conway's PRIMEGAME which is a FRACTRAN-based algorithm (or program) designed specifically to generate prime numbers sequentially through producing powers of 2 whose exponents are precisely the prime numbers in ascending order. PRIMEGAME uses the following 14 fractions to generate prime numbers:

$$\frac{17}{91}, \frac{78}{85}, \frac{19}{51}, \frac{23}{38}, \frac{29}{33}, \frac{77}{29}, \frac{95}{23}, \frac{77}{19}, \frac{1}{17}, \frac{11}{13}, \frac{13}{11}, \frac{15}{2}, \frac{1}{7}, \frac{55}{1} \tag{166}$$

It is worth noting that FRACTRAN is an esoteric programming language in which programs consist of lists of fractions. Although FRACTRAN is theoretically capable of universal computation, it is generally highly impractical for most real-world software development or efficient mathematical calculation (including prime generation by PRIMEGAME).

9.9 Residue Classes of Primes

Primes within modular residue classes obey deep arithmetic laws governing divisibility, asymptotic distribution, and subtle statistical biases. For a given modulus q, primes not dividing q can occur only in residue classes a satisfying $\gcd(a, q) = 1$. There are exactly $\phi(q)$ such reduced residue classes. Dirichlet's theorem on arithmetic progressions (see § 5.1.11) guarantees that each reduced residue class contains infinitely many primes. We may also refer in this context to the prime number theorem for arithmetic progressions (see § 5.1.32) which shows that primes are asymptotically equidistributed among the reduced residue classes modulo q.

Despite this asymptotic symmetry, finite ranges exhibit striking irregularities. One of the best-known examples is Chebyshev's bias, in which certain residue classes, typically quadratic non-residues modulo q, tend to lead the prime race more often than quadratic residues, although the lead changes infinitely many times.[795] Thus, the bias concerns how often one class is ahead in the counting function rather than a permanent excess of primes.

An additional phenomenon is the apparent "conspiracy" among consecutive primes. Recent research shows that consecutive primes are not independent with respect to residue classes modulo q. Instead, a prime is less likely than expected to occupy the same residue class as its immediate predecessor and more

[795] We refer the reader to § 8.7.1 for an introductory discussion of Chebyshev's bias. Although concise, it should provide a sufficient background to appreciate this issue and the related discussion in the present section.

likely to appear in a different admissible class. This phenomenon is now understood as a consequence of arithmetic constraints together with the fine-scale structure of prime gaps.

9.10 Integers as Sums of Natural Powers of Primes

This is a topic in additive number theory that studies representations of integers as sums of powers of prime numbers, namely:

$$n = p_1^{k_1} + p_2^{k_2} + \cdots + p_r^{k_r} \tag{167}$$

where each p_i is a prime and each exponent k_i is a positive integer. This area includes classical theorems (such as Goldbach's ternary conjecture; see § 5.1.16) and conjectures (such as Goldbach's conjecture; see § 6.1.19), as well as questions concerning representations by sums of prime squares, prime cubes, or more general combinations of prime powers.

Researchers study these problems using techniques from analytic number theory, most notably the Hardy-Littlewood circle method and sieve methods. Many results show that every sufficiently large integer satisfying appropriate local or congruence conditions can be represented as a sum of a fixed number of prime powers. However, there is no general theorem characterizing exactly which integers admit representations as sums of arbitrary powers of primes, and many fundamental problems in this area remain open.

9.11 Relationships between Primes and Other Types of Numbers

The relationships between primes and other types and variants of numbers (mainly positive integers) constitute a broad subject and hence it is deferred to future volumes of this book. However, in the following list we provide some points that may help outline the items and structure of such investigation:

1. Primes and perfect powers (like perfect squares).
2. Primes and deficient/perfect/abundant numbers.
3. Primes and almost-perfect/quasi-perfect numbers.
4. Primes and amicable/sociable numbers.
5. Primes and triangular numbers.
6. Primes and factorial/primorial numbers.
7. Primes and powerful numbers.
8. Primes and pseudoprimes.
9. Primes and almost-primes.
10. Primes and sequences such as Fibonacci, Lucas, and Catalan (noting that some of these were introduced within the investigation of types of primes; see § 2.1).
11. Primes and complex numbers (see for instance § 5.1.14, § 6.1.29 and § 9.4).
12. Mersenne primes and perfect numbers.
13. Mersenne primes and triangular numbers.
14. Mersenne primes and untouchable numbers.
15. Thabit primes and amicable numbers.
16. Wagstaff primes and Mersenne numbers.
17. Wolstenholme primes and Bernoulli numbers.

In fact, this list can be extended substantially to include many other items, but this sample should be sufficient for illustrating the kind of issues that deserve investigation under this title. We may even include prime-related issues of different kinds (such as "primes and quadratic residues" and "primes and primitive roots").

We may also list the following statements as examples of the propositions and issues that represent this subject:

A. A prime number cannot be a perfect power.
B. No Mersenne prime can be an untouchable number.
C. For any fixed positive integer k there are only finitely many odd perfect numbers having exactly k distinct prime factors (a corollary of Dickson's theorem).
D. A composite integer $n > 1$ divides $a^n - a$ for all integers a *iff* n is square-free and $p - 1$ divides $n - 1$ for all the prime divisors p of n (Korselt's criterion for Carmichael numbers).
E. The only prime triangular number is 3.
F. Every cuban prime of the first kind is a centered hexagonal number.
G. For every prime $p \geq 7$ there is at least one pair of consecutive quadratic residues (modulo p) and one pair of consecutive quadratic non-residues.
H. Every prime modulus p admits primitive roots (mod p).
I. If p is a prime ≥ 5 then its primitive roots occur in incongruent pairs (r, r^*) where r^* is the modular multiplicative inverse of r (modulo p).
J. The product of all primitive roots modulo a prime $p \geq 5$ is congruent to 1 (mod p).

Also see § 5.2.9 and § 6.2.9.

Chapter 10
Applications of Primes

In this chapter we briefly investigate some of the common applications of prime numbers. However, before we go through these details we should note the following:

1. Prime numbers are found in many places (and even in some unexpected places) in the literature of various scientific disciplines such as biology and physics. However, the so-called "applications of prime numbers in Nature" (e.g. the alleged involvement of prime numbers in the structure of some plants and flowers or in the life cycle of some insects) are not included in the subject of this chapter since such "applications" are not really applications of prime numbers in their conceptual sense (which is what this book is about). Moreover, some of these "applications" are questionable (even in this stretched sense of "applications") as they seem to be projections of subjective contemplations and inner personal experiences on real life events and outside world phenomena.
2. Much research on prime numbers is theoretical, reflecting the fact that prime numbers belong to a fundamental area of pure mathematics. Although prime numbers have some useful applications in cryptography, computer science, and related fields, most results have no known immediate practical applications. This is echoed in the sentiment of some mathematicians who considered number theory to be among the most obviously useless branches of pure mathematics. This raises a broader question about the allocation of intellectual and financial resources to mathematical research for which the practical benefits are limited or uncertain.

   One view is that the pursuit of useful applications is not the sole justification for mathematical investigation. Pure mathematics is often motivated by intellectual curiosity, the desire to understand abstract structures, and the challenge of solving fundamental problems. Moreover, research that initially appears to have little or no immediate practical relevance may subsequently contribute to important developments in mathematics, science, or technology. The history of number theory and its eventual applications in cryptography illustrate this possibility.

   On the other hand, it is reasonable to question whether every mathematical problem merits the attention it receives. Some conjectures and specialized problems may have limited significance beyond their immediate context, and researchers and funding institutions must make choices about how best to allocate limited resources.

   Such judgments, however, require careful consideration of mathematical depth, originality, connections with other fields, and potential long-term contributions. The absence of an immediate practical application does not, by itself, establish that a problem is trivial or worthless.

   It is also worth examining how academic incentives influence research priorities. Excessive emphasis on publication counts, citation metrics, or prestige may sometimes encourage the pursuit of narrowly defined results at the expense of more substantial or exploratory work. Such concerns should be supported by evidence and should not be used to assume that researchers are primarily motivated by personal recognition rather than intellectual curiosity.

   Early-career mathematicians should therefore approach their research choices thoughtfully, considering not only the prospects for publication and professional advancement but also the mathematical significance of the problems they investigate. A balanced perspective recognizes both the intrinsic value of pure mathematics and the importance of critically evaluating research priorities, without assuming that the value of a mathematical problem can always be determined in advance.

10.1 Cryptography

Prime numbers play an important role in several cryptographic applications, particularly in public-key cryptography. They are used in certain cryptographic algorithms and protocols to help protect data and establish secure communications over wireless systems and open networks. For example, the RSA cryptosystem uses two large prime numbers to generate its keys, with its security traditionally relying on the computational difficulty of factoring their product. Cryptographic applications include military and diplomatic communications, Internet security, financial transactions, private online messaging and voice communications. In fact, cryptography is one of the most significant practical applications of prime numbers. However, although prime numbers are fundamental to several widely used cryptographic techniques, not all cryptographic systems rely on them directly.

10.2 Number Theory

Prime numbers are found almost everywhere in number theory as they represent the basic building blocks of the structure of numbers (i.e. integers) which are the primary subject of number theory, and hence primes underlie the entire theoretical and practical structures of the number system and its theoretical framework. In fact, it is hard to find a topic in number theory in which primes do not play a vital role theoretically and practically (inspect for instance the topics of modular arithmetic and Diophantine equations to appreciate the importance of primes in number theory). Primes are also at the center of most important open problems and conjectures in number theory. As we noted earlier, most of the important open problems and conjectures in number theory (e.g. Goldbach's conjecture and Riemann's hypothesis) are about primes or related to primes (see chapter 6 and § 6.1 in particular).

10.3 Computing

Primes also play an important role in many topics and applications of computing where they enter in many computational algorithms and protocols. For example, prime numbers participate in the building and functioning of numerous error-correcting codes, hashing algorithms, digital signal processing techniques and random number generators. In fact, many protocols and algorithms that employ modular arithmetic (which is widely used in computing) rely substantially on prime numbers in their structure, performance and robustness. Prime numbers may also be met in some novel topics and fields (which are effectively at the level of cutting-edge research) such as quantum computing algorithms and advanced image compression techniques.

Chapter 11
General Resources for Primes

In this final chapter we present a list of some useful resources for getting information about prime numbers (as well as performing tasks related to prime numbers as part of research and learning activities). In this regard we note the following:
• The list is obviously not comprehensive (noting that the topic of prime numbers is huge). However, the list is largely diverse and representative of the main types of resources in this field.
• The list includes online and offline resources (e.g. specialized website and books).
• The listed resources are partly for general knowledge and activities and partly for specialized knowledge and activities.
• The list is ordered alphabetically (and hence the order has no significance other than this).
• Some of the listed resources are for getting fixed information (like theorems about prime numbers), while other resources are for getting changeable information (e.g. the largest known primes of certain types). Some resources are for both types of information.

11.1 Books

There are many books about prime numbers (which vary in many aspects such as depth, level, scope, etc.). Examples of such books (ordered alphabetically according to their titles) are:
• Closing the Gap: The Quest to Understand Prime Numbers, by Vicky Neale.
• Introduction to Modern Prime Number Theory, by T. Estermann.
• Primality Testing for Beginners, by Lasse Rempe-Gillen and Rebecca Waldecker.
• Prime Curios!: The Dictionary of Prime Number Trivia, by Chris K. Caldwell and G.L. Honaker, Jr.
• Prime Numbers: A Computational Perspective, by Richard Crandall and Carl Pomerance.
• Prime Numbers and Computer Methods for Factorization, by Hans Riesel.
• Prime Numbers and the Riemann Hypothesis, by Barry Mazur and William Stein.
• Prime Numbers: The Holy Grail of Mathematics: A Brief Introduction to Prime Numbers, by Thamer Naouech.
• Prime Numbers: The Most Mysterious Figures in Math, by David Wells.
• Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics, by John Derbyshire.
• The Development of Prime Number Theory: From Euclid to Hardy and Littlewood, by Wladyslaw Narkiewicz.
• The Distribution of Prime Numbers, by A.E. Ingham.
• The Distribution of Prime Numbers, by Dimitris Koukoulopoulos.
• The Little Book of Bigger Primes, by Paulo Ribenboim.
• The Music of the Primes, by Marcus du Sautoy.
• The New Book of Prime Number Records, by Paulo Ribenboim.
• The Prime Number Theorem, by G.J.O. Jameson.
• We should also mention online courses and lecture notes (and similar documents and materials) prepared by respected lecturers and professors in higher education institutions (which are usually posted on the

universities websites). Presentations (e.g. in power point or pdf formats), tutorials, and recorded videos (of lectures and proceedings) can also be a useful source of information if prepared by qualified individuals.
• We should also note that textbooks and references on number theory should include some discussion and information on prime numbers since the topic of primes is central to number theory. See for example: An Introduction to the Theory of Numbers (by G.H. Hardy and E.M. Wright), and Elementary Number Theory: Primes, Congruences, and Secrets (by William Stein).

11.2 General Encyclopedias

General encyclopedias (like Wolfram MathWorld and Wikipedia) can be rich sources of information and data about prime numbers. However, the credibility and reliability of these encyclopedias (as well as of the specific contents provided by these encyclopedias) must be verified and guaranteed (where the required level of verification and check can depend on how and where the acquired content is used). In fact, the main value of these encyclopedias mostly lies in the provided references and external links which usually point to their primary sources like academic textbooks, refereed papers, and peer-reviewed databases.

So, while such encyclopedias and the provided materials can be acceptable for initial exploration and investigation (as well as for common purpose and non-critical usages), their utility in academic investigation and critical computational work must depend on how their contents are verified, and this may require further checks with other (and more reliable) sources of information and data (such as scholarly textbooks, research papers, dedicated online databases curated by respected academics, and so on). For example, it may be acceptable to use such encyclopedias as sources and references for educational articles or review papers, but it is not acceptable to use such encyclopedias as sources and references for cutting edge research or computational projects or for constructing seminal ideas and novel proposals. Anyway, it is always recommended to use these encyclopedias as indicators and leads to their primary sources which should be the ultimate source of data and information and the real references.

11.3 GIMPS

GIMPS stands for the **G**reat **I**nternet **M**ersenne **P**rime **S**earch.[796] This is a large-scale distributed computing project that harnesses the collective computing power of thousands of volunteer computers worldwide to discover new Mersenne primes (see § 2.1.41). Despite its limitations and constraints (which will be outlined), GIMPS is regarded as one of the most prominent pioneering and enduring examples of successful distributed scientific collaborations on the world wide web. Since its foundation in 1996, GIMPS has discovered eighteen Mersenne primes, including the current world record prime number, i.e. $2^{136279841} - 1$.

Even though this project is limited to the search for Mersenne primes, it is important from the perspective of measuring the progress in the hunt for very large prime numbers, which are usually of Mersenne type. This is highlighted by the fact that sixteen of the eighteen Mersenne primes discovered by GIMPS were the largest known primes at the time of their discovery (as well as by the aforementioned fact of current world record prime). Beyond discovering new Mersenne primes and setting world records, GIMPS contributes to research in number theory and computational mathematics, e.g. by refining primality testing algorithms. Despite the fact that the scope of GIMPS (as a source of information) is very limited, it is important to be aware of this project and its activities (as well as similar projects) for those interested in prime numbers, whether for the purpose of general knowledge or for specialized knowledge like prime-related research.

[796] See `https://www.mersenne.org/`.

11.4 Journals

Peer-reviewed academic journals are typically the ultimate resource and source of information for cutting-edge research and latest reviews on historical and contemporary issues. Moreover, they typically maintain extensive archives of articles from their past issues and volumes, and hence they represent a huge collection of references. However, research and review papers in these journals may not be accessible to the public (as they are normally masked by paywall when they are not open access). Moreover, their contents are usually difficult to read and comprehend, except to the elite of specialized experts in the specific field. Also, caution should be exercised to avoid predatory journals which pretend to be refereed journals and respected scholarly venues.

In fact, even the contents of legitimate refereed papers in peer-reviewed academic journals may require caution and checks since the quality and reliability of scholarly journals (as well as the peer review and refereeing process) can vary, and can even be compromised in many cases and circumstances. Moreover, novel research papers may require some time before gaining the required acceptance and approval of the scholar community since the process of inspection and verification (or "audience reviewing") by the expert scholars require some time, which is usually measured in months and years, although this should depend on many factors such as the complexity of the reported work and whether the subject is of high interest or not. In general, the credibility of peer-reviewed findings is established in part by the prestige of the publishing venue, but its ultimate validation relies on broad consensus among mainstream scholars and authoritative institutions.

11.5 Large Language Models

Large language models (abbreviated as LLMs) in the form of interactive AI chatbots are useful tools for prime investigation and research. These days there are many artificial intelligence chatbots that can be used for getting information about prime numbers (for both general and specialized knowledge) as well as doing prime-related research, especially when integrated with symbolic tools. Prominent examples of such chatbots are: ChatGPT (from OpenAI), Gemini (from Google), and Claude (from Anthropic). However, we should note the following:

1. One must be aware of the possibility of hallucination and incorrect information. The advice in this regard is to double-check the obtained information by comparing the results obtained from more than one chatbot. It is also useful to ask the chatbot to re-examine the provided information, as the chatbot may identify and correct errors in its answer. In fact, it is often necessary to double-check by comparing the information obtained from the chatbots with other reliable sources of information such as books and specialized websites. Agreement between chatbots, or confirmation by the same chatbot, does not guarantee correctness. Mathematical claims should be verified independently, using rigorous proofs, reliable computational tools, or authoritative sources, as appropriate.
2. It is important to have some skill and experience in writing prompts, i.e. how to formulate questions for the chatbot. A carefully phrased prompt can be crucial for obtaining the required information suitably and accurately. Sometimes, it may be useful to put the question in various forms and within various contexts, by phrasing the prompt differently and within different chains of questioning or even in different sessions of conversation. However, rephrasing a question does not guarantee that the answer will be correct.
3. Chatbots vary in their reliability with regard to the subject, although this may change with time and further development, and hence the users should always be aware of these differences. For example, a certain chatbot may be more reliable than another chatbot with regard to mathematical subjects. In short, the reliability of chatbots is largely dependent on the subject and task, and hence it is important to have an idea about the appropriate chatbot(s) to use for getting information about prime numbers

(and mathematical subjects in general).

4. It may be important to choose and use the right version of the language model, noting that more recent versions may be more reliable. However, newer versions are not necessarily more accurate for every task, so the choice of model should depend on its demonstrated suitability for the particular mathematical problem.
5. The arithmetic capabilities of current chatbots are rather poor. However, they seem to have notably stronger symbolic reasoning capabilities. A potential reason is that they learn mathematical concepts, notation, and symbolic manipulation patterns from published literature and other training resources (which is generally unparalleled by basic arithmetic manipulations). Nevertheless, their symbolic reasoning capabilities are also limited, and their performance depends on the particular task and the used model.
6. Our advice is to use current chatbots primarily as advanced search engines that provide leads and facilitate the initial exploration of relevant subjects. The ultimate sources of data, information, citations, analyses, proofs, and so on, should be academically reliable sources and tools (such as peer-reviewed papers, authoritative websites, well-tested computer codes and algorithms, and well-established analytical methods). However, chatbots are not simply search engines, as they can also assist with explanations, synthesis, coding, plotting, and mathematical exploration, although their outputs in these respects should be independently verified against appropriate, reliable sources and tools.

11.6 Mathematical Software

Mathematical software (including specialized computing libraries) can serve as powerful assistants for both learning and research activities related to prime numbers. These include general purpose ones (like SageMath and Mathematica) and prime-specific ones (like Primesieve) where both can be very useful as educational and computational tools for performing ordinary prime-related tasks. They can also be very handy for managing creative activities like building models, developing ideas, testing conjectures, experimenting on patterns, and so on. In fact, they are indispensable tools for most serious research work on prime numbers (like searching for prime numbers, testing conjectures, processing massive data sets, plotting and visualization, algebraic manipulation, analytical formulation, and so on). In short, they are essential proactive tools for most prime-related projects and activities (whether for education and learning, or for research and action).

We note that "Mathematical Software" should be extended to include similar Internet resources (such as online calculators, computational engines, visualizers, and similar proactive and engaging websites). For example, Wolfram Alpha can be used for prime factoring and prime counting as well as many other prime-related tasks and activities which are essential for education and research (and even recreation). Many other interactive websites that offer similar products and materials (such as prime charts, visual prime sieves, distributions, interactive graphs, and so on) can be found on the Internet. However, the scientific reliability of such websites and the offered materials should be checked before accepting their contents.

11.7 OEIS

OEIS stands for the **O**n-Line **E**ncyclopedia of **I**nteger **S**equences.[797] This is one of the oldest (founded in 1964 and moved online in 1996) and most useful resources on prime numbers, despite its broader scope, namely integer sequences. A quick inspection of the present book should reveal the exceptional richness and usefulness of this encyclopedia as a source of information on prime numbers, as well as integers and even beyond. It is a comprehensive, freely accessible database dedicated to cataloging integer sequences

[797] See `https://oeis.org/`.

that arise in mathematics, science, and related fields. In short, the OEIS is an essential resource for mathematicians, scientists, educators, students, and anyone interested in numbers.

The OEIS serves as the authoritative global repository for integer sequences of mathematical significance, including sequences of primes. In fact, the OEIS is one of the largest and most reliable resources of its kind as it hosts a peer-reviewed database of hundreds of thousands of sequence entries (currently over 400 thousand) which are largely subject to rigorous scholarly criteria and academic relevance. Moreover, the OEIS serves as a powerful research and discovery tool, i.e. one can input a short list of numbers and often identify the underlying sequence, along with formulae, generating functions, references, code snippets, and links to relevant literature. The primary objective of the OEIS was to aid researchers in identifying patterns and providing searchable "fingerprints" for sequences of integers. Accordingly, it is a powerful tool for researchers in number theory and prime numbers (and beyond) through accelerating research by revealing unexpected connections, patterns and relationships.

The main limitations of the OEIS include its rather primitive text-based interface and somewhat poor readability. It may also be criticized for occasionally offering limited information and having uneven breadth and depth. Casual errors and typos may also be encountered on rare occasions. However, these limitations do little to undermine the OEIS's standing as a leading reference database and reliable source of information, although individual entries should still be verified against other authoritative sources and references when used in research and other critical applications.

11.8 Online Educational Materials

There are many websites that offer online educational materials related to prime numbers such as articles, plots, charts, questions and answers, solved problems, frequently asked questions (FAQs), and so on. This category also includes educational videos posted on various websites and social media platforms such as YouTube and TikTok. However, such materials should generally be treated with skepticism and caution because they mostly lack authoritative legitimacy, as the majority of these materials are not produced by qualified scholars and experts, and hence they can contain errors and may lack rigor and accuracy.

A more reliable online source that may be included in this category is what we indicated previously in § 11.1, i.e. online courses and lecture notes (and similar contents) which are prepared and distributed by respected academics in universities and research institutes.[798] This also includes university lecture uploads and accredited online courses, which are prepared and run by esteemed universities and accredited educational institutes. Such materials generally have high educational value and hence they can be utilized as valuable and reliable sources of information, as well as suitable resources for learning and training.

11.9 Online Forums and Chat Rooms

Online mathematical forums and discussion platforms, such as Stack Exchange and MathOverflow, contain numerous posts and discussions on prime numbers and related topics, including dedicated sections addressing particular mathematical subjects. However, the information provided on these platforms should be evaluated critically, as the accuracy and reliability of individual contributions can vary. Posts may be written by participants with differing levels of mathematical expertise, ranging from professional mathematicians and experienced researchers to amateur mathematicians and beginners. Consequently, some contributions may contain errors, incomplete arguments, or insufficiently rigorous explanations. Furthermore, the conversational and sometimes fragmented structure of forum discussions can occasionally lead to confusion, ambiguity, or misinterpretation.

Nevertheless, these platforms can be valuable resources for clarifying mathematical concepts, discussing specific problems, and exploring alternative approaches to their solution. They can also serve as useful

[798] See for instance `https://empslocal.ex.ac.uk/people/staff/mrwatkin/zeta/tutorial.htm`.

starting points for further research, since posts and discussions often refer to textbooks, research articles, mathematical publications, and other relevant sources that can be consulted directly and cited where appropriate. Moreover, some platforms are moderated by knowledgeable individuals or subject specialists, and their discussions may involve contributions from respected mathematicians and researchers. Such participation can enhance the quality of the discussions, although it does not guarantee the correctness of every contribution.

Overall, online mathematical forums and discussion platforms can be valuable supplementary resources for learning about prime numbers and related topics. However, their contents should be assessed on a case-by-case basis, and important mathematical claims should be verified against reliable references, particularly when these claims are used in formal academic writing or research.

11.10 Preprint Repositories

Preprint repositories, such as arXiv, play an important role in disseminating emerging research by providing scholars and the general public with rapid access to scholarly work before or during the formal peer-review process. These repositories can also serve as valuable resources for learning and education, particularly when preprints contain accessible explanations of mathematical concepts, expository material, or results that readers can explore independently.

However, because preprints generally have not undergone conventional editorial and peer-review processes before posting, their reliability varies, which necessitates appropriate caution and scrutiny. Readers should therefore exercise critical evaluation, particularly when using repositories whose screening and moderation procedures are limited or unclear, as well as when assessing work for which the authors' expertise or research credentials are difficult to verify. It is also advisable to check whether a peer-reviewed version of the work is available.

Nevertheless, preprint repositories remain valuable resources for research, learning, and education. Their usefulness depends on the nature and quality of the material, the reader's ability to evaluate it critically, and the purpose for which it is used. Preprints can be particularly beneficial for exploratory learning and gaining familiarity with emerging ideas, while claims intended to support important research conclusions or consequential decisions should be assessed with appropriate care and, where possible, corroborated by reliable sources and peer-reviewed literature.

11.11 The Prime Pages

The Prime Pages is among the most comprehensive online resources about prime numbers, and may be considered a kind of "Guinness Book" for prime numbers.[799] It acts as a premier database for prime number records and research, providing, for instance, a search tool for finding the n^{th} prime number (see the upcoming Point 5), and featuring the 5000 largest known primes including "the top 10" and "the top 20" lists of various forms and types (see Point 1).

The site also provides extensive records and educational resources which include the "Prime Curios!" section (see Point 3), a comprehensive "Prime Glossary" (see Point 4), a frequently asked questions section covering topics like the Mersenne primes, and a database that tracks the individuals and projects behind new discoveries. Users of this site can also access detailed instructions on proving primality and submitting new findings for verification (see Point 2).

In the following points, we give some examples of the contents of the Prime Pages to give an idea about the nature and structure of this site:

1. Largest Known Primes: this is a searchable database of the 5000 largest known primes.[800]

[799] See `https://t5k.org/`.

[800] See `https://t5k.org/largest.html`.

2. Primality Proving: this is a collection of technical instructions for proving a number is prime, as well as information about relevant verification procedures.[801]
3. Prime Curios!: this is a collection of curiosities, wonders and trivia related to prime numbers.[802]
4. Prime Glossary: this is a collection of basic definitions about prime numbers.[803]
5. The Nth Prime Page: this is a search tool for finding the n^{th} prime number.[804]

However, despite its status as a highly respected specialist database for prime numbers, individual records, proofs, research claims, and other information should still be evaluated according to the relevant mathematical evidence and independent authoritative sources and scholarly literature.

[801] See `https://t5k.org/prove/`.
[802] See `https://t5k.org/curios/`.
[803] See `https://t5k.org/glossary/`.
[804] See `https://t5k.org/nthprime/`.

References

We listed some general "conventional" references in § 11.1. In fact, during the preparation of this book, we consulted and used many other books, scholarly papers, general articles, websites, online databases, computational engines, and other research resources and sources of information about prime numbers and related subjects. In short, chapter 11 largely outlines the kinds of references and resources consulted during the preparation of this book.

Index

1^{st} order recursively-defined sequence, 103
1-almost-prime, 278
2^{nd} order recursively-defined sequence, 103
2-almost-prime, 90, 277, 278
3^{rd} order recursively-defined sequence, 103
3-almost-prime, 278
180° rotation, 33

A
abc conjecture, 156, 176, 190, 192, 197–199
Abelian group, 179
Absolute
    prime, 56
    pseudoprime (absolute Fermat pseudoprime), 136, 156, 166, 234, 279, 280
    value, 13, 35
Absolutely normal number, 194
Abundant number, 21, 208, 284
Additive
    combinatorics, 137
    number theory, 68, 134, 284
Agoh-Giuga conjecture (Giuga conjecture), 176, 191, 195, 196, 219, 220
Agrawal conjecture, 177, 195, 220
Agrawal-Kayal-Saxena (AKS), 209
AKS test, 177, 196, 209, 220, 229, 230, 236, 240
Algebraic
    curve, 69, 178
    norm, 247, 252, 275–277
    number field, 247
    number theory, 33, 69, 94, 132, 138, 139, 148
    structure, 114, 136, 162, 205, 242, 243, 247, 260, 275
Algorithmic
    analysis, 268
    sieve, 221, 224, 225, 231–233, 237, 238
Aliquot sequence, 270
Almost-perfect number, 284
Almost-prime, 90, 134, 139, 224, 232, 240, 277, 278, 284
Alternating
    harmonic series of primes, 273
    series test, 273
    sum rule (for divisibility by 11), 207
Amicable number, 69, 270, 284
Anagrammatic prime, 56
Analysis, 44, 274
Analytic
    density (or Dirichlet density), 158, 161
    function, 257
    number theory, 131–134, 138, 140–142, 145–148, 224–226, 232, 254, 274, 284
    sieve, 221, 224, 225, 231–233, 238
Andrica conjecture, 177, 193, 196–199, 260, 264
Applied mathematics, 44, 94, 102
APR test, 209, 210, 229, 230
APR-CL test, 210
Arbitrarily
    close, 139
    large gap, 20, 82, 152, 158, 254, 264
    large prime number, 151
    long arithmetic progression, 137, 157
    long sequences of consecutive composites, 152
    minimized, 214
    small error probability, 236
    sparse, 131
Arithmetic
    mean (average), 101, 126, 127, 135
    progression, 15, 16, 25, 30, 132, 133, 135, 137, 140, 144, 145, 147, 150, 151, 153, 154, 156, 157
Artin
    conjecture on primitive roots, 38, 177, 190–193, 195–197, 273
    constant, 13, 177, 273
Asymptotic
    bound, 228, 258
    complexity, 205, 209, 222, 228, 237
    density, 155, 158, 177, 194, 263, 273
Atkin sieve, 221, 223, 233, 237, 238
Average, 20, 27, 68, 74, 101, 126, 132, 135, 146, 147, 155, 180, 186, 206, 232, 239, 240, 254, 261–265, 267
    of nearest primes, 27, 68, 74, 101, 126, 127
    prime gap, 20, 254, 262–265

B
Bad prime, 40, 78
Baillie-PSW test, 190, 195, 210, 212, 220, 229, 230, 235, 241, 242
Baker-Harman-Pintz theorem, 131, 151, 157
Balanced prime, 23, 24, 27, 28, 68, 69, 74, 99, 101, 126, 127, 155, 188, 207, 218
Bang theorem, 150, 151, 166
Base 2, 20, 48, 49, 64, 75, 79, 80, 83, 84, 121
Base 8, 20
Base 10, 16, 18, 20, 21, 24, 30, 33, 34, 40, 51, 54–56, 59, 64, 67, 68, 70, 72
Base dependency, 97, 203
Base-dependent, 21, 30, 33, 34, 38, 41, 42, 51, 54–56, 59, 64, 66–68, 70, 72, 75, 78–84, 86, 95, 97, 102, 105, 117, 160, 194, 202, 203, 216, 266
Bateman-Horn
    conjecture, 63, 177–180, 182, 187, 193, 194, 197, 198, 200, 260–262
    factor, 13, 178
Bateman-Selfridge-Wagstaff conjecture, 178, 184, 194
Beal conjecture, 178, 190, 195
Bell
    number, 13, 28, 169
    prime, 28, 102, 103, 128, 129, 188, 207
    sequence, 103, 128
Bernoulli
    congruence, 176
    irregular prime (B-irregular prime), 43, 44, 76, 77, 98, 122–124, 154, 164, 166, 189
    number B_n, 13, 43, 44, 76, 98, 122, 123, 176, 284
    regular prime (B-regular prime), 43, 44, 98, 122, 123, 189, 196
Bertrand, 131
    postulate, 25, 63, 131, 132, 134, 138, 148, 151, 157, 164, 172–174, 183, 199, 200, 264, 267
Bertrand-Chebyshev theorem, 131
Bevaprime, 90

Big O notation, 15, 141, 146, 147, 179, 237, 258
Bilinear form, 224
Binary, 48, 49, 64, 80, 83, 84, 94, 97, 132, 154, 158, 160, 161, 166, 203, 213, 217, 238, 250, 251, 274
  exponent vector, 250
  quadratic form, 132, 154, 238, 251
  quadratic prime theorem, 132, 158
Binomial coefficient, 13, 22, 24, 28, 29, 76, 97, 103, 106, 128, 139, 148, 151, 153, 160, 166, 168, 208, 218
Biprime, 277
Birch-Swinnerton-Dyer conjecture, 178, 190
Bombieri-Vinogradov theorem, 132, 147, 157, 164, 174, 180, 199, 200, 225
Bounded
  gap, 30, 149, 180, 200, 226
  gaps theorem, 30, 149, 200
Bourgain theorem, 152, 158, 161
Brocard
  conjecture, 179, 183, 190, 193, 197–199, 260
  problem, 193, 197
Brown number, 197
Brun
  constant, 13, 72, 132, 273
  sieve, 224, 232, 238–240
  theorem, 45, 72, 132, 133, 157, 162, 163, 199
Brun-Titchmarsh theorem, 133, 157, 163, 173, 199
Bunyakovsky conjecture, 32, 35, 52, 53, 63, 132, 179, 180, 187, 191, 193, 194, 197–200, 261

C

Carmichael
  number, 136, 152, 153, 156, 163, 164, 169, 176, 183, 211, 219, 234, 236, 240–242, 279, 282, 285
  theorem, 150, 151, 166
Carol
  number, 106
  prime, 28, 46, 88, 95, 96, 105, 106, 164, 188, 207
Catalan
  conjecture, 24, 176, 199
  number, 13, 22, 28, 29, 155, 168, 208, 279
  prime, 28, 88, 95, 97, 105, 106, 156, 192
  pseudoprime, 193, 279
Catalan-Dickson conjecture, 195, 270
Catalan-Mersenne
  chain, 270
  conjecture, 270
  number, 192, 196, 270
  prime, 192
  sequence, 270
Ceiling function, 13, 246, 250
Centered
  8-gonal number, 29, 89, 153, 156, 160, 188, 208
  9-gonal number, 29, 89, 153, 156, 160, 188, 208
  hexagonal number, 32, 114, 160, 285
  hexagonal prime, 32, 108, 114, 160
  k-gonal prime, 29, 89, 153, 156, 160, 188
  pentagonal number, 29
  pentagonal prime, 29
  polygonal number, 29
  polygonal prime, 29
  prime, 29, 32, 89, 95, 96, 105, 108, 114, 160, 188, 285
  square number, 29
  square prime, 29, 96
  triangular number, 29
  triangular prime, 29, 96
Central binomial coefficient, 151, 153, 168, 208
Chebyshev, 131, 133, 134
  bias, 77, 158, 161, 262, 266, 283
  first prime-counting function $\theta(x)$, 16, 174, 257–259, 274
  polynomials, 77
  prime, 77, 129, 130, 156
  prime-counting functions, 16, 77, 132, 147, 257, 258, 274
  second prime-counting function $\psi(x)$, 16, 132, 147, 174, 257–259
  theorem, 77, 131, 133, 151, 157, 173, 174, 200
Chen
  prime, 29, 30, 72, 90, 101, 125, 126, 134, 154, 157, 165, 189
  theorem I, 90, 134, 162, 182, 199, 278
  theorem II, 30, 90, 134, 154, 157, 163, 200, 278
Circular prime, 30, 32, 57, 97, 99, 102, 117, 118, 122, 125, 153, 160, 165, 189, 216
Clement theorem, 134, 135, 163, 166, 219
Closure (of group), 21
Cluster prime, 30, 86, 103, 158
Coding theory, 139
Colombian number, 66
Combinatorial sieve, 221, 224, 225, 231–233, 238, 239
Combinatorics, 35, 44, 97, 137, 139, 233
Commutative monoid, 162
Complete
  prime, 78, 79
  prime factorization, 213, 230, 251
  residue system, 23, 181
  sequence, 70
Complex
  analysis, 136, 147, 171, 186, 209, 232
  cube root of 1, 276
  integer, 91, 93
  number, 14, 20, 91, 93, 186, 275–277, 284
  plane, 115, 186, 276
  prime number, 93
  variable, 15, 16, 136, 153, 186
Composite number, 17, 19–21, 79, 254
Composite-indexed prime, 79, 87, 100, 101, 226
Compositeness, 19, 21, 207, 211, 214, 228, 231, 236
  test, 21, 205, 207, 211, 214, 216, 228, 231
Compositorial prime, 31, 36, 61, 95, 97, 105, 112–114
Computational
  complexity, 205, 206, 209, 228, 233, 236, 282
  number theory, 32, 136, 139, 140, 145, 231, 240, 242, 243, 247
Computer science, 229, 231, 286
Computing, 94, 102, 213, 223, 233, 244, 287, 291
Concatenation, 42, 43, 67, 89, 98, 121, 161, 189, 195, 274
Confirmed prime, 93, 206
Congruence of squares, 245, 247, 248, 251, 252
Continued fraction
  expansion, 244, 247, 251
  factorization (CFRAC), 13, 243–247, 251
Contraposition, 21, 211
Contrapositive, 218
Convergence, 45, 72, 132, 133, 136, 142, 144, 199, 224, 244, 257, 273
Converse, 22, 33, 53, 87, 115, 123, 136, 159, 163, 166, 168, 179, 188, 203, 208, 213, 227, 235, 237, 239, 275
Copeland-Erdos
  constant, 13, 161, 194, 274
  theorem, 161, 163, 274

Coprimality, 113, 135, 180
Coprime (relatively prime), 20–23, 25, 35, 36, 39, 49, 51, 61, 65, 84, 135, 136, 140, 145, 149, 151, 153, 158, 160, 161, 167, 168, 173, 176, 177, 180, 181, 197, 211, 216, 223, 234, 236, 238, 240, 242, 246, 247, 249, 271, 279, 280, 282
Counting function of semiprimes $\pi_2(x)$, 16, 277, 278
Cousin prime, 24, 31, 47, 72, 90, 99, 101, 125, 126, 149, 187, 188, 197–200, 226
  conjecture, 197–200
Cramer, 179, 188
  conjecture, 131, 179, 181, 193, 195–199, 260–262, 264, 268
  model, 140, 188
Cramer-Granville
  conjecture, 197
  model, 261
Cramer-Shanks conjecture, 188
Critical
  line, 186, 200
  strip, 146
Cryptographic primes (or RSA primes), 94
Cryptography, 17, 19, 67, 68, 74, 94, 102, 136, 139, 145, 211, 230, 239, 242, 243, 247, 253, 272, 277, 286, 287
Cryptosystem, 15, 136, 247, 277, 287
Cuban prime, 31, 32, 95, 96, 105, 108, 114, 115, 160, 188, 285
  of the first kind, 31, 32, 108, 114, 160, 285
  of the second kind, 31, 32, 114
Cube root of 1, 276
Cubic equation, 69, 178
Cullen
  number, 32, 106, 208
  prime, 32, 61, 62, 76, 88, 95, 96, 105–107, 116, 164, 188
Cunningham
  chain, 67, 191, 193, 270, 271
  chain of the first kind, 270, 271
  chain of the second kind, 271
  chains conjecture, 191, 193, 271
Cyclic
  group, 153
  multiplicative group, 23, 219
  permutation, 30, 97, 118
  prime, 32
Cyclotomic
  field, 43, 123, 210
  polynomial $\Phi_n(x)$, 16, 33, 97, 115, 168, 219
  prime, 33, 36, 48, 73, 95, 97, 105, 115–117, 164, 165
  ring, 210
  structure, 210
Cyclotomic-based test, 219

D
D2357 prime, 78–80, 82, 83
D4689 prime, 80
D014689 prime, 79, 80, 82, 83
Decimal, 13, 18, 20, 22, 24, 28, 29, 31, 34
Deficient number, 21, 284
Delicate prime, 33, 97, 102, 117, 120, 122, 153, 154, 162
Denominator, 41, 146, 246
Descartes-Frenicle-Sorli conjecture, 190, 195
Deterministic primality test, 113, 206, 212–214, 216, 219, 220, 228–230, 235, 236, 242
Devlali number, 66
Dickson
  conjecture, 66, 180, 185, 187, 191, 193, 194, 197–200
  theorem, 285
Digitally delicate prime, 33
Digit-decreasing prime, 80, 81
Digit-increasing prime, 80, 81
Digit-nondecreasing prime, 81
Digit-nonincreasing prime, 81
Digit-oscillating prime, 81
Dihedral
  calculator prime, 33
  prime, 33, 34, 54, 68, 97, 99, 102, 117, 121, 122, 153, 161, 164, 165, 188, 216
Diophantine
  analysis, 176
  equation, 132, 138, 148, 150, 287
Dirichlet
  density (or analytic density), 158, 161
  L-functions, 266
  theorem on arithmetic progressions, 25, 45, 62, 65, 84, 132, 135, 140, 145, 150, 151, 154, 155, 157, 158, 161, 163, 164, 169, 173, 174, 177, 179, 180, 186, 187, 199, 200, 261, 265, 283
Discrete index (or discrete logarithm), 14, 169
Discriminant, 132, 182, 211, 214, 246, 253
Distribution
  function, 255, 258
  of primes, 19, 20, 74, 77, 88, 157, 158, 193, 194, 254, 255, 258, 259, 266, 267
Divergence, 24, 41, 43, 45, 133, 141, 142, 174, 270, 273
Division test, 61, 210, 218, 229–231
Divisor function $\sigma(n)$, 16, 22, 50, 146, 147, 166, 219
Divisor-counting function $\tau(n)$, 16, 22, 26, 167, 219
Dixon factorization method, 243–245, 250, 251
Double
  logarithm, 274
  Mersenne number, 49
  Mersenne prime, 15, 49, 87, 88, 99, 100, 105, 164, 188, 193
  summation, 170
Double-and-add algorithm, 246
Dubner conjecture, 197, 198

E
Eisenstein
  integer, 169, 276
  prime, 91, 275, 276
Elementary number theory, 139, 145, 146, 148, 150
Elliott-Halberstam conjecture, 180, 193, 197, 199, 200, 261
Elliptic
  curve, 15, 69, 104, 154, 178, 211, 246, 279
  curve method (ECM), 13, 243–246, 253, 277
  curve primality proving (ECPP), 13, 211, 220, 229, 230, 236
  pseudoprime, 279
Emirp prime, 34, 64, 86, 97, 99, 102, 117–119, 122, 164, 188
Equidistribution, 145, 160, 161, 168, 283
Equilateral triangle, 29
Eratosthenes sieve, 47, 221–225, 232, 233, 237, 238, 243, 282, 283
Eratosthenes-Legendre sieve, 225
Erdos
  proof, 24
  theorem on delicate primes, 33, 153
Erdos-Kac theorem, 135, 137, 157, 162
Erdos-Mollin-Walsh conjecture, 195
Error

bound, 132, 186, 200, 212, 220, 235, 236, 258, 262
estimate, 200
probability, 228, 229, 235, 236, 242
rate, 220
reduction, 229
term, 141, 146, 200, 239, 262
Euclid
lemma, 21, 150, 162, 166, 173
number, 60
prime, 60
proof, 24, 60, 113, 142, 271
theorem, 20, 145, 150, 151, 154, 162, 174
Euclidean prime, 60
Euclidean-type, 113
Euclid-Euler theorem, 50, 162
Euclid-Mullin sequence, 156, 193, 196, 271
conjecture, 193, 271
Euler
(linear) sieve, 222, 233, 237, 238
constant (Euler-Mascheroni constant), 274
criterion, 135, 136, 146, 149, 150, 163, 166, 216, 279
irregular prime (E-irregular prime), 44, 77, 98, 122–124, 154, 189
number, 13, 35, 44, 98, 122
prime, 34, 35, 95, 96, 105, 114–116, 187, 188, 192
prime polynomial, 114
product, 174
product formula, 136, 150, 157, 162
proof of infinitude of primes, 24, 174
pseudoprime, 234, 280
regular prime (E-regular prime), 44, 98, 122, 123, 189
totient function $\phi(n)$, 16, 22, 41, 42, 103, 132, 133, 145, 147, 152, 160, 163, 167, 169, 173, 174, 183, 191, 195, 196, 219, 283
totient theorem, 173, 174
Eulerian
component, 152, 163
form, 190, 195
number, 35
Euler-Jacobi pseudoprime, 166, 242, 279, 280, 282
Euler-Mascheroni constant (Euler constant), 16, 143, 146, 179, 274
Even
base, 39, 66, 125, 189
gap size, 185
perfect number, 15, 48, 50, 162, 169
prime, 20, 23, 43, 88, 89, 93, 125, 152, 156
semiprime, 183
sequence, 182
Existence, 151, 152, 190
Exponent, 36, 49, 50, 53, 69, 96, 98, 131, 139, 162, 166, 178, 184, 197, 248–250, 253, 283, 284
vector, 245, 247, 250, 252
Exponential, 65, 85, 95, 96, 103, 209, 228, 229, 235, 236, 242, 267
sum, 139, 224
time (test complexity), 209, 228
transformation, 85
Extended Riemann hypothesis, 195, 196

F

Factorial, 13, 23, 31, 35, 61, 97, 135, 139, 149, 159, 171, 191, 196, 197, 208, 218, 264, 284
prime, 23, 35, 36, 61, 88, 95, 97, 105, 112–114, 139, 159, 164, 188, 189, 227
Factorization, 19, 22, 25, 26, 42, 43, 98, 136, 139, 152, 162, 189, 205, 206, 213, 215, 221, 230, 234, 238, 242–244, 247–252, 282
algorithm, 221, 234, 242–245, 247, 248, 250–252, 282
False
positive, 207
prime, 279
Falsified conjectures, 200
Farhadian conjecture, 197
Feit-Thompson conjecture, 181, 190, 191, 196, 202
Fermat
factorization method, 243, 245, 246, 250, 251, 277
last theorem (FLT), 43, 52, 67, 75, 76, 123, 124, 176, 178, 182, 186
little theorem, 22, 75, 136, 150, 163, 166, 168, 173, 174, 208, 211, 213, 214, 240, 249, 280
number, 13, 17, 25, 36, 39, 106, 153, 155, 160, 167, 168, 201, 215, 235, 252
prime, 17, 24, 33, 36, 38, 58, 62, 88, 93, 95, 99–101, 105–107, 115–117, 125, 159–161, 164, 165, 189, 191, 196, 201, 215–217, 230
primes conjecture, 189, 201
pseudoprime, 136, 166, 191, 193, 234, 241, 279–282
test, 208, 211, 212, 229, 230, 234, 236, 241
two-square theorem, 115
Fermat-Catalan conjecture, 197
Fibonacci
number, 13, 37, 47, 58, 74, 98, 124, 153, 155, 163, 168, 208, 212, 226, 280
prime, 24, 37, 46, 58, 87, 88, 100, 102, 103, 125, 128, 153, 164, 188, 211, 226
pseudoprime, 280
sequence, 37, 47, 58, 128, 192, 211, 212, 215, 270, 280, 284
test, 211, 212, 215, 229, 230, 280
Fibonacci-Wieferich prime, 74
Field (abstract algebra), 23, 43, 69, 123, 139, 178, 210, 212, 245, 247, 248, 252, 275
Finite
constant, 45, 149, 155
digit string, 155
field, 139, 245, 247, 252
interval, 268
period, 153
sequence, 156, 214, 270
set, 20, 43, 133, 156, 162, 175, 181, 186, 191, 235
sum, 56
value, 72, 132, 144
Finitude, 88, 156, 157, 189, 190, 193
Firoozbakht conjecture, 181, 193, 197, 199, 261
First
Chebyshev prime-counting function $\theta(x)$, 16, 174, 257–259, 274
order recurrence relation, 128
Floor function, 13, 51, 103, 139, 143, 155, 170, 171, 272
Fortunate
number, 13, 37, 38, 182, 191, 195, 196
numbers conjecture, 182, 191, 195
prime, 37, 38, 95, 97, 105, 113, 114, 182, 188, 191
Fraction, 41, 43, 168, 181, 218, 246
Friable number, 58
Friedlander-Iwaniec theorem, 63, 154
Frobenius
automorphism, 212
pseudoprime, 242, 281

test, 212, 229, 230, 242, 281
Full
repetend prime, 38
reptend prime, 32, 38, 97, 98, 117, 169, 188, 219
Functional analysis, 224
Fundamental theorem of
arithmetic, 19, 22, 25, 150, 151, 162, 173
probabilistic number theory, 135
Furstenberg topological proof, 25

G
Galois field 2, 248
Gandhi formula, 169, 172
Gap (prime gap), 14, 20, 24, 27, 30, 31, 68, 71, 72, 74, 82, 101, 131, 153, 155, 158, 177, 179–181, 184, 185, 188, 192, 193, 197–201, 239, 254, 260–266, 268, 272, 284
Gaussian
elimination, 245, 250
integer, 93, 115, 148, 169, 275, 276
Mersenne prime, 15, 275, 276
prime, 91, 93, 115, 275, 276
General number field sieve (GNFS), 14, 242–244, 247, 249–253
Generalization of
balanced prime, 69, 74
Bang theorem, 150
Bertrand postulate, 63, 148
Fermat d-pseudoprime, 281
Fermat factorization method, 251
Fermat little theorem, 168
Hardy-Littlewood first conjecture, 182
Mersenne number, 213
Mersenne prime, 39
PNT, 174
Pollard $p-1$ algorithm, 246
primality, 91–93, 275
Riemann hypothesis, 186, 262
strong prime, 74
twin prime conjecture, 182, 262
weak prime, 69
Wilson theorem, 218
Zsigmondy theorem, 150, 151, 166
Generalized
balanced prime, 27
cuban prime, 32
Cunningham chain, 271
dihedral prime, 34
Elliott-Halberstam conjecture, 180, 197
Euclid lemma, 21, 150, 162, 166
factorial prime, 35
Fermat number, 13, 14, 39
Fermat prime, 13, 14, 38, 39, 62, 63, 95, 105, 107, 116, 160, 165, 188, 216
full reptend prime, 38
gap, 265
Higgs prime, 42
Mersenne prime, 15, 39, 40, 95, 96, 105, 108, 116, 165
pentagonal number, 219
primality, 91
Proth prime, 62
repunit prime, 64
Riemann hypothesis (GRH), 14, 132, 133, 140, 177, 190, 194–197, 199, 200, 209, 210, 214, 216, 220, 235, 266
Riesel prime, 65
twin prime conjecture, 184
unique prime, 72
Wieferich condition, 77
Wieferich prime, 52, 75, 89, 124, 165, 192
Wilson prime, 75
General-purpose
factorization algorithm, 242–244, 247, 250, 251
primality test, 209, 213, 214, 230, 235
prime sieve, 233
Genocchi
irregular prime (G-irregular prime), 44, 77, 98, 123, 124, 154, 164, 189
number G_n, 14, 44, 45, 98, 123
regular prime (G-regular prime), 44, 98, 123, 189
Geometric
mean (average), 101, 126, 127
sequence, 150
series, 136
Gigantic prime, 90
Gigaprime, 90
Gilbreath conjecture, 185
Giuga conjecture (Agoh-Giuga conjecture), 176
Goldbach, 25
conjecture, 73, 134, 182, 186, 190, 191, 195, 197–200, 239, 261, 284, 287
other conjecture, 201
ternary (weak) conjecture, 137, 148, 151, 157, 162, 174, 182, 183, 199, 200, 261, 284
Goldbach-like conjecture for lucky numbers, 48
Goldbach-type problems, 68
Golomb conjecture, 201
Good prime, 40, 78, 101, 126, 127, 154
Gram series, 257
Grand Riemann hypothesis, 14, 186
Great Internet Mersenne Prime Search (GIMPS), 289
Greatest common divisor (gcd), 14, 132, 162, 179, 245–252
Greedy algorithm (representation), 271
Green-Tao theorem, 137, 151, 156, 157, 173, 199, 200, 265
Green-Tao-Ziegler theorem, 156
Group, 21, 23, 69, 136, 150, 153, 179, 187, 219, 246, 252, 253, 279
order, 69, 150, 253
theory, 69, 88, 94, 136, 150
Group-theoretic primes, 94
Guy-Selfridge conjecture, 195, 270

H
Happy
number, 40, 41
prime, 40, 97, 102, 117, 188
Hardy-Littlewood
circle method, 284
conjecture F, 35, 52, 182, 191, 193, 194
constant, 182, 274
fifth conjecture, 189
first (or k-tuples) conjecture, 48, 66, 181, 182, 188, 191, 193, 198–200, 261–263, 265
second conjecture, 188, 194, 198
Hardy-Ramanujan theorem, 137, 162, 226
Hardy-Wright formula, 170, 172
Harman sieve, 224, 238
Harmonic
analysis, 224, 232, 238
number, 14, 41, 98, 155, 168, 218

prime, 41, 98, 99, 122, 188
series, 41, 141, 274
series of primes, 24, 174, 272–274
Hasse-Weil L-function, 179
Heath-Brown theorem, 154
Hensel theorem (lemma), 138, 150, 166
Hexadecimal, 203
Higgs prime, 41, 42, 86, 88, 98, 103, 122, 156, 188
of the first order, 42, 88, 156
of the third order, 42
Higher orders of
balanced primes, 27
factorial primes, 35
Higgs primes, 42
strong primes, 69
type-indexed primes, 86, 87
weak primes, 74
Wilson primes, 75
Highly cototient
number, 42
prime, 42, 103, 188
Hoheisel theorem, 138, 151, 157
Home prime, 14, 42, 43, 97, 98, 117, 189, 195
Homogeneous linear system of equations, 248
Hurwitz
integer, 277
prime, 93, 275, 276
quaternion, 93, 275–277
Hybrid primality test, 235
Hyperbolic
function, 43, 44
tangent function, 43

I
Identity (of group), 21
Image
compression techniques, 287
prime, 85, 86
Imaginary
part of complex numbers, 146, 275, 277
unit of complex numbers, 14, 275, 276
units of quaternion system, 14, 277
Inclusion-exclusion
approach, 282
principle, 169, 224, 225, 232, 233, 239
sieve, 226
terms, 239
Index-added prime
of the first kind (I), 81
of the second kind (II), 81
Index-addition transformation, 86
Index-subtracted prime
of the first kind (I), 82
of the second kind (II), 82
Index-subtraction transformation, 86
Inert primes, 94
Infinite
product, 136, 273
sequence, 51, 171, 193, 202, 271, 272
set, 20, 43, 51, 77, 133, 175
sum, 136
Infinitude, 24, 25, 87, 154–156, 188, 189, 191–193
Integer
coefficients, 21, 33, 39, 85, 138, 139, 153, 172, 177, 179, 180, 186, 191, 260
factorization, 205, 206, 221, 234, 238, 242–244, 247–252, 282
Integers (set of integers), 16, 91, 181, 224, 225, 232
Integral transform, 232
Internal
binomial coefficient, 218
digit, 203
Inverse (of group), 21
Irrational number, 21, 143, 155, 251, 274
Irreducible polynomial, 33, 85, 132, 177, 179, 186, 198, 247, 260
Irregular prime
(Bernoulli irregular or B-irregular), 43, 44, 76, 77, 98, 122–124, 154, 164, 166, 189
(Euler irregular or E-irregular), 44, 77, 98, 122–124, 154, 189
(Genocchi irregular or G-irregular), 44, 77, 98, 123, 124, 154, 164, 189
Irregular-Wolstenholme prime, 77
Isolated prime, 45, 72, 101, 125, 126, 154
Iwaniec theorem, 138, 139, 156, 158, 162, 278
Iwasawa theory, 123

J
Jacobi
sum, 210, 212, 215, 216
symbol, 15, 163, 210, 212, 214–216, 280
Jacobsthal
number, 14, 45, 96, 208
prime, 24, 45, 73, 74, 88, 95, 96, 100, 102, 103, 105, 111, 112, 125, 128, 153, 160, 164, 166, 188, 216
sequence, 45, 128
Jones
conjecture, 168
formula, 170, 171
Jump prime, 82

K
Korselt criterion, 163, 169, 242, 285
Kronecker conjecture, 191, 195, 198, 199
Kummer theorem, 139, 166
Kummer-Vandiver conjecture, 123
Kurepa conjecture (or left factorial hypothesis), 191, 196
Kynea
number, 106
prime, 28, 46, 95, 96, 105, 106, 165, 188

L
Lagarias-Miller-Odlyzko algorithm, 282
Lagrange
four-square theorem, 159
polynomial roots theorem, 139, 150, 166
Landau
conjecture, 189
fourth problem, 52, 138, 139, 189, 192, 203
problem, 189
Large sieve, 224, 225, 232
Las Vegas algorithm, 230
Last digit, 20, 37, 158, 160, 161, 203, 207, 216
Leading
coefficient, 139, 177, 179, 186, 260, 281
constant, 188
digit, 158, 161, 203
zero, 33, 81
Least common multiple (lcm), 14, 162

Left factorial hypothesis (or Kurepa conjecture), 191, 196
Left-and-right truncatable prime, 70, 71, 120
Left-right (or horizontal) mirror reflection, 33, 34
Left-truncatable prime, 70, 71, 99, 120
Legendre
  conjecture, 177, 183, 184, 190, 194, 197–199, 220, 260–262, 264
  formula, 139, 150, 162, 166
  sieve, 212, 215, 216, 221, 225
  symbol, 15, 23, 74, 136, 146, 149, 155, 168, 216, 248
Lehmer
  number, 183
  totient problem (conjecture), 183, 191, 195, 196
Lemoine conjecture, 90, 183, 195, 199, 200
Lenstra, 245
  distribution, 220
Lenstra-Pomerance-Wagstaff (LPW) conjecture, 48, 184, 188
Lesser fortunate number, 182
Less-fortunate number, 182
Leyland
  number, 46
  number of the second kind, 46
  prime, 32, 46, 95, 97, 99, 105, 115, 116, 188
  prime of the first kind, 46
  prime of the second kind, 46, 116
L-function, 179, 232, 266
Liar (in primality tests), 234, 236
Lifting The Exponent (LTE) lemma, 166
Limit
  inferior, 14, 141
  superior, 14, 141, 179
Linear
  (Euler) sieve, 222, 238
  algebra, 244, 245, 247, 249, 250, 252
  dependency, 245, 247, 248
  polynomial, 247, 252
  recurrence, 128, 155
  sieves, 233, 282
  system of equations, 248, 250
Linnik
  constant, 14, 140, 274
  theorem, 140, 151, 157, 173, 274
Littlewood theorem, 140, 144, 157, 202
Logarithm, 14, 131, 141, 179, 188, 262, 274
Logarithmic, 48, 141, 158, 173, 254, 263, 265, 266, 278
  integral function $\mathrm{li}(x)$ or offset $\mathrm{Li}(x)$, 14, 140, 143, 144, 147, 200, 202, 255–259
Long prime, 38
LPW conjecture, 48, 184, 188
Lucas, 212
  d-pseudoprime, 281
  number, 14, 46, 47, 208
  prime, 46, 47, 77, 87, 88, 102, 103, 128, 164, 188
  pseudoprime, 191, 193, 235, 241, 281
  sequence, 47, 128, 150, 166, 183, 210, 212–214, 253, 281, 284
  sequence test, 210, 212, 241
  test, 113, 163, 210–213, 220, 229, 230, 281
  theorem, 166
Lucas-Fibonacci condition, 212
Lucas-Lehmer
  sieve frameworks, 234
  test, 113, 207, 213–215, 217, 227, 229–231, 234, 235
Lucas-Lehmer-Riesel test, 213, 214, 217, 229, 230, 241
Lucas-Wieferich prime, 76, 77
Lucky
  number, 14, 47, 48, 103
  prime, 47, 102, 103, 188

M
Maier theorem, 140, 157
Maillet conjecture, 195, 198, 199
Marin Mersenne, 184
  conjecture, 184, 201
Massias-Robin bounds, 173
Maximal
  period prime, 38
  prime gap, 179, 181, 188, 261, 262, 266
Maximum prime gap, 131, 177, 188, 261, 268
Mean (average), 27, 101, 126, 127, 135
Megaprime, 90
Meissel-Lehmer algorithm, 282
Meissel-Mertens constant (or Mertens constant), 14, 141, 274
Mersenne
  conjectures, 73, 178, 184, 194
  divisor, 50, 51, 98, 108, 122, 154, 160, 165
  number, 14, 22, 23, 25, 48–51, 73, 75, 98, 155, 160, 161, 167, 168, 184, 193, 213, 215, 217, 235, 252, 284
  prime, 17, 20, 24, 33, 39, 40, 48–52, 58, 62, 64–66, 75, 87–90, 93, 95, 96, 99, 100, 105, 108, 109, 113, 116, 117, 122, 125, 159–162, 164–166, 169, 178, 184, 188, 205, 207, 213, 214, 217, 227, 230, 234, 276, 284, 285, 289, 293
  prime exponent, 51, 95, 96, 105, 109, 188
  primes conjecture, 51, 184, 188
  transformation, 85
Mertens
  conjecture, 201
  constant (or Meissel-Mertens constant), 274
  first theorem, 141, 157, 173, 174
  function, 15, 201
  second theorem, 135, 141–143, 157, 173, 174
  third theorem, 142, 143, 157, 173, 174
Mihailescu theorem, 24, 176, 199
Miller test, 210, 214, 220
Miller-Rabin test, 163, 210–214, 229, 230, 234–236, 241–243, 249, 281
Mills
  constant, 13, 51, 103, 143, 272, 274
  construction, 171, 172
  prime, 51, 103, 154
  sequence, 272
  theorem, 51, 143, 151, 158, 171, 172
Minimal prime, 51, 52, 79, 88, 97, 98, 102, 117, 120, 122, 156, 161, 162, 217
Mirimanoff prime, 52, 75, 88, 98, 100, 124, 165, 188
Mirror reflection, 33, 34, 54
Mixed-digit prime, 82, 83
Mobius
  function $\mu(n)$, 16, 22, 170, 201, 257
  inversion, 257
  inversion formula, 257
Modular
  arithmetic, 114, 134, 136, 138, 212, 214, 221, 237, 238, 243, 287
  exponentiation, 213, 215, 249, 253, 279
Monic polynomial, 33, 281
Monodigit, 208
Monoid, 162
Monster group, 69

Monstrous moonshine theory, 69, 156
Monte Carlo algorithm, 230
Monus operator, 13, 170
Morrison test, 163, 210, 214, 229, 230
Moving average, 263
Multi-digit, 20, 24, 51, 57, 63, 64, 71, 80–83, 120, 152, 153, 160, 161, 167, 208, 217
Multi-factorial prime, 35
Multiple polynomial quadratic sieve (MPQS), 15, 243, 244, 248, 250
Multiplicative
  factor, 188
  group, 23, 136, 153, 219, 246
  inverse, 14, 23, 138, 246, 285
  monoid, 162
  number theory, 139
  order, 167, 213

N
n^2+1 prime, 52, 53, 95, 96, 105, 111, 138, 139, 153, 154, 160, 165, 177, 187, 188, 191, 192, 194, 198, 217, 227
n^4+1 prime, 52, 53, 95, 96, 105, 111, 160, 165, 187, 189, 217
Natural
  logarithm, 14, 141, 188, 262, 274
  number, 15, 19, 21, 22, 25, 36, 41–43, 47, 50, 53, 66, 67, 73, 76, 90, 98, 112, 137, 162, 178, 189, 194, 209, 213, 214, 216, 221, 222, 233, 256, 270, 277, 278
  power, 20, 23, 42, 284
Near-linear sieves, 233, 237
Near-repdigit palindromic prime, 55
Near-square prime, 28, 46, 52, 53, 95, 96, 105, 106, 111, 160, 164, 165, 189
Negative number, 25, 53, 140, 152, 171, 186, 248
Nested double summation, 170
Nesting prime, 83
Neutral element (on elliptic curve), 15, 211
New Mersenne conjecture, 73, 178, 184
n-friable number, 58
Nicholson conjecture, 197
Non-
  constant arithmetic progression, 153, 156
  constant polynomial, 153, 172, 186, 260
  Eulerian component, 152, 163
  existence, 152, 153, 190, 191
  generous prime, 53, 88, 104, 189
  good prime, 40
  linear polynomial, 192, 247
  Mersenne prime, 52, 62
  negative number, 15, 19, 21, 24, 56, 83, 100, 159, 164, 241, 245, 271, 276, 277, 283
  nesting prime, 83
  prime, 19, 31, 45, 79, 82, 100, 101, 112, 126, 153, 171, 203, 266
  Pythagorean prime, 65, 66, 74, 109, 122, 154, 165–167, 217, 266
  recursive sequence, 45, 53
  repunit, 30, 34, 54, 56, 57, 68, 88, 189, 208, 217
  strict pandigital prime, 55, 156
  trivial bounds on prime gaps, 138
  trivial dependency, 247, 250, 252
  trivial factor, 244–251, 253
  trivial factorization, 252
  trivial linear dependency, 245, 247
  trivial perfect power, 24
  trivial product, 148
  trivial square roots of 1, 163
  trivial zeros of Riemann zeta function, 146, 186, 200, 219, 256, 259, 262
  twin prime, 45, 72, 126
  unit Eisenstein integers, 276
  unit elements of Hurwitz quaternions, 276
  unit Gaussian integers, 275
  unit integers, 275
  visual symmetries, 33, 34, 54
  Wieferich prime, 75, 156, 192, 198
  zero, 23, 44, 53, 99, 134, 136, 139, 146, 156, 187, 200, 201, 218, 236, 256, 275, 276
Nonaliquot number, 73
Norm, 115, 247, 252, 275–277
Normal
  distribution, 135, 137
  number, 161, 194, 195, 274
  order, 137, 226
Normalization, 137
n-smooth number, 58, 244, 245, 249, 250
NSW
  number, 15, 53, 54
  prime, 53, 89, 95, 96, 102, 103, 128, 189
  sequence, 53
Number theory, 17–19, 40, 44
Numerator, 41, 43, 98, 122, 146, 155, 168, 218, 244

O
Octal, 203
Odd
  perfect number, 50, 152, 162, 163, 190, 195, 208, 285
  prime, 15, 20, 22, 23, 25, 28, 30, 36, 38
  prime gap, 24, 266
  quartan prime, 63
  sequence, 182
  untouchable number, 73, 125
On-Line Encyclopedia of Integer Sequences (OEIS), 15, 53, 73, 78, 111, 291, 292
Oppermann conjecture, 177, 183, 184, 190, 194, 197–199, 260, 262, 264
Order
  of integer, 15, 38, 169
  theory, 162
Ordinary
  integer, 93, 275
  prime, 63, 78, 91, 93, 275–277
  sieve, 283

P
p-adic
  analysis, 138
  valuation, 139
Padovan
  number, 15, 54
  prime, 54, 102, 103, 128, 189, 190
  sequence, 54
Pairwise
  coprime (pairwise relatively prime), 20, 25, 36, 39, 51, 197
  disjoint sets, 121
Palindrome, 34, 54, 68, 163
Palindromic
  number, 54, 208
  prime, 24, 34, 54, 55, 59, 64, 68, 88, 97, 99, 102, 117–122, 161, 165, 189, 217

wing prime, 54, 55, 97, 99, 118, 119, 121, 161, 165, 189
Pandigital
number, 55, 163, 208
prime, 55, 89, 97, 102, 117, 121, 153, 156, 161, 165
Parity, 31, 63, 65, 93, 114, 160, 201, 226, 227
barrier, 226
problem, 224, 233, 261
Partial
overlap, 107, 116
prime factorization, 213, 215
summation, 142, 173
Partition
function, 15, 56
number, 55, 56
prime, 55, 56, 102, 103, 128, 129, 189
sequence, 129
Pascal triangle, 218
Pell
number, 15, 56, 59, 163, 168, 208, 215
prime, 56, 58, 89, 100, 102, 103, 125, 128, 153, 164, 189
pseudoprime, 215
sequence, 56, 128, 215
test, 212, 215, 229, 230
Pentagon, 29
Pepin test, 163, 168, 211, 215, 217, 229–231, 235
Perfect
number, 15, 17, 21, 48–50, 73, 152, 162, 163, 169, 190, 195, 208, 270, 284, 285
power, 21, 24, 64, 88, 89, 156, 195, 210, 284, 285
square, 21–23, 53, 62, 64, 99, 115, 132, 148, 152, 159, 177, 182, 193, 197, 208, 212, 218, 244–246, 251, 284
Periodic
decimal, 13, 22, 24, 38, 98, 161
sequence, 37
Permutable prime, 30, 56, 57, 89, 97, 99, 102, 117–120, 122, 125, 153, 161, 165, 189, 217
Permutation of
digits, 30, 41, 56, 57, 59, 97, 118, 119, 217
numbers, 35
Perrin
number, 15, 57, 163, 168, 208
prime, 57, 103, 128, 189
pseudoprime, 281
sequence, 57, 281
Per-round error
bound, 236
probability, 236
Pierpont prime, 57, 58, 95, 96, 105–107, 109, 110, 116, 117, 160, 165, 189, 217
of the first kind, 58, 117
of the second kind, 58, 117, 165
Pillai
prime, 58, 98, 122, 154
sequence, 271
Pisano period, 37, 192
Plane algebraic curve, 69, 178
Pocklington test, 163, 215, 229, 230
Pocklington-Lehmer test, 215
Point addition, 246
Polignac
conjecture, 30, 31, 66, 184, 187, 190–192, 194, 195, 198–200, 262–264
formula, 139
Pollard
$p-1$ algorithm, 243, 244, 246, 249, 253
rho algorithm, 243, 244, 249
Polygon, 29
Polynomial
equation, 138, 139
sequences, 260
time (test complexity), 196, 209, 220, 228, 236, 243
Polynomial-time primality testing conjecture, 209, 220
Positive
constant, 147, 151, 258
divisor, 19, 21, 22, 25, 166, 167, 277
integer, 15, 19, 21, 22, 24, 25, 28–31
leading coefficient, 177, 179, 186, 260
power, 21
real number, 141, 147
Positive-definite, 132
Poulet number, 280
Power series, 257
Powerful number, 195, 284
Primality, 19–21, 92, 122, 209, 231, 275
test, 20, 32, 35, 48, 57, 60, 65, 92, 163, 195, 205–207, 209, 219, 227, 234, 240, 267, 279
Prime
chart, 291
constant, 16, 274
decomposition, 25, 167
factorization, 19, 22, 25, 26, 42, 43, 98, 136, 139, 152, 162, 189, 206, 213, 215, 230, 242, 243, 251, 252
gap, 14, 20, 24, 27, 30, 31, 68, 71, 72, 74, 82, 101, 131, 153, 155, 158, 177, 179–181, 184, 185, 188, 192, 193, 197–201, 239, 254, 260–266, 268, 272, 284
gaps sequence, 272
number, 15, 17, 19
number race, 266
number theorem (PNT), 15, 133, 135, 140–147, 150, 151, 153, 157, 158, 161, 163, 164, 172–174, 177, 186, 200, 206, 226, 254, 255, 257, 259, 260, 262–264, 267, 277, 282, 283
number theorem for arithmetic progressions (PNTAP), 15, 133, 144, 145, 150, 151, 154, 155, 157, 158, 160, 161, 163, 164, 168, 169, 173, 174, 200, 261, 283
sieve, 163, 164, 195, 205, 207, 221, 224, 226, 227, 231–234, 237, 239–241, 267, 283, 291
spiral, 266
with repeated digits, 21, 83
without repeated digits, 21, 83
Prime-counting
function in arithmetic progression $\pi(x; q, a)$, 16, 133, 144, 147
function $\pi(x)$, 16, 63, 104, 129, 130, 133–135, 140, 141, 143, 144, 147, 171, 172, 181, 186, 188, 195, 200, 202, 241, 254–259, 262, 267, 269, 271, 277, 278, 282, 283
sequence, 271
Prime-encoding number (constant), 13, 274
Prime-generating
algorithm, 232
constant, 272, 274
formula, 171, 172
integer, 178, 187
sieve, 221, 223
Prime-indexed prime (super prime), 58, 59, 79, 99, 100, 154, 162, 164
Prime-indexing transformation, 86

Primes
modulo 4 theorem, 145, 150, 158, 166
modulo 6 theorem, 145, 150, 158, 166
Prime-sum prime, 84
Primeval
number, 59
prime, 59, 97, 102, 117, 122, 189
Primitive
complex cube root of 1, 276
Pythagorean triangle, 109
Pythagorean triple, 115
root, 23, 38, 53, 104, 169, 177, 190–193, 195–197, 219, 273, 284, 285
Primorial
number, 15, 31, 38, 60, 61, 97, 113, 170, 208, 264, 284
number of the first kind, 15, 38, 60, 61, 97, 100, 113
number of the second kind, 15, 31, 61, 97
prime, 15, 31, 36, 60, 61, 89, 95, 97, 100, 105, 112–114, 125, 164, 189, 227
Probabilistic
model, 140, 182, 188, 261
number theory, 135, 137, 226
primality test, 20, 93, 206, 207, 210–213, 215, 216, 220, 228, 229, 235, 236, 239–241, 279, 281
Probability
of error (error probability), 212, 214, 228, 229, 235, 236, 242
of primality, 113, 228
theory, 135
Probable prime, 20, 27, 30, 32, 37, 45, 46, 51, 54, 56, 57, 64, 70, 72, 73, 88, 89, 93, 206, 210–215, 228, 229, 236, 240
Probable-prime endpoints, 265
Product-digit prime, 84
Proper
divisor, 21, 22, 49, 69, 73, 99, 208, 270
prime, 38
Proth
number, 61, 62, 107, 215
prime, 61, 62, 65, 95, 96, 105–107, 109, 110, 116, 117, 164, 165, 189, 215, 217, 230
test, 215, 217, 229–231, 241
theorem, 62, 163, 166, 215
Proth-Gilbreath
conjecture, 185, 190, 195
triangle, 185
Proven prime, 27, 32, 46, 92, 93, 206
Proven-prime endpoints, 265
Pseudoprimes, 90, 153, 156, 207, 211, 220, 229, 234, 235, 241, 242, 279–282, 284
Pure
mathematics, 19, 44, 94, 136, 286
sieve (Brun sieve), 224, 239
Pythagorean
prime, 36, 52, 62, 63, 86, 95, 96, 98, 105, 109, 114, 115, 122, 154, 159, 160, 165, 167, 217, 266
triangle, 109
triple, 115

Q
Quadratic
congruence relation, 135, 136
field, 123, 212, 253
form, 114, 115, 132, 148, 154, 191, 221, 233, 237–239, 251
Frobenius test (QFT), 212
non-residue, 23, 146, 253, 283, 285
reciprocity, 136, 145, 146, 150, 216
residue, 18, 23, 135, 136, 146, 167, 168, 238, 245, 250, 253, 283–285
sieve (QS), 15, 243–245, 248–251
transformation, 85
Quadruplet (of primes), 66, 90
Quantum computing, 244, 287
Quartan prime, 53, 62, 63, 95, 96, 105, 111, 160, 165, 189, 217
Quasi-perfect number, 284
Quasi-polynomial time (test complexity), 210, 228
Quaternion, 14, 20, 93, 275–277
Quintuplet (of primes), 24, 66, 152
Quotient, 26, 187
group, 187
of shifted primes, 187

R
Ramanujan prime, 15, 25, 63, 104, 129, 130, 132, 154
Ramified primes, 95
Rassias conjecture, 185, 190, 191, 194, 196, 198
Rational
function, 153
norm, 252
number, 15, 22, 43, 187
number field, 247
point, 178, 179
Real
number, 15, 20, 51, 93, 141, 143, 147, 151, 155, 156, 161, 170, 171, 195, 255, 272, 275–277
part of complex numbers, 15, 136, 153, 186, 275, 277
Reciprocal, 22, 24, 38, 41, 45, 72, 98, 132, 133, 141, 143, 199, 208, 224, 272, 273
Record prime (record-breaking prime), 90, 93, 94, 207, 289
Recurrence relation, 28, 56, 102, 103, 127–129, 169, 172, 202, 212, 214, 253
Recursive
formula, 36, 128, 219
sequence, 102, 103, 127, 128
Reduced
fractional form (in lowest terms), 41, 43, 168, 218
residue classes, 145, 283
residue system, 23
Reflection (symmetry), 33, 34, 54, 97, 102, 121
Regular
pentagon, 29
polygon, 29
prime (Bernoulli regular or B-regular), 43, 44, 98, 122, 123, 189, 196
prime (Euler regular or E-regular), 44, 98, 122, 123, 189
prime (Genocchi regular or G-regular), 44, 98, 123, 189
Repdigit, 64, 208
Repeating
decimal (periodic), 13, 22, 24, 38, 98, 161
primality test, 212, 214, 236
Repunit
number, 16, 63, 95, 168, 208, 217
prime, 21, 24, 30, 34, 39, 48, 54, 57, 63, 64, 68, 73, 81, 88, 89, 95, 97, 100, 105, 117–121, 125, 153, 156, 161, 164–166, 189, 217
Residue
class, 133, 139, 140, 145, 158, 160, 161, 168, 169, 202, 218, 224, 225, 238, 283

primes, 84
system, 23, 181
Restricted divisor function $s(n)$, 15, 22, 50, 99, 166, 219
Reversible prime, 34, 57, 64, 97, 99, 117–120, 122, 164, 165
Riemann
hypothesis, 14, 15, 51, 131–133, 138, 140, 143, 146, 147, 177, 186, 190, 194–201, 209, 210, 214, 216, 220, 229, 235, 258, 260, 262, 287
prime-power counting function $J(x)$ or $\Pi(x)$, 14, 16, 256–258
R-function $R(x)$, 15, 257, 258
zeta function $\zeta(s)$, 16, 43, 136, 138, 146, 147, 153, 174, 186, 200, 219, 256–259, 262
Riemann-von Mangoldt formula, 146, 157, 162
Riesel
number, 65, 156, 195, 241
prime, 64, 65, 95, 96, 105, 108, 110, 116, 117, 165, 166, 217, 230
problem, 65, 241
Right-angle triangle, 62, 109, 115
Right-truncatable prime, 70, 71, 120, 121
Ring, 16, 20, 23, 93, 162, 209–212, 275, 276
theory, 162
Robin theorem, 146, 147, 157
Rotation (symmetry), 33, 97, 102, 121
Round (to nearest integer), 13, 45, 96, 112
Rowland formula, 170, 171
RSA primes (or cryptographic primes), 94
RSA public-key cryptosystem, 15, 94, 242, 247, 250, 277, 287
RSA-129, 250

S

Sad prime (unhappy prime), 41
Safe prime, 15, 65–67, 77, 86, 99, 100, 104, 106, 122, 125, 129, 164, 167, 189, 192, 198, 199, 217, 226, 271
Sarrus number, 280
Schinzel hypothesis H, 179, 180, 185–187, 191, 194, 197–200, 262
Schinzel-Sierpinski conjecture, 187, 191, 195, 196
Search space, 206, 210, 214, 223, 226, 227, 237
sec function, 44
Secant number, 35
sech function, 44
Second Chebyshev prime-counting function $\psi(x)$, 16, 132, 147, 174, 257–259
Second-moment (variance), 226, 239
Segmentation, 205, 237
Segmented sieve, 206, 233, 237
Selberg
formula, 147, 157
sieve, 164, 224–226, 232, 239, 240
Self
number, 66
prime, 66, 97, 99, 102, 117, 124, 125, 154, 189
Semi-logarithmic scale, 267, 269
Semiprime, 16, 29, 90, 101, 126, 134, 138, 183, 189, 192, 245, 246, 249, 277, 278
Sequence of
integers, 15, 44, 87, 102, 127, 128, 135, 150, 183, 291, 292
primes, 40, 58, 59, 63, 68, 74, 81, 82, 86, 127, 137, 143, 170, 171, 178, 193, 263, 270, 272
Sexy prime, 24, 47, 66, 72, 90, 99, 101, 125, 126, 149, 152, 187, 189, 197–200, 226
conjecture, 197–200
quintuplet, 24, 66, 152
Shanks, 188
conjecture, 181, 188, 194, 198, 199, 261, 262
square forms factorization (SQUFOF), 16, 243, 244, 251
Shifted primes, 134, 187
Shor algorithm, 244
Siegel-Walfisz theorem, 147, 151, 157, 173, 174, 200
Sierpinski
formula, 13, 170, 171, 274
number, 156, 195, 241
problem, 241
theorem, 151
Sieve
(or sieving), 163, 164, 195, 205, 207, 221, 224, 226, 227, 231–234, 237, 239–241, 267, 283, 291
theory, 133, 139, 163, 180, 224, 232, 240, 261
Sifted set, 225, 226, 233
Sifting, 224, 226, 227, 232, 234, 308
Single prime, 45, 72
Singular series, 182
Smarandache-Wellin
number, 67, 121
prime, 67, 89, 97, 98, 102, 117, 121, 189
Smooth
number, 58, 244, 245, 249, 250
plane algebraic curve, 69
relation, 244, 245, 248, 250
value, 245, 250
Smoothness, 243, 247, 252, 262
bound, 245, 246, 250, 253
Sociable number, 270, 284
Solinas prime, 39
Solovay-Strassen test, 136, 149, 164, 211, 216, 220, 229, 230, 234–236, 242
Somer-Lucas pseudoprime (Somer-Lucas d-pseudoprime), 281
Sophie Germain
prime, 65–67, 77, 85, 86, 99, 104, 106, 125, 129, 160, 167, 189, 192, 198, 199, 217, 226, 270, 271
safe primes, 67
transformation, 85, 86
Space complexity, 237
Special
case, 28, 39, 46, 106, 107, 145, 150–152, 154, 165, 166, 168, 173, 174, 178–180, 185, 187, 194, 197–199, 203, 214, 228, 248, 261, 263
number field sieve (SNFS), 16, 243, 244, 247, 250–252
Special-purpose
factorization algorithm, 243, 244, 246, 251
primality test, 230, 235
prime sieve, 233, 234
Specific type of primality, 231
Split primes, 95
Spread (standard deviation), 135
Square root, 21, 62, 163, 246, 247, 249, 252
Square-free, 21, 22, 25, 152, 155, 163, 169, 176, 177, 183, 242, 277, 278, 281, 285
Standard deviation (spread), 135
Stern prime, 67, 68, 89, 99, 100, 124, 125, 189, 201
Stochastic primality test, 229, 230
Strict
pandigital integer, 208
pandigital prime, 55, 165
sub-string, 83
String, 52, 83, 97, 102, 127, 155, 160, 194
String theory, 69

Strobogrammatic prime, 68, 97, 99, 102, 117, 121, 122, 153, 161, 165, 189, 217
Strong
  Fermat pseudoprime, 191, 193
  Fermat test, 213
  Lucas pseudoprime, 191, 193, 241
  Lucas test, 210, 213
  prime, 23, 28, 68, 69, 72, 74, 101, 126, 127, 154, 157
  pseudoprime, 166, 234, 235, 241, 242, 281, 282
  semiprime, 277
Subadditive function, 188
Sub-exponential time (test complexity), 228, 245
Sub-linear sieves, 233, 237
Sub-sequence (of digits), 51, 52, 78, 79, 98, 102, 120, 122, 161
Subset (proper subset), 20, 30, 34, 36, 38, 40, 43–45, 48–50, 52–55, 57, 58, 61–65, 68, 73–76, 78–81, 83, 86, 87, 90, 95, 106–111, 116, 117, 121–124, 126, 133, 164–166, 192, 195, 196, 203, 208, 217, 226, 234, 241, 245, 248, 275–277, 280, 282
Sub-string, 83, 102, 155
Sum of
  digits, 15, 66, 97, 99, 155, 161, 191, 202
  two squares theorem, 115, 148, 150, 152, 158, 167
Summation, 16, 142, 170, 173, 176
  congruence, 176
  formula, 176
  operator, 16
Sum-minus prime, 85
Sum-plus prime, 85
Sundaram sieve, 223, 233, 237, 238
Super prime (prime-indexed prime), 58, 59, 79, 100, 125
Superset (proper superset), 78, 81, 217
Supersingular
  elliptic curve, 69
  prime, 69, 88, 104, 154, 156
Surface mirror reflection, 33
Sylvester-Schur theorem, 148, 151, 157
Symmetric, 54, 236, 251
Symmetry, 33, 34, 97, 102, 121, 215, 218, 276, 283

T
Taylor
  coefficient, 179
  series expansion, 35, 43, 44
Terminating
  decimal, 24, 38, 208
  digit, 203
Test of primality, 20, 32, 35, 48, 57, 60, 65, 92, 163, 195, 205, 207, 209, 219, 227, 234, 240, 267, 279
Thabit
  number, 69, 70
  number of the first kind, 70
  number of the second kind, 69, 70
  prime, 69, 89, 95, 96, 106, 109–111, 165, 189, 284
  prime of the first kind, 69, 110, 111, 165
  prime of the second kind, 69, 109, 110, 165
Time complexity, 233, 237
Titanic prime, 90
Topology, 44
Transformation
  (exponential), 85
  (index-addition), 86
  (index-subtraction), 86
  (Mersenne), 85
  (prime-indexing), 86
  (quadratic), 85
  (Sophie Germain), 85, 86
  (Wagstaff), 86
Transformed prime, 85, 86
Trial division
  factorization algorithm, 243, 244, 246, 252, 253, 277
  primality test, 61, 210, 218, 240
Triangle, 29, 62, 109, 115
Triangular number, 24, 50, 159, 208, 284, 285
Tribonacci
  number, 16, 70, 160
  prime, 70, 103, 128, 189
  sequence, 70
Trigonometric function, 35, 43, 44, 171
Trigonometry, 171
Triple factorial prime, 35
Triplet (of primes), 24, 31, 66, 71, 72, 90, 152, 158, 181
Trivial zeros of Riemann zeta function, 186
Truncatable prime, 70, 71, 88, 97, 99, 102, 117, 120–122, 156, 162, 193
Turan sieve, 226, 239
Twin
  compositorial primes, 31, 113
  factorial primes, 35, 113, 189
  factorial primes conjecture, 189
  lucky numbers, 47
  prime, 13, 24, 29–31, 35, 37, 45, 47, 60, 61, 68, 71, 72, 74, 76, 90, 99–101, 113, 125, 126, 132–134, 149, 152, 157, 159, 160, 165, 168, 177, 180, 182, 184, 187, 189, 192, 197–200, 203, 217, 219, 224–227, 232–234, 238, 254, 262–264, 273
  prime conjecture, 30, 72, 134, 149, 177, 180, 182, 184, 187, 189, 192, 197–200, 203, 262
  prime triplet, 72, 152
  primes constant, 13, 273, 274
  primorial primes, 60, 61, 113, 189
  Thabit primes, 69
Twin-triplet primes, 71
Two-sided truncatable prime, 70, 71, 120, 121
Type-indexed prime
  of the first kind (I), 86, 87
  of the second kind (II), 87
Type-specific
  primality test, 208, 216–218, 227, 230
  prime sieve, 226, 227, 234

U
Ulam spiral, 266–268
Unfortunate number, 182
Unhappy prime (sad prime), 41
Unique prime, 72, 73, 89, 97, 98, 117, 165, 189
Uniqueness, 19, 61, 115, 116
Unit
  Eisenstein integer, 276
  Gaussian integer, 275
  group, 252
  integer, 275
Units in Hurwitz quaternions, 277
Untouchable
  number, 50, 73, 125, 284, 285
  prime, 73, 89, 99, 124, 125, 190
Up-down (or vertical) mirror reflection, 33, 34
Upper bound
  in Zhang theorem framework, 149
  on density of twin primes, 199

on number of integers escaping sifting process, 226
on number of polynomial congruence solutions, 139
on number of primes in arithmetic progression, 133
on prime gap, 131, 199, 260, 264
on smallest prime in arithmetic progression, 140, 274

V
Variable-order recurrence relation, 103, 128, 129
Variance (second-moment), 226
Vinogradov theorem, 148, 162, 174, 182, 200
Visual symmetries, 33, 97, 102, 121
von Mangoldt function, 16, 147

W
Wagstaff
prime, 16, 24, 33, 45, 73, 74, 86, 89, 95, 96, 99, 100, 106, 111, 112, 116, 117, 122, 160, 164–166, 178, 184, 189, 217, 284
transformation, 86
Wall-Sun-Sun prime, 74, 89, 98, 124, 189–191
Waring conjecture (or problem), 148, 149, 162, 182
Weak
irregular prime, 77
prime, 23, 28, 33, 68, 69, 72, 74, 101, 126, 127, 154, 156, 157
Weakly prime, 33, 74
Weird number, 208
Wheel
factorization, 223, 233, 237, 239
sieve, 223, 237, 238
Wieferich
prime, 52, 74, 75, 77, 89, 98, 100, 124, 156, 165, 189, 192, 198, 218, 279, 282
pseudoprime, 191, 282
Willans formula, 170–172, 219
Williams $p + 1$ algorithm, 243, 244, 253
Wilson
prime, 75, 89, 98–100, 124, 189
test, 208, 216, 218, 229–231
theorem, 22, 36, 75, 134, 135, 149, 151, 163, 166, 168, 170–172, 174, 208, 216, 218
Witness (in primality tests), 214, 228, 229, 236
Wolstenholme
prime, 75–77, 89, 98, 100, 124, 166, 189, 190, 284
theorem, 168, 218
Woodall
number, 76, 208
prime, 76, 89, 95, 96, 106, 108, 110, 116, 117, 164, 166, 189
Woodall-Cullen twin prime, 76
World record prime, 90, 289
Wright
constant, 16, 151, 156, 171, 272, 274
construction, 171, 172
sequence, 272
theorem, 151, 156, 171, 172

Z
Zeros of Riemann zeta function, 136, 138, 146, 186, 200, 219, 256, 258, 259, 262
zeta function $\zeta(s)$, 16, 43, 136, 138, 146, 147, 153, 174, 186, 200, 219, 256–259, 262
Zhang theorem, 149, 155, 157, 190, 192, 200
Zsigmondy theorem, 149–151, 162, 166