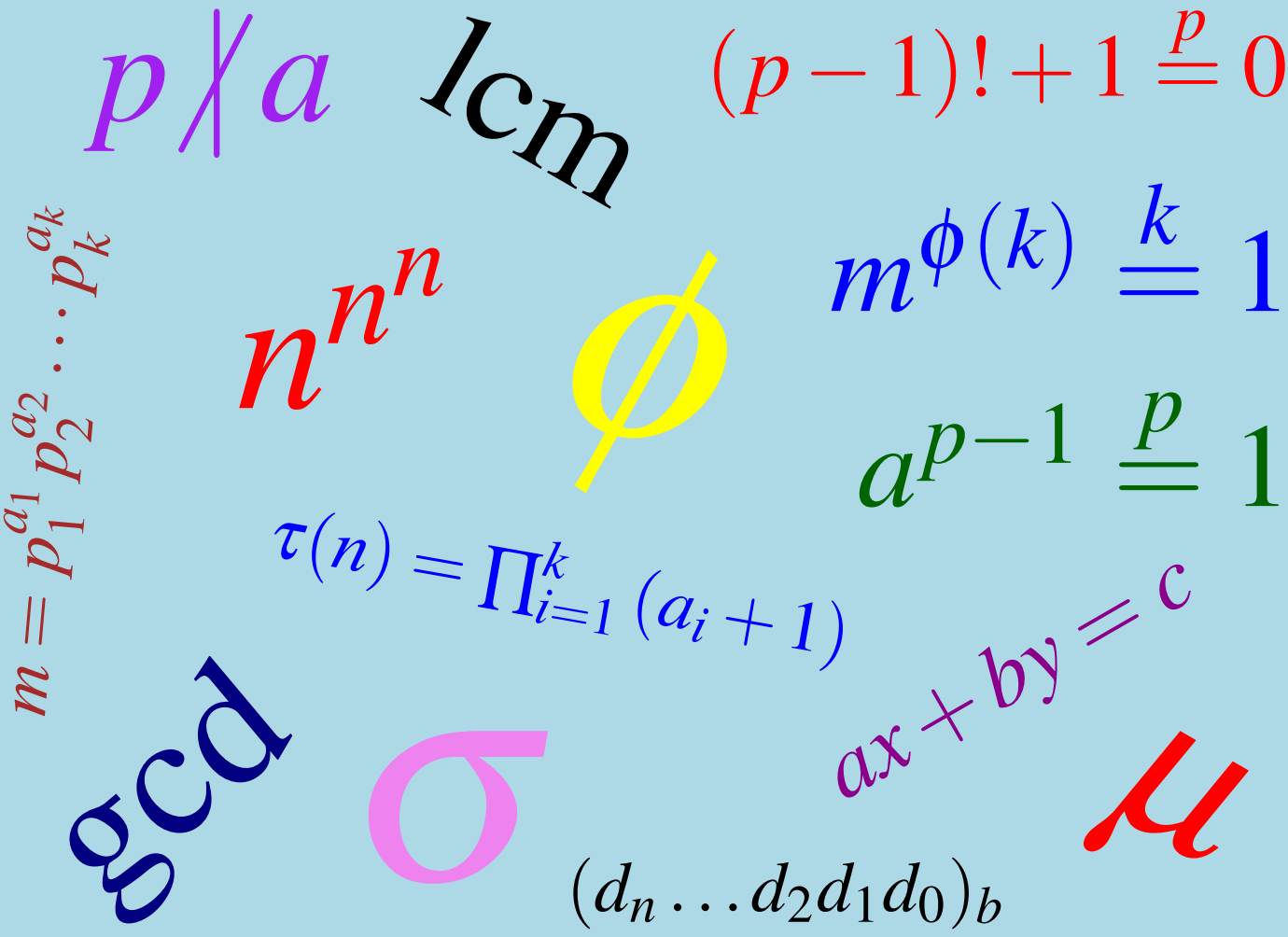
Notes and Problems in Number Theory

Volume II



Taha Sochi

Preface

This is the second volume of my book "Notes and Problems in Number Theory". It is important to note the following points (which are largely about this volume):

• We take all the results and materials in the previous volume of this book for granted. Therefore, the reader should consult the previous volume when necessary. For this purpose (and to help the reader) we refer frequently to the previous volume.

• We focus in this volume on the type of problems that develop the basic and most essential skills which are required for dealing with number theory problems.

• We introduced some new topics in the first chapter (i.e. Introduction), while the remaining chapters are largely dedicated to solved problems from the main topics of elementary number theory (which are introduced in V1 or in the Introduction chapter of the present volume). We also introduced the subject of cryptography and computing in number theory in the last two chapters. So in brief, the materials in this volume are largely a mix of applications to the materials of V1 and some theoretical background of new topics as well as applications to the new topics. This is to ensure the continuity and graduality and reduce the gradient of the learning curve.

• For the sake of originality, we deliberately reduced the amount of solved problems which have been previously investigated by others (especially the widely circulating problems) to the bare minimum. In fact, even when we investigate problems of this type we mostly follow novel or improved approach or/and presentation.

• As in my previous books, my topmost priority in the structure and presentation is clarity and graduality so that the readers have the best chance of understanding the content with minimum effort and with maximum enjoyment. For this purpose (as well as for other obvious purposes) the book is full of cross references (which are hyperlinked in the electronic versions although the hyperlinks are not highlighted with color or other marking techniques to avoid distortion and ugliness). As indicated earlier, we also refer frequently to the previous volume.

• The readers who want to benefit maximally from this book should try solving the Problems in this book before reading their solutions. They should resist the temptation to read the solutions immediately or just after a few attempts. Mathematical knowledge and skill cannot be acquired by just reading without practice.

• As indicated, the last chapter of the present volume is dedicated to computing in number theory and hence computer codes (in C++ language) represent the main part of the solutions of the Problems of the last chapter. These codes are available from my webpage on ResearchGate. We recommend inspecting these codes carefully and trying to figure out the algorithms behind them. These codes (as well as the algorithms behind them) are mostly very simple and hence they do not require specialized knowledge in computing or in C++. However, they can be very useful in acquiring the essential knowledge and developing the basic skills in dealing with essential topics in number theory by computational methods and tools.

• The book can be used as a text or as a reference for an introductory course on number theory and may also be used for general reading in mathematics (especially by those who have the hobby of problem solving). The book may also be adopted as a source of pedagogical materials which can supplement, for instance, tutorial sessions (e.g. in undergraduate courses on mathematics or computing or cryptography or related subjects).

Taha Sochi
London, May 2024

Contents

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.

$\forall$	for all
$\times$, $\cdot$	multiplication sign
$\{\cdots\}$	set
$!$	factorial
$\in$	in (or belong to)
$\ni$	(backward) in (or belong to)
$\notin$	not in
$[A;B]$	continued fraction symbol
$\lfloor a \rfloor$	floor function (the greatest integer less than or equal to a)
$\lceil a \rceil$	ceiling function (the smallest integer greater than or equal to a)
$\lvert a \rvert$	absolute value of a
$\overline{a}$	negation of a
$\mathbb{C}$	the set of complex numbers
C_m^n	binomial coefficient (number of combinations of m in n with no repetition)
$C_{n_1,n_2,\ldots,n_k}^n$	multinomial coefficient
$\mathbb{E}$	the set of even numbers
Eq., Eqs.	Equation, Equations
F_k	Fermat number (i.e. k^{th} Fermat number where $k = 0, 1, \ldots$)
$\gcd(m,n)$	greatest common divisor of m and n
iff	if and only if
$I_{k,r}n$	index of integer n relative to primitive root r (modulo k)
$\operatorname{lcm}(m,n)$	least common multiple of m and n
LHS, RHS	left hand side, right hand side
$m \mid n$	m divides n
$m \nmid n$	m does not divide n
$m \uparrow n$	tetration of m to n
$(m)_n$	the number m in base n
$m \overset{k}{=} n$	m and n are congruent modulo k
$m \overset{k}{\neq} n$	m and n are not congruent modulo k
$m, n, k, \ldots$	integers
m^*	modular multiplicative inverse of m
m_k^*	modular multiplicative inverse of m modulo k
$\max(a,b)$	the maximum of a and b
$\min(a,b)$	the minimum of a and b
mod	modulo (or modulus)
M_p	Mersenne prime
$\widehat{n}$	factorial power of 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. $0, 1, 2, 3, \ldots$)
$\left(\frac{n}{N}\right)$	Jacobi's symbol
$\left(\frac{n}{p}\right)$	Legendre's symbol

$\mathbb{O}$	the set of odd numbers
$O_k n$	the order of integer n (modulo k)
p	prime number
$\mathbb{P}$	the set of prime numbers
P_e	even perfect number
P_m^n	number of permutations of m in n (with no repetition)
$\mathbb{Q}$	the set of rational numbers
$\mathbf{r}, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3$	position vectors (in 3D space)
$\mathbb{R}$	the set of real numbers
$s(n)$	the restricted divisor function
S_c	complete residue system
S_r	reduced residue system
S_{rk}	reduced residue system modulo k
U_n	the n-digit repunit number
V1	volume 1 (of this book)
x, y, z	variables (mostly integers)
$\mathbb{Z}$	the set of integers
Δ	discriminant of quadratic polynomial
$\mu(n)$	the Mobius function
Π	the product symbol (for repeated multiplication)
$\sigma(n)$	the divisor function
Σ	the summation symbol
$\tau(n)$	the tau function
$\phi(n)$	the totient (or phi or Euler) function

Chapter 1
Introduction

In this chapter we briefly investigate some new topics in number theory which we did not investigate (at least sufficiently) in V1 and which are needed for our future investigations (in this and upcoming volumes).

1.1 Continued Fractions

In this section we define the continued fraction representation of a given positive real number and illustrate the main technique used to obtain this representation and how it is employed to approximate numbers as rational fractions (i.e. as ratios of integers). In brief, this is the representation of the number as a sum of an integer part and a recursive fraction part. The latter part is a fraction ladder obtained by recursively taking the reciprocal of the reciprocal of the fraction part in the previous step in the ladder. However, various tricks and techniques are usually used some of which may obscure or not reflect this pattern explicitly (noting that they are usually employed to obtain this representation in a more efficient way or more neat form).

The best way to understand the continued fraction representation and the techniques used to obtain it is to apply these techniques to specific numbers. So, let us do this now to $\sqrt{2}$ (noting that more illustrating examples will follow). We have (by adding and subtracting 1):

$$\sqrt{2} = 1 + \sqrt{2} - 1$$

So, the fraction part in the first step is $(\sqrt{2} - 1)$. Now, if we take the reciprocal of the reciprocal of this fraction part and repeat this in the next steps then we get the following:

$$\begin{aligned}
\sqrt{2} &= 1 + \sqrt{2} - 1 = 1 + \frac{1}{\frac{1}{\sqrt{2}-1}} = 1 + \frac{1}{\frac{\sqrt{2}+1}{2-1}} = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2 + \sqrt{2} - 1} \\
&= 1 + \frac{1}{2 + \frac{1}{\frac{1}{\sqrt{2}-1}}} = 1 + \frac{1}{2 + \frac{1}{\frac{\sqrt{2}+1}{2-1}}} = 1 + \frac{1}{2 + \frac{1}{\sqrt{2}+1}} = 1 + \frac{1}{2 + \frac{1}{2 + \sqrt{2} - 1}} \\
&= 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\frac{1}{\sqrt{2}-1}}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \ddots}}}
\end{aligned}$$

As we see, this pattern of $1 + \dfrac{1}{2 + \dfrac{1}{2 + \ddots}}$ will repeat itself for ever and hence we can symbolize this succinctly as:

$$\sqrt{2} = [1; \overline{2}]$$

where 1 represents the integer part while $\overline{2}$ represents the fractional part (noting that the bar indicates that 2 is repeated infinitely).

Regarding the use of continued fraction to approximate the number that is expressed in this form (i.e. $\sqrt{2}$ in this case), we can say that we can truncate the ladder of continued fraction at any step on the ladder by ignoring the last fraction (i.e. $\ddots$) at that step and hence we get a rational fraction approximation to the given number as illustrated in the following (using our example of $\sqrt{2}$):

$$\sqrt{2} \simeq 1 + \frac{1}{2} = \frac{3}{2} = 1.5$$

$$\sqrt{2} \simeq 1 + \frac{1}{2 + \frac{1}{2}} = 1 + \frac{2}{5} = \frac{7}{5} = 1.4$$

$$\sqrt{2} \simeq 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = 1 + \frac{1}{2 + \frac{2}{5}} = 1 + \frac{5}{12} = \frac{17}{12} \simeq 1.42$$

It is obvious that we get better and better approximations as we go further down on this fraction ladder (as can be seen in the above example where we get persistently better approximations to $\sqrt{2}$ as we go further down on the ladder). In other words, the successive rational fractions obtained from successive stepping down on this ladder converge persistently towards the given number.
Finally, it is useful to take notice of the following remarks:
• Rational numbers are represented by finite (or terminating) continued fraction ladder, while irrational numbers require infinitely long (or infinitely deep or non-terminating) continued fraction ladder.
• As indicated above, the continued fraction expression is symbolized by $[A; B]$ where A is the integer part (which is a single integer) while B is the (continued) fraction part which can be a single integer (e.g. $1.2 = [1; 5]$) or a number of integers separated by commas (e.g. $1.23 = [1; 4, 2, 1, 7]$) where these integers are the successive integer parts in the ladder. Now, we have 3 main cases with regard to the fraction part B:
Case 1: the given number is rational and hence B is a single integer like $1.2 = [1; 5]$ or B is a block of finitely-many integers like $1.23 = [1; 4, 2, 1, 7]$.
Case 2: the given number is irrational and B is a single integer or a block of integers which is repeated cyclically. In this case we put a bar on the top of B to indicate this cyclic behavior, e.g. $\sqrt{2} = [1; \overline{2}]$ and $\sqrt{3} = [1; \overline{1, 2}]$.
Case 3: the given number is irrational and B is a block of integers with no cyclic pattern (within the number of acquired steps or for ever). In this case the block of integers is trailed with an ellipsis (i.e. three dots ...), e.g. $\pi = [3; 7, 15, 1, 292, \ldots]$.

Problems

1. Obtain the continued fraction of $\sqrt{2}$ using this time the technique of substitution.
   Solution: In the technique of substitution we obtain the fraction ladder by recursive substitution of the first step in the ladder for each occurrence of the given number in this ladder (as will be demonstrated in the following), that is:

$$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \frac{2 - 1}{\sqrt{2} + 1} = 1 + \frac{1}{1 + \sqrt{2}}$$

   So, the first step of the ladder is $\sqrt{2} = 1 + \frac{1}{1 + \sqrt{2}}$. What we do next is to substitute this expression of $\sqrt{2}$ $\left(\text{i.e. } 1 + \frac{1}{1 + \sqrt{2}}\right)$ recursively for each occurrence of $\sqrt{2}$ in each successive step in the ladder, that

is:

$$\sqrt{2} = 1 + \frac{1}{1 + \left(\sqrt{2}\right)} = 1 + \frac{1}{1 + \left(1 + \frac{1}{1 + \sqrt{2}}\right)} = 1 + \frac{1}{2 + \frac{1}{1 + \sqrt{2}}}$$

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{1 + \left(\sqrt{2}\right)}} = 1 + \frac{1}{2 + \frac{1}{1 + \left(1 + \frac{1}{1 + \sqrt{2}}\right)}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \sqrt{2}}}}$$

As we see, this pattern of $1 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}$ will repeat itself for ever (as seen previously) because $\sqrt{2} = 1 + \frac{1}{1 + \sqrt{2}}$ (as seen above) and hence when we substitute the expression $1 + \frac{1}{1 + \sqrt{2}}$ recursively for the $\sqrt{2}$ in the denominator we must always get $2 + \ddots$.

2. Obtain the continued fraction form of the following numbers and hence get a number of successive rational fraction approximations from these forms:

(**a**) 1.2. (**b**) 1.23. (**c**) $\sqrt{5}$. (**d**) $\sqrt{3}$. (**e**) π.

Solution:

(**a**) We have $1.2 = 6/5$ and hence:

$$\frac{6}{5} = 1 + \frac{1}{5}$$

Hence, $1.2 = [1; 5]$. The first "approximation" is $6/5$ which is exact.

(**b**) We have $1.23 = 123/100$ and hence:

$$\begin{aligned}\frac{123}{100} &= 1 + \frac{23}{100} = 1 + \frac{1}{\frac{100}{23}} = 1 + \frac{1}{4 + \frac{8}{23}} = 1 + \frac{1}{4 + \frac{1}{\frac{23}{8}}} = 1 + \frac{1}{4 + \frac{1}{2 + \frac{7}{8}}} = 1 + \frac{1}{4 + \frac{1}{2 + \frac{1}{\frac{8}{7}}}} \\ &= 1 + \frac{1}{4 + \frac{1}{2 + \frac{1}{1 + \frac{1}{7}}}} = 1 + \frac{1}{4 + \frac{1}{2 + \frac{1}{1 + \frac{7}{1}}}} = 1 + \frac{1}{4 + \frac{1}{2 + \frac{1}{1 + \frac{1}{7 + 0}}}} = 1 + \frac{1}{4 + \frac{1}{2 + \frac{1}{1 + \frac{1}{7}}}}\end{aligned}$$

As we see, the fraction part of $7/1$ is zero and hence this ladder is terminating (as expected since 1.23 is rational). Thus, $1.23 = [1; 4, 2, 1, 7]$. The first 3 rational fraction approximations are:

$$1 + \frac{1}{4} = 1.25 \qquad 1 + \frac{1}{4 + \frac{1}{2}} \simeq 1.222 \qquad 1 + \frac{1}{4 + \frac{1}{2 + \frac{1}{1}}} \simeq 1.231$$

As we see, these approximations persistently converge towards 1.23.

(**c**) We have:

$$\begin{aligned}\sqrt{5} &= 2+\sqrt{5}-2 = 2+\frac{1}{\frac{1}{\sqrt{5}-2}} = 2+\frac{1}{\sqrt{5}+2} = 2+\frac{1}{4+\sqrt{5}-2} = 2+\frac{1}{4+\frac{1}{\frac{1}{\sqrt{5}-2}}} \\ &= 2+\frac{1}{4+\frac{1}{\sqrt{5}+2}} = 2+\frac{1}{4+\frac{1}{4+\sqrt{5}-2}} = 2+\frac{1}{4+\frac{1}{4+\ddots}}\end{aligned}$$

As we see, this pattern of repetitive (or periodic) 4 should continue for ever. Hence, $\sqrt{5} = \left[2;\overline{4}\right]$. The first 3 rational fraction approximations are:

$$2+\frac{1}{4} = 2.25 \qquad 2+\frac{1}{4+\frac{1}{4}} \simeq 2.235 \qquad 2+\frac{1}{4+\frac{1}{4+\frac{1}{4}}} \simeq 2.236$$

As we see, these approximations persistently converge towards $\sqrt{5} \simeq 2.2361$.
(**d**) We have:

$$\begin{aligned}\sqrt{3} &= 1+\sqrt{3}-1 = 1+\frac{1}{\frac{1}{\sqrt{3}-1}} = 1+\frac{1}{\frac{\sqrt{3}+1}{2}} = 1+\frac{1}{\frac{2+\sqrt{3}-1}{2}} = 1+\frac{1}{1+\frac{\sqrt{3}-1}{2}} \\ &= 1+\frac{1}{1+\frac{1}{\frac{2}{\sqrt{3}-1}}} = 1+\frac{1}{1+\frac{1}{\frac{2(\sqrt{3}+1)}{2}}} = 1+\frac{1}{1+\frac{1}{\sqrt{3}+1}} = 1+\frac{1}{1+\frac{1}{2+\sqrt{3}-1}} \\ &= 1+\frac{1}{1+\frac{1}{2+\frac{1}{\frac{1}{\sqrt{3}-1}}}}\end{aligned}$$

This pattern of repeated (1, 2) should continue for ever. Hence, $\sqrt{3} = \left[1;\overline{1,2}\right]$. The first 3 rational fraction approximations are:

$$1+\frac{1}{1} = 2 \qquad 1+\frac{1}{1+\frac{1}{2}} \simeq 1.667 \qquad 1+\frac{1}{1+\frac{1}{2+\frac{1}{1}}} = 1.75$$

As we see, these approximations persistently converge towards $\sqrt{3} \simeq 1.7321$.
(**e**) We have:

$$\pi = 3+\pi-3 = 3+\frac{1}{\frac{1}{\pi-3}} = 3+\frac{1}{\frac{1}{0.141592\ldots}} = 3+\frac{1}{7.062513\ldots} = 3+\frac{1}{7+0.062513\ldots}$$

$$= 3+\cfrac{1}{7+\cfrac{1}{\cfrac{1}{0.062513\ldots}}} = 3+\cfrac{1}{7+\cfrac{1}{15.996594\ldots}} = 3+\cfrac{1}{7+\cfrac{1}{15+0.996594\ldots}}$$

$$= 3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{\cfrac{1}{0.996594\ldots}}}} = 3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1.003417231}}} = 3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+0.003417231}}}$$

$$= 3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{\cfrac{1}{0.003417231}}}}} = 3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{292+\ddots}}}}$$

Hence, $\pi = [3; 7, 15, 1, 292, \ldots]$. The first 3 rational fraction approximations are:

$$3+\frac{1}{7} \simeq 3.142857143 \qquad 3+\cfrac{1}{7+\cfrac{1}{15}} \simeq 3.141509434 \qquad 3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1}}} \simeq 3.14159292$$

As we see, these approximations persistently converge towards $\pi \simeq 3.141592654$.

1.2 Pell's Equation

In this section we introduce Pell's equation and how it is solved.[1] Pell's equation is a Diophantine quadratic equation in two variables of the following form:

$$x^2 - dy^2 = 1 \tag{1}$$

where x and y are non-zero integers (also see footnote [3]) and d is a positive non-square integer (noting that if d is a square integer then the equation has no solution because the difference between two non-zero squares cannot be 1). Pell's equation has infinitely many solutions. The method for finding these solutions is to find the fundamental solution (which is the minimal solution in $\mathbb{N}$), i.e. $x = x_1$ and $y = y_1$ where x_1 is the least natural number that solves (with the corresponding y, i.e. y_1) this equation.[2] All natural solutions are then generated by the formula:

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n \qquad (n \in \mathbb{N}) \tag{2}$$

All other solutions are then obtained by sign alteration noting that x and y are squared and hence each one can be negative as well as positive (i.e. we have 4 solutions for each natural solution).

It is important to note the following about Pell's equation:

- The existence of solution[3] of Pell's equation is guaranteed.

[1] This section is no more than an introduction to the subject of Pell's equation and the methods of its solution. This subject will be extended and elaborated gradually.

[2] The fundamental solution (x_1, y_1) may also be defined as the solution that minimizes $x_1 + y_1\sqrt{d}$ in comparison to any other solution. It is noteworthy that the fundamental solution is unique (and hence there should be no difference).

[3] We mean by "solution" the "non-trivial" solution noting that the "trivial" solution $(x, y) = (1, 0)$ always exists. This should explain why we imposed the condition that x and y are *non-zero* integers (i.e. to make this statement substantial and extra informative).

• Based on what we said, obtaining a solution to Pell's equation is essentially about (searching for and) finding the fundamental solution (noting that all the rest is usually trivial). So, how to obtain the fundamental solution? In simple cases we may find the fundamental solution by guess or by inspection, e.g. by searching by computer for the lowest (combination of) x and y in $\mathbb{N}$ that solve the given Pell equation. However, in more general circumstances (and more complicated cases) we may need a more regular and systematic technical approach for this search. The commonly-used such approach is the one based on the technique of continued fraction (noting that this approach generally works; see § 1.1). The essence of this method is to use the continued fraction expansion of $\sqrt{d}$ where we try successive rational fraction approximations on the continued fraction ladder until we find a solution to the given equation, i.e. the first found solution in this successive stepping down on the ladder is the fundamental solution.[4] This is based on the fact that if a_k/b_k $(k = 1, 2, \ldots)$ is the k^{th} rational fraction approximation of $\sqrt{d}$ on the continued fraction ladder of $\sqrt{d}$ then $x_1 = a_k$ and $y_1 = b_k$ for some k (i.e. the smallest k that satisfies $a_k^2 - db_k^2 = 1$). So, to find (x_1, y_1) we simply try $a_1/b_1, a_2/b_2, \ldots$ successively until we find the a_k/b_k that solves the given Pell equation (and hence $x_1 = a_k$ and $y_1 = b_k$). This issue will be clarified further (practically) in the following Problems.
• Pell's equation is generalized to the form $x^2 - dy^2 = c$ where $0 \neq 1 \neq c \in \mathbb{Z}$.[5] However, we will not investigate this issue in this volume (although we plan to investigate this, as well as other details about Pell's equation, more thoroughly in the future).
• General quadratic Diophantine equation in two variables may be transformed to Pell's equation form to be solved as a Pell equation (where the solution of the original equation is obtained by reversing the transformation). Some examples of this transformation technique will be given in the following Problems (as well as in the upcoming chapters; see for instance Problem 2 of § 5.2). However, it should be noticed that the existence of solution to the transformed Pell equation does not guarantee the existence of solution to the original equation (as will be seen in some of the upcoming Problems) because the reverse transformation may not produce integer solutions (totally or partially).
• Considering what we have said, although Pell's equation may seem very restrictive, it is possible (in many cases of quadratic Diophantine equation in two variables) to transform the equation to a standard Pell equation (by using algebraic manipulation and scaling) and hence solve it by the Pell's equation techniques (as will be shown in the future). Anyway, if it is not possible to transform it to a standard Pell equation then it is usually possible to transform it to a generalized Pell equation and hence it may become possible to solve it as a generalized Pell equation.[6]
• When tackling a Pell equation it is recommended to search for the fundamental solution by inspection before trying sophisticated processes and techniques like continued fraction technique. For example, a few-seconds inspection to the Pell equation $x^2 - 5y^2 = 1$ should lead to the fundamental solution $(x_1, y_1) = (9, 4)$ and hence to all other solutions using the aforementioned formulations and instructions. Also, basic computational effort (e.g. through the use of a spreadsheet or a simple code) can be more economic in the search for the fundamental solution.[7]

Problems

1. Put the following equations in a standard Pell equation form and determine if these equations have solutions or not:
   (**a**) $4x^2 - 6y^2 + 12x + 108y - 478 = 0$. (**b**) $9x^2 - 325y^2 - 42x - 130y + 35 = 0$.
   Solution:
   (**a**) We have:

[4] In fact, there are detailed rules about how to get the fundamental solution (and the other solutions). However, we do not want to get involved in these details at this stage and level.
[5] We should note that whether $0 \neq 1 \neq c \in \mathbb{Z}$ or $\mathbb{N} \ni c > 1$ seems to follow different conventions (noting that this may affect the method of solution in some cases).
[6] We should take note (in both cases) of the aforementioned possibility of having no solution by the reverse transformation (i.e. when the reverse transformation does not produce an integer solution).
[7] See the Pell.cpp code which is in the "Codes" directory (noting that this code is very simple and limited in applicability since it is only for the purpose of demonstration and illustration).

$(4x^2+12x)-(6y^2-108y)-478=0 \quad \rightarrow \quad (4x^2+12x+9)-(6y^2-108y)-478-9=0 \quad \rightarrow$

$(2x+3)^2-(6y^2-108y)-487=0 \quad \rightarrow \quad (2x+3)^2-(6y^2-108y+486)-1=0 \quad \rightarrow$

$(2x+3)^2-6(y^2-18y+81)-1=0 \quad \rightarrow \quad (2x+3)^2-6(y-9)^2=1$

As we see, the last equation is in a standard Pell equation form, i.e. $X^2-6Y^2=1$ where $X=2x+3$ and $Y=y-9$. Now, if we solve this Pell equation we can easily obtain the fundamental solution $(X,Y)=(5,2)$ as well as all other solutions such as $(X,Y)=(\pm5,\pm2)$ $(\pm49,\pm20)$ and $(\pm485,\pm198)$. We can also see that the reverse transformation $\big[$i.e. $x=(X-3)/2$ and $y=(Y+9)\big]$ produces integer solutions to the original equation, e.g. $(x,y)=(1,11)$, $(1,7)$, $(-4,7)$, $(-4,11)$, $(23,29)$, $(241,207)$, etc.
(**b**) We have:

$(9x^2-42x)-(325y^2+130y)+35=0 \quad \rightarrow \quad (9x^2-42x+49)-(325y^2+130y)+35-49=0 \quad \rightarrow$

$(3x-7)^2-(325y^2+130y)-14=0 \quad \rightarrow \quad (3x-7)^2-(325y^2+130y+13)-1=0 \quad \rightarrow$

$(3x-7)^2-13(25y^2+10y+1)=1 \quad \rightarrow \quad (3x-7)^2-13(5y+1)^2=1$

As we see, the last equation is in a standard Pell equation form, i.e. $X^2-13Y^2=1$ where $X=3x-7$ and $Y=5y+1$. Now, if we solve this Pell equation we can easily obtain the fundamental solution $(X,Y)=(649,180)$ as well as all other solutions (as described above). However, the original equation has no solution because the reverse transformation $\big[$i.e. $x=(X+7)/3$ and $y=(Y-1)/5\big]$ does not produce integer solutions.

2. Find the first 4 natural solutions of the following Pell equations:
(**a**) $x^2-2y^2=1$. (**b**) $x^2-3y^2=1$. (**c**) $x^2-17y^2=1$. (**d**) $x^2-7y^2=1$.
Solution:
(**a**) By inspection we can see that the fundamental solution is: $(x_1,y_1)=(3,2)$. Hence, the first 4 natural solutions are (see Eq. 2):
$(x_1,y_1)=(3,2)$ $(x_2,y_2)=(17,12)$ $(x_3,y_3)=(99,70)$ $(x_4,y_4)=(577,408)$
(**b**) By inspection we can see that the fundamental solution is: $(x_1,y_1)=(2,1)$. Hence, the first 4 natural solutions are:
$(x_1,y_1)=(2,1)$ $(x_2,y_2)=(7,4)$ $(x_3,y_3)=(26,15)$ $(x_4,y_4)=(97,56)$
(**c**) We have $\sqrt{17}=\big[4;\overline{8}\big]$. The first rational fraction approximation on the continued fraction ladder of $\sqrt{17}$ is:

$$4+\frac{1}{8}=\frac{33}{8}$$

Now, $33^2-17\times8^2=1$ and thus $(x_1,y_1)=(33,8)$. Hence, the first 4 natural solutions are:
$(x_1,y_1)=(33,8)$ $(x_2,y_2)=(2177,528)$ $(x_3,y_3)=(143649,34840)$ $(x_4,y_4)=(9478657,2298912)$
(**d**) We have $\sqrt{7}=\big[2;\overline{1,1,1,4}\big]$. The first 4 rational fraction approximations on the continued fraction ladder of $\sqrt{7}$ are:[8]

$$[2;1]=\frac{3}{1} \qquad [2;1,1]=\frac{5}{2} \qquad [2;1,1,1]=\frac{8}{3} \qquad [2;1,1,1,4]=\frac{37}{14}$$

The first approximation that satisfies the given equation is the third (since $8^2-7\times3^2=1$) and thus $(x_1,y_1)=(8,3)$. Hence, the first 4 natural solutions are:
$(x_1,y_1)=(8,3)$ $(x_2,y_2)=(127,48)$ $(x_3,y_3)=(2024,765)$ $(x_4,y_4)=(32257,12192)$

3. Show that there are infinitely many triangular numbers (i.e. numbers of the form $\frac{n^2+n}{2}$ where $n\in\mathbb{N}$) which are perfect squares.
Solution: For a triangular number to be a perfect square we must have $\frac{n^2+n}{2}=m^2$ where $m\in\mathbb{N}$), i.e.

[8] We use $[2;1]$ to represent $2+\frac{1}{1}$ (i.e. the first rational fraction approximation on the continued fraction ladder of $\sqrt{7}$). The similar symbols (such as $[\overline{2};1,1]$) have similar interpretation.

$n^2+n-2m^2=0$. This is a quadratic equation in n and hence it has a solution if its discriminant Δ is a perfect square, i.e.

$$\Delta=1^2-4(-2m^2)=k^2 \qquad \rightarrow \qquad k^2-8m^2=1 \qquad (k\in\mathbb{N})$$

As we see, the latter equation is a Pell equation and hence it has infinitely many solutions, e.g. $(k,m)=(3,1),\ (17,6),\ (99,35),\ (577,204)$ corresponding to $n=1,8,49,288$ (and hence to triangular square numbers 1, 36, 1225, 41616). Accordingly, there are infinitely many triangular numbers which are perfect squares.

1.3 The Order of Integer

The order of an integer n (modulo k) is the least positive integer m such that $n^m \overset{k}{=} 1$ (where n and k are coprime).[9] We symbolize this by writing: $O_k n=m$. For example:

- $2^{1,2,3,4,\ldots} \overset{3}{=} 2,1,2,1,\ldots$ and hence the order of 2 (modulo 3) is 2, i.e. $O_3 2=2$.
- $5^{1,2,3,4,5,6,7,\ldots} \overset{9}{=} 5,7,8,4,2,1,5,\ldots$ and hence the order of 5 (modulo 9) is 6, i.e. $O_9 5=6$.
- $7^{1,2,3,\ldots,16,17,\ldots} \overset{17}{=} 7,15,3,\ldots,1,7,\ldots$ and hence the order of 7 (modulo 17) is 16, i.e. $O_{17}7=16$.

It is important to note the following points about the order of an integer:

1. $n^b \overset{k}{=} 1$ *iff* $O_k n|b$ ((where n and k are coprime and $b\in\mathbb{N}^0$).
2. $n^a \overset{k}{=} n^b$ *iff* $a \overset{O_k n}{=} b$ (where n and k are coprime and $a,b\in\mathbb{N}^0$).

Problems

1. Show that $n^b \overset{k}{=} 1$ *iff* $O_k n|b$ (where n and k are coprime and $b\in\mathbb{N}^0$).
   Solution: Regarding **the if part**, if $O_k n|b$ then $b=aO_k n$ (for some $a\in\mathbb{N}^0$) and hence:

$$n^b=n^{aO_k n}=\left(n^{O_k n}\right)^a \overset{k}{=} 1^a=1$$

   Regarding **the only if part**, if $n^b \overset{k}{=} 1$ where $O_k n\not| b$ then $b=aO_k n+r$ where $a\in\mathbb{N}^0$ and $0<r<O_k n$. Therefore, we must have:

$$1\overset{k}{=} n^b=n^{aO_k n+r}=\left(n^{O_k n}\right)^a\times n^r \overset{k}{=} 1^a\times n^r=n^r$$

   i.e. $n^r \overset{k}{=} 1$ which is a contradiction because $0<r<O_k n$ while $O_k n$ is supposed to be the least positive integer such that $n^{O_k n} \overset{k}{=} 1$.
2. Show that $n^a \overset{k}{=} n^b$ *iff* $a \overset{O_k n}{=} b$ (where n and k are coprime and $a,b\in\mathbb{N}^0$).
   Solution: Let us assume (with no loss of generality) that $a\geq b$.
   Regarding **the if part**, if $a \overset{O_k n}{=} b$ then $a=sO_k n+b$ (for some $s\in\mathbb{N}^0$) and hence:

$$n^a=n^{sO_k n+b}=\left(n^{O_k n}\right)^s\times n^b \overset{k}{=} 1^s\times n^b=n^b$$

   Regarding **the only if part**, if $n^a \overset{k}{=} n^b$ then we have:

$$n^a \overset{k}{=} n^b \qquad \rightarrow \qquad n^{a-b}n^b \overset{k}{=} n^b \qquad \rightarrow \qquad n^{a-b} \overset{k}{=} 1$$

   where canceling n^b in the last step is because n^b and k are coprime since n and k are coprime (see part n of Problem 1 of 2.2 of V1, as well as point 7 in the preamble of § 2.7 of V1). Now, from Problem 1 we conclude that $O_k n|(a-b)$, i.e. $a \overset{O_k n}{=} b$.

[9] The "order of an integer" is actually the *multiplicative* order (which should remind those with knowledge of group theory of the order in the multiplicative group). However, for simplicity (and because we have no rival or competitor so far on this terminology) we label this as the "order of an integer".

3. Show that $O_k n|\phi(k)$ (where n and k are coprime).

   Solution: According to Euler's theorem we have $n^{\phi(k)} \overset{k}{=} 1$. Hence, from Problem 1 we conclude that $O_k n|\phi(k)$.
4. Show that if $O_k n = a$ then $O_k n^b = a/g$ where $b \in \mathbb{N}$ and $g = \gcd(a, b)$.

   Solution: Let $c \equiv O_k n^b$. We have $a = g\alpha$ and $b = g\beta$ (noting that α and β are coprime) and hence:

$$\left(n^b\right)^\alpha = \left(n^{g\beta}\right)^{a/g} = \left(n^\beta\right)^a = (n^a)^\beta \overset{k}{=} 1^\beta = 1$$

   where step 4 is because $a = O_k n$. So, from Problem 1 we have $O_k n^b|\alpha$, i.e. $c|\alpha$.

   Also, from the definition of $O_k n^b$ we have: $\left(n^b\right)^c = n^{bc} \overset{k}{=} 1$ and hence from Problem 1 we have $a|(bc)$, i.e. $(g\alpha)|(g\beta c)$ or $\alpha|(\beta c)$. Now, since α and β are coprime then $\alpha|c$.

   So, $c|\alpha$ and $\alpha|c$ and hence $c = \alpha$ (noting that c and α are positive), that is:

$$O_k n^b \equiv c = \alpha = \frac{a}{g}$$

   Note: based on this proposition we have:

$$O_{11}5^7 = \frac{O_{11}5}{\gcd(O_{11}5, 7)} = \frac{5}{\gcd(5, 7)} = \frac{5}{1} = 5 \qquad O_7 9^6 = \frac{O_7 9}{\gcd(O_7 9, 6)} = \frac{3}{\gcd(3, 6)} = \frac{3}{3} = 1$$

5. Show that if $O_k n = ab$ then $O_k n^b = a$.

   Solution: From Problem 4 we have:

$$O_k n^b = \frac{O_k n}{\gcd(O_k n, b)} = \frac{ab}{\gcd(ab, b)} = \frac{ab}{b\gcd(a, 1)} = a$$

6. Show that if $O_p n = 2b$ then $n^b \overset{p}{=} -1$ (where p is an odd prime).

   Solution: According to Problem 5 (noting that we have $O_p n = 2b$), $O_p n^b = 2$. This means that $\left(n^b\right)^2 \overset{p}{=} 1$ whose solutions are $n^b \overset{p}{=} \pm 1$. However, since $O_p n^b = 2$ then we must have $n^b \overset{p}{=} -1$.
7. Find the following:

   (**a**) $O_{1775}13$. (**b**) $O_{23156}41$.

   Solution:

   (**a**) According to Problem 3, $O_{1775}13|\phi(1775)$. Now, $\phi(1775) = 1400$ whose divisors are 1, 2, 4, 5, 7, 8, 10, 14, 20, 25, 28, 35, 40, 50, 56, 70, 100, 140, 175, 200, 280, 350, 700, 1400. On trying these divisors (in their increasing order) we find that 140 is the first integer t in this list (according to the increasing order) that makes $13^t \overset{1775}{=} 1$. Hence, $O_{1775}13 = 140$.

   (**b**) According to Problem 3, $O_{23156}41|\phi(23156)$. Now, $\phi(23156) = 9912$ whose divisors are 1, 2, 3, 4, 6, 7, 8, 12, 14, 21, 24, 28, 42, 56, 59, 84, 118, 168, 177, 236, 354, 413, 472, 708, 826, 1239, 1416, 1652, 2478, 3304, 4956, 9912. On trying these divisors (in their increasing order) we find that 826 is the first integer t in this list (according to the increasing order) that makes $41^t \overset{23156}{=} 1$. Hence, $O_{23156}41 = 826$.
8. Find an integer x such that:

   (**a**) $O_{13}x^5 = 4$. (**b**) $O_9 14^x = 6$.

   Solution: We use the proposition of Problem 4.

   (**a**) For example, $x = 5$ should do because:

$$O_{13}x^5 = \frac{O_{13}x}{\gcd(O_{13}x, 5)} = \frac{O_{13}5}{\gcd(O_{13}5, 5)} = \frac{4}{\gcd(4, 5)} = \frac{4}{1} = 4$$

   (**b**) Any x that is coprime to 6 should do because:

$$O_9 14^x = \frac{O_9 14}{\gcd(O_9 14, x)} = \frac{6}{\gcd(6, x)} = \frac{6}{1} = 6$$

9. Show that $O_k n = O_k n^*$ where n^* is the modular multiplicative inverse of n modulo k (assuming n has a modular inverse).
Solution: If $\rho \equiv O_k n$ then we have:

$$1 = 1^\rho \overset{k}{=} (nn^*)^\rho = n^\rho (n^*)^\rho \overset{k}{=} 1 \times (n^*)^\rho = (n^*)^\rho$$

Hence, from Problem 1 we get $O_k n^* | \rho$ and hence $O_k n^* \leq \rho$, i.e. $O_k n^* \leq O_k n$. Now, noting that modular multiplicative inversion is a symmetric relation (see point 5 in the preamble of § 2.7.1 of V1) we must also have $O_k n \leq O_k n^*$. Hence, $O_k n = O_k n^*$.

10. Let n_1, n_2 be integers which are coprime to $k \in \mathbb{N}$. Show that $O_k(n_1 n_2) \big| (O_k n_1 \times O_k n_2)$. Moreover, if $O_k n_1$ and $O_k n_2$ are relatively prime then $O_k(n_1 n_2) = O_k n_1 \times O_k n_2$.
Solution: Let $a \equiv O_k n_1$, $b \equiv O_k n_2$ and $c \equiv O_k(n_1 n_2)$. Now:

$$(n_1 n_2)^{ab} = n_1^{ab}\, n_2^{ab} = (n_1^a)^b \left(n_2^b\right)^a \overset{k}{=} 1^b\, 1^a = 1$$

Hence, from Problem 1 we get $c|(ab)$, i.e. $O_k(n_1 n_2) \big| (O_k n_1 \times O_k n_2)$.
Now, let assume that $O_k n_1$ and $O_k n_2$ are relatively prime. We have:

$$1 \overset{k}{=} (n_1 n_2)^c = n_1^c\, n_2^c \qquad \rightarrow \qquad 1^a \overset{k}{=} (n_1^c\, n_2^c)^a = (n_1^a)^c\, n_2^{ac} = n_2^{ac}$$

Hence, from Problem 1 we get $b|(ac)$ and thus $b|c$ (noting that we are assuming now that a and b are relatively prime).
We can similarly show that $a|c$ (noting that this can also be deduced from the symmetry).
Now, since $a|c$ and $b|c$ then $(ab)|c$ because a and b are relatively prime (see point 20 in the preamble of § 1.9 of V1).
So in brief, $c|(ab)$ and $(ab)|c$ and hence $c = ab$ (noting that $a, b, c > 0$), i.e. if $O_k n_1$ and $O_k n_2$ are relatively prime then $O_k(n_1 n_2) = O_k n_1 \times O_k n_2$.

11. Show that if $O_k n = (k-1)$ then k is prime (where $\mathbb{N} \ni k > 1$).
Solution: According to Problem 3 we have $(k-1)|\phi(k)$ which implies $(k-1) \leq \phi(k)$. However, for all $k > 1$ we have $\phi(k) \leq (k-1)$ (see point 7 in the preamble of § 2.6.4 of V1). Hence, $\phi(k) = (k-1)$, i.e. k is prime (see Problem 7 of § 10).

1.4 Primitive Root

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 $n \overset{k}{=} r^s$ for some $s \in \mathbb{N}$ with n and k being coprime. For example:

• 3 and 5 are primitive roots (modulo 7) because the numbers coprime to 7 are $n \overset{7}{=} 1, 2, 3, 4, 5, 6$ and we have:

$3^6 \overset{7}{=} 1$ $\quad 3^2 \overset{7}{=} 2$ $\quad 3^1 \overset{7}{=} 3$ $\quad 3^4 \overset{7}{=} 4$ $\quad 3^5 \overset{7}{=} 5$ $\quad 3^3 \overset{7}{=} 6$

$5^6 \overset{7}{=} 1$ $\quad 5^4 \overset{7}{=} 2$ $\quad 5^5 \overset{7}{=} 3$ $\quad 5^2 \overset{7}{=} 4$ $\quad 5^1 \overset{7}{=} 5$ $\quad 5^3 \overset{7}{=} 6$

but $1, 2, 4, 6$ are not primitive roots (modulo 7) because (for instance):

$$1^s \overset{7}{\neq} 2 \qquad 2^s \overset{7}{\neq} 3 \qquad 4^s \overset{7}{\neq} 3 \qquad 6^s \overset{7}{\neq} 2$$

for any s.

• 8 has no primitive root because the numbers coprime to 8 are $n \overset{8}{=} 1, 3, 5, 7$ and we have (for instance):

$$1^s \overset{8}{\neq} 3 \qquad 3^s \overset{8}{\neq} 5 \qquad 5^s \overset{8}{\neq} 3 \qquad 7^s \overset{8}{\neq} 3$$

for any s.

It is important to note the following points about primitive roots:

1. We may also define primitive root (modulo k) as an element in a reduced residue system (modulo k) whose natural powers generate all the elements in the system. It is worth noting that S_{rk} (i.e. reduced

residue system modulo k) is a group under modular multiplication (modulo k). So, primitive root is an element in S_{rk} whose order (or period; see § 1.3) is $\phi(k)$ and hence the sequence of its natural powers generates all the elements in S_{rk}. So, we can say: $\rho \in S_{rk}$ is a primitive root *iff* the order of ρ is equal to $\phi(k)$, i.e. $O_k\rho = \phi(k)$.[10]

2. Based on what have been said, when k has a primitive root (say ρ) then S_{rk} can be written as: $S_{rk} = \{\rho^1, \rho^2, \ldots, \rho^{\phi(k)}\}$.[11] Accordingly, multiplication of two elements of S_{rk} in modulo k will become addition of their indices in modulo $\phi(k)$.
3. As seen above, some (modular) integers (like 8) have no primitive root. In brief, only the following (modular) integers have primitive roots: 2, 4, p^a and $2p^a$ (where p is an odd prime and $a \in \mathbb{N}$). This issue will be investigated further in the future.
4. Referring to the proposition of Problem 4 of § 1.3 (as well as point 1 above), if ρ is a primitive root (modulo k) then we have:
$$O_k\rho^b = \frac{O_k\rho}{\gcd\left(O_k\rho, b\right)} = \frac{\phi(k)}{\gcd\left[\phi(k), b\right]}$$
This means that ρ^b is a primitive root (modulo k) *iff* $\gcd\left[\phi(k), b\right] = 1$.
5. Every prime has at least one primitive root.

Problems

1. Referring to point 1 in the preamble, find the order of all the elements of S_{r12} (i.e. the reduced residue system modulo 12) and hence determine the primitive roots of 12.
Solution: $S_{r12} = \{1, 5, 7, 11\}$ and hence $\phi(12) = 4$. We have:
   - $1^{1,2,\ldots} \overset{12}{=} 1, 1, \ldots$ and hence the order of 1 is 1.
   - $5^{1,2,\ldots} \overset{12}{=} 5, 1, \ldots$ and hence the order of 5 is 2.
   - $7^{1,2,\ldots} \overset{12}{=} 7, 1, \ldots$ and hence the order of 7 is 2.
   - $11^{1,2,\ldots} \overset{12}{=} 11, 1, \ldots$ and hence the order of 11 is 2.

   Therefore, 12 has no primitive root.
2. Repeat Problem 1 for S_{r9}.
Solution: $S_{r9} = \{1, 2, 4, 5, 7, 8\}$ and hence $\phi(9) = 6$. We have:
   - $1^{1,2,\ldots} \overset{9}{=} 1, 1, \ldots$ and hence the order of 1 is 1.
   - $2^{1,2,3,4,5,6,\ldots} \overset{9}{=} 2, 4, 8, 7, 5, 1, \ldots$ and hence the order of 2 is 6.
   - $4^{1,2,3,\ldots} \overset{9}{=} 4, 7, 1, \ldots$ and hence the order of 4 is 3.
   - $5^{1,2,3,4,5,6,\ldots} \overset{9}{=} 5, 7, 8, 4, 2, 1, \ldots$ and hence the order of 5 is 6.
   - $7^{1,2,3,\ldots} \overset{9}{=} 7, 4, 1, \ldots$ and hence the order of 7 is 3.
   - $8^{1,2,\ldots} \overset{9}{=} 8, 1, \ldots$ and hence the order of 8 is 2.

   Therefore, the primitive roots of 9 are 2 and 5.
3. Repeat Problem 1 for S_{r5}.
Solution: $S_{r5} = \{1, 2, 3, 4\}$ and hence $\phi(5) = 4$. We have:
   - $1^{1,2,\ldots} \overset{5}{=} 1, 1, \ldots$ and hence the order of 1 is 1.
   - $2^{1,2,3,4,\ldots} \overset{5}{=} 2, 4, 3, 1, \ldots$ and hence the order of 2 is 4.
   - $3^{1,2,3,4,\ldots} \overset{5}{=} 3, 4, 2, 1, \ldots$ and hence the order of 3 is 4.
   - $4^{1,2,\ldots} \overset{5}{=} 4, 1, \ldots$ and hence the order of 4 is 2.

   Therefore, the primitive roots of 5 are 2 and 3.
4. Show that if r is a primitive root of p (where p is an odd prime) then $r^{(p-1)/2} \overset{p}{=} -1$.
Solution: From Fermat's little theorem we have:
$$r^{p-1} \overset{p}{=} 1 \quad \rightarrow \quad r^{p-1} - 1 \overset{p}{=} 0 \quad \rightarrow \quad (r^{(p-1)/2} - 1)(r^{(p-1)/2} + 1) \overset{p}{=} 0$$

[10] More rigorously and generally, $O_k n = \phi(k)$ *iff* n is a primitive root modulo k (where n and k are coprime). In fact, this may be used as a definition for "primitive root".

[11] It is useful to note that $\rho^{\phi(k)} \overset{k}{=} 1$ according to Euler's theorem (which can be regarded, in this context, as a definition of primitive root taking into account other related concepts and definitions as well as the restriction on the order of ρ).

where the factorization in the last step is because $(p-1)$ is even. Now, $r^{(p-1)/2}-1 \overset{p}{\neq} 0$ because r is supposedly a primitive root (noting that $r^{(p-1)/2}-1 \overset{p}{=} 0$ which implies $r^{(p-1)/2} \overset{p}{=} 1$ means that the order of r is less than $p-1$ in contradiction to being a primitive root). Hence, $r^{(p-1)/2}+1 \overset{p}{=} 0$, i.e. $r^{(p-1)/2} \overset{p}{=} -1$.

5. Show that if k has a primitive root then it must have $\phi\big[\phi(k)\big]$ distinct primitive roots.
Solution: $\{\rho^1, \rho^2, \ldots, \rho^{\phi(k)}\}$ is a reduced residue system (modulo k) when ρ is a primitive root of k (see points 1 and 2 in the preamble). So, when we say "k has a primitive root" we are assuming that we have an element ρ in the reduced residue system whose powers $\big[$i.e. $\rho^1, \rho^2, \ldots, \rho^{\phi(k)}\big]$ generate all the elements in this system. Accordingly, any primitive root of k (i.e. any element that generates the entire system) must be among these ρ^i $\big[i = 1, 2, \ldots, \phi(k)\big]$ because these ρ^i represent the entire system. Now, from point 4 in the preamble ρ^b is a primitive root (modulo k) *iff* $\gcd\big[\phi(k), b\big] = 1$, i.e. $\phi(k)$ and b are coprime. The number of positive integers b $\big[\leq \phi(k)\big]$ which are coprime to $\phi(k)$ is $\phi\big[\phi(k)\big]$ and hence the number of primitive roots among these distinct elements $\big[$i.e. $\rho^1, \rho^2, \ldots, \rho^{\phi(k)}\big]$ must be $\phi\big[\phi(k)\big]$.
Note: referring to Problems 2 and 3, we have:

$$\phi\big[\phi(9)\big] = \phi\big[6\big] = 2 \qquad \text{and} \qquad \phi\big[\phi(5)\big] = \phi\big[4\big] = 2$$

This should serve as a simple check that we did not make a gross mistake.

6. How many primitive roots the following numbers have:
(**a**) 113. (**b**) 254. (**c**) 311.
Solution: All these numbers have a primitive root (noting that 113 and 311 are primes while 254 is 2 times a prime; see point 3 in the preamble) and hence we can use the proposition of Problem 5.
(**a**) $\phi\big[\phi(113)\big] = \phi\big[112\big] = 48$ and hence 113 has 48 primitive roots.
(**b**) $\phi\big[\phi(254)\big] = \phi\big[126\big] = 36$ and hence 254 has 36 primitive roots.
(**c**) $\phi\big[\phi(311)\big] = \phi\big[310\big] = 120$ and hence 311 has 120 primitive roots.

7. Show that the product of two distinct primitive roots (modulo an odd prime) is not a primitive root (of that prime).
Solution: Let r and ρ be two distinct primitive roots modulo p (where p is an odd prime). Now, from Problem 4 we have:

$$r^{(p-1)/2} \overset{p}{=} -1 \quad \text{and} \quad \rho^{(p-1)/2} \overset{p}{=} -1 \qquad \rightarrow \qquad (r\rho)^{(p-1)/2} \overset{p}{=} 1$$

Hence, $r\rho$ cannot be a primitive root of p because its order is less than $p-1$.

8. Determine the number of primitive roots of all $\mathbb{N} \ni k > 1$.
Solution: Referring to point 3 in the preamble (as well as Problem 5):
- 2 has $\phi\big[\phi(2)\big] = \phi\big[1\big] = 1$ primitive root (which is 1).
- 4 has $\phi\big[\phi(4)\big] = \phi\big[2\big] = 1$ primitive root (which is 3).
- p^a has $\phi\big[\phi(p^a)\big] = \phi\big[p^a - p^{a-1}\big]$ primitive roots.
- $2p^a$ has $\phi\big[\phi(2p^a)\big] = \phi\big[\phi(p^a)\big] = \phi\big[p^a - p^{a-1}\big]$ primitive roots (see part a of Problem 13 of § 10).
- All other k have no primitive root.

9. Show that if r is a primitive root (modulo k) then its modular multiplicative inverse r^* is also a primitive root (modulo k).
Solution: According to Problem 9 of § 1.3, r and r^* have the same order (modulo k) and hence if r is a primitive root then r^* must also be a primitive root.

10. Show that if r is a primitive root of k then $-r$ is not necessarily a primitive root of k.
Solution: For example, $r = 2$ is a primitive root of $k = 9$ while $r = -2$ is not a primitive root of $k = 9$. On the other hand, both $r = 2$ and $r = -2$ are primitive roots of $k = 5$.

11. Show that if r is a primitive root of a prime $p = 4k+1$ ($k \in \mathbb{N}$) then $-r$ is also a primitive root of p.
Solution: We have:

$$(-r)^{p-1} = r^{p-1} = r^{\phi(p)} \overset{p}{=} 1$$

where the last step is from Euler's theorem (noting that r is a primitive root of p and hence they are coprime). So, from Problem 3 of § 1.3 we have $O_p(-r) | (p-1)$, i.e. $O_p(-r) \leq (p-1)$. Now, if $O_p(-r) < (p-1)$ then we have two cases to consider:

• $O_p(-r)$ is even $\big[$say $O_p(-r) = 2a$ for some $a \in \mathbb{N}\big]$ and hence:

$$(-r)^{2a} \stackrel{p}{=} 1 \qquad \rightarrow \qquad r^{2a} \stackrel{p}{=} 1$$

which means that the order of r is less than $(p-1)$ in contradiction to the presumption that r is a primitive root.

• $O_p(-r)$ is odd $\big[$say $O_p(-r) = 2a-1$ for some $a \in \mathbb{N}\big]$ and hence:

$$(-r)^{2a-1} \stackrel{p}{=} 1 \qquad \rightarrow \qquad r^{2(2a-1)} \stackrel{p}{=} 1$$

So, from Problem 1 of § 1.3 we have:

$O_p r \big| \big[2(2a-1)\big] \quad \rightarrow \quad (p-1) \big| \big[2(2a-1)\big] \quad \rightarrow \quad (4k) \big| \big[2(2a-1)\big] \quad \rightarrow \quad (2k)|(2a-1)$

However, this is impossible because $2k$ is even while $(2a-1)$ is odd (noting that no odd number is divisible by an even number).

So, it is not possible to have $O_p(-r) < (p-1)$ and hence we must have $O_p(-r) = (p-1)$, i.e. $-r$ is also a primitive root of p.

12. Find all the primitive roots of the following moduli:

(**a**) 22. (**b**) 49. (**c**) 17932.

Solution:

(**a**) $22 = 2 \times 11$ and hence it should have primitive roots (see point 3 in the preamble). The number of these primitive roots is: $\phi\big[11^1 - 11^0\big] = \phi(10) = 4$ (see Problem 8). Now, if we test the natural numbers > 1 which are coprime to 22 (i.e. $3, 5, 7, 9, 13, 15, 17, 19, 21$) we will find out that only $7, 13, 17, 19$ have order (mod 22) of $\phi(22) = 10$. Accordingly, $7, 13, 17, 19$ are the primitive roots of 22.

(**b**) $49 = 7^2$ and hence it should have primitive roots (see point 3 in the preamble). The number of these primitive roots is: $\phi\big[7^2 - 7^1\big] = \phi(42) = 12$ (see Problem 8). Now, if we test the natural numbers > 1 which are coprime to 49 we will find out that only $3, 5, 10, 12, 17, 24, 26, 33, 38, 40, 45, 47$ have order (mod 49) of $\phi(49) = 42$. Accordingly, $3, 5, 10, 12, 17, 24, 26, 33, 38, 40, 45, 47$ are the primitive roots of 49.

(**c**) $17932 = 2^2 \times 4483$ and hence it has no primitive root (see point 3 in the preamble).

13. Find all integers n such that $O_{31} n = 5$.

Solution: The smallest primitive root of modulo 31 is 3 and hence $O_{31} 3 = \phi(31) = 30$ (see point 1 in the preamble). We also note that since 3 is a primitive root then any integer (coprime to 31) can be expressed as $3^a \pmod{31}$ for some $a \in \{1, 2, \ldots, 30\}$. So, let $n \stackrel{31}{=} 3^a$ and hence we are looking for all values of a such that $O_{31} 3^a = 5$. Now, from Problem 4 of § 1.3 we have:

$$O_{31} 3^a = \frac{O_{31} 3}{\gcd\left(O_{31} 3, a\right)} = \frac{30}{\gcd\left(30, a\right)}$$

So, to find all values of a such that $O_{31} 3^a = 5$ we need to find all values of a such that $\gcd(30, a) = 6$. Now, $\gcd(30, a) = 6$ (among the integers $a \in \{1, 2, \ldots, 30\}$) are $6, 12, 18, 24$. Accordingly, $O_{31} n = 5$ for $3^6, 3^{12}, 3^{18}, 3^{24} \stackrel{31}{=} 16, 8, 4, 2$. So, $O_{31} n = 5$ for all $n \stackrel{31}{=} 2, 4, 8, 16$.

14. Show that 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).

Solution: Based on the given assumptions we have:

• $n \stackrel{p}{=} \pm 1$ cannot be primitive roots of p (because their order is 1 and 2 while the order of a primitive root must be $p-1$ which is ≥ 4). Hence, any primitive root r must be in the range $1 < r < (p-1) \pmod{p}$.

• From part (f) of Problem 2 of § 2.7.1 of V1, the multiplicative inverse of any $1 < r < (p-1)$ must be incongruent to r (i.e. $r \stackrel{p}{\neq} r^*$).

• From part (h) of Problem 2 of § 2.7.1 of V1, each member of the set $S = \{1, 2, \ldots, (p-1)\}$ must have a multiplicative inverse in S (modulo p) noting that S contains an even number of elements.

• From Problem 9, the multiplicative inverse r^* of any primitive root r is also a primitive root.

Accordingly, each primitive root (mod p) must have an incongruent multiplicative inverse which is also a primitive root, i.e. the primitive roots of p occur in incongruent pairs (r, r^*).

Note: a simpler proof (though it may be less rigorous and illuminating) is to note that (where we use Fermat's little theorem):

$$r^{p-1} \overset{p}{=} 1 \qquad \rightarrow \qquad r^a\, r^{p-1-a} \overset{p}{=} 1 \qquad \left(a = 1, \ldots, \tfrac{p-3}{2}\right)$$

Now, r^a and r^{p-1-a} are obviously incongruent modular multiplicative inverses (within some of the above conditions). So, if r^a is a primitive root then (by Problem 9) r^{p-1-a} is also a primitive root. Similarly, if r^{p-1-a} is a primitive root then r^a is also a primitive root. Hence, primitive roots occur in incongruent pairs.

15. Let p be a prime ≥ 5. Show that the product of all the primitive roots of p is congruent to 1 (mod p).
Solution: According to Problem 14, the primitive roots of p occur in incongruent pairs (r, r^*) where r^* is the modular multiplicative inverse of r. Now, the product of each pair is congruent to 1 (mod p), i.e. $rr^* \overset{p}{=} 1$. Hence, the product of all the primitive roots of p is congruent to 1 (mod p).

1.5 The Index of Integer

The index of an integer n (modulo k) relative to a primitive root r of k (where n and k are coprime) is the least positive integer m such that $n \overset{k}{=} r^m$. We symbolize this by writing: $I_{k,r}n = m$. For example:

- 3 is a primitive root (modulo 7) and 2 is the least positive integer such that $9 \overset{7}{=} 3^2$. Hence, $I_{7,3}9 = 2$.
- 2 is a primitive root (modulo 11) and 6 is the least positive integer such that $20 \overset{11}{=} 2^6$. Hence, $I_{11,2}20 = 6$.

It is important to note the following rules about the index of integer:

1. $I_{k,r}r = 1$.
2. $I_{k,r}1 = O_k r = \phi(k)$.
3. $I_{k,r}(ab) \overset{\phi(k)}{=} I_{k,r}(a) + I_{k,r}(b)$ (where a and b are coprime to k).
4. $I_{k,r}(a^b) \overset{\phi(k)}{=} b\, I_{k,r}(a)$.
5. $I_{p,r}(-1) = I_{p,r}(p-1) = \frac{p-1}{2}$ (where p is an odd prime).

These rules (which are similar to the rules of logarithms) can be exploited to solve congruence equations as will be demonstrated in the following Problems. However, we should notice the limitation of this method for solving congruence equations since it depends on the existence of a primitive root to the modulo k.

Problems

1. Solve the following congruence equations using the rules of indices:

(**a**) $8x^9 \overset{53}{=} 17$. (**b**) $6x^{25} \overset{49}{=} 22$. (**c**) $9x^4 \overset{17}{=} 32$.

Solution:[12]

(**a**) A primitive root of 53 is 2 and we have [noting that $\phi(53) = 52$]:

$$8x^9 \overset{53}{=} 17 \rightarrow I_{53,2}\left(8x^9\right) \overset{\phi(53)}{=} I_{53,2}(17) \rightarrow I_{53,2}(8) + 9I_{53,2}(x) \overset{52}{=} I_{53,2}(17) \rightarrow$$
$$3 + 9I_{53,2}(x) \overset{52}{=} 10 \rightarrow 9I_{53,2}(x) \overset{52}{=} 7 \rightarrow I_{53,2}(x) \overset{52}{=} 9^* \times 7 \overset{52}{=} 29 \times 7 \overset{52}{=} 47$$

So, $I_{53,2}(x) \overset{52}{=} 47$ [i.e. $I_{53,2}(x) \overset{\phi(53)}{=} 47$] which means $x \overset{53}{=} 2^{47} \overset{53}{=} 5$. Hence, the solution of the given congruence equation is $x \overset{53}{=} 5$.

(**b**) A primitive root of 49 is 3 and we have [noting that $\phi(49) = 42$]:

$$6x^{25} \overset{49}{=} 22 \rightarrow I_{49,3}\left(6x^{25}\right) \overset{\phi(49)}{=} I_{49,3}(22). \rightarrow I_{49,3}(6) + 25I_{49,3}(x) \overset{42}{=} I_{49,3}(22) \rightarrow$$
$$27 + 25I_{49,3}(x) \overset{42}{=} 24 \rightarrow 25I_{49,3}(x) \overset{42}{=} 39 \rightarrow I_{49,3}(x) \overset{42}{=} 25^* \times 39 \overset{42}{=} 15$$

So, $I_{49,3}(x) \overset{42}{=} 15$ [i.e. $I_{49,3}(x) \overset{\phi(49)}{=} 15$] which means $x \overset{49}{=} 3^{15} \overset{49}{=} 41$. Hence, the solution of the given congruence equation is $x \overset{49}{=} 41$.

[12] The IndexOfInt.cpp code (see Problem 1 of § 18.1) can be used to calculate the indices of integers [e.g. $I_{53,2}(17)$] in this Problem.

(**c**) A primitive root of 17 is 3 and we have $\big[$noting that $\phi(17)=16\big]$:

$9x^4 \overset{17}{=} 32 \quad \rightarrow \quad I_{17,3}\left(9x^4\right) \overset{\phi(17)}{=} I_{17,3}(32). \quad \rightarrow \quad I_{17,3}(9)+4I_{17,3}(x) \overset{16}{=} I_{17,3}(32) \quad \rightarrow$

$2+4I_{17,3}(x) \overset{16}{=} 6 \quad \rightarrow \quad 4I_{17,3}(x) \overset{16}{=} 4 \quad \rightarrow \quad I_{17,3}(x) \overset{4}{=} 1$

So, $I_{17,3}(x) \overset{16}{=} 1,5,9,13$ $\big[$i.e. $I_{17,3}(x) \overset{\phi(17)}{=} 1,5,9,13\big]$ which means $x \overset{17}{=} 3^1, 3^5, 3^9, 3^{13} \overset{17}{=} 3,5,14,12$. Hence, the solutions of the given congruence equation are $x \overset{17}{=} 3,5,12,14$.

1.6 Quadratic Residue

We say $n \in \mathbb{Z}$ is a *quadratic residue* (modulo k) if n and k are coprime and the congruence equation $x^2 \overset{k}{=} n$ has a solution. If this congruence has no solution then n is a *quadratic non-residue* (mod k). For example, 4 is a quadratic residue (mod 3) since $x^2 \overset{3}{=} 4$ has a solution (e.g. $x \overset{3}{=} 1$), while 2 is a quadratic non-residue (mod 3) because $x^2 \overset{3}{=} 2$ has no solution.

It is important to note that some authors impose the condition of coprimality (i.e. n and k should be coprime) while others do not. Also, some authors seem to restrict the definition of quadratic residue to prime moduli (i.e. $k \equiv p$ where $p \in \mathbb{P}$) and hence the purpose of the condition of coprimality is to exclude 0 (mod p) which makes the number of quadratic residues and quadratic non-residues equal (see Problem 2). Anyway, these details (related to these differences in conventions) should not be important as long as we are aware of them and as long as we take notice of them when reading to different authors (with strong emphasis on keeping consistency and sensibility). Accordingly, in this book we may follow one convention in one place and another convention in another place[13] and hence the reader should be vigilant. However, we generally make the situation clear (either by explicit announcement or by obvious contextual indications).

Problems

1. Prove that $x^2 \overset{p}{=} n$ has either exactly two (distinct modular) solutions or none (where $n \in \mathbb{Z}$, p is an odd prime and n and p are coprime).
   Solution: We have three things to prove:
   • $x^2 \overset{p}{=} n$ can have no solution: this is obvious because we have many examples where $x^2 \overset{p}{=} n$ has no solution, e.g. $x^2 \overset{3}{=} 2$.
   • If $x^2 \overset{p}{=} n$ has a solution then it has no more than two solutions: this is obvious from Lagrange's polynomial roots theorem (see § 2.9.4 of V1).
   • If $x^2 \overset{p}{=} n$ has a solution then it has exactly two (distinct modular) solutions: let $x^2 \overset{p}{=} n$ has a solution X and hence $X^2 \overset{p}{=} n$. Therefore, we must also have $(-X)^2 \overset{p}{=} n$, i.e. $-X$ is also a solution. So, all we need to complete the proof is to show that $X \overset{p}{\neq} -X$. This should be obvious because otherwise $X \overset{p}{=} -X$, i.e. $2X \overset{p}{=} 0$ which means that $p|X$ (since p is an odd prime and hence $p\not|2$). Now, if $p|X$ then (from $X^2 \overset{p}{=} n$) we have $n \overset{p}{=} 0$, i.e. $p|n$ which contradicts the assumption that n and p are coprime.
2. Prove that there are exactly $(p-1)/2$ quadratic residues (mod p), and $(p-1)/2$ quadratic non-residues (mod p) where p is an odd prime. Moreover, the $(p-1)/2$ quadratic residues (mod p) are: $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$.
   Solution: We have:

$$-1 \overset{p}{=} p-1 \qquad -2 \overset{p}{=} p-2 \qquad \cdots \qquad -\tfrac{p-1}{2} \overset{p}{=} p-\tfrac{p-1}{2}$$

   Now, if we square both sides of these congruences we get:

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

[13] This is for convenience and because each convention has an advantage in certain situations and contexts.

Now, let us analyze this:

• Eq. 3 means that each integer in the set $\left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$ is a quadratic residue (mod p) because each of the congruences:

$$x^2 \overset{p}{=} 1^2 \qquad x^2 \overset{p}{=} 2^2 \qquad \cdots \qquad x^2 \overset{p}{=} \left(\tfrac{p-1}{2}\right)^2$$

has two (distinct modular) solutions, e.g. $x^2 \overset{p}{=} 1^2$ has the solutions $x \overset{p}{=} 1, (p-1)$ while $x^2 \overset{p}{=} 2^2$ has the solutions $x \overset{p}{=} 2, (p-2)$.[14]

• Eq. 3 shows that we have *no more than* $(p-1)/2$ quadratic residues [since 1^2 is congruent to $(p-1)^2$ and so on] where each one of these $(p-1)/2$ quadratic residues corresponds to two distinct solutions from the integers $\{1, 2, \ldots, p-1\}$.

• If we remember that all the (modular) solutions of the congruence $x^2 \overset{p}{=} n$ must belong to the set $\{1, 2, \ldots, p-1\}$ (noting that these are the only integers in mod p which are coprime to p) then we can conclude that the number of possible (modular) solutions is no more than $p-1$. Now, we already found that all these numbers (i.e. $1, 2, \ldots, p-1$) are solutions grouped in $(p-1)/2$ pairs where the solutions in each pair are distinct, i.e. $(1, p-1)$, $(2, p-2), \ldots, \left(\frac{p-1}{2}, p - \frac{p-1}{2}\right)$. So, if we prove that two distinct integers (say n_1 and n_2) of the set $\{1, 2, \ldots, (p-1)/2\}$ must satisfy $n_1^2 \overset{p}{\neq} n_2^2$ then we actually proved that the congruence $x^2 \overset{p}{=} n$ has *exactly* $(p-1)/2$ quadratic residues representing $(p-1)$ distinct solutions [i.e. the solutions that correspond to $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$] and hence it cannot have more solutions.

• So in brief, since all these $(p-1)$ distinct solutions correspond to these distinct $(p-1)/2$ quadratic residues [i.e. $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$], then we conclude that the (modular) integers $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are the quadratic residues (mod p) and all the remaining $(p-1)/2$ (modular) integers are the quadratic non-residues (mod p) since none of the remaining (modular) integers can be a quadratic residue since all the possible $(p-1)$ solutions are already taken by the $(p-1)/2$ quadratic residues [noting that the remaining (modular) integers cannot have solutions among these $(p-1)$ solutions which are already taken].

So to complete the proof we just need to show that when n_1 and n_2 of the set $\{1, 2, \ldots, (p-1)/2\}$ are distinct then $n_1^2 \overset{p}{\neq} n_2^2$. Now, let assume (for the sake of argument) that $n_1^2 \overset{p}{=} n_2^2$ and hence:

$$n_1^2 - n_2^2 \overset{p}{=} 0 \qquad \rightarrow \qquad (n_1 - n_2)(n_1 + n_2) \overset{p}{=} 0 \qquad \rightarrow \qquad p \,\big|\, \big[(n_1 - n_2)(n_1 + n_2)\big]$$

Now, $p \nmid (n_1+n_2)$ because $1 < (n_1+n_2) < p$ [noting that n_1 and n_2 belong to the set $\{1, 2, \ldots, (p-1)/2\}$]. Also, $p \nmid (n_1 - n_2)$ because $0 < |n_1 - n_2| < p$ (noting that n_1 and n_2 are supposedly distinct). This nonsensical result should lead to the conclusion that if $n_1 \overset{p}{\neq} n_2$ then $n_1^2 \overset{p}{\neq} n_2^2$ (and this should complete the proof).

3. Find all the quadratic residues and quadratic non-residues of the following (modular) prime numbers:

(**a**) 7. (**b**) 11. (**c**) 17.

Solution: We refer the reader to Problem 2 for justification and explanation to the given solutions (noting the consistency of these solutions with the proposition of Problem 2).[15]

(**a**) The quadratic residues of 7 are (noting that what is between parentheses are the solutions corresponding to the given quadratic residue):

$$1^2 \overset{7}{=} 1 \ (x \overset{7}{=} 1, 6) \qquad 2^2 \overset{7}{=} 4 \ (x \overset{7}{=} 2, 5) \qquad 3^2 \overset{7}{=} 2 \ (x \overset{7}{=} 3, 4)$$

The quadratic non-residues of 7 are: $3, 5, 6$.

(**b**) The quadratic residues of 11 are:

$$1^2 \overset{11}{=} 1 \ (x \overset{11}{=} 1, 10) \qquad 2^2 \overset{11}{=} 4 \ (x \overset{11}{=} 2, 9) \qquad 3^2 \overset{11}{=} 9 \ (x \overset{11}{=} 3, 8) \qquad 4^2 \overset{11}{=} 5 \ (x \overset{11}{=} 4, 7) \qquad 5^2 \overset{11}{=} 3 \ (x \overset{11}{=} 5, 6)$$

[14] We note that we use $1^2, 2^2$ to represent the integers which are congruent to $1, 4$ (mod p), i.e. $1 + kp$ and $4 + kp$. This laxity is for the sake of simplicity and to avoid some complications in the presentation.

[15] In fact, the examples given in the present Problem (and the given solutions) should also clarify the proposition of Problem 2 and remove any ambiguity or confusion about the proof given in Problem 2. We advise the reader to inspect the pattern in these solutions and take note of it as this should improve the understanding of Problem 2.

The quadratic non-residues of 11 are: $2, 6, 7, 8, 10$.
(**c**) The quadratic residues of 17 are:

$1^2 \overset{17}{=} 1$ ($x \overset{17}{=} 1, 16$) $2^2 \overset{17}{=} 4$ ($x \overset{17}{=} 2, 15$) $3^2 \overset{17}{=} 9$ ($x \overset{17}{=} 3, 14$) $4^2 \overset{17}{=} 16$ ($x \overset{17}{=} 4, 13$)

$5^2 \overset{17}{=} 8$ ($x \overset{17}{=} 5, 12$) $6^2 \overset{17}{=} 2$ ($x \overset{17}{=} 6, 11$) $7^2 \overset{17}{=} 15$ ($x \overset{17}{=} 7, 10$) $8^2 \overset{17}{=} 13$ ($x \overset{17}{=} 8, 9$)

The quadratic non-residues of 17 are: $3, 5, 6, 7, 10, 11, 12, 14$.

4. Find all the quadratic residues and quadratic non-residues of the following (modular) composite numbers (ignoring the condition of coprimality which we stated and discussed in the preamble):
   (**a**) 6. (**b**) 9. (**c**) 12.
   Solution:
   (**a**) The quadratic residues of 6 are: 0 (corresponding to $x \overset{6}{=} 0$), 1 ($x \overset{6}{=} 1, 5$), 3 ($x \overset{6}{=} 3$), 4 ($x \overset{6}{=} 2, 4$).
   The quadratic non-residues of 6 are: $2, 5$.
   (**b**) The quadratic residues of 9 are: 0 ($x \overset{9}{=} 0, 3, 6$), 1 ($x \overset{9}{=} 1, 8$), 4 ($x \overset{9}{=} 2, 7$), 7 ($x \overset{9}{=} 4, 5$).
   The quadratic non-residues of 9 are: $2, 3, 5, 6, 8$.
   (**c**) The quadratic residues of 12 are: 0 ($x \overset{12}{=} 0, 6$), 1 ($x \overset{12}{=} 1, 5, 7, 11$), 4 ($x \overset{12}{=} 2, 4, 8, 10$), 9 ($x \overset{12}{=} 3, 9$).
   The quadratic non-residues of 12 are: $2, 3, 5, 6, 7, 8, 10, 11$.
5. Show that if n is a quadratic residue (modulo $k > 2$) then $n^{\frac{\phi(k)}{2}} \overset{k}{=} 1$.[16]
   Solution: "n is a quadratic residue (modulo k)" means we have $x \in \mathbb{Z}$ such that $x^2 \overset{k}{=} n$ with n and k being coprime (and hence x and k are coprime). So, from Euler's theorem we have:

$$x^{\phi(k)} \overset{k}{=} 1 \qquad \rightarrow \qquad \left(x^2\right)^{\left[\frac{\phi(k)}{2}\right]} \overset{k}{=} 1 \qquad \rightarrow \qquad n^{\frac{\phi(k)}{2}} \overset{k}{=} 1$$

6. Show that a primitive root (modulo $k > 2$) cannot be a quadratic residue (modulo k).
   Solution: This can be concluded from the proposition of Problem 5 because the order of a quadratic residue n (modulo k) is less than $\phi(k)$ since $n^{\frac{\phi(k)}{2}} \overset{k}{=} 1$, while the order of a primitive root (modulo k) is $\phi(k)$ (see point 1 in the preamble of § 1.4).
   We may also argue that if r is a primitive root (modulo k) then $r \overset{k}{=} r^1$. On the other hand, any quadratic residue n must be an even power of r [i.e. $n \overset{k}{=} r^{2s} = (r^s)^2$ where $s \in \mathbb{N}$] so that the congruence $x^2 \overset{k}{=} n$ can have a solution. Hence, a primitive root cannot be a quadratic residue.
   Yes, there is one exception which is 1 (modulo 2) since 1 is a primitive root (mod 2) and 1 is a quadratic residue (mod 2), and hence we imposed $k > 2$. Also see Problem 6 of § 1.9.
7. Let r be a primitive root of an odd prime p. Show that the quadratic residues (mod p) are the even powers of r while the quadratic non-residues (mod p) are the odd powers of r.
   Solution: Any $x \in \{1, 2, \ldots .p-1\}$ should be equal (mod p) to r^s for some $s \in \mathbb{N}$. Now, if n is a quadratic residue (mod p) then from Problem 2 we must have $n = x^2 = (r^s)^2 = r^{2s}$, i.e. n is an even power of r. So, the quadratic non-residues must be the (remaining) odd powers of r (also see Problem 6).
8. Show that if r is a primitive root of an odd prime p then:

$$\prod QR \overset{p}{=} r^{(p^2-1)/4} \qquad \text{and} \qquad \prod QnR \overset{p}{=} r^{(p-1)^2/4}$$

   where $\prod QR$ is the product of all quadratic residues (mod p) and $\prod QnR$ is the product of all quadratic non-residues (mod p).
   Solution: The quadratic residues are the even powers of r while the quadratic non-residues are the odd powers of r (see Problem 7). Hence:

$$\prod QR \overset{p}{=} r^2 \times r^4 \times \cdots \times r^{2(p-1)/2} = r^{2\sum_{k=1}^{(p-1)/2} k} = \left(r^2\right)^{(p^2-1)/8} = r^{(p^2-1)/4}$$

[16] It is worth noting that the converse of this statement is not true in general. For instance, $5^{\frac{\phi(12)}{2}} = 5^{4/2} = 5^2 \overset{12}{=} 1$ but 5 is not a quadratic residue (modulo 12).

where we used the arithmetic series formula in step 3 (see Eq. 15 in V1).
Similarly:

$$\prod QnR \overset{p}{=} r^1 \times r^3 \times \cdots \times r^{p-2} = r^{\sum_{k=1}^{(p-1)/2}(2k-1)} = r^{(p-1)^2/4}$$

where we used the formula $\sum_{k=1}^{n}(2k-1) = n^2$ in step 3.

1.7 The Quadratic Congruence Theorem

According to this theorem (noting that $n \in \mathbb{N}$, $p \in \mathbb{P}$ and $n < p$):
• If n is a quadratic residue (mod p) then p divides $(p-1)! + n^{(p-1)/2}$.
• If n is a quadratic non-residue (mod p) then p divides $(p-1)! - n^{(p-1)/2}$.

Problems

1. Prove the quadratic congruence theorem.
Solution: For $p = 2$ the theorem is obviously true, i.e. 1 is a quadratic residue (mod 2) and 2 divides $(2-1)! + 1^{(2-1)/2} = 2$. So, in the following we assume $p > 2$. Considering the above two cases we have:
• Because n is a quadratic residue (mod p) then we have:

$$x^2 \overset{p}{=} n \quad \rightarrow \quad \left(x^2\right)^{(p-1)/2} \overset{p}{=} n^{(p-1)/2} \quad \rightarrow \quad n^{(p-1)/2} \overset{p}{=} x^{p-1} \quad \rightarrow$$
$$n^{(p-1)/2} \overset{p}{=} 1 \quad \rightarrow \quad n^{(p-1)/2} \overset{p}{=} -(p-1)! \quad \rightarrow \quad (p-1)! + n^{(p-1)/2} \overset{p}{=} 0$$

where we used Fermat's little theorem in step 3 (noting that x and p must be coprime since n and p are coprime), and we used Wilson's theorem in step 4.
• Regarding the case when n is a quadratic non-residue (mod p), we start by examining the following linear congruence:

$$ax \overset{p}{=} n \tag{4}$$

which by the LCE theorem (see § 3.2.1 of V1) must have a single modular solution[17] where this solution belongs to the set $\{1, 2, \ldots, p-1\}$. Now, if c is a solution then we have $ac \overset{p}{=} n$ and hence if the congruence $x^2 \overset{p}{=} n$ has no solution (i.e. n is a quadratic non-residue mod p) then $a \overset{p}{\neq} c$. Noting that a and c belong to the set $\{1, 2, \ldots, p-1\}$,[18] this set can be partitioned into $(p-1)/2$ pairs (a_i, c_i) $\left[i = 1, 2, \ldots, (p-1)/2 \text{ and } a_i \overset{p}{\neq} c_i\right]$ where Eq. 4 applies to each one of these pairs. Now, if we multiply these $(p-1)/2$ congruences side by side (see rule 10 in the preamble of § 2.7 of V1) then we get:

$$(p-1)! \overset{p}{=} n^{(p-1)/2} \quad \rightarrow \quad (p-1)! - n^{(p-1)/2} \overset{p}{=} 0$$

i.e. p divides $(p-1)! - n^{(p-1)/2}$.

1.8 Legendre's Symbol

Let n be an integer and p is an odd prime and n and p are coprime. The Legendre symbol is defined as:

$$\left(\frac{n}{p}\right) = \begin{cases} +1 & (n \text{ is a quadratic residue mod } p) \\ -1 & (n \text{ is a quadratic non-residue mod } p) \end{cases} \tag{5}$$

Legendre's symbol is defined to be zero if $p|n$. For example:

$$\left(\frac{1}{3}\right) = +1 \qquad \left(\frac{2}{3}\right) = -1 \qquad \left(\frac{3}{3}\right) = 0$$

It is important to note the following about Legendre's symbol:

[17] In brief, $n > 0$ and hence a and p must be coprime, i.e. their gcd is 1 (which divides n) and hence the congruence has a solution. Now, since the gcd of a and p is 1 then we must have a single solution (see Eq. 58 of V1 and the surrounding text).
[18] It should be obvious that we are talking in modular arithmetic.

1. $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$ where $m, n \in \mathbb{Z}$ and p is an odd prime with n and p being coprime and $m \overset{p}{=} n$.
2. If p is an odd prime then:
$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \tag{6}$$
3. If p is an odd prime then:
$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & (p \overset{8}{=} \pm 1) \\ -1 & (p \overset{8}{=} \pm 3) \end{cases} \tag{7}$$
4. Legendre's symbol is a totally multiplicative function,[19] that is:
$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \tag{8}$$
where p is an odd prime.
5. If p is an odd prime then:
$$\left(\frac{n^2}{p}\right) = \left(\frac{n}{p}\right)^2 \tag{9}$$
6. The separation of the zero case in the above definition of Legendre's symbol means that when we talk about Legendre's symbol then we assume (by default) that n and p are coprime, and hence the zero case is considered or included only if it is mentioned or indicated explicitly.

Problems

1. Prove property 1 above.
Solution: Since n and p are coprime then m and p must also be coprime (because otherwise $m \overset{p}{=} 0$ which contradicts $m \overset{p}{=} n$ noting that $n \overset{p}{\neq} 0$ since n and p are coprime). Moreover, since $m \overset{p}{=} n$ then m and n must be both quadratic residues (mod p) or both quadratic non-residues (mod p) which means that $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$.
2. Prove property 5 above.
Solution: This is an instance of property 4 (which will be proved in Problem 4 of § 1.9) with $m = n$.
3. Let p be an odd prime and $m, n \in \mathbb{Z}$ such that $p \nmid m$ and $p \nmid n$. Show that the number of quadratic residues (mod p) among m, n, mn is either exactly one or three (i.e. it cannot be zero or two).
Solution: Since $p \nmid m$ and $p \nmid n$ then $p \nmid (mn)$, i.e. mn and p are coprime. Hence, from Eq. 8 (noting that Legendre's symbol is either $+1$ or -1) we get:
$$\left(\frac{mn}{p}\right)\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = 1$$
This means that if we have any -1 on the LHS of this equation (i.e. if any of m, n, mn is a quadratic non-residue) then we should have either two -1 or zero -1 (i.e. we should have either exactly one or three quadratic residues among m, n, mn).
4. Show that for any prime $p \geq 7$ we must have at least one pair of consecutive quadratic residues.
Solution: If $p = 7$ then we have 1 and 2 (which are consecutive quadratic residues of 7). So, in the following we consider the cases of $p > 7$.
Let $S = \{1, 2, \ldots, p-1\}$ be the set of residue classes of p (excluding 0), i.e. S represents the union of all quadratic residues and quadratic non-residues of p (see Problem 2 of § 1.6). Now, for $p > 7$ we have $2, 5, 10 \in S$. So, from Problem 3 we conclude that at least one of $2, 5, 10$ must be a quadratic residue of p. However, $1, 4, 9$ (i.e. $1^2, 2^2, 3^2$) are quadratic residues of p (see Problem 2 of § 1.6). Now, if we note that $2 = 1 + 1$, $5 = 4 + 1$ and $10 = 9 + 1$ then we conclude that we must have at least one pair of consecutive quadratic residues (i.e. in S).

[19] Totally (or completely) multiplicative function is defined as an arithmetic function (see § 1.1 of V1) such that $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$.

5. Show that for any prime $p \geq 7$ we must have at least one pair of consecutive quadratic non-residues.
   Solution: If $p = 7$ then we have 5 and 6 (which are consecutive quadratic non-residues of 7). So, in the following we consider the cases of $p > 7$.
   We note first that $1, 4, 9$ (i.e. $1^2, 2^2, 3^2$) are quadratic residues of p (see Problem 2 of § 1.6). Now, if we have a pair of consecutive quadratic non-residues among $1, 2, 3, 4, 5, 6, 7, 8, 9$ then we got what we want. If not then we must have an alternation in quadratic residues and quadratic non-residues in such a way that prevents the occurrence of consecutive quadratic non-residues among $1, 2, 3, 4, 5, 6, 7, 8, 9$. This means that at least one of $2, 3$ must be a quadratic residue and at least two of $5, 6, 7, 8$ must be quadratic residues. So, in total we must have at least six quadratic residues among $1, 2, 3, 4, 5, 6, 7, 8, 9$. Now, if we remember that quadratic residues and quadratic non-residues are equal in number (see Problem 2 of § 1.6) then we will not have enough quadratic residues after 9 to have a similar alternation that prevents the occurrence of consecutive quadratic non-residues after 9, i.e. we must have at least one pair of consecutive quadratic non-residues after 9. So in brief, we must have a pair of consecutive quadratic non-residues among $1, 2, 3, 4, 5, 6, 7, 8, 9$ or after 9.
   Note: the obvious conclusion of this Problem and the previous Problem is that for $p \geq 7$ we must always have pairs of consecutive quadratic residues and consecutive quadratic non-residues.
6. Determine the value of the following Legendre symbols: $\left(\frac{6863}{7883}\right)$ and $\left(\frac{1137}{5821}\right)$.
   Solution: The congruence $x^2 \overset{7883}{=} 6863$ has no solution (i.e. 6863 is a quadratic non-residue mod 7883) and hence $\left(\frac{6863}{7883}\right) = -1$.
   The congruence $x^2 \overset{5821}{=} 1137$ is solvable (i.e. 1137 is a quadratic residue mod 5821) and hence $\left(\frac{1137}{5821}\right) = 1$.
7. Determine the value of the Legendre symbol: $\left(\frac{n}{11}\right)$ for all $n \in \mathbb{Z}$.
   Solution: Referring to part (b) of Problem 3 of § 1.6:
   - $\left(\frac{n}{11}\right) = +1$ for $n \overset{11}{=} 1, 3, 4, 5, 9$.
   - $\left(\frac{n}{11}\right) = -1$ for $n \overset{11}{=} 2, 6, 7, 8, 10$.
   - $\left(\frac{n}{11}\right) = 0$ for $n \overset{11}{=} 0$.
8. Evaluate the following Legendre symbols:
   (**a**) $\left(\frac{122}{19}\right)$. (**b**) $\left(\frac{225}{41}\right)$. (**c**) $\left(\frac{-183}{61}\right)$. (**d**) $\left(\frac{-20}{101}\right)$.
   Solution: In this Problem we use the rules of Legendre's symbol (as well as the general rules such as those of modular arithmetic and quadratic residues).[20]
   (**a**) We have:

$$\begin{aligned}
\left(\frac{122}{19}\right) &= \left(\frac{8}{19}\right) && (122 \overset{19}{=} 8)\\
&= \left(\frac{2^3}{19}\right)\\
&= \left(\frac{2}{19}\right)\left(\frac{2}{19}\right)\left(\frac{2}{19}\right) && (\text{Eq. 8})\\
&= \left(\frac{2}{19}\right) && \left[\left(\frac{2}{19}\right) = \pm 1\right]\\
&= -1 && (2 \overset{19}{\neq} 1^2, 2^2, \ldots, 9^2;\ \text{see Problem 2 of § 1.6})
\end{aligned}$$

   A simpler approach is to note that $122 \overset{19}{=} 8 \overset{19}{\neq} 1^2, 2^2, \ldots, 9^2$ and hence we need no more than two steps.
   (**b**) We have:

$$\left(\frac{225}{41}\right) = \left(\frac{3^2 \times 5^2}{41}\right)$$

[20] We note that in some of the following solutions we do extra work for pedagogical purposes (otherwise some solutions can be obtained in less steps). We also note that there are various ways for obtaining these results and hence what we present in the following solutions is just a sample of these various ways.

$$\begin{aligned}
&= \left(\frac{3^2}{41}\right)\left(\frac{5^2}{41}\right) && \text{(Eq. 8)}\\
&= \left(\frac{3}{41}\right)^2\left(\frac{5}{41}\right)^2 && \text{(Eq. 9)}\\
&= 1 \times 1 = 1 && \left[(\pm 1)^2 = 1 \text{ noting that 3 and 5 are coprime to 41}\right]
\end{aligned}$$

A simpler approach is to use Eq. 9 from the beginning (noting that $225 = 15^2$ and 15 and 41 are coprime).
(**c**) $61|(-183)$ and hence this Legendre symbol is zero.
(**d**) We have:

$$\begin{aligned}
\left(\frac{-20}{101}\right) &= \left(\frac{81}{101}\right) && (-20 \overset{101}{=} 81)\\
&= \left(\frac{9^2}{101}\right)\\
&= \left(\frac{9}{101}\right)^2 && \text{(Eq. 9)}\\
&= 1 && \left[(\pm 1)^2 = 1 \text{ noting that 9 and 101 are coprime}\right]
\end{aligned}$$

9. Use property 2 (in the preamble) to determine the Legendre symbol $\left(\frac{-1}{p}\right)$ for all odd primes according to their modularity in modulo 4.
Solution: Every odd prime must be either of the form $(4k+1)$ or of the form $(4k-1)$ where $k \in \mathbb{N}$ (see Problem 16 of § 2.2 of V1). Now, if $p = 4k+1$ then from property 2 we have:

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

On the other hand, if $p = 4k-1$ then from property 2 we have:

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

So in brief, the Legendre symbol $\left(\frac{-1}{p}\right)$ is $+1$ for all $p = 4k+1$ and -1 for all $p = 4k-1$.

10. Show that for all $n \in \mathbb{Z}$ such that $p \not| n$ (with p being an odd prime) we have $\left(\frac{n^2}{p}\right) = 1$.
Solution: We have (see Eq. 9):

$$\left(\frac{n^2}{p}\right) = \left(\frac{n}{p}\right)^2 = (\pm 1)^2 = 1$$

11. Let n be a quadratic residue of p (which is an odd prime). Show that $-n$ is a quadratic residue if $p = 4k+1$, while $-n$ is a quadratic non-residue if $p = 4k-1$.
Solution: $\left(\frac{n}{p}\right) = +1$ because n is a quadratic residue of p. From Eq. 8 (as well as the result of Problem 9) we have:

$$\left(\frac{-n}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{-1}{p}\right)(+1) = \left(\frac{-1}{p}\right) = \begin{cases} +1 & (p = 4k+1)\\ -1 & (p = 4k-1)\end{cases}$$

i.e. $-n$ is a quadratic residue if $p = 4k+1$, and $-n$ is a quadratic non-residue if $p = 4k-1$.

12. Show the following:
(**a**) $\left(\frac{m}{p}\right)\left(\frac{m}{p}\right) = 1$. (**b**) $\left(\frac{m^2}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p}\right)$. (**c**) $\left(\frac{m}{p^2}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p}\right)$. (**d**) $\left(\frac{m^2}{p}\right) = \left(\frac{m}{p^2}\right)$.

Solution: All these relations are proved in Problem 9 of § 1.11 for Jacobi symbol and hence they should apply to Legendre symbol as well (noting that Legendre symbol is a special case of Jacobi symbol; see point 9 of § 1.11). We should also note that some of these relations are trivial to prove since they are no more than a special case of relations which are proved for Legendre symbol independently, e.g. $\left(\frac{m^2}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p}\right)$ is a special case of the relation $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$ which we proved in Problem 4 of § 1.9.[21]

13. Show that mn is a quadratic residue of p (where p is an odd prime) *iff* m and n are either both quadratic residues of p or both quadratic non-residues of p.
Solution: We note first that mn is coprime to p *iff* m and n are both coprime to p. From property 4 we have:
$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$
So, $\left(\frac{mn}{p}\right) = 1$ *iff* either $\left(\frac{m}{p}\right) = 1$ and $\left(\frac{n}{p}\right) = 1$ or $\left(\frac{m}{p}\right) = -1$ and $\left(\frac{n}{p}\right) = -1$, i.e. mn is a quadratic residue of p *iff* m and n are either both quadratic residues of p or both quadratic non-residues of p.
14. Show that n and n^* are either both quadratic residues of p or both quadratic non-residues of p (where n^* is the multiplicative inverse of n and p is an odd prime).
Solution: We have $nn^* \stackrel{p}{=} 1$. Now, 1 is a quadratic residue of p (see Problem 2 of § 1.6) and hence by the proposition of Problem 13, n and n^* are either both quadratic residues of p or both quadratic non-residues of p.
15. State Gauss lemma and use it to calculate the following Legendre symbols:
(**a**) $\left(\frac{13}{17}\right)$. (**b**) $\left(\frac{21}{31}\right)$.
Solution: Gauss lemma states: if m is an integer coprime to the odd prime p, and n is the number of least positive residues (modulo p) of the integers $m, 2m, \ldots, \frac{(p-1)m}{2}$ which are greater than $p/2$, then:
$$\left(\frac{m}{p}\right) = (-1)^n$$
(**a**) Let S be the set $m, 2m, \ldots, \frac{(p-1)m}{2}$ and LPR be the set of the least positive residues of S. Accordingly, we have:
$$S = \{13, 26, 39, 52, 65, 78, 91, 104\} \qquad LPR = \{13, 9, 5, 1, 14, 10, 6, 2\}$$
So, $13, 9, 14, 10$ are greater than $17/2$ and hence $n = 4$. Therefore, $\left(\frac{13}{17}\right) = (-1)^4 = 1$.
(**b**) We have:
$$S \stackrel{31}{=} LPR = \{21, 11, 1, 22, 12, 2, 23, 13, 3, 24, 14, 4, 25, 15, 5\}$$
So, $21, 22, 23, 24, 25$ are greater than $31/2$ and hence $n = 5$. Therefore, $\left(\frac{21}{31}\right) = (-1)^5 = -1$.

1.9 Euler's Criterion

Euler's criterion was introduced in § 3.2.3 of V1 of this book. According to this criterion, the quadratic congruence equation $x^2 \stackrel{p}{=} n$ has a solution *iff* $n^{(p-1)/2} \stackrel{p}{=} 1$ (where $n \in \mathbb{Z}$, p is an odd prime and $p \nmid n$). This can be expressed (with some additional content) in terms of Legendre's symbol (see § 1.8) as:
$$\left(\frac{n}{p}\right) \stackrel{p}{=} n^{(p-1)/2} \qquad (n \in \mathbb{Z},\ p \text{ is an odd prime},\ p \nmid n) \tag{10}$$
We note that since $\phi(p) = p - 1$, some authors replace $(p-1)$ by $\phi(p)$.

Problems

[21] In fact, the relation of part (a) is self evident because $\left(\frac{m}{p}\right) = \pm 1$.

1. Prove Eq. 10.
   Solution: By the definition of Legendre's symbol (noting that $p \nmid n$) we have $\left(\frac{n}{p}\right) = \pm 1$. So, we have two cases to consider (where we will show that in both cases Eq. 10 is valid):
   - $\left(\frac{n}{p}\right) = +1$: in this case n is a quadratic residue (mod p) and hence we have:

$$\begin{aligned}
(p-1)! + n^{(p-1)/2} &\overset{p}{\equiv} 0 && \text{(quadratic congruence theorem; see § 1.7)}\\
-(p-1)! &\overset{p}{\equiv} n^{(p-1)/2} &&\\
+1 &\overset{p}{\equiv} n^{(p-1)/2} && \text{(Wilson's theorem)}\\
\left(\frac{n}{p}\right) &\overset{p}{\equiv} n^{(p-1)/2} && \text{(given)}
\end{aligned}$$

   We may also argue that in this case n is a quadratic residue (mod p) and hence we have $x \in \mathbb{Z}$ such that:

$$x^2 \overset{p}{\equiv} n \qquad \rightarrow \qquad \left(x^2\right)^{(p-1)/2} \overset{p}{\equiv} n^{(p-1)/2} \qquad \rightarrow \qquad n^{(p-1)/2} \overset{p}{\equiv} x^{p-1}$$

   Now, $x^2 \overset{p}{\equiv} n$ (noting that $p \nmid n$) implies $p \nmid x^2$ and hence $p \nmid x$ (i.e. p and x are coprime). Therefore, from Fermat's little theorem we have $x^{p-1} \overset{p}{\equiv} 1$, i.e. $n^{(p-1)/2} \overset{p}{\equiv} 1 = \left(\frac{n}{p}\right)$ as required.
   - $\left(\frac{n}{p}\right) = -1$: in this case n is a quadratic non-residue (mod p) and hence we have:

$$\begin{aligned}
(p-1)! - n^{(p-1)/2} &\overset{p}{\equiv} 0 && \text{(quadratic congruence theorem; see § 1.7)}\\
(p-1)! &\overset{p}{\equiv} n^{(p-1)/2} &&\\
-1 &\overset{p}{\equiv} n^{(p-1)/2} && \text{(Wilson's theorem)}\\
\left(\frac{n}{p}\right) &\overset{p}{\equiv} n^{(p-1)/2} && \text{(given)}
\end{aligned}$$

   As we see, in both cases Eq. 10 is valid (and this completes the proof).
2. Prove property 2 of § 1.8.
   Solution: According to Euler's criterion we have:

$$\left(\frac{-1}{p}\right) \overset{p}{\equiv} (-1)^{(p-1)/2} \qquad \rightarrow \qquad p \left| \left[\left(\frac{-1}{p}\right) - (-1)^{(p-1)/2}\right]\right.$$

   Now, $\left(\frac{-1}{p}\right)$ and $(-1)^{(p-1)/2}$ can be only $+1$ or -1 (and hence the dividend can only be 0 or 2 or -2). Moreover, p is an odd prime. Hence, this divisibility statement is valid only if the dividend is 0, i.e. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
3. Prove property 3 of § 1.8.
   Solution: We have:

$$p-1 \overset{p}{\equiv} 1\,(-1)^1 \qquad 2 \overset{p}{\equiv} 2\,(-1)^2 \qquad p-3 \overset{p}{\equiv} 3\,(-1)^3 \qquad 4 \overset{p}{\equiv} 4\,(-1)^4 \qquad \cdots \qquad A \overset{p}{\equiv} \tfrac{p-1}{2}\,(-1)^{(p-1)/2}$$

   where $A = p - \frac{p-1}{2} = \frac{2p-p+1}{2} = \frac{p+1}{2}$ if $p \overset{4}{\equiv} -1$ and $A = \frac{p-1}{2}$ if $p \overset{4}{\equiv} 1$. Now, if we multiply these $(p-1)/2$ congruences side by side (see rule 10 in the preamble of § 2.7 of V1) then we get:

$$(p-1) \times 2 \times (p-3) \times 4 \times \ldots \times A \overset{p}{\equiv} \left(\frac{p-1}{2}\right)! \,(-1)^{\sum_{i=1}^{(p-1)/2} i} \tag{11}$$

   Now, the LHS is equal to $2 \times 4 \times \ldots \times (p-1)$.[22] Moreover, from the arithmetic series formula we have

[22] This is just rearrangement of the terms in this product, that is:

$$(p-1) \times 2 \times (p-3) \times 4 \times \ldots \times \frac{p+1}{2} \quad = \quad 2 \times 4 \times \ldots \times \frac{p+1}{2} \times \ldots \times (p-3) \times (p-1) \qquad \left[A = \frac{p+1}{2}\right]$$

$\sum_{i=1}^{(p-1)/2} i = (p^2-1)/8$. Hence, Eq. 11 becomes:

$$2 \times 4 \times \ldots \times (p-1) \stackrel{p}{=} \left(\frac{p-1}{2}\right)! \, (-1)^{(p^2-1)/8} \tag{12}$$

Now, if we note that:

$$2 \times 4 \times \ldots \times (p-1) = 2(1) \times 2(2) \times \ldots \times 2\left(\frac{p-1}{2}\right) = \left(\frac{p-1}{2}\right)! \, 2^{(p-1)/2}$$

then Eq. 12 will become:

$$\left(\frac{p-1}{2}\right)! \, 2^{(p-1)/2} \stackrel{p}{=} \left(\frac{p-1}{2}\right)! \, (-1)^{(p^2-1)/8}$$

Noting that $\left(\frac{p-1}{2}\right)!$ and p are coprime (see for instance rule 4 of § 6.11 of V1) we can cancel the factorial in the last equation (see rule 7 of § 2.7 of V1) and get:

$$2^{(p-1)/2} \stackrel{p}{=} (-1)^{(p^2-1)/8} \tag{13}$$

Now, according to Euler's criterion we have (see Eq. 10):

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

and hence Eq. 13 becomes:

$$\left(\frac{2}{p}\right) \stackrel{p}{=} (-1)^{(p^2-1)/8} \qquad \rightarrow \qquad p \,\Big|\, \left[\left(\frac{2}{p}\right) - (-1)^{(p^2-1)/8}\right]$$

Now, $\left(\frac{2}{p}\right)$ and $(-1)^{(p^2-1)/8}$ can be only $+1$ or -1 (and hence the dividend can only be 0 or 2 or -2). Moreover, p is an odd prime. Hence, this divisibility statement is valid only if the dividend is 0, i.e.

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

Now, an odd prime can only be of the following forms: $p = 8k \pm 1$ and $p = 8k \pm 3$ where $k \in \mathbb{N}$ (because otherwise it will be even). So, if $p = 8k \pm 1$ then $(p^2-1)/8 = 8k^2 \pm 2k$ (which is even), while if $p = 8k \pm 3$ then $(p^2-1)/8 = 8k^2 \pm 6k + 1$ (which is odd). Hence:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & (p \stackrel{8}{=} \pm 1) \\ -1 & (p \stackrel{8}{=} \pm 3) \end{cases}$$

4. Prove property 4 of § 1.8.
Solution: mn and p are coprime and hence m and p are coprime and n and p are coprime (because mn has no prime factor p and hence m and n cannot have a prime factor p). Accordingly:

$$\left(\frac{mn}{p}\right) \stackrel{p}{=} \left[mn\right]^{(p-1)/2} \qquad \text{(Eq. 10)}$$

$$\left(\frac{mn}{p}\right) \stackrel{p}{=} m^{(p-1)/2} \, n^{(p-1)/2} \qquad \text{(rules of indices)}$$

$(p-1) \times 2 \times (p-3) \times 4 \times \ldots \times \frac{p-1}{2} \;=\; 2 \times 4 \times \ldots \times \frac{p-1}{2} \times \ldots \times (p-3) \times (p-1) \qquad \left[A = \frac{p-1}{2}\right]$

$$\left(\frac{mn}{p}\right) \overset{p}{=} \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \qquad \text{(Eq. 10)}$$

Now, if we note that each of $\left(\frac{mn}{p}\right)$, $\left(\frac{m}{p}\right)$ and $\left(\frac{n}{p}\right)$ is equal either to $+1$ or to -1 (noting that mn, m, n are coprime to p) then we have the following 8 (comprehensive) cases:

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

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

As we see, the $2^{nd}, 3^{rd}, 5^{th}, 8^{th}$ cases are impossible (noting that p is an odd prime and hence $p \not| 2$). So, the only possible cases are the other four and this should establish Eq. 8 and complete the proof.

5. Repeat Problem 7 of § 1.8 using this time Euler's criterion (i.e. Eq. 10).
Solution: $p = 11$ and $(p-1)/2 = 5$ and we have:

$1^5 \overset{11}{=} 1$ $\quad 2^5 \overset{11}{=} -1$ $\quad 3^5 \overset{11}{=} 1$ $\quad 4^5 \overset{11}{=} 1$ $\quad 5^5 \overset{11}{=} 1$ $\quad 6^5 \overset{11}{=} -1$ $\quad 7^5 \overset{11}{=} -1$ $\quad 8^5 \overset{11}{=} -1$ $\quad 9^5 \overset{11}{=} 1$ $\quad 10^5 \overset{11}{=} -1$

Hence, $\left(\frac{n}{11}\right) = +1$ for $n \overset{11}{=} 1, 3, 4, 5, 9$ and $\left(\frac{n}{11}\right) = -1$ for $n \overset{11}{=} 2, 6, 7, 8, 10$. Also, $0^5 \overset{11}{=} 0$ and hence $\left(\frac{n}{11}\right) = 0$ for $n \overset{11}{=} 0$. These results are identical to the results of Problem 7 of § 1.8.

6. Use Euler's criterion to show that a quadratic residue of an odd prime p cannot be a primitive root of p.
Solution: If n is a quadratic reside then by Euler's criterion we have $n^{(p-1)/2} \overset{p}{=} 1$, i.e. $n^{\phi(p)/2} \overset{p}{=} 1$. This means that $O_p n < \phi(p)$ and hence n cannot be a primitive root (see point 1 of § 1.4). Also see Problem 6 of § 1.6.
Note: it is important to note that this proposition means that an integer cannot be a quadratic residue and a primitive root (of an odd prime) at the same time. This does not mean that a non-quadratic residue must be a primitive root. For instance, 6 is a quadratic non-residue (mod 7) and it is not a primitive root (mod 7). So in brief, a quadratic residue cannot be a primitive root (and similarly a primitive root cannot be a quadratic residue), but a quadratic non-residue can be a primitive root (such as 3 in mod 7) and can be not a primitive root (such as 6 in mod 7). Also see Problem 7.

7. Show that if p is an odd prime then there are $\frac{p-1}{2} - \phi(p-1)$ quadratic non-residues (mod p) which are not primitive roots (mod p).
Solution: According to Problem 6, a quadratic residue cannot be a primitive root. So, primitive roots must be among the $\frac{p-1}{2}$ quadratic non-residues (see Problem 2 of § 1.6). Also, according to Problem 8 of § 1.4 the number of primitive roots of p is $\phi\big[\phi(p)\big] = \phi(p-1)$. Hence, the number of quadratic non-residues which are not primitive roots is $\frac{p-1}{2} - \phi(p-1)$.

1.10 Quadratic Reciprocity

According to the law of quadratic reciprocity, if p and q are distinct odd primes then:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \qquad (14)$$

where $\left(\frac{p}{q}\right)$ $\left(\frac{q}{p}\right)$ are Legendre's symbols. To make use of this law we usually use some subsidiary results (or methods or tricks or etc.) some of which will be outlined in the following Problems.

Problems

1. Use the law of quadratic reciprocity to determine whether or not the following are quadratic residues:
(**a**) 7 (mod 29). (**b**) 11 (mod 23).
Solution:
(**a**) We have $29 \overset{7}{=} 1$ and 1 is a quadratic residue of 7 (see Problem 2 of § 1.6) and hence 29 is a quadratic residue (mod 7), i.e. $\left(\frac{29}{7}\right) = 1$. Moreover, from the law of quadratic reciprocity we have:

$$\left(\frac{7}{29}\right)\left(\frac{29}{7}\right) = (-1)^{(7-1)(29-1)/4} = (-1)^{42} = 1$$

which implies $\left(\frac{7}{29}\right) = 1$ since $\left(\frac{29}{7}\right) = 1$. Therefore, 7 is a quadratic residue (mod 29).

(**b**) We have $23 \overset{11}{=} 1$ and 1 is a quadratic residue of 11 (see Problem 2 of § 1.6) and hence 23 is a quadratic residue (mod 11), i.e. $\left(\frac{23}{11}\right) = 1$. Moreover, from the law of quadratic reciprocity we have:

$$\left(\frac{11}{23}\right)\left(\frac{23}{11}\right) = (-1)^{(11-1)(23-1)/4} = (-1)^{55} = -1$$

which implies $\left(\frac{11}{23}\right) = -1$ since $\left(\frac{23}{11}\right) = 1$. Therefore, 11 is a quadratic non-residue (mod 23).

2. Let p and q be odd primes. Use the law of quadratic reciprocity to correlate the solvability of the congruence $x^2 \overset{p}{=} q$ to the solvability of the congruence $x^2 \overset{q}{=} p$ according to the modularity of p and q in modulo 4.

Solution: Every odd prime must be either of the form $(4k+1)$ or of the form $(4k-1)$ where $k \in \mathbb{N}$ (see Problem 16 of § 2.2 of V1). Now, if $p = 4k \pm 1$ and $q = 4\kappa \pm 1$ then we have 4 cases:

• $p = 4k+1$ and $q = 4\kappa + 1$ and hence (by the law of quadratic reciprocity):

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = (-1)^{(4k+1-1)(4\kappa+1-1)/4} = (-1)^{4k\kappa} = 1$$

• $p = 4k+1$ and $q = 4\kappa - 1$ and hence:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = (-1)^{(4k+1-1)(4\kappa-1-1)/4} = (-1)^{4k\kappa-2k} = 1$$

• $p = 4k-1$ and $q = 4\kappa + 1$ and hence:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = (-1)^{(4k-1-1)(4\kappa+1-1)/4} = (-1)^{4k\kappa-2\kappa} = 1$$

• $p = 4k-1$ and $q = 4\kappa - 1$ and hence:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = (-1)^{(4k-1-1)(4\kappa-1-1)/4} = (-1)^{4k\kappa-2k-2\kappa+1} = -1$$

As we see, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$ when $p = 4k+1$ or/and $q = 4\kappa+1$ while $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$ when both $p = 4k-1$ and $q = 4\kappa - 1$. This means:

⋆ When $p = 4k+1$ or/and $q = 4\kappa+1$ then either both the aforementioned congruences (i.e. $x^2 \overset{p}{=} q$ and $x^2 \overset{q}{=} p$) are solvable or both are non-solvable.

⋆ When $p = 4k-1$ and $q = 4\kappa-1$ then one of these congruences is solvable and the other is non-solvable.

Note: for instance, knowing that $x^2 \overset{6521}{=} 5701$ is solvable and $5701 \overset{4}{=} 1$ we can immediately conclude that $x^2 \overset{5701}{=} 6521$ is also solvable. Similarly, knowing that $x^2 \overset{6367}{=} 5701$ is non-solvable and $5701 \overset{4}{=} 1$ we can immediately conclude that $x^2 \overset{5701}{=} 6367$ is also non-solvable.

On the other hand, knowing that $x^2 \overset{6043}{=} 5711$ is non-solvable and $5711 \overset{4}{=} 6043 \overset{4}{=} -1$ we can immediately conclude that $x^2 \overset{5711}{=} 6043$ is solvable.

1.11 Jacobi's Symbol

This is a generalization of Legendre's symbol (see § 1.8) and is defined as follows:

$$\left(\frac{n}{N}\right) = \begin{cases} +1 & (N = 1) \\ \prod_{i=1}^{k} \left(\frac{n}{p_i}\right)^{a_i} & (N = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}) \end{cases} \tag{15}$$

where N is an odd positive integer, n is an integer coprime to N, and the $\left(\frac{n}{p_i}\right)$'s are Legendre's symbols.

It is important to note the following:

1. The Jacobi symbol takes only the values $+1$ and -1 (since the Legendre symbol takes only these values; see Eq. 15).
2. Following the style of Legendre's symbol, we define Jacobi's symbol to be zero when n and N are not coprime (also see point 6 in the preamble of § 1.8).
3. If $mn \in \mathbb{Z}$ is coprime to N (or each of $m, n \in \mathbb{Z}$ is coprime to N) then:[23]

$$\left(\frac{mn}{N}\right) = \left(\frac{m}{N}\right)\left(\frac{n}{N}\right) \qquad (N \text{ is odd positive integer}) \tag{16}$$

4. If MN is coprime to $n \in \mathbb{Z}$ (or each of M, N is coprime to $n \in \mathbb{Z}$) then:

$$\left(\frac{n}{MN}\right) = \left(\frac{n}{M}\right)\left(\frac{n}{N}\right) \qquad (M, N \text{ are odd positive integers}) \tag{17}$$

5. If $m, n \in \mathbb{Z}$ are coprime to N and $m \overset{N}{=} n$ then:

$$\left(\frac{m}{N}\right) = \left(\frac{n}{N}\right) \qquad (N \text{ is odd positive integer}) \tag{18}$$

6. If M, N are odd coprime positive integers then:

$$\left(\frac{M}{N}\right)\left(\frac{N}{M}\right) = (-1)^{(M-1)(N-1)/4} \tag{19}$$

   This means that the law of quadratic reciprocity (or rather an analogue or generalization of it) applies to Jacobi's symbols as to Legendre's symbols (see § 1.10).
7. The significance of Jacobi's symbol is that:
   • If m is a quadratic residue (mod N) then $\left(\frac{m}{N}\right) = 1$. However, the converse is not true in general, i.e. if $\left(\frac{m}{N}\right) = 1$ then it is not necessary that m is a quadratic residue (mod N). For example, $\left(\frac{10}{237}\right) = 1$ and 10 is a quadratic residue (mod 237), while $\left(\frac{14}{237}\right) = 1$ and 14 is not a quadratic residue (mod 237).
   • If $\left(\frac{m}{N}\right) = -1$ then m is a quadratic non-residue (mod N). In fact, this point is essentially the contraposition of the previous point (noting that Jacobi's symbol is either $+1$ or -1 if we exclude the case of m and N not being coprime).
8. Point 7 highlights an important difference between Legendre's symbol and Jacobi's symbol, i.e. for Legendre's symbol $\left(\frac{n}{p}\right) = +1$ *iff* n is a quadratic residue, while for Jacobi's symbol $\left(\frac{n}{N}\right) = +1$ if n is a quadratic residue. Practically, this means that if we know that n is a quadratic residue (non-residue) then we can conclude that $\left(\frac{n}{p}\right) = +1$ (-1) and vice verse. On the other hand, if we know that n is a quadratic residue then we can conclude that $\left(\frac{n}{N}\right) = +1$ and if we know that $\left(\frac{n}{N}\right) = -1$ then we can conclude that n is a quadratic non-residue $\big[$but if we know that $\left(\frac{n}{N}\right) = +1$ then we cannot conclude that n is a quadratic residue and if we know that n is a quadratic non-residue then we cannot conclude that $\left(\frac{n}{N}\right) = -1\big]$.
9. Jacobi's symbol reduces to Legendre's symbol when N is an odd prime. Accordingly, Legendre's symbol is a special case of Jacobi's symbol and hence the attributes (represented in algebraic relations) of Jacobi's symbol should generally apply to Legendre's symbol (as long as we observe the restriction imposed on the relation between the value of these symbols and quadratic residue which we discussed in points 7 and 8). Therefore, the proofs related to Jacobi's symbol are also proofs to Legendre's symbol (as long as quadratic residues are not involved and the proofs are not dependent on corresponding proofs related to Legendre's symbol).

Problems

1. Calculate the following Jacobi symbols:
   (a) $\left(\frac{21}{6137}\right)$. **(b)** $\left(\frac{45}{98237}\right)$. **(c)** $\left(\frac{66}{4145072814 07}\right)$. **(d)** $\left(\frac{49}{343}\right)$.

[23] This (as well as some of the next points) applies even without the condition of coprimality (but we ignore this trivial case).

Solution:
(**a**) $6137 = 17^1 \times 19^2$ and hence:

$$\left(\frac{21}{6137}\right) = \left(\frac{21}{17}\right)^1 \left(\frac{21}{19}\right)^2 = (+1)(-1)^2 = +1$$

(**b**) $98237 = 193^1 \times 509^1$ and hence:

$$\left(\frac{45}{98237}\right) = \left(\frac{45}{193}\right)^1 \left(\frac{45}{509}\right)^1 = (-1)^1(+1)^1 = -1$$

(**c**) 414507281407 is prime and hence this is a Legendre symbol. Thus $\left(\frac{66}{414507281407}\right) = -1$.
(**d**) 49 and 343 are not coprime and hence $\left(\frac{49}{343}\right) = 0$.

2. Calculate the following Jacobi symbol: $\left(\frac{13}{166182225}\right)$.
Solution: We can calculate this in a straightforward (and rather lengthy) way (as we did in Problem 1) by using Eq. 15. However, we can exploit the properties and algebraic relations of Jacobi and Legendre symbols (which we investigated earlier) to make some (rather essential) simplifications, that is:

$$\left(\frac{13}{166182225}\right) = \left(\frac{166182225}{13}\right) = \left(\frac{1}{13}\right) = +1$$

where in step 1 we used Eq. 19 $\big[$noting that $(13-1)(166182225-1)/4 = 498546672$ which is even and hence $(-1)^{(M-1)(N-1)/4} = 1\big]$, and used property 1 of § 1.8 in step 2 (noting that $166182225 \overset{13}{=} 1$).

3. Justify point 3 in the preamble of this section.
Solution: We note first that the coprimality of mn to N and the coprimality of each of m, n to N are equivalent. Now, if $N = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ then we have (see Eq. 15):

$$\begin{aligned}
\left(\frac{m}{N}\right)\left(\frac{n}{N}\right) &= \left[\prod_{i=1}^{k}\left(\frac{m}{p_i}\right)^{a_i}\right] \times \left[\prod_{i=1}^{k}\left(\frac{n}{p_i}\right)^{a_i}\right] \\
&= \prod_{i=1}^{k}\left[\left(\frac{m}{p_i}\right)^{a_i} \times \left(\frac{n}{p_i}\right)^{a_i}\right] \\
&= \prod_{i=1}^{k}\left[\left(\frac{m}{p_i}\right) \times \left(\frac{n}{p_i}\right)\right]^{a_i} \\
&= \prod_{i=1}^{k}\left(\frac{mn}{p_i}\right)^{a_i} \\
&= \left(\frac{mn}{N}\right)
\end{aligned}$$

where we used property 4 of § 1.8 in line 4, and used Eq. 15 in line 5.

4. Justify point 4 in the preamble of this section.
Solution: We note first that the coprimality of MN to n and the coprimality of each of M, N to n are equivalent. Now, if $M = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and $N = q_1^{b_1} q_2^{b_2} \dots q_s^{b_s}$ then $MN = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} q_1^{b_1} q_2^{b_2} \dots q_s^{b_s}$ and hence (see Eq. 15):

$$\begin{aligned}
\left(\frac{n}{MN}\right) &= \left(\frac{n}{p_1}\right)^{a_1} \times \left(\frac{n}{p_2}\right)^{a_2} \times \dots \times \left(\frac{n}{p_k}\right)^{a_k} \times \left(\frac{n}{q_1}\right)^{b_1} \times \left(\frac{n}{q_2}\right)^{b_2} \times \dots \times \left(\frac{n}{q_s}\right)^{b_s} \\
&= \left[\left(\frac{n}{p_1}\right)^{a_1} \times \left(\frac{n}{p_2}\right)^{a_2} \times \dots \times \left(\frac{n}{p_k}\right)^{a_k}\right] \times \left[\left(\frac{n}{q_1}\right)^{b_1} \times \left(\frac{n}{q_2}\right)^{b_2} \times \dots \times \left(\frac{n}{q_s}\right)^{b_s}\right] \\
&= \left(\frac{n}{M}\right)\left(\frac{n}{N}\right)
\end{aligned}$$

5. Justify point 5 in the preamble of this section.
Solution: If $N = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$ then $m \overset{p_i}{=} n$ $(i = 1, 2, \dots, k)$ where this is justified by $m \overset{N}{=} n$.[24] Therefore, from point 1 of § 1.8 we get:

$$\left(\frac{m}{p_i}\right) = \left(\frac{n}{p_i}\right) \qquad \rightarrow \qquad \left(\frac{m}{p_i}\right)^{a_i} = \left(\frac{n}{p_i}\right)^{a_i} \qquad (i = 1, 2, \dots, k)$$

Now, if we multiply these equations side by side and use Eq. 15 then we get:

$$\prod_{i=1}^{k}\left(\frac{m}{p_i}\right)^{a_i} = \prod_{i=1}^{k}\left(\frac{n}{p_i}\right)^{a_i} \qquad \rightarrow \qquad \left(\frac{m}{N}\right) = \left(\frac{n}{N}\right)$$

6. Prove (the two parts of) point 7 in the preamble of this section.
Solution: We have two parts to prove:
• If m is a quadratic residue (mod N) then $\left(\frac{m}{N}\right) = 1$: let $N = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$ noting that all p_i $(i = 1, 2, \dots, k)$ are odd primes because N is odd (according to the definition of Jacobi's symbol). Now, since m is a quadratic residue (mod N) then $x^2 \overset{N}{=} m$ is solvable, i.e. there is $x \in \mathbb{Z}$ (call it X) such that:

$$X^2 \overset{p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}}{=} m \qquad \rightarrow \qquad X^2 \overset{p_i}{=} m \quad (i = 1, 2, \dots, k)$$

where this can be more easily understood in terms of divisibility.[25] This means that m is a quadratic residue (mod p_i) and hence $\left(\frac{m}{p_i}\right) = 1$ (noting that we are using here Legendre's symbol not Jacobi's symbol because p_i is prime). Hence, from Eq. 15 we get $\left(\frac{m}{N}\right) = 1$ since all $\left(\frac{m}{p_i}\right)$ are 1.
We prove that the converse is not true by the method of proof by example (see § 1.5.4 of V1) since we have many examples (e.g. the example given in the preamble) where the converse does not hold true.
• If $\left(\frac{m}{N}\right) = -1$ then m is a quadratic non-residue (mod N): as indicated in the preamble, this part is essentially the contraposition of the previous part and hence it is true by contraposition, i.e. it does not require another (or independent) proof (see § 1.1 of V1 as well as § 1.5.4 of V1).
7. Show that if N is an odd positive integer then:

$$\left(\frac{-1}{N}\right) = (-1)^{(N-1)/2}$$

Solution: If $N = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$ then we have:

$$\left(\frac{-1}{N}\right) = \prod_{i=1}^{k}\left(\frac{-1}{p_i}\right)^{a_i} = \prod_{i=1}^{k}\left[(-1)^{(p_i-1)/2}\right]^{a_i} = \prod_{i=1}^{k}(-1)^{a_i(p_i-1)/2} = (-1)^{\sum_{i=1}^{k}a_i(p_i-1)/2} \tag{20}$$

where we used Eq. 15 in step 1 and used property 2 of § 1.8 in step 2 (noting that N is odd and hence each p_i is an odd prime).
We also have:

$$p_i^{a_i} = [1 + (p_i - 1)]^{a_i} = 1 + a_i(p_i - 1) + \sum_{j=2}^{a_i} C_j^{a_i}(p_i - 1)^j \overset{4}{=} 1 + a_i(p_i - 1) \tag{21}$$

where in step 2 we used the binomial theorem while in step 3 we used the fact that $(p_i - 1)$ is even and hence $(p_i - 1)^j$ is divisible by 4 for $j \geq 2$. Thus:

$$N = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k} \overset{4}{=} \big[1 + a_1(p_1 - 1)\big]\big[1 + a_2(p_2 - 1)\big]\dots\big[1 + a_k(p_k - 1)\big] \overset{4}{=} 1 + \sum_{i=1}^{k} a_i(p_i - 1)$$

---

[24] This is because $m \overset{N}{=} n$ means N (which is equal to $p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$) divides $m - n$ and hence each p_i must divide $m - n$, i.e. $m \overset{p_i}{=} n$.

[25] The congruence $X^2 \overset{p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}}{=} m$ is equivalent to $(p_1^{a_1}p_2^{a_2}\dots p_k^{a_k})|(X^2 - m)$, and this implies $p_i|(X^2 - m)$ which is equivalent to $X^2 \overset{p_i}{=} m$.

where step 2 is from Eq. 21 while step 3 is because all non-linear terms are 0 (mod 4) since $(p_i - 1)$ is even. Hence (see rule 9 of § 2.7 of V1):

$$N - 1 \overset{4}{=} \sum_{i=1}^{k} a_i(p_i - 1) \qquad \rightarrow \qquad \frac{N-1}{2} \overset{2}{=} \sum_{i=1}^{k} \frac{a_i(p_i-1)}{2}$$

i.e. $(N-1)/2$ and $\sum_{i=1}^{k} a_i(p_i-1)/2$ have the same parity and hence $(-1)^{\sum_{i=1}^{k} a_i(p_i-1)/2} = (-1)^{(N-1)/2}$. So, from Eq. 20 we conclude:

$$\left(\frac{-1}{N}\right) = (-1)^{(N-1)/2}$$

8. Show that if N is an odd positive integer then:

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

Solution: If N is prime then this is no more than property 3 of § 1.8 (which we proved in Problem 3 of § 1.9). So, let assume that N is a composite whose prime factorization is $N = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Accordingly:

$$\left(\frac{2}{N}\right) = \prod_{i=1}^{k} \left(\frac{2}{p_i}\right)^{a_i} = \prod_{i=1}^{k} \left[(-1)^{(p_i^2-1)/8}\right]^{a_i} = \prod_{i=1}^{k} (-1)^{a_i(p_i^2-1)/8} = (-1)^{\sum_{i=1}^{k} a_i(p_i^2-1)/8} \tag{22}$$

where we used Eq. 15 in step 1 and used property 3 of § 1.8 in step 2.
We also have:

$$\left[p_i^2\right]^{a_i} = \left[1 + (p_i^2 - 1)\right]^{a_i} = 1 + a_i(p_i^2 - 1) + \sum_{j=2}^{a_i} C_j^{a_i} (p_i^2 - 1)^j \overset{64}{=} 1 + a_i(p_i^2 - 1) \tag{23}$$

where in step 2 we used the binomial theorem while in step 3 we used the fact that $(p_i^2 - 1)$ is divisible by 8 and hence $(p_i^2 - 1)^j$ is divisible by 64 for $j \geq 2$.[26] Thus:

$$\begin{aligned} N^2 &= \left[p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}\right]^2 = \left[p_1^2\right]^{a_1} \left[p_2^2\right]^{a_2} \dots \left[p_k^2\right]^{a_k} \\ &\overset{64}{=} \left[1 + a_1(p_1^2 - 1)\right] \left[1 + a_2(p_2^2 - 1)\right] \dots \left[1 + a_k(p_k^2 - 1)\right] \overset{64}{=} 1 + \sum_{i=1}^{k} a_i(p_i^2 - 1) \end{aligned}$$

where step 3 is from Eq. 23 while step 4 is because all non-linear terms are 0 (mod 64) since $(p_i^2 - 1)$ is divisible by 8. Hence (see rule 9 of § 2.7 of V1 noting that since 8 divides $p_i^2 - 1$ then it must divide $N^2 - 1$):

$$N^2 - 1 \overset{64}{=} \sum_{i=1}^{k} a_i(p_i^2 - 1) \qquad \rightarrow \qquad \frac{N^2-1}{8} \overset{8}{=} \sum_{i=1}^{k} \frac{a_i(p_i^2-1)}{8}$$

This implies that $(N^2-1)/8$ and $\sum_{i=1}^{k} a_i(p_i^2-1)/8$ have the same parity[27] and hence $(-1)^{\sum_{i=1}^{k} a_i(p_i^2-1)/8} = (-1)^{(N^2-1)/8}$. So, from Eq. 22 we conclude:

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

---

[26] As we noted earlier, from the arithmetic series formula we have $\sum_{i=1}^{(p-1)/2} i = (p^2-1)/8$ and hence $(p^2-1)/8$ is an integer which implies $8|(p^2 - 1)$. Alternatively, any odd prime is of the form $4k \pm 1$ ($k \in \mathbb{N}$) and hence $(p^2 - 1)/8 = 2k^2 \pm k$ (which are integers).

[27] It is obvious that:

$$\frac{N^2-1}{8} \overset{8}{=} \sum_{i=1}^{k} \frac{a_i(p_i^2-1)}{8} \qquad \text{means 8 divides} \qquad \left[\frac{N^2-1}{8}\right] - \left[\sum_{i=1}^{k} \frac{a_i(p_i^2-1)}{8}\right]$$

Now, if $(N^2 - 1)/8$ and $\sum_{i=1}^{k} a_i(p_i^2 - 1)/8$ have opposite parity then their difference will be odd and hence it cannot be divisible by 8 which is even.

9. Show the following:
   (**a**) $\left(\frac{m}{N}\right)\left(\frac{m}{N}\right)=1$. (**b**) $\left(\frac{m^2}{N}\right)=\left(\frac{m}{N}\right)\left(\frac{m}{N}\right)$. (**c**) $\left(\frac{m}{N^2}\right)=\left(\frac{m}{N}\right)\left(\frac{m}{N}\right)$. (**d**) $\left(\frac{m^2}{N}\right)=\left(\frac{m}{N^2}\right)$.
   Solution: All these relations can be proved in one go, that is:

$$1=\left(\frac{m}{N}\right)\left(\frac{m}{N}\right)=\left(\frac{m^2}{N}\right)=\left(\frac{m}{N^2}\right)$$

   (**a**) $\left(\frac{m}{N}\right)\left(\frac{m}{N}\right)=1$ is because $\left(\frac{m}{N}\right)$ is either $+1$ or -1.
   (**b**) $\left(\frac{m^2}{N}\right)=\left(\frac{m}{N}\right)\left(\frac{m}{N}\right)$ is from property 3 (see the preamble and Problem 3).
   (**c**) $\left(\frac{m}{N^2}\right)=\left(\frac{m}{N}\right)\left(\frac{m}{N}\right)$ is from property 4 (see the preamble and Problem 4).
   (**d**) $\left(\frac{m^2}{N}\right)=\left(\frac{m}{N^2}\right)$ is just a combination of (b) and (c).
10. Find all the integers m which are coprime to 33 and $\left(\frac{m}{33}\right)=1$.
    Solution: We have (see Eq. 15 noting that $33=3^1\times 11^1$):

$$\left(\frac{m}{33}\right)=\left(\frac{m}{3}\right)^1\left(\frac{m}{11}\right)^1$$

    Now, the quadratic residue of 3 is 1, and the quadratic non-residue of 3 is 2. Hence, $\left(\frac{m}{3}\right)=+1$ for $m\overset{3}{=}1$ and $\left(\frac{m}{3}\right)=-1$ for $m\overset{3}{=}2$ (see § 1.6 and § 1.8).
    Similarly, $\left(\frac{m}{11}\right)=+1$ for $m\overset{11}{=}1,3,4,5,9$ and $\left(\frac{m}{11}\right)=-1$ for $m\overset{11}{=}2,6,7,8,10$ (see Problem 7 of § 1.8).
    Now, if we combine these cases we get all the possibilities for the product $\left(\frac{m}{3}\right)^1\left(\frac{m}{33}\right)^1$ and hence $\left(\frac{m}{33}\right)$, that is:

		$\left(\frac{m}{11}\right)$									
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
$\left(\frac{m}{3}\right)$	**1**	$+1$	-1	$+1$	$+1$	$+1$	-1	-1	-1	$+1$	-1
	2	-1	$+1$	-1	-1	-1	$+1$	$+1$	$+1$	-1	$+1$

    So, we have $\left(\frac{m}{33}\right)=+1$ in the following cases:
    $m\overset{3}{=}1$ & $m\overset{11}{=}1$ $m\overset{3}{=}1$ & $m\overset{11}{=}3$ $m\overset{3}{=}1$ & $m\overset{11}{=}4$ $m\overset{3}{=}1$ & $m\overset{11}{=}5$ $m\overset{3}{=}1$ & $m\overset{11}{=}9$
    $m\overset{3}{=}2$ & $m\overset{11}{=}2$ $m\overset{3}{=}2$ & $m\overset{11}{=}6$ $m\overset{3}{=}2$ & $m\overset{11}{=}7$ $m\overset{3}{=}2$ & $m\overset{11}{=}8$ $m\overset{3}{=}2$ & $m\overset{11}{=}10$
    Now, if we solve these 10 systems of congruence equations (using for instance the Chinese remainder theorem) then we get:
    $m\overset{33}{=}1$ $m\overset{33}{=}25$ $m\overset{33}{=}4$ $m\overset{33}{=}16$ $m\overset{33}{=}31$ $m\overset{33}{=}2$ $m\overset{33}{=}17$ $m\overset{33}{=}29$ $m\overset{33}{=}8$ $m\overset{33}{=}32$
    So, these are all the integers m which are coprime to 33 and $\left(\frac{m}{33}\right)=1$.
11. Find all the integers m which are coprime to 33 and m is a quadratic residue of 33.
    Solution: Referring to points 7 and 8 in the preamble, the quadratic residues of 33 must be among those m whose Jacobi symbol is 1. So, although having a Jacobi symbol of value 1 is not sufficient to determine if m is a quadratic residue or not, we can still make use of our results in Problem 10 by searching for the quadratic residues of 33 among only those m whose Jacobi symbol is 1.
    On investigating the quadratic congruence $x^2\overset{33}{=}m$ for $m\overset{33}{=}1,2,4,8,16,17,25,29,31,32$ we find that this congruence is solvable only for $m\overset{33}{=}1,4,16,25,31$. So, these are the quadratic residues modulo 33 among the integers which are coprime to 33.
12. Give an example of an odd positive integer N whose Jacobi symbol $\left(\frac{m}{N}\right)$ is $+1$ for all $m\in\mathbb{Z}$ (where m and N are coprime).
    Solution: N is a perfect square (which includes any integer that is an even natural power of an integer) should do (as can be seen from Eq. 15).
13. Solve (and analyze the implications of) the following equation involving Jacobi's symbols (i.e. a is an

integer coprime to the odd positive integers M and N):

$$\left(\frac{a}{M}\right)\left(\frac{a}{N}\right) = \left(\frac{a}{M}\right) + \left(\frac{a}{N}\right) + 3$$

Solution: We have 4 cases:
- $\left(\frac{a}{M}\right) = \left(\frac{a}{N}\right) = 1$ and hence $1 = 5$ which is not acceptable.
- $\left(\frac{a}{M}\right) = \left(\frac{a}{N}\right) = -1$ and hence $1 = 1$ which is acceptable.
- $\left(\frac{a}{M}\right) = 1$ and $\left(\frac{a}{N}\right) = -1$ and hence $-1 = 3$ which is not acceptable.
- $\left(\frac{a}{M}\right) = -1$ and $\left(\frac{a}{N}\right) = 1$ and hence $-1 = 3$ which is not acceptable.

So in brief, only $\left(\frac{a}{M}\right) = \left(\frac{a}{N}\right) = -1$ is acceptable and hence the solution of the given equation is: every integer a (coprime to M and N) which is a quadratic non-residue of both M and N (see points 7 and 8 in the preamble).

1.12 Mobius Inversion

Mobius inversion can be summarized in the following conditional statement:

$$F(n) = \sum_{d|n} f(d) \qquad \rightarrow \qquad f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) \qquad (n \in \mathbb{N}) \tag{24}$$

Problems

1. Prove the Mobius inversion formula which is given by:

$$f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) \qquad (n \in \mathbb{N})$$

where μ is the Mobius function and F is the summatory function of f, i.e. $F(n) = \sum_{d|n} f(d)$.[28]
Solution: We have:

$$\sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{\delta|(n/d)} f(\delta) = \sum_{d|n} \sum_{\delta|(n/d)} \mu(d)\, f(\delta) \tag{25}$$

where we used the definition of summatory function (which is given above) in the first step. Now, let us analyze the double sum in the last step of this equation. This double sum means that we take all the (product) combinations of $\mu(d)$ and $f(\delta)$ where d represents all the divisors of n while δ represents all the divisors of n/d. In other words, we need to loop over all the divisors (i.e. d) of n in combination with all the divisors of n/d (i.e. δ). However, if we note that "all the divisors of n" are the same as "all the divisors of n/d" (noting that d is looping over all the divisors of n from 1 to n inclusive) then this double loop (representing the double sum) can be done equivalently (although the order of the generated combinations generally differs) by taking all the (product) combinations of $\mu(\delta)$ and $f(d)$ and hence we can continue Eq. 25 as follows:

$$\begin{aligned}\sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{\delta|(n/d)} f(\delta) = \sum_{d|n} \sum_{\delta|(n/d)} \mu(d)\, f(\delta) = \sum_{d|n} \sum_{\delta|(n/d)} \mu(\delta)\, f(d) \\ &= \left[\sum_{d|n} f(d)\right]\left[\sum_{\delta|(n/d)} \mu(\delta)\right]\end{aligned}$$

Now, $\sum_{\delta|(n/d)} \mu(\delta) = 0$ (see Problem 3 of § 2.6.5 of V1) except when $n/d = 1$ (i.e. $d = n$) and hence:

$$\left[\sum_{d|n} f(d)\right]\left[\sum_{\delta|(n/d)} \mu(\delta)\right] = \left[\sum_{n|n} f(n)\right]\left[\sum_{\delta|(n/n)} \mu(\delta)\right] = \Big[f(n)\Big]\left[\sum_{\delta|1} \mu(\delta)\right]$$

[28] For more details about the "summatory function", see Problem 15 of § 10.

$$= \quad \Big[f(n)\Big]\left[\sum_{1}\mu(1)\right] = f(n)\times 1 = f(n)$$

which completes the proof.
It is worth noting (see Eq. 24) that the Mobius inversion formula may be given as:

$$f(n) = \sum_{d|n}\mu\Big(\frac{n}{d}\Big)\ F(d)$$

since both d and n/d represent all the divisors of n since each divisor d is matched by a corresponding divisor n/d noting that $d\times(n/d) = n$ (see Problem 19 of § 1.9 of V1).

2. Verify the Mobius inversion formula with regard to:
(**a**) The divisor function $\sigma(n)$. (**b**) The tau function $\tau(n)$.
Solution:
(**a**) $\sigma(n)$ is the summatory function of $f(d) = d$. Hence:

$$\begin{aligned}\sum_{d|n}\mu(d)\,F\Big(\frac{n}{d}\Big) &= \sum_{d|n}\mu(d)\,\sigma\Big(\frac{n}{d}\Big) = \sum_{d|n}\mu(d)\sum_{\delta|(n/d)}f(\delta) = \sum_{d|n}\mu(d)\sum_{\delta|(n/d)}\delta = \sum_{d|n}\sum_{\delta|(n/d)}\mu(d)\,\delta\\ &= \sum_{d|n}\sum_{\delta|(n/d)}\mu(\delta)\,d = \left[\sum_{d|n}d\right]\left[\sum_{\delta|(n/d)}\mu(\delta)\right] = \left[\sum_{n|n}n\right]\times 1 = n\times 1 = n = f(n)\end{aligned}$$

where the explanations are as given in Problem 1.
(**b**) $\tau(n)$ is the summatory function of $f(d) = 1$. Hence:

$$\begin{aligned}\sum_{d|n}\mu(d)\,F\Big(\frac{n}{d}\Big) &= \sum_{d|n}\mu(d)\,\tau\Big(\frac{n}{d}\Big) = \sum_{d|n}\mu(d)\sum_{\delta|(n/d)}f(\delta) = \sum_{d|n}\mu(d)\sum_{\delta|(n/d)}1 = \sum_{d|n}\sum_{\delta|(n/d)}\mu(d)\times 1\\ &= \sum_{d|n}\sum_{\delta|(n/d)}\mu(\delta)\times 1 = \left[\sum_{d|n}1\right]\left[\sum_{\delta|(n/d)}\mu(\delta)\right] = \left[\sum_{n|n}1\right]\times 1 = 1\times 1 = 1 = f(n)\end{aligned}$$

where the explanations are as given in Problem 1.

3. Derive the formula $\phi(p^a) = p^a - p^{a-1}$ (see Eq. 42 in V1) by using the Mobius inversion formula.
Solution: Let $n = p^a$ and hence:

$$n = p^a = \sum_{d|p^a}\phi(d) = \sum_{k=0}^{a}\phi(p^k) \tag{26}$$

where step 2 is from Eq. 45 of V1 (with $n = p^a$; also see Problem 1 of § 2.6.4 of V1), while step 3 is because the divisors of p^a are $p^0, p^1, \ldots, p^a$. Now, we have:

$$\begin{aligned}\phi(p^a) &= \sum_{d|p^a}\mu(d)\,F\left(\frac{p^a}{d}\right) = \sum_{k=0}^{a}\mu(p^k)\,F\left(\frac{p^a}{p^k}\right) = \sum_{k=0}^{a}\mu(p^k)\,F(p^{a-k}) = \sum_{k=0}^{a}\mu(p^k)\,p^{a-k}\\ &= \mu(p^0)\,p^{a-0} + \mu(p^1)\,p^{a-1} + \mu(p^2)\,p^{a-2} + \cdots + \mu(p^a)\,p^{a-a}\\ &= p^a - p^{a-1} + 0 + \cdots + 0 = p^a - p^{a-1}\end{aligned}$$

where:
step 1 is from the Mobius inversion formula,
step 2 is because the divisors of p^a are $p^0, p^1, \ldots, p^a$,
step 4 is from Eq. 26 $\big[$i.e. $F(p^{a-k}) \equiv \sum_{d|p^{a-k}}\phi(d) = \sum_{i=0}^{a-k}\phi(p^i) = p^{a-k}\big]$, and
step 6 is because $\mu(p^0) = \mu(1) = 1$ and $\mu(p^1) = (-1)^1 = -1$ while $\mu(p^2) = \ldots = \mu(p^a) = 0$ (since they are not square free).

Chapter 2
Miscellaneous

1. Determine the parity of $a^m + b^n + c^k$ for all $a, b, c \in \mathbb{Z}$ and all $m, n, k \in \mathbb{N}^0$.
   Solution: We note first that we consider 0^0 as undefined and hence any case of 0^0 is not considered in the following. Now, let represent the parity of a, b, c (as well as the parity of $a^m + b^n + c^k$) with e for even and o for odd. Also, let represent m, n, k with 0 when m, n, k is 0 and ignore its symbol otherwise (e.g. e^0o^0e represents the case when a, b, c is even, odd, even with $m = n = 0$ and $k \neq 0$ noting that e^0o^0e represents sum not product). Accordingly, the parity of $a^m+b^n+c^k$ is given by the following table:

$e^0e^0e^0=o$	$e^0e^0o^0=o$	$e^0o^0e^0=o$	$e^0o^0o^0=o$	$o^0e^0e^0=o$	$o^0e^0o^0=o$	$o^0o^0e^0=o$	$o^0o^0o^0=o$
$e^0e^0e=e$	$e^0e^0o=o$	$e^0o^0e=e$	$e^0o^0o=o$	$o^0e^0e=e$	$o^0e^0o=o$	$o^0o^0e=e$	$o^0o^0o=o$
$e^0ee^0=e$	$e^0eo^0=e$	$e^0oe^0=o$	$e^0oo^0=o$	$o^0ee^0=e$	$o^0eo^0=e$	$o^0oe^0=o$	$o^0oo^0=o$
$ee^0e^0=e$	$ee^0o^0=e$	$eo^0e^0=e$	$eo^0o^0=e$	$oe^0e^0=o$	$oe^0o^0=o$	$oo^0e^0=o$	$oo^0o^0=o$
$e^0ee=o$	$e^0eo=e$	$e^0oe=e$	$e^0oo=o$	$o^0ee=o$	$o^0eo=e$	$o^0oe=e$	$o^0oo=o$
$ee^0e=o$	$ee^0o=e$	$eo^0e=o$	$eo^0o=e$	$oe^0e=e$	$oe^0o=o$	$oo^0e=e$	$oo^0o=o$
$eee^0=o$	$eeo^0=o$	$eoe^0=e$	$eoo^0=e$	$oee^0=e$	$oeo^0=e$	$ooe^0=o$	$ooo^0=o$
$eee=e$	$eeo=o$	$eoe=o$	$eoo=e$	$oee=o$	$oeo=e$	$ooe=e$	$ooo=o$

2. Find all $n \in \mathbb{Z}$ such that $P_1 = P_2 = P_3 = P_4 = P_5$ where:

$$\begin{aligned} P_1(n) &= n^5 - 96n^4 + 2752n^3 - 16950n^2 - 221777n + 2104724 \\ P_2(n) &= n^5 - 96n^4 + 2860n^3 - 22350n^2 - 214541n + 2685980 \\ P_3(n) &= -n^5 + 110n^4 - 3526n^3 + 21588n^2 + 292167n - 2437684 \\ P_4(n) &= -n^5 + 136n^4 - 4452n^3 + 4630n^2 + 457157n - 424816 \\ P_5(n) &= -n^4 - 31n^3 + 3983n^2 - 10809n - 403288 \end{aligned}$$

   Solution: If $P_1 = P_2 = P_3 = P_4 = P_5$ then:
   $P_1 = P_2$ & $P_1 = P_3$ & $P_1 = P_4$ & $P_1 = P_5$
   So, it is a problem of solving a system of univariate equations (see § 3.3 of V1). On solving the following system:
   $P_1 - P_2 = 0$ $P_1 - P_3 = 0$ $P_1 - P_4 = 0$ $P_1 - P_5 = 0$
   we get: $n = -9, 13, 46$. So, we have $P_1 = P_2 = P_3 = P_4 = P_5$ for these values of n.
3. Determine the sign of the polynomial $f(n) = -n^5+58n^4+462n^3-4913n^2-4972n-5376$ for all $n \in \mathbb{Z}$.
   Solution: If we factorize $f(n)$ to its simplest factors (i.e. linear and non factorizable quadratic) then we get:

$$f(n) = (n + 12)(7 - n)(n - 64)(n^2 + n + 1)$$

   We can now build the following sign table:

$\boldsymbol{n =}$	$\boldsymbol{< -12}$	$\boldsymbol{-12}$		$\boldsymbol{7}$		$\boldsymbol{64}$	$\boldsymbol{> 64}$
$\boldsymbol{n + 12}$	$-$	0	$+$	$+$	$+$	$+$	$+$
$\boldsymbol{7 - n}$	$+$	$+$	$+$	0	$-$	$-$	$-$
$\boldsymbol{n - 64}$	$-$	$-$	$-$	$-$	$-$	0	$+$
$\boldsymbol{n^2 + n + 1}$	$+$	$+$	$+$	$+$	$+$	$+$	$+$
$\boldsymbol{f(n)}$	$+$	0	$-$	0	$+$	0	$-$

As we see, the sign of $f(n)$ is given in the last row, i.e. $f(n)$ is positive for $n < -12$ and $7 < n < 64$, $f(n)$ is negative for $-12 < n < 7$ and $n > 64$, and $f(n) = 0$ for $n = -12, 7, 64$.

4. Find a formula for the number of sets N_s of (distinct) natural numbers of size k (≥ 2) whose sum of elements is equal to a given natural number N_n.
Solution: We have at least three methods to tackle this Problem: the use of generating function, the use of recursive formula and the use of combinatorics argument. In the following, we discuss the first method and only give the result of the second method.[29]
For $N_n < \sum_{i=1}^{k} i$ we have zero set, and hence in the following we assume $N_n \geq \sum_{i=1}^{k} i$. Now, let $N_0 = \sum_{i=1}^{k} i$ and $N_n = N_0 + n$ (where $n = 0, 1, 2, \ldots$). The generating function f_g of the sequence of N_s for a given k is given by:

$$f_g(z,k) = \frac{1}{\prod_{j=1}^{k}(1-z^j)}$$

For example:

$$f_g(z,2) = \frac{1}{(1-z)(1-z^2)} \qquad f_g(z,3) = \frac{1}{(1-z)(1-z^2)(1-z^3)}$$

Accordingly, the number of sets $N_s(k, N_n)$ (i.e. N_s as a function of k and N_n) are given by the coefficients c_n of the series expansion of the generating function $f_g(z,k)$ at $z = 0$ (i.e. Taylor series). For instance, the Taylor series of $f_g(z,3)$ is given by:

$$f_g(z,3) = 1 + z + 2z^2 + 3z^3 + 4z^4 + 5z^5 + 7z^6 + 8z^7 + 10z^8 + 12z^9 + 14z^{10} + \cdots$$

and hence (noting that for $k = 3$ we have $N_0 = 1 + 2 + 3 = 6$ and thus $N_4 = 10$ and $N_9 = 15$) we have:

$$N_s(3,6) = c_0 = 1 \qquad N_s(3,10) = c_4 = 4 \qquad N_s(3,15) = c_9 = 12$$

Regarding the recursive formula we say the following: for $N_n = N_0, N_1, \ldots, N_{k-1}$ we have

$$N_s(k, N_n) = N_s(k-1, N_n)$$

(where we should note the difference in the meaning of N_n on the two sides because of the dependency of N_n on k) while for $N_n > N_{k-1}$ we have:

$$N_s(k, N_n) = N_s(k-1, N_n) + N_s(k, N_{n-k})$$

5. Referring to Problem 4, find all the sets of (distinct) natural numbers of:
(**a**) Size 4 with sum 15. (**b**) Size 7 with sum 32. (**c**) Size 8 with sum 35.
Solution:
(**a**) We have: $k = 4$, $N_0 = 1 + 2 + 3 + 4 = 10$ and $N_n = 15$ and hence $n = N_n - N_0 = 15 - 10 = 5$. The coefficient c_5 of the Taylor series of $f_g(z,4)$ is 6 and hence $N_s(4,15) = c_5 = 6$. These 6 sets are:
{1,2,3,9} {1,2,4,8} {1,2,5,7} {1,3,4,7} {1,3,5,6} {2,3,4,6}
(**b**) We have: $k = 7$, $N_0 = 1+2+3+4+5+6+7 = 28$ and $N_n = 32$ and hence $n = N_n - N_0 = 32 - 28 = 4$. The coefficient c_4 of the Taylor series of $f_g(z,7)$ is 5 and hence $N_s(7,32) = c_4 = 5$. These 5 sets are:
{1,2,3,4,5,6,11} {1,2,3,4,5,7,10} {1,2,3,4,5,8,9} {1,2,3,4,6,7,9} {1,2,3,5,6,7,8}
(**c**) We have: $k = 8$, $N_0 = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 = 36$ and $N_n = 35$. Since $N_n < N_0$ we have zero set, i.e. $N_s(8,35) = 0$.

[29] The combinatorics method is rather messy and requires lengthy explanation and hence we leave it (noting that we may discuss it in the future). We refer the reader to the literature about the topics of sequence representation and generation using the generating function and z-transform techniques (noting that these topics are out of scope of our book which is about number theory).

6. Find all the partitions of the following set into two disjoint subsets such that the product of the members of one subset is equal to the product of the members of the other subset:

$$\{49, 27, 3125, 32, 243, 8, 343, 9, 16807, 25, 125, 4\}$$

Solution: We prime-factorize these numbers so that we can group and partition them in a way that ensures that the number of prime factors (i.e. of any given prime number) in each subset is the same as the number of prime factors in the other subset, that is:

$$\{7^2, 3^3, 5^5, 2^5, 3^5, 2^3, 7^3, 3^2, 7^5, 5^2, 5^3, 2^2\}$$

So we must have $2^2, 2^3$ (i.e. 4, 8) in one subset and 2^5 (i.e. 32) in the other, $3^2, 3^3$ (i.e. 9, 27) in one subset and 3^5 (i.e. 243) in the other, $5^2, 5^3$ (i.e. 25, 125) in one subset and 5^5 (i.e. 3125) in the other, and $7^2, 7^3$ (i.e. 49, 343) in one subset and 7^5 (i.e. 16807) in the other. So, we can do this partitioning in 8 possible ways, i.e.

$\{4, 8, 9, 27, 25, 125, 49, 343\}\{32, 243, 3125, 16807\}$ $\{4, 8, 9, 27, 25, 125, 16807\}\{32, 243, 3125, 49, 343\}$

$\{4, 8, 243, 25, 125, 49, 343\}\{32, 9, 27, 3125, 16807\}$ $\{4, 8, 243, 25, 125, 16807\}\{32, 9, 27, 3125, 49, 343\}$

$\{4, 8, 9, 27, 3125, 49, 343\}\{32, 243, 25, 125, 16807\}$ $\{4, 8, 9, 27, 3125, 16807\}\{32, 243, 25, 125, 49, 343\}$

$\{4, 8, 243, 3125, 49, 343\}\{32, 9, 27, 25, 125, 16807\}$ $\{4, 8, 243, 3125, 16807\}\{32, 9, 27, 25, 125, 49, 343\}$

7. Find all natural numbers of the form $n^2 + 3n + 1$ which terminate in 2021 (where $n \in \mathbb{N}^0$).

Solution: These numbers are the solutions of the congruence equation $n^2 + 3n + 1 \overset{10000}{=} 2021$, i.e. $n = m + 10000k$ where $m = 2732, 4140, 5857, 7265$ and $k \in \mathbb{N}^0$.

8. Propose a simple way for the prime factorization of factorials (which should be very useful, and possibly the only practical way, for the prime factorization of very large factorials).

Solution: We propose using the formula of the highest power of a prime p that divides $n!$ (see Eq. 83 in V1) where p represents all the primes which are less than or equal to n. These calculations can be easily done using a spreadsheet or a few lines of computer code. For example, let us find the prime factorization of 123!.

On using the aforementioned formula (with p representing all the 30 primes which are less than 123, i.e. $2, 3, 5, \ldots, 107, 109, 113$) we obtain the following prime factorization:

$123! = 2^{117} \times 3^{59} \times 5^{28} \times 7^{19} \times 11^{12} \times 13^9 \times 17^7 \times 19^6 \times 23^5 \times 29^4 \times 31^3 \times 37^3 \times 41^3 \times 43^2 \times 47^2 \times 53^2 \times 59^2 \times 61^2 \times 67 \times 71 \times 73 \times 79 \times 83 \times 89 \times 97 \times 101 \times 103 \times 107 \times 109 \times 113.$

9. Propose a simple way for calculating the number of digits of factorials (which should be very useful, and possibly the only practical way, for calculating the number of digits of very large factorials).

Solution: The simplest way is to use the rules of logarithms, that is:

$$\log_{10}(n!) = \log_{10}\left(\prod_{k=1}^{n} k\right) = \sum_{k=1}^{n} \log_{10}(k)$$

where the latter sum can be easily calculated using a spreadsheet or a few lines of computer code. Hence, the number of digits in $n!$ is:

$$\left\lfloor \sum_{k=1}^{n} \log_{10}(k) \right\rfloor + 1$$

For example, the number of digits of 1000! is:

$$\left\lfloor \sum_{k=1}^{1000} \log_{10}(k) \right\rfloor + 1 = \lfloor 2567.604644 \rfloor + 1 = 2568$$

10. What is the number of digits in $\widehat{5}$?

Solution: We have:

$$\widehat{5} \equiv 5^{4^{3^2}} = 5^{4^9} = 5^{262144}$$

Hence, the number of digits in $\widehat{5}$ is:

$$\left\lfloor \log_{10} \widehat{5} \right\rfloor + 1 = \lfloor 262144 \times \log_{10} 5 \rfloor + 1 = \lfloor 183230.7928 \rfloor + 1 = 183231$$

11. What is the number of digits in P_r^n and C_r^n (where P_r^n is the number of permutations and C_r^n is the binomial coefficient).
Solution: Regarding P_r^n we have:

$$P_r^n = \frac{n!}{(n-r)!} = n \times (n-1) \times \cdots \times (n-r+1)$$

Hence, the number of digits of P_r^n is:

$$\left\lfloor \sum_{k=n-r+1}^{n} \log_{10}(k) \right\rfloor + 1$$

For example, the number of digits of P_{288}^{723} is:

$$\left\lfloor \sum_{k=723-288+1}^{723} \log_{10}(k) \right\rfloor + 1 = \left\lfloor \sum_{k=436}^{723} \log_{10}(k) \right\rfloor + 1 = \lfloor 794.448 \rfloor + 1 = 795$$

Regarding C_r^n we have:

$$C_r^n = \frac{n!}{r!(n-r)!} = \frac{n \times (n-1) \times \cdots \times (n-r+1)}{r!}$$

Hence, the number of digits of C_r^n is:

$$\left\lfloor \sum_{k=n-r+1}^{n} \log_{10}(k) - \sum_{k=1}^{r} \log_{10}(k) \right\rfloor + 1$$

For example, the number of digits of C_{1562}^{2109} is:

$$\left\lfloor \sum_{k=548}^{2109} \log_{10}(k) - \sum_{k=1}^{1562} \log_{10}(k) \right\rfloor + 1 = \lfloor 4834.723 - 4312.157741 \rfloor + 1 = \lfloor 522.566 \rfloor + 1 = 523$$

12. Find every 10-digit integer the sum of its digits is equal to the product of its digits.
Solution: Let S be the sum of digits and P the product of digits. We have 3 main cases:
• $S = P = 0$: since $P = 0$ then at least one of the digits must be 0 and hence all the digits must be 0 so that $S = 0$. So, we have only one possibility which is 0000000000.
• $S = P = 16$: we have 1111111144 and its permutations which are 45 in total.[30]
• $S = P \neq 0, 16$: we have no 10-digit integer that satisfies this condition because no factorization of P (noting that $1 \leq S \leq 90$ excluding 16) can satisfy the condition $S = P$.
So, we have 45 permutations of 1111111144 as well as 0000000000, i.e. 46 such integers. Now, if we consider the negatives of the 45 permutations of 1111111144 then we should have 91 such integers.
13. Identify (or characterize) the integers which have the following number of positive divisors (exactly):
(**a**) Infinitely many. (**b**) Zero. (**c**) One. (**d**) Two. (**e**) Three. (**f**) Four. (**g**) Five.
Solution:
(**a**) Only 0 (because 0 can be divided by any other integer).
(**b**) None (because any integer can be divided at least by 1).

[30] The permutations of eight 1's and two 4's are given by the multinomial coefficient $\frac{10!}{2!\,8!} = 45$.

(**c**) Only ± 1 (because if $a|b$ and $b \neq 0$ then $|a| \leq |b|$ and hence ± 1 can be divided only by 1 noting that any other non-zero integer can be divided by 1 and by its absolute value).
(**d**) Primes (because by definition a prime number can be divided only by 1 and itself).
(**e**) Squares of primes (because the divisors of p^2 where $p \in \mathbb{P}$ are only 1, p and p^2).
(**f**) Cubes of primes (because the divisors of p^3 where $p \in \mathbb{P}$ are only $1, p, p^2$ and p^3). Also, composite numbers of the form $p_1 p_2$ where $p_1, p_2 \in \mathbb{P}$ and $p_1 \neq p_2$ (because the divisors of $p_1 p_2$ are only $1, p_1, p_2$ and $p_1 p_2$).
(**g**) Fourth powers of primes (because the divisors of p^4 where $p \in \mathbb{P}$ are only $1, p, p^2, p^3$ and p^4).

14. Find all $x, y \in \mathbb{Z}$ such that $x^y = y^x$.
Solution: An obvious solution is $x = y$. So, in the following we search for solutions where $x \neq y$. In Problem 5 of § 7.3 we find that $x^y > y^x$ for all $2 < x < y$. We also find that $x^y < y^x$ when $(x, y) = (1, y)$ where $\mathbb{N} \ni y > 1$. So, assuming $x, y \in \mathbb{N}$ and $x < y$, the only possibility for $x^y = y^x$ is for $x = 2$, that is: $2^y = y^2$ whose only solution (assuming $x \neq y$) is $y = 4$. So, another solution to $x^y = y^x$ is $(x, y) = (2, 4)$. Now, if we lift the restriction that $x < y$ (noting the symmetry in x, y) as well as the restriction that $x, y \in \mathbb{N}$ (noting that 2 and 4 are even) then we get three more solutions, i.e. $(x, y) = (4, 2), (-2, -4), (-4, -2)$. So in brief, the solutions of $x^y = y^x$ (where $k \in \mathbb{Z}$) are:
$(x, y) = (k, k)$ $(x, y) = (2, 4)$ $(x, y) = (4, 2)$ $(x, y) = (-2, -4)$ $(x, y) = (-4, -2)$

15. Conduct an initial check on the following integers to see if they can be perfect numbers or not:
(**a**) 348923082239. (**b**) 5762859329434. (**c**) 116398323238.
Solution:
(**a**) All known perfect numbers (up to very large integers) are even and hence this cannot be a perfect number because it is odd.
(**b**) All even perfect numbers end in 6 or 8 (see point 6 of § 2.8 of V1) and hence this cannot be a perfect number because it ends in 4.
(**c**) All even perfect numbers (excluding 6) end in 16, 28, 36, 56, 76, or 96 (see point 7 of § 2.8 of V1) and hence this cannot be a perfect number because it ends in 38.

16. Show that $\frac{x}{y} = \frac{y}{z} = \frac{z}{x}$ *iff* $x = y = z$ (where $\mathbb{Z} \ni x, y, z \neq 0$).[31]
Solution: Regrading **the if part**, if $x = y = z$ then $\frac{x}{y} = 1$, $\frac{y}{z} = 1$ and $\frac{z}{x} = 1$ and hence $\frac{x}{y} = \frac{y}{z} = \frac{z}{x} = 1$.
Regrading **the only if part**, we prove this part by contraposition where we first consider the case of $x, y, z \in \mathbb{N}$. So, let assume that the triple equality $x = y = z$ does not hold. This means that one of the variables x, y, z must be greater than another one of these variables. So, let assume (without loss of generality since it is a matter of labeling) that x is the greater variable. Hence, (with a proper labeling of y and z) we have one of the following three cases:
• $x = y > z$ and hence $\frac{x}{y} \neq \frac{y}{z}$ since $\frac{x}{y} = 1$ while $\frac{y}{z} > 1$.
• $x > y = z$ and hence $\frac{x}{y} \neq \frac{y}{z}$ since $\frac{x}{y} > 1$ while $\frac{y}{z} = 1$.
• $x > y > z$ and hence $\frac{x}{y} \neq \frac{z}{x}$ since $\frac{x}{y} > 1$ while $\frac{z}{x} < 1$.
So, in all cases the triple equality $\frac{x}{y} = \frac{y}{z} = \frac{z}{x}$ does not hold if the triple equality $x = y = z$ does not hold, and hence by contraposition the triple equality $x = y = z$ does hold if the triple equality $\frac{x}{y} = \frac{y}{z} = \frac{z}{x}$ does hold, i.e. if $\frac{x}{y} = \frac{y}{z} = \frac{z}{x}$ then $x = y = z$.
We finally need to extend from $x, y, z \in \mathbb{N}$ to $\mathbb{Z} \ni x, y, z \neq 0$. Now, we have four cases:
• All x, y, z are greater than 0: this is the case of $x, y, z \in \mathbb{N}$ which is already considered.
• All x, y, z are less than 0: this is equivalent to the previous case because the minus sign will be canceled (or rather it has no effect because the ratio of two positive numbers is the same as the ratio of their negatives).
• Only one of x, y, z is less than 0: so assume (with no loss of generality) that $x < 0$ and hence $\frac{x}{y}$ and $\frac{z}{x}$ are negative while $\frac{y}{z}$ is positive and hence they cannot be equal.
• Only one of x, y, z is greater than 0: so assume (with no loss of generality) that $x > 0$ and hence $\frac{x}{y}$ and $\frac{z}{x}$ are negative while $\frac{y}{z}$ is positive and hence they cannot be equal.
Hence, the proposition applies to all $\mathbb{Z} \ni x, y, z \neq 0$ and not only to $x, y, z \in \mathbb{N}$.

[31] The purpose of such "trivial" questions is to learn systematic investigation and analysis.

Chapter 3
Primes, Composites and Coprimes

1. Find all prime numbers of the following forms:
   (**a**) n^3+3n^2+5n+6 $(n\in\mathbb{Z})$. (**b**) $3^n\pm 1$ $(n\in\mathbb{N}^0)$. (**c**) $4^{n+2}+2^n$ $(n\in\mathbb{N}^0)$.
   Solution:
   (**a**) This expression is divisible by 3 for all $n\in\mathbb{Z}$ (noting that $n^3+3n^2+5n+6\overset{3}{=}0$ identically). Hence, it is composite except if it is equal to 0 (which is neither composite nor prime) or 3 (which is prime). So, if this expression is to be prime then we must have $n^3+3n^2+5n+6=3$ for some $n\in\mathbb{Z}$. This equation has a solution $n=-1$ and hence 3 is the only prime number of this form (corresponding to $n=-1$).
   (**b**) $3^n\pm 1$ is even for all $n\in\mathbb{N}^0$ and hence it is prime only when it is equal to 2 (corresponding to $n=0$ for 3^n+1 and to $n=1$ for 3^n-1).
   (**c**) $4^{n+2}+2^n$ is even and greater than 2 for all $n\in\mathbb{N}^0$ except when $n=0$ where it is equal to 17. Hence, 17 is the only prime number of this form (corresponding to $n=0$).
2. Find all prime numbers of the following forms: aa, $abab$, $abcabc$, $abcdabcd$, $abcdeabcde$, $abcdefabcdef$ (where a,b,c,d,e,f are digits and $a\neq 0$).
   Solution: All integers of the form aa are divisible by 11 and hence they are all composite except 11 itself. Regarding the other forms we have:
   $abab=101\times ab$ $abcabc=1001\times abc$ $abcdabcd=10001\times abcd$
   $abcdeabcde=100001\times abcde$ $abcdefabcdef=1000001\times abcdef$
   Hence, they are all composite. So, the only prime of the given forms is 11.
3. Let $n=9m+6$ $(m\in\mathbb{N})$ and $\tau(n)=4$ (where τ is the tau function). Show that $3m+2$ is prime.
   Solution: We have:[32]
   $$\tau(n)=\prod_{i=1}^{k}(a_i+1)=4=2\times 2$$
   i.e. $k=2$ and $a_1=a_2=1$. This means that n is square free with two prime factors, that is: $n=9m+6=3(3m+2)=3p$ where $p=3m+2$ is prime.
4. Investigate the prime numbers of the following form:
   $$p=\overbrace{m\ldots mm}^{n\text{ times}} \qquad (m,n\in\mathbb{N},\ n>1)$$
   where mm means concatenation not multiplication
   Solution: If k is the number of digits of m then we can write:
   $$p=10^{k(n-1)}m+\cdots+10^km+10^0m=m(10^{k(n-1)}+\cdots+10^k+10^0)$$
   This is obviously composite if $m>1$ since $(10^{k(n-1)}+\cdots+10^k+10^0)>1$ (noting that $n>1$). Hence, to have a prime we must have $m=1$ and thus $p=(10^{n-1}+\cdots+10^1+10^0)=1\ldots11$. Now, for $n=2$ we have $1\ldots11=11$ which is prime. Regarding $n>2$, if n is even then $1\ldots11$ is divisible by 11 (see rule 33 of § 1.9 of V1), while if n is a natural multiple of 3 then $1\ldots11$ is divisible by 3 (see rule 25 of § 1.9 of V1) and hence they cannot be prime. In fact, the primality of the natural numbers of the form $1\ldots11$ is a research issue. Those who are interested in further details should refer to the problem of repunit numbers (i.e. repeated unit numbers such as 11, 111, 1111) in the literature noting that there are several known repunit primes (other than 11).

[32] We note that $n=p^3$ is not a possibility because $p^3=9m+6$ (i.e. $3m+2=9$) has no solution.

5. Find all p such that p, $11p^3+2$ and $5p^3+4$ are primes.
Solution: $p=2$ is not a possibility (because $11p^3+2$ and $5p^3+4$ will be even). Similarly, $p=3$ is not a possibility (because $11p^3+2=299$ which is composite). So, let us investigate $p>3$. It is obvious that for $p>3$ we have $p \overset{3}{\neq} 0$ because p cannot be divisible by 3 (since p is supposedly prime). So, either $p \overset{3}{=} 1$ or $p \overset{3}{=} 2$:
• If $p \overset{3}{=} 1$ then $5p^3+4 \overset{3}{=} 0$ and hence $5p^3+4$ is not prime.
• If $p \overset{3}{=} 2$ then $11p^3+2 \overset{3}{=} 0$ and hence $11p^3+2$ is not prime.
So in brief, there is no p such that p, $11p^3+2$ and $5p^3+4$ are primes.
6. Find all composite numbers of the following forms (where $n \in \mathbb{Z}$):
(**a**) n^2-2n+1. (**b**) $n!+5$. (**c**) n^5+1.
Solution:
(**a**) We have $n^2-2n+1=(n-1)^2$. Now, for $n=0$ and $n=2$ we have $(n-1)^2=1$ which is not composite. Similarly, for $n=1$ we have $(n-1)^2=0$ which is not composite. For all other $n \in \mathbb{Z}$, $(n-1)^2$ is a product of two integers whose magnitude is >1 and hence it is composite. So in brief, (n^2-2n+1) is composite for all $n \in \mathbb{Z}$ excluding $n=0,1,2$.
(**b**) We note first that $n!$ is defined only for $n \in \mathbb{N}^0$. Now, it is obvious that $n!+5$ is divisible by 5 for all $n>4$ and hence it is composite for all these values of n. So, all we need is to inspect $n!+5$ for $n=0,1,2,3,4$. Now, for $n=0,1,2,3,4$ we have $n!+5=6,6,7,11,29$. So in brief, $n!+5$ is prime for $n=2,3,4$ and composite for all other $n \in \mathbb{N}^0$.
(**c**) From Eq. 11 of V1 we can see that (n^5+1) is composite for all $n<-2$ and $n>1$. So, all we need is to inspect (n^5+1) for $n=-2,-1,0,1$. Now, for $n=-2,-1,0,1$ we have $n^5+1=-31,0,1,2$. So in brief, (n^5+1) is composite for all $n \in \mathbb{Z}$ excluding $n=-2,-1,0,1$.[33]
7. Show that there are no prime numbers of the following forms (where $m,n \in \mathbb{Z}$):
(**a**) n^2-2n+1. (**b**) $n^5-15n^3+4n+20$. (**c**) $6m^3-19m^2n+19mn^2-6n^3$.
Solution:
(**a**) This is a consequence of part (a) of Problem 6 (noting that by definition 0 and 1 are not prime numbers).
(**b**) This expression is divisible by 5 for all $n \in \mathbb{Z}$ (noting that $n^5-15n^3+4n+20 \overset{5}{=} 0$ identically). Moreover, this expression is not equal to 0 or 5 (which are the only non-composite numbers divisible by 5)[34] for any $n \in \mathbb{Z}$. Therefore, this expression is always composite and hence it cannot represent a prime.
(**c**) Let $f(m,n)=6m^3-19m^2n+19mn^2-6n^3$ and hence we have:

$$\begin{aligned} f(m,n) &= 6m^3-6n^3-19m^2n+19mn^2 = 6(m^3-n^3)-19(m^2n-mn^2) \\ &= 6(m-n)(m^2+mn+n^2)-19mn(m-n) = (m-n)\left[6(m^2+mn+n^2)-19mn\right] \\ &= (m-n)(6m^2-13mn+6n^2) = (m-n)(3m-2n)(2m-3n) \end{aligned}$$

Now, a prime number p can be factorized as a product of three integer factors only in 3 different ways, i.e.

$$p=(1)(-1)(-p)=(1)(1)(p)=(-1)(-1)(p)$$

So, if $f=p$ then we have 3 cases to consider:
First case: $f=(1)(-1)(-p)$ and hence one of the factors $(m-n),(3m-2n),(2m-3n)$ must be equal to 1 and another factor of these must be equal to -1. So, if we consider the 6 systems of simultaneous equations obtained from equating $(m-n),(3m-2n),(2m-3n)$ to 1 combined with the equations obtained from equating $(m-n),(3m-2n),(2m-3n)$ to -1 (noting that a single factor cannot be

[33] We should note that if "composite" is restricted (by definition) to natural numbers (see § 2.2. of V1) then we should exclude all the negatives. We may also add: n^5+1 is prime for $n=1$ and neither prime nor composite for $n=-2,-1,0$ (noting the sign of -31 in the case of $n=-2$).
[34] If we consider -5 as well (by ignoring the sign) then we can also confirm that this expression is not equal to -5.

equal to 1 and -1 at the same time) then we can identify m and n values that can possibly make $f = p$. These 6 systems with their solutions and the corresponding values of f $\big[$in the form $(m, n, f)\big]$ are given in the following table:

	$\boldsymbol{m-n=1}$	$\boldsymbol{3m-2n=1}$	$\boldsymbol{2m-3n=1}$
$\boldsymbol{m-n=-1}$		$(3,4,6)$	$(-4,-3,6)$
$\boldsymbol{3m-2n=-1}$	$(-3,-4,-6)$		$(-1,-1,0)$
$\boldsymbol{2m-3n=-1}$	$(4,3,-6)$	$(1,1,0)$	

As we see, $f = 0, \pm 6$ in this case and hence it is not prime.
Second case: $f = (1)(1)(p)$ and hence if we follow the argument and procedure of the first case then we get the following table (where NS means "No Solution"):

	$\boldsymbol{m-n=1}$	$\boldsymbol{3m-2n=1}$	$\boldsymbol{2m-3n=1}$
$\boldsymbol{m-n=1}$		$(-1,-2,4)$	$(2,1,4)$
$\boldsymbol{3m-2n=1}$			NS
$\boldsymbol{2m-3n=1}$			

As we see, $f = 4$ in this case and hence it is not prime.
Third case: $f = (-1)(-1)(p)$ and hence if we follow the argument and procedure of the first case then we get the following table:

	$\boldsymbol{m-n=-1}$	$\boldsymbol{3m-2n=-1}$	$\boldsymbol{2m-3n=-1}$
$\boldsymbol{m-n=-1}$		$(1,2,-4)$	$(-2,-1,-4)$
$\boldsymbol{3m-2n=-1}$			NS
$\boldsymbol{2m-3n=-1}$			

As we see, $f = -4$ in this case and hence it is not prime.
So, in all cases f cannot represent a prime number and hence there are no prime numbers of the given form.

8. Show that the gap between two successive prime numbers can be arbitrarily large.
Solution: It was shown in Problem 8 of § 6.15 of V1 that for any $n \in \mathbb{N}$ there are n consecutive composite numbers. This implies that the gap between prime numbers can be arbitrarily large. So, although there is a lower limit on the size of the gap between two successive prime numbers (i.e. 1 in the case of twin primes noting the exception of 2, 3) there is no upper limit on the size of this gap.
9. Determine if the following pairs of polynomials are coprime for all $n \in \mathbb{N}$, or coprime for none of $n \in \mathbb{N}$, or coprime for only some of $n \in \mathbb{N}$:
(**a**) $2n^2 - 1$ and $5n^2 - 3$. (**b**) $4n^3 - 1$ and $7n^4 + 5$. (**c**) $n^5 + 10n^4 - n = 0$ and $3n^9 - n$.
Solution:
(**a**) By Bezout theorem we have:

$$\gcd(2n^2 - 1, 5n^2 + 3) = 5(2n^2 - 1) - 2(5n^2 - 3) = 1$$

Thus, these polynomials are coprime for all $n \in \mathbb{N}$.
(**b**) For example, these polynomials are coprime for $n = 2$ and not coprime for $n = 1$. Thus, these polynomials are coprime for only some of $n \in \mathbb{N}$.
(**c**) These polynomials are even for all $n \in \mathbb{N}$ and hence they are coprime for none of $n \in \mathbb{N}$.
10. Find all $p, q \in \mathbb{P}$ such that $5p^2 - 8pq + 11q^2 = 1175$.
Solution: If we treat this equation as a quadratic in p with a discriminant Δ then we have:

$$\Delta = 64q^2 - 20(11q^2 - 1175) = -156q^2 + 23500 \geq 0 \qquad \rightarrow \qquad q \leq \sqrt{\frac{23500}{156}} \simeq 12.27$$

So, we need to consider only $q = 2, 3, 5, 7, 11$. On substituting these values in the given equation and solving for p (accepting only prime values for p) we get: $(p, q) = (2, 11)$ which is the only solution to this Problem.
11. Find all $p, q, r \in \mathbb{P}$ such that:
(**a**) $p(q - r) = 2(q + r)$. (**b**) $p(q + r) = 5(q - r)$.

Solution:
(**a**) It is obvious that $q \neq r$ because $2(q+r) > 0$. Also, $p \neq 2$ because $q - r \neq q + r$ (since it leads to $r = 0$). So, p is an odd prime. Moreover, $(q-r)$ must be even (because of the 2 on the RHS) and hence both q and r are odd primes. So in brief, p, q, r are odd primes. Rewriting the equation as (noting that $q + r$ is even and p is odd):

$$p = \frac{2(q+r)}{q-r}$$

we conclude that $(q - r)$ is a multiple of 4. So, based on this equation we can write:

$$q - r = 4\left(p_1^{a_1} \dots p_k^{a_k}\right) \qquad\qquad q + r = \frac{p(q-r)}{2} = \frac{p\,4\left(p_1^{a_1} \dots p_k^{a_k}\right)}{2} = 2p\left(p_1^{a_1} \dots p_k^{a_k}\right)$$

Now:
• If we add these equations we get:

$$2q = 4\left(p_1^{a_1} \dots p_k^{a_k}\right) + 2p\left(p_1^{a_1} \dots p_k^{a_k}\right) \quad \rightarrow \quad q = \left(p_1^{a_1} \dots p_k^{a_k}\right)(2+p) \quad \rightarrow \quad p_1^{a_1} \dots p_k^{a_k} = 1 \quad \rightarrow$$

$$q = 2 + p \quad \rightarrow \quad p = q - 2$$

where step 2 is because if $q = p_1^{a_1} \dots p_k^{a_k}$ (noting that q is prime) then $2 + p = 1$ (i.e. $p = -1$) which is impossible.
• If we subtract these equations we get:

$$2r = 2p\left(p_1^{a_1} \dots p_k^{a_k}\right) - 4\left(p_1^{a_1} \dots p_k^{a_k}\right) \quad \rightarrow \quad r = \left(p_1^{a_1} \dots p_k^{a_k}\right)(p-2) \quad \rightarrow \quad p_1^{a_1} \dots p_k^{a_k} = 1 \quad \rightarrow$$

$$r = p - 2 \quad \rightarrow \quad p = r + 2$$

where step 2 is because if $r = p_1^{a_1} \dots p_k^{a_k}$ (noting that r is prime) then $p - 2 = 1$ (i.e. $p = 3$) which is impossible because q will be 5 (since $p = q - 2$) and hence $r = 1$ (which is nonsensical since r is prime). So in brief, we have $p = q - 2$ and $p = r + 2$. Now, if we remember that 5 is the only prime number that is shared by two different pairs of twin primes (see point 3 in the preamble of § 2.2.1 of V1), then we can conclude that $(p, q, r) = (5, 7, 3)$ which is the only solution to the given equation.
(**b**) If we write this equation as $5(q - r) = p(q + r)$ and compare it to the equation of part (a) noting its unique solution then we can conclude that $(p, q, r) = (2, 7, 3)$. However, let assume that we do not have part (a) and its solution and hence we solve this equation from scratch.
It is obvious that $q > r$ (since the LHS is > 0). Now, since $(q + r) > (q - r)$ then $p < 5$ and hence we have only two possibilities:
• $p = 2$ and hence we have $2(q + r) = 5(q - r)$ which simplifies to $3q = 7r$. So, 3 divides r and hence $r = 3$ (noting that r is prime) and $q = 7$. Thus, we have the solution $(p, q, r) = (2, 7, 3)$.
• $p = 3$ and hence we have $3(q + r) = 5(q - r)$ which simplifies to $q = 4r$, i.e. q is composite and hence it is unacceptable.
Accordingly, the only solution to the given equation is $(p, q, r) = (2, 7, 3)$.

12. Find solutions to the following equation: $p^2(q - r) = 12(q + r)$ where $p, q, r \in \mathbb{P}$.
Solution: $p \neq 2$ because $4(q - r) < 12(q + r)$. $p \neq 3$ because $9(q - r) < 12(q + r)$. Hence, p is an odd prime ≥ 5.
On comparing the two sides of the given equation we must have:

$$q - r = 12\left(p_1^{a_1} \dots p_k^{a_k}\right) \qquad\qquad q + r = p^2\left(p_1^{a_1} \dots p_k^{a_k}\right)$$

On adding and subtracting these equations we get:

$$q = \frac{\left(p^2+12\right)\left(p_1^{a_1} \dots p_k^{a_k}\right)}{2} \qquad\qquad r = \frac{\left(p^2-12\right)\left(p_1^{a_1} \dots p_k^{a_k}\right)}{2}$$

Now, since p is odd then $p^2 + 12$ and $p^2 - 12$ are odd (i.e. they are not divisible by 2) and hence 2 divides $p_1^{a_1} \dots p_k^{a_k}$. Moreover, since $p^2 + 12$ and $p^2 - 12$ are greater than 1 (since $p \geq 5$) then $p_1^{a_1} \dots p_k^{a_k}$ must be equal to 2 (noting that q and r are primes). Therefore, we must have $q = p^2 + 12$ and $r = p^2 - 12$. On inspecting the low values of p we found the following solutions, i.e. (p, q, r):
(5,37,13) (7,61,37) (13,181,157) (19,373,349) (29,853,829) (41,1693,1669) (61,3733,3709)

13. Investigate the prime numbers of the following forms (where $n \in \mathbb{N}$):
(**a**) n^2-1. (**b**) n^2+1. (**c**) n^3-1. (**d**) n^3+1. (**e**) n^2-2.
Solution:
(**a**) $n^2-1=(n-1)(n+1)$ which is composite for all $n>2$. For $n=1$ we have $n^2-1=0$ (which is not prime), while for $n=2$ we have $n^2-1=3$ (which is prime). So, the only prime of the form n^2-1 is 3.
(**b**) There are many primes of the form n^2+1 (e.g. 2, 5, 17) and it is conjectured that there are infinitely many primes of this form.
(**c**) $n^3-1=(n-1)(n^2+n+1)$ and hence it is composite for all $n>2$. For $n=1$ we have $n^3-1=0$ (which is not prime), while for $n=2$ we have $n^3-1=7$ (which is prime). So, the only prime of the form n^3-1 is 7.
(**d**) The only prime of the form n^3+1 is 2 (corresponding to $n=1$) because $n^3+1=(n+1)(n^2-n+1)$ which is composite for all $n>1$.
(**e**) If n is even then the only prime of this form is 2 (corresponding to $n=2$) because n^2-2 is even. If n is odd then we have many primes of this form (e.g. 7, 23, 47) and it is conjectured that there are infinitely many of them.

14. Show that any divisor of a Mersenne number $M_p=2^p-1$ (where p is an odd prime) is of the form $2kp+1$ (where $k \in \mathbb{N}$).
Solution: Let q be a prime number dividing M_p (and hence q is odd since M_p is odd). Now, by Fermat's little theorem we have $q|(2^{q-1}-1)$. Moreover:

$$\gcd(2^p-1, 2^{q-1}-1)=2^{\gcd(p,q-1)}-1 \qquad \text{(see Problem 2 of § 13)}$$

Noting that q supposedly divides both 2^p-1 and $2^{q-1}-1$, q must divide their gcd which is $2^{\gcd(p,q-1)}-1$ (see Problem 10 of § 2.4 of V1). Now, since q is an odd prime then $\gcd(p,q-1)>1$ which implies $\gcd(p,q-1)=p$, i.e. p is a factor of $q-1$ and hence $p|(q-1)$. So, we can write $q-1=sp$ where s must be an even natural number because $q-1$ is even (noting that q is an odd prime as indicated earlier and because p divides $q-1$). Hence, we can write $q=2kp+1$ (where $k \in \mathbb{N}$). This means that any prime divisor of M_p is of the form $2kp+1$. However, this should apply even to the composite divisors of M_p because the composite divisor is a product of prime factors where each one of these prime factors is of the form $2kp+1$ and hence their product must be of this form, e.g.

$$(2k_1p+1)(2k_2p+1)=4k_1k_2p+2k_1p+2k_2p+1=2(2k_1k_2+k_1+k_2)p+1$$

Note 1: the theorem of this Problem can be used to prove that there are infinitely many primes because if there are only finitely many primes with p being the largest of them then M_p (which must be greater than p) is composite. However, according to the theorem of this Problem any prime divisor of M_p must be of the form $2kp+1$ which must be greater than p in contradiction to the claim that p is the largest prime.[35]
Note 2: the theorem of this Problem is very useful for the search of Mersenne primes (or composites) since it can be used to accelerate the search for Mersenne primes. The idea is that Mersenne numbers which are composite are divisible only by factors of the form $2kp+1$. This restriction on the form of divisors limits the possibilities of potential divisors substantially, i.e. if a Mersenne number is not divisible by any factor of the form $2kp+1$ then it must be prime (otherwise it is composite). This will be illustrated in Problem 15.

[35] It is worth noting that we can find many proofs in the literature about the infinitude of primes, e.g. the proof of Euclid which we discussed in Problem 12 of § 2.2 of V1 and the proof about the coprimality of Fermat numbers which we discussed in Problem 7 of § 2.2.3 of V1 (as well as the proof indicated in the present note; also see Problem 18). These proofs can be classified as direct proofs (i.e. they are intended to prove the infinitude of primes; e.g. the proof of Euclid) and indirect proofs (i.e. they are intended to prove something else but their outcome implies the infinitude of primes; e.g. the proof of Problem 7 of § 2.2.3 of V1 and the proof of the present note). In fact, some of the proofs of propositions about the infinitude of primes of certain forms and types are also proofs of the infinitude of primes (assuming that these proofs do not presume the infinitude of primes or based on such presumption).

15. Determine if the following Mersenne numbers are prime or composite: M_{17} and M_{23}.
Solution: Regrading M_{17}, we need to test only the primes of the form $34k+1$ which are $< \sqrt{M_{17}} \simeq 362$, i.e. $p = 103, 137, 239, 307$. None of these primes divides M_{17} and hence M_{17} is a Mersenne prime.
Regrading M_{23}, we need to test only the primes of the form $46k+1$ which are $< \sqrt{M_{23}} \simeq 2896$. The first of these primes is 47 which divides M_{23} and hence M_{23} is a composite Mersenne number (with no need for doing more tests).
16. Let m and n be coprime integers. Show that $2m+n$ and $3m+2n$ are coprime.
Solution: Let $A = 2m+n$ and $B = 3m+2n$. Accordingly:
$$2A - B = m \qquad \text{and} \qquad 2B - 3A = n$$
Now, if we note that m and n are coprime and we use the rules of gcd (as given in the preamble of § 2.4 of V1) then we have:
$$\begin{aligned} 1 &= \gcd(m,n) = \gcd(2A-B, 2B-3A) = \gcd(B-2A, 2B-3A) \\ &= \gcd(B-2A, [2B-3A]-[B-2A]) = \gcd(B-2A, B-A) \\ &= \gcd(B-2A, [B-A]-[B-2A]) = \gcd(B-2A, A) = \gcd(2A-B, A) = \gcd([2A-B]-A, A) \\ &= \gcd(A-B, A) = \gcd([A-B]-A, A) = \gcd(-B, A) = \gcd(B, A) = \gcd(A, B) \end{aligned}$$
i.e. $2m+n$ and $3m+2n$ are coprime.
17. Show that any multi-digit twin primes (i.e. excluding 3,5 and 5,7) must end with 1 and 3 (like 11,13) or with 7 and 9 (like 17,19) or with 9 and 1 (like 29,31).
Solution: A multi-digit integer whose last digit is $0, 2, 4, 5, 6, 8$ must be composite because it is either even (> 2) or divisible by 5 (> 5). Hence, the last digit of any multi-digit prime must be $1, 3, 7, 9$. Now:
• If a prime ends in 1 then its potential twin must end either in 9 or in 3, and both these possibilities are acceptable (because the potential twin ends with an acceptable last digit of a prime).
• If a prime ends in 3 then its potential twin must end either in 1 (which is considered in the previous point) or in 5 (which is not acceptable because the "twin" is divisible by 5).
• If a prime ends in 7 then its potential twin must end either in 5 (which is not acceptable because the "twin" is divisible by 5) or in 9 (which is acceptable because the twin ends with an acceptable last digit of a prime).
• If a prime ends in 9 then its potential twin must end either in 7 or in 1 (where both these possibilities are considered in the previous points).
18. Show the following (where $n \in \mathbb{N}$):
(**a**) $n!$ and $n!+1$ have no common prime factor. (**b**) Any prime factor of $n!+1$ is $> n$.
Solution:
(**a**) If $n!$ and $n!+1$ have a common prime factor then this factor will divide both of them and hence it will divide their difference which is 1. This contradiction should prove the given proposition.
(**b**) If $n!+1$ has a prime factor $\leq n$ then this prime factor will be common to both $n!$ and $n!+1$ which contradicts the result of part (a).
Note: the result of part (b) is an indirect proof for the infinitude of primes because we can always find a prime $> n$ that divides $n!+1$. Also see note 1 of Problem 14.
19. List some of the famous conjectures related to prime numbers.
Solution: For example:
• Goldbach conjecture which states: every even integer > 2 can be written as the sum of two primes.
• Twin primes conjecture which states: there are infinitely many twin primes.
• Mersenne primes conjecture which states: there are infinitely many Mersenne primes.
• The n^2+1 conjecture which states: there are infinitely many primes of the form n^2+1 where $n \in \mathbb{N}$.

Chapter 4
Representation of Numbers

1. Show that if $n \in \mathbb{Z}$ is any integer multiple of 4 then $n = 7xy - xyz$ for some $x, y, z \in \mathbb{Z}$.
   Solution: For example, if $x = 1$ and $y = 4$ then we have:
   $$n = 7xy - xyz = xy(7 - z) = 1 \times 4 \times (7 - z) = 4(7 - z)$$
   Now, if we note that $(7 - z)$ can represent any integer then we can see that n can represent any integer multiple of 4. This implies that if n is any integer multiple of 4 then we can always find $x, y, z \in \mathbb{Z}$ such that $n = 7xy - xyz$.
2. Show that if $p \in \mathbb{P}$ is of the form $p = 3n+1$ then it cannot be expressed as $2x^2+3y^2$ (where $n, x, y \in \mathbb{N}$).
   Solution: p is obviously greater than 3. Now, $2x^2 + 3y^2$ can be congruent (mod 3) only to 0 and 2. However, since p is prime (and greater than 3) it cannot be congruent (mod 3) to 0. Also, if p is congruent (mod 3) to 2 then we must have: $3n + 1 \overset{3}{=} 2$ (i.e. $1 \overset{3}{=} 2$) which is nonsensical. So, if $p = 3n + 1$ then it cannot be expressed as $2x^2 + 3y^2$.
3. Give some examples of pairs (a, b) of distinct natural numbers such that ab is a perfect square and $a - 2b$ is a perfect (positive) cube.
   Solution: This sort of problems can be easily solved computationally by writing a simple code or script to search for examples of such pairs. However, let us try a more rational (or analytical) approach. Let (for simplicity) assume that ab and $a - 2b$ are natural powers of primes, i.e. $ab = p^{2s}$ and $a - 2b = q^{3t}$ (where $p, q \in \mathbb{P}$ and $s, t \in \mathbb{N}$). Accordingly (noting that $c, d \in \mathbb{N}$):
   $$p = q = 2 \quad \rightarrow \quad a = 2^c \text{ and } b = 2^d \quad \rightarrow \quad a - 2b = 2^c - 2^{d+1} \quad \rightarrow$$
   $$a - 2b = 2^{d+1}(2^{c-d-1} - 1) \quad \rightarrow \quad c - d - 1 = 1 \quad \rightarrow \quad c = d + 2$$
   Now, if we try $d = 1, 2, 3, \ldots$ we can find many examples. For instance, $d = 2, 5, 8, 11, 14$ produce the following examples of (a, b) pairs:
   $$(16, 4) \qquad (128, 32) \qquad (1024, 256) \qquad (8192, 2048) \qquad (65536, 16384)$$
   In fact, every pair $(a, b) = (2^{4+3k}, 2^{2+3k})$ where $k \in \mathbb{N}^0$ should meet the given requirement.
4. Find the smallest positive integer k which is equal to twice a cube (of an integer) and thrice a square (of an integer).
   Solution: We have $k = 2m^3 = 3n^2$ $(m, n \in \mathbb{N})$. It is obvious that m is a multiple of 3 (and hence $m = 3\mu$ where $\mu \in \mathbb{N}$) while n is a multiple of 2 (and hence $n = 2\nu$ where $\nu \in \mathbb{N}$). Hence, we have $3^2\mu^3 = 2\nu^2$, i.e. $\nu = \sqrt{9\mu^3/2}$. Now, if we try the smallest values of μ then we find that $\mu = 2$ yields $\nu = 6$ and hence $k = 2(3 \times 2)^3 = 3(2 \times 6)^2 = 432$.
5. Find all $n \in \mathbb{Z}$ such that:
   (**a**) $f(n) = n^2 - n + 1$ is a perfect square. (**b**) $g(n) = n^3 + 3n + 1$ is a perfect cube.
   (**c**) $h(n) = n^2 + 3n - 1$ is a perfect square.
   Solution:
   (**a**) We have three main cases:
   • $n = 0, 1$ and hence $f(n) = 1$ which is a perfect square.
   • $n < 0$ and hence:
   $$n^2 < (n^2 - n + 1) < (n - 1)^2$$
   which means that $f(n)$ is not a perfect square (because there is no perfect square between two consecutive perfect squares).
   • $n > 1$ and hence:
   $$(n - 1)^2 < (n^2 - n + 1) < n^2$$

which means that $f(n)$ is not a perfect square (as in the previous point).
So in brief, $f(n)$ is a perfect square only for $n = 0$ and $n = 1$.
(**b**) If we follow the method of part (a) then we conclude that $g(n)$ is a perfect cube only for $n = 0$ because:

$$(n-1)^3 < (n^3+3n+1) < n^3 \quad (\text{for } n<0) \qquad \& \qquad n^3 < (n^3+3n+1) < (n+1)^3 \quad (\text{for } n>0)$$

noting that there is no perfect cube between two consecutive perfect cubes.
(**c**) Because $h(n)$ is a perfect square, we have $n^2 + 3n - 1 = m^2$ (where $m \in \mathbb{Z}$). Hence (noting that $N = 2n$ and $M = 2m$):

$$4n^2+12n-4 = 4m^2 \quad \rightarrow \quad 4n^2+12n = 4m^2+4 \quad \rightarrow \quad N^2+6N = M^2+4 \quad \rightarrow$$
$$N^2+6N+9 = M^2+13 \quad \rightarrow \quad (N+3)^2 = M^2+13 \quad \rightarrow \quad (N+3)^2 - M^2 = 13 \quad \rightarrow$$
$$(N+3-M)(N+3+M) = 13 \quad \rightarrow$$

Noting that $13 = (-1)(-13) = (1)(13)$ and considering all the 4 possibilities (i.e. with regard to equating the factors on the two sides in both orders), we get 4 systems of equations in N and M. On solving these systems we get: $(N, M) = (-10, -6)$, $(-10, 6)$, (4,6), $(4, -6)$. So, $h(n)$ is a perfect square only for $n = -5$ and $n = 2$ (corresponding to $m^2 = 9$).

6. Find all $x, y \in \mathbb{N}^0$ such that $x^2 + 4y$ and $y^2 + 4x$ are both perfect squares.
Solution: We have four cases to consider:
• $x = y = 0$ and hence $(x, y) = (0, 0)$.
• $x = 0$ and $y \neq 0$, i.e. $4y$ and y^2 are perfect squares. Noting that 4 is a perfect square, any $y = k^2$ ($k \in \mathbb{Z}$) is a valid solution. Hence, $(x, y) = (0, k^2)$.
• $x \neq 0$ and $y = 0$: from the previous point (noting the symmetry) we have $(x, y) = (k^2, 0)$.
• $x > 0$ and $y > 0$ and hence:[36]

$$(x+1)^2 \leq (x^2+4y) \quad \rightarrow \quad (x^2+2x+1) \leq (x^2+4y) \quad \rightarrow \quad (2x+1) \leq 4y$$

Now, $2x+1$ is odd while $4y$ is even and hence the equality is not possible. Accordingly, we must have:[37]

$$(x+2)^2 \leq (x^2+4y) \quad \rightarrow \quad (x^2+4x+4) \leq (x^2+4y) \quad \rightarrow \quad (x+1) \leq y$$

By a similar argument (or by symmetry) we must also have $(y + 1) \leq x$. However, this contradicts $(x + 1) \leq y$ because $(x + 1) \leq y$ implies $x < y$ while $(y + 1) \leq x$ implies $y < x$. This contradiction means that we have no solution in this case.
So in brief, $x^2 + 4y$ and $y^2 + 4x$ are both perfect squares only for $(x, y) = (0, k^2)$ and $(x, y) = (k^2, 0)$ where $k \in \mathbb{Z}$.

7. Let $A \equiv x^2 + y + z$, $B \equiv x + y^2 + z$ and $C \equiv x + y + z^2$ (where $x, y, z \in \mathbb{Z}$). Show that A, B, C cannot be perfect squares simultaneously if:
(**a**) All of x, y, z are > 0. (**b**) One of x, y, z is < 0 and the other two are > 0.
(**c**) Exactly one of x, y, z is 0.
Solution: We note first that no perfect square can lie between consecutive squares, i.e. the squares of two consecutive integers. For example, if k is an integer then there is no perfect square between k^2 and $(k + 1)^2$ or between k^2 and $(k - 1)^2$.
(**a**) This is because x^2 and $(x + 1)^2$ are consecutive squares and hence if A is a perfect square then it cannot lie between them. This similarly applies to B with regard to y^2 and $(y + 1)^2$ and to C with regard to z^2 and $(z + 1)^2$. Now, if we note that A, B, C are greater than x^2, y^2, z^2 (respectively) then we must have:

$$(x+1)^2 \quad \leq \quad (x^2+y+z) \qquad \rightarrow \qquad (2x+1) \leq (y+z)$$

[36] In this argument we are using the fact that no perfect square can lie between consecutive squares, i.e. the squares of two consecutive integers. For example, if k is an integer then there is no perfect square between k^2 and $(k + 1)^2$ or between k^2 and $(k - 1)^2$. In brief, $x^2 < (x^2 + 4y)$, moreover $(x^2 + 4y)$ cannot be between x^2 and $(x + 1)^2$ and hence we must have $(x + 1)^2 \leq (x^2 + 4y)$.
[37] Again, we are using the fact that no perfect square can lie between consecutive squares, i.e. $(x + 1)^2 < (x^2 + 4y)$, moreover $(x^2 + 4y)$ cannot be between $(x + 1)^2$ and $(x + 2)^2$ and hence we must have $(x + 2)^2 \leq (x^2 + 4y)$.

$$\begin{aligned}(y+1)^2 &\leq (x+y^2+z) \qquad \rightarrow \qquad (2y+1) \leq (x+z)\\ (z+1)^2 &\leq (x+y+z^2) \qquad \rightarrow \qquad (2z+1) \leq (x+y)\end{aligned}$$

Now, if we add the three inequalities on the right (side by side) we obtain:

$$2(x+y+z)+3 \leq 2(x+y+z) \qquad \rightarrow \qquad 3 \leq 0$$

which is nonsensical. So, we conclude that A, B, C cannot be perfect squares simultaneously if all of x, y, z are > 0.
(**b**) Noting the symmetry in the variables, it is sufficient to consider the case of $x < 0$ and $y, z > 0$. Moreover, we can assume (with no loss of generality) that $y \leq z$. Now, we have three cases:
• $|x| < y$ and hence:

$$\begin{aligned}(x-1)^2 &\leq (x^2+y+z) \qquad \rightarrow \qquad (-2x+1) \leq (y+z)\\ (y+1)^2 &\leq (x+y^2+z) \qquad \rightarrow \qquad (2y+1) \leq (x+z)\\ (z+1)^2 &\leq (x+y+z^2) \qquad \rightarrow \qquad (2z+1) \leq (x+y)\end{aligned}$$

On adding the three inequalities on the right (side by side) and simplifying we obtain $-4x+3 \leq 0$ which is nonsensical noting that $x < 0$.
• $y \leq |x| \leq z$ and hence:

$$\begin{aligned}(x-1)^2 &\leq (x^2+y+z) \qquad \rightarrow \qquad (-2x+1) \leq (y+z)\\ (y-1)^2 &\leq (x+y^2+z) \qquad \rightarrow \qquad (-2y+1) \leq (x+z)\\ (x+y+z^2) &\leq z^2 \qquad \rightarrow \qquad (x+y) \leq 0\end{aligned}$$

Now, the first inequality minus the second inequality plus the third inequality lead to $2y \leq 0$ which is nonsensical noting that $y > 0$.
• $|x| > z$ and hence:

$$\begin{aligned}(x-1)^2 &\leq (x^2+y+z) \qquad \rightarrow \qquad (-2x+1) \leq (y+z)\\ (x+y^2+z) &\leq y^2 \qquad \rightarrow \qquad (x+z) \leq 0\\ (x+y+z^2) &\leq z^2 \qquad \rightarrow \qquad (x+y) \leq 0\end{aligned}$$

On adding the three inequalities on the right (side by side) we obtain $1 \leq 0$ which is nonsensical.
So, we conclude that A, B, C cannot be perfect squares simultaneously if one of x, y, z is < 0 and the other two are > 0.
(**c**) Let us assume that only $x = 0$ (noting that the cases of only $y = 0$ and only $z = 0$ can be obtained from the case of only $x = 0$ due to the symmetry of A, B, C in the variables x, y, z). This means that $(y+z)$, (y^2+z) and $(y+z^2)$ are perfect squares. Now, y and z cannot be both < 0 because $(y+z)$ is supposedly a perfect square. So, we must have either $y, z > 0$ or one of y, z is > 0 and the other is < 0. Accordingly:
• $y, z > 0$ and hence:

$$\begin{aligned}(y+1)^2 &\leq (y^2+z) \qquad \rightarrow \qquad (2y+1) \leq z\\ (z+1)^2 &\leq (y+z^2) \qquad \rightarrow \qquad (2z+1) \leq y\end{aligned}$$

On adding the two inequalities on the right (side by side) and simplifying we obtain $(y+z+2) \leq 0$ which is nonsensical noting that $y, z > 0$.
• $y > 0$ and $z < 0$ and hence:

$$\begin{aligned}(y^2+z) &\leq (y-1)^2 \qquad \rightarrow \qquad z \leq (-2y+1)\\ (z-1)^2 &\leq (y+z^2) \qquad \rightarrow \qquad (-2z+1) \leq y\end{aligned}$$

On adding the two inequalities on the right (side by side) and simplifying we obtain $-z \leq -y$ which is nonsensical noting that $y > 0$ and $z < 0$.

• $y < 0$ and $z > 0$: this is similar to the previous case (noting the symmetry).

So, we conclude that A, B, C cannot be perfect squares simultaneously if exactly one of x, y, z is 0.

8. Let $A \equiv x^2 + y + z$, $B \equiv x + y^2 + z$ and $C \equiv x + y + z^2$ (where $x, y, z \in \mathbb{Z}$). Investigate (with regard to the sign of x, y, z) the possibility of A, B, C being perfect squares simultaneously.
Solution: We have eight cases:
• All of x, y, z are 0: this is possible because 0 is a perfect square.
• Two of x, y, z are 0 and the other is positive: this is possible, i.e. $(x, y, z) = (k^2, 0, 0)$, $(0, k^2, 0)$, $(0, 0, k^2)$ where $k \in \mathbb{Z}$.
• Two of x, y, z are 0 and the other is negative: this is impossible because (where we exploit the symmetry to generalize the argument) if $x < 0$ and $y = z = 0$ then A is a perfect square but B and C cannot be perfect squares because they are negative.
• Exactly one of x, y, z is 0: this is impossible (see part c of Problem 7).
• All of x, y, z are < 0: this is possible, e.g. $(x, y, z) = (-3, -4, -4)$, $(-2, -2, -2)$.
• Two of x, y, z are < 0 and the other is > 0: this is possible, e.g. $(x, y, z) = (2, -2, -2)$.
• One of x, y, z is < 0 and the other two are > 0: this is impossible (see part b of Problem 7).
• All of x, y, z are > 0: this is impossible (see part a of Problem 7).

9. Find all $a, b \in \mathbb{Z}$ such that $(a + b)$, $(a^2 + b)$, $(a + b^2)$ are all perfect squares.
Solution: According to part (c) of Problem 7 these cannot be perfect squares simultaneously if $ab \neq 0$. So, the only possibility of these being perfect squares simultaneously is when $ab = 0$, i.e. $(a, b) = (k^2, 0)$ and $(a, b) = (0, k^2)$ where $k \in \mathbb{Z}$.

10. Find all $n \in \mathbb{Z}$ such that $4n^4 + 8n^3 + 12n^2 + 8n + 4$ is a perfect square.
Solution: We have:

$$\begin{aligned} 4n^4 + 8n^3 + 12n^2 + 8n + 4 &= 4\left[n^4 + 2n^3 + 3n^2 + 2n + 1\right] \\ &= 4\left[n^4 + \left(2n^3 + 2n^2\right) + \left(n^2 + 2n + 1\right)\right] \\ &= 4\left[\left(n^2\right)^2 + 2n^2(n+1) + (n+1)^2\right] \\ &= 4\left[n^2 + (n+1)\right]^2 = 2^2\left(n^2 + n + 1\right)^2 = \left[2\left(n^2 + n + 1\right)\right]^2 \end{aligned}$$

Hence, $4n^4 + 8n^3 + 12n^2 + 8n + 4$ is a perfect square for all $n \in \mathbb{Z}$.

11. Find all $n \in \mathbb{Z}$ such that the following expression is a perfect cube: $n^3 + 2n^2 + n + 1$.
Solution: We use in the following solution the fact that no perfect cube can lie between consecutive cubes, i.e. the cubes of two consecutive integers. For example, if k is an integer then there is no perfect cube between k^3 and $(k+1)^3$ or between k^3 and $(k-1)^3$.
Let:

$$\begin{aligned} n^3 &< n^3 + 2n^2 + n + 1 < (n+1)^3 \\ n^3 &< n^3 + 2n^2 + n + 1 < n^3 + 3n^2 + 3n + 1 \\ 0 &< 2n^2 + n + 1 < 3n^2 + 3n + 1 \end{aligned}$$

The solution of the last inequality is $n < -2$ and $n > 0$. This means that $n^3 + 2n^2 + n + 1$ cannot be a perfect cube if $n < -2$ or $n > 0$ because it is between two perfect cubes, and hence $n^3 + 2n^2 + n + 1$ can possibly be a perfect cube only for $n = -2, -1, 0$. On testing these values we find that $n^3 + 2n^2 + n + 1$ is a perfect cube for all these values, (i.e. $n = -2, -1, 0$) and hence these are the solutions to our Problem.

12. Find every integer n that has the following forms simultaneously: $n = 5 + 14k$, $n = 3 + 23s$ and $n = 7 + 33t$ (where $k, s, t \in \mathbb{Z}$).
Solution: We are required to solve the following system of simultaneous congruence equations:

$$n \overset{14}{=} 5 \qquad n \overset{23}{=} 3 \qquad n \overset{33}{=} 7$$

The solution of this system (which can be obtained by the Chinese remainder theorem) is $n \overset{10626}{=} 2119$. So, every $n = 2119 + 10626u$ (where $u \in \mathbb{Z}$) meets the stated requirement.

13. Find all $n \in \mathbb{N}^0$ such that the following expressions are perfect cubes:
(**a**) $n! + 5$. (**b**) $n! + 7$. (**c**) $n! - 14$.
Solution:
(**a**) This is equivalent to solving the Diophantine equation $m^3 = n! + 5$. Now, for $n > 6$ we have $n! \overset{7}{=} 0$ and hence $m^3 \overset{7}{=} 5$. However, $m^3 \overset{7}{=} 5$ has no solution. So, if there is any solution then we must have $0 \leq n \leq 6$. On testing these values of n we find that only $n = 5$ is a solution. So, $n! + 5$ is a perfect cube only for $n = 5$.
(**b**) This is equivalent to solving the Diophantine equation $m^3 = n! + 7$. Now, for $n > 8$ we have $n! \overset{9}{=} 0$ and hence $m^3 \overset{9}{=} 7$. However, $m^3 \overset{9}{=} 7$ has no solution. So, if there is any solution then we must have $0 \leq n \leq 8$. On testing these values of n we find that only $n = 0, 1$ are solutions. So, $n! + 7$ is a perfect cube only for $n = 0, 1$.
(**c**) This is equivalent to solving the Diophantine equation $m^3 = n! - 14$. Now, for $n > 3$ we have $n! \overset{4}{=} 0$ and hence $m^3 \overset{4}{=} -14$. However, $m^3 \overset{4}{=} -14$ has no solution. So, if there is any solution then we must have $0 \leq n \leq 3$. On testing these values of n we find that only $n = 3$ is a solution. So, $n! - 14$ is a perfect cube only for $n = 3$.
14. Show that $(n^5 - 4)$ cannot be a perfect square for any $n \in \mathbb{Z}$.
Solution: For $n < 2$ we have $(n^5 - 4) < 0$ and hence it cannot be a perfect square. Regarding $n \geq 2$, we note that being a perfect square is equivalent to $m^2 = n^5 - 4$ for some $m \in \mathbb{Z}$. However, this equation has no solution.[38] Hence, $(n^5 - 4)$ cannot be a perfect square for any $n \in \mathbb{Z}$.
15. Find all the natural numbers which can be expressed as $n^3 + 5n - 1807$ and end in 1121.
Solution: These numbers are the solutions of the following congruence equation:

$$n^3 + 5n - 1807 \overset{10000}{=} 1121$$

The solutions of this equation are $n = 32 + 10000k$ where $k \in \mathbb{N}^0$ (see § 3.2.1 of V1).

16. Show that every $\mathbb{N} \ni n > 2$ can be written as $n = pk$ or as $n = 4k$ (where p is an odd prime and $k \in \mathbb{N}$).
Solution: If n is odd then $n = pk$ (for some odd $p \in \mathbb{P}$ and $k \in \mathbb{N}$).
If n is even then $n = 2s$ (where $s \in \mathbb{N}$). Now, if s is even then $s = 2k$ and hence $n = 4k$, while if s is odd then $s = tp$ (where $t \in \mathbb{N}$) and hence $n = kp$ (where $k = 2t$). So, is all cases we can write n as $n = pk$ or as $n = 4k$.
17. Show that the sum of two odd squares cannot be a perfect square.
Solution: If $m = 2s + 1$ and $n = 2t + 1$ (where $s, t \in \mathbb{Z}$) then:

$$m^2 + n^2 = 4s^2 + 4s + 1 + 4t^2 + 4t + 1 \overset{4}{=} 2$$

and hence it cannot be a perfect square because the residue of a square (mod 4) is either 0 or 1.
18. Show that any square of an odd number can be written as $8k + 1$ where $k \in \mathbb{N}^0$.
Solution: An odd number n can be written as $n = 2s + 1$ (where $s \in \mathbb{Z}$) and hence:

$$n^2 = (2s + 1)^2 = 4s^2 + 4s + 1 = 4(s^2 + s) + 1 = 4(2k) + 1 = 8k + 1$$

where step 4 is because $(s^2 + s)$ is even (and ≥ 0).

[38] For example, $m^2 \overset{11}{=} n^5 - 4$ has no solution and hence $m^2 = n^5 - 4$ has no solution (see § 2.7.6 of V1).

Chapter 5
Diophantine Equations

This chapter is essentially a continuation to our investigation of Diophantine equations (e.g. their types and the methods of their solution) which we started in the first volume of this book. So, we mostly build (and elaborate) on the material of the first volume about Diophantine equations.

5.1 General Issues about Diophantine Equations

1. It is useful (and recommended) to narrow the domain or/and range of solution when tackling a Diophantine problem (and indeed any number theory or mathematical problem in general).[39] Try to suggest some criteria and considerations that can help in narrowing the domain/range of solution (and hence they should be considered in this effort).
   Solution: The following is just a sample of the criteria and considerations that should be taken into account in this context:
   • Sign considerations: e.g. if the domain/range can be limited to positive or negative numbers.
   • Parity considerations: e.g. if the domain/range can be limited to even or odd numbers (or even to neither and hence we can conclude that there is no solution).
   • Magnitude considerations, e.g. if the domain/range of solution has an upper or a lower limit or a bounded interval.
   • Obvious solutions considerations: e.g. considering the small integers (i.e. those in the neighborhood of 0) solutions by using inspection and intuition.
   • Special and limited cases considerations: e.g. solutions at 0 or infinity or in the absence of certain variable(s).
   • Algebraic manipulations and techniques considerations, e.g. factoring or division/multiplying by a factor could reveal the impossibility or necessity of specific solutions.
   Also see § 6.4.
2. Motivated by Problem 1, try to narrow the domain/range of solution of the following Diophantine equation: $5x^3 + 4y^3 - 9 = 0$ (where $x, y \in \mathbb{Z}$).
   Solution: For example, the domain should be limited by the following restrictions (noting that $5x^3 + 4y^3 = 9$):
   • At least one of x and y must be > 0.
   • $x = 0$ is not a possibility (because $4y^3 = 3^2$ has no solution).
   • $y = 0$ is not a possibility (because $5x^3 = 3^2$ has no solution).
   • x must be odd (to avoid parity violation).
   From the first 3 points we conclude that we must have either $x > 0$ and $y > 0$, or $x > 0$ and $y < 0$, or $x < 0$ and $y > 0$. Now:
   If $x > 0$ and $y > 0$ then (from magnitude considerations) x and y cannot be > 1 and hence we must have $(x, y) = (1, 1,)$ which is a valid solution.
   If $x > 0$ and $y < 0$ then by simple inspection we may find $(x, y) = (13, -14)$ which is another solution (although this does not prove that there is no other solution of this kind).
   If $x < 0$ and $y > 0$ then by inspection we do not find a solution of this kind (although this does not prove that there is no such solution).
   So in brief, this approach of narrowing and inspection can lead us to building the solution step by step (with the possibility of reaching through this to a general logical/mathematical argument that proves

[39] In fact, narrowing the domain of solution does not only make the search for solution easier (by excluding certain possibilities) but can lead to a clue or an insight about the solution or its nature.

that what we found is the entire solution).

3. A common approach for solving a Diophantine equation is to compare it to a similar equation whose solutions are known or whose solutions are easier to obtain. Use this approach to infer the solutions of the following Diophantine equations by comparing them to the solutions of $5x^3+4y^3-9=0$ which we found in Problem 2:
   (**a**) $5x^3-4y^3+9=0$. (**b**) $5x^3+4y^3+9=0$.
   Solution:
   (**a**) If we multiply the given equation by -1 we obtain $5(-x)^3+4y^3-9=0$. On comparing this equation to the equation of Problem 2 we can easily conclude that the solutions of the given equation that correspond to the two solutions found in Problem 2 are $(x,y)=(-1,1)$ and $(x,y)=(-13,-14)$.
   (**b**) If we multiply the given equation by -1 we obtain $5(-x)^3+4(-y)^3-9=0$. On comparing this equation to the equation of Problem 2 we can easily conclude that the solutions of the given equation that correspond to the two solutions found in Problem 2 are $(x,y)=(-1,-1)$ and $(x,y)=(-13,14)$.
   Also see § 6.4.
4. What we mean by "solving a Diophantine equation"?
   Solution: "Solving" (or "finding the solution") of a Diophantine equation should mean *proving* (by an irrefutable logical/mathematical argument) that there is no solution (i.e. when there is no solution) or *finding* all the solutions (either explicitly or through a sort of closed form formula or formulae) with an incontestable argument that there are no other solutions. So, a Diophantine equation is not solved, for instance, by finding a number of solutions (e.g. through inspection or through computational search) even if we know for sure that the equation has no other solutions.
5. Discuss initial sensibility checks and the importance of applying them when tackling a Diophantine equation problem.
   Solution: It is important (and highly recommended) to conduct initial (and basic) sensibility checks as a first step in tackling a Diophantine equation problem before going through the process of solving the problem in detail. The purpose of these checks is to assess the sensibility of the equation quickly (by inspecting its general characteristics) to see if it is possible to have a solution or not. These initial checks may also reveal the obvious solutions of the equation easily without effort or use of any complicated treatment. In fact, applying an initial sensibility checks investigation can save a lot of time trying to solve an equation that has no solution or has an obvious solution and hence it does not require any effort to solve. In the following points we outline some of the most common initial sensibility checks:
   • **Parity checks**: these should be regarded as the first item in the list of sensibility checks. This is due to their simplicity and intuitivity. For example, if we are asked to find the general solution of the Diophantine equation $x^4+4y^3-7x^2-12y+7=0$ (where $x,y\in\mathbb{Z}$) then before we try to solve this equation by using the familiar rules and traditional methods of solving polynomial Diophantine equations (in two variables) we should simply check the parity of this polynomial, and hence we can easily conclude (by checking the parity) that this equation has no solution because the polynomial is always odd and hence it cannot be equal to 0 which is even.
   Parity checks can also reduce the possibilities that to be considered (or the domain or the range of the problem). For example, the equation $18^x+16^y=19^z$ (where $x,y,z\in\mathbb{N}^0$) can have a solution (in principle) but because of parity considerations any potential solution must have either $x=0$ (and $y\neq 0$) or $y=0$ (and $x\neq 0$). So, we have only these possibilities to consider which by simple inspection should lead to the only solution, i.e. $(x,y,z)=(1,0,1)$.
   • **Primality and composity checks**: for example, if we conduct an initial primality check on the Diophantine equation $12x^2+99y^2=7159$ (where $x,y\in\mathbb{Z}$) then it should become obvious that this equation has no solution because 7159 is prime while $12x^2+99y^2=3(4x^2+33y^2)$ which is composite and hence they cannot be equal considering their prime factorization.
   • **Sign and magnitude checks**: for example, the Diophantine equation $3x^4+y^2+z!=0$ (where $x,y,z\in\mathbb{Z}$) has obviously no solution because $3x^4+y^2$ cannot be negative and hence when it is added to $z!$ (which is always positive) the result cannot be zero. Similarly, it is fairly obvious that the Diophantine equation $\frac{1}{x}+\frac{2}{y}+\frac{3}{z}=7$ (where $x,y,z\in\mathbb{Z}$ and $xyz\neq 0$) has no solution because of a magnitude issue

(i.e. the left hand side cannot be greater than 6). Also, the equation $13x^2 + 6y^2 + 5z^4 = 0$ (where $x, y, z \in \mathbb{Z}$) has the obvious (and only) trivial solution (i.e. $x = y = z = 0$) because any sum of (positive multiples of) even natural powers of integers must be a positive natural number unless all the integers are 0.

• **Simple divisibility checks**: for example, it is fairly obvious that the equation $x^4+y^4-x^2-y^2 = 34$ (where $x, y \in \mathbb{Z}$) has no solution because the left hand side is divisible by 4 $\big[$noting that $x^4 - x^2 = (x^2 - x)(x^2 + x)$ where both factors are even and this similarly applies to $y^4 - y^2\big]$ while the right hand side is not divisible by 4.

• **Simple modularity checks**: we mean by this using modular arithmetic rules and techniques to inspect and test the solvability of the given Diophantine equation (where we largely exploit and benefit from the rules that we outlined in § 2.7.6 of V1). For example, it should be fairly obvious (to someone with modest experience in solving Diophantine equations) that the Diophantine equation $20x^2+21y^2 = 22$ (where $x, y \in \mathbb{Z}$) has no solution because by a simple modularity inspection (i.e. via reducing the equation in modulo 5) we find that this equation implies $y^2 \overset{5}{=} 2$ which obviously has no solution (because 2 is a quadratic non-residue of 5) and hence the original Diophantine equation is not solvable.[40]
Also see Problem 7 of § 6.1 as well as § 6.4.

5.2 Polynomial Diophantine Equations

1. Show that the Diophantine equation $x^2 - y^2 = z^3$ has a solution (x, y) for any z (where $x, y, z \in \mathbb{Z}$).
Solution: We have:

$$\begin{aligned} z^3 &= \frac{z^4 + 2z^3 + z^2}{4} - \frac{z^4 - 2z^3 + z^2}{4} = \frac{z^2(z^2 + 2z + 1)}{4} - \frac{z^2(z^2 - 2z + 1)}{4} \\ &= \left[\frac{z(z+1)}{2}\right]^2 - \left[\frac{z(z-1)}{2}\right]^2 \end{aligned}$$

So, for any $z \in \mathbb{Z}$ we have $x = z(z + 1)/2$ and $y = z(z - 1)/2$ that satisfy this equation $\big[$noting that $z(z + 1)$ and $z(z - 1)$ are even$\big]$. The obvious implication of this result is that any cube (of an integer) can be expressed as a difference of two squares (of integers).[41]

2. Solve the following Diophantine equations (where $x, y \in \mathbb{Z}$):

(**a**) $x^5 - 4x^4 + 7x^2 - 11y - 9 = 0$. (**b**) $10x^2 + 2x - 8y^2 = 0$. (**c**) $x + xy + y = 0$.

(**d**) $x^4 + y^4 = 4096$. (**e**) $x^5 - y^5 = 16807$. (**f**) $x^2 + 4x + y^2 - 14y + 48 = 0$.

(**g**) $x^2y - xy^2 - 13 = 0$. (**h**) $x^2 + y^2 = 43275$. (**i**) $x^2 - y^5 - 18 = 0$.

Solution:

(**a**) If we write this equation as $x^5-4x^4+7x^2-9 = 11y$ then we are looking for all $x \in \mathbb{Z}$ such that $P(x) \equiv x^5-4x^4+7x^2-9$ is a multiple of 11. Now, $P(x \overset{11}{=} 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \overset{11}{=} 2, 6, 9, 6, 4, 10, 8, 2, 4, 0, 4$. Therefore, $x = 9 + 11k$ and $y = \frac{P(9+11k)}{11}$ and hence the solutions are (where $k \in \mathbb{Z}$):

$$(x, y) = (9 + 11k,\ 14641k^5 + 54571k^4 + 80586k^3 + 58883k^2 + 21267k + 3033)$$

(**b**) It is obvious that $x = y = 0$ is a solution. So, in the following we consider non-trivial solutions. We convert this equation to a Pell equation form (see § 1.2) by transforming x, that is:

[40] It is worth noting that we can consider parity checks (which we investigated in the first point) as an example of simple modularity (or modular arithmetic) checks. In fact, we can consider parity checks as the simplest modularity checks (since parity checks are based on the modular arithmetic of 2 which is the least modulo in modular arithmetic). However, parity checks (unlike common modularity checks) are not limited to explicit modularity inspection and checks, and hence from this perspective we may consider parity checks as more general than simple modularity checks.

[41] In fact, if we exclude $z = 0$ then we can make a more specific statement, i.e. any cube can be expressed as a difference of two distinct squares.

$10x^2+2x-8y^2=0 \quad \rightarrow \quad 100x^2+20x-80y^2=0 \quad \rightarrow \quad 100x^2+20x+1-1-80y^2=0 \quad \rightarrow$
$(10x+1)^2-1-80y^2=0 \quad \rightarrow \quad X^2-80y^2=1$

This is a Pell equation. Now, $\sqrt{80}=\left[8;\overline{1,16}\right]$. On inspecting the successive rational fraction approximations on the continued fraction ladder we find that the first approximation $[8;1]=9/1$ satisfies the given equation (since $9^2-80\times 1^2=1$) and thus $(X_1,y_1)=(9,1)$. Now, to find the solutions (x,y) of the original equation we need to use the reverse transformation, i.e. $x=(X-1)/10$. However, the last digit of X_n is 9 for odd n and 1 for even n (see § 1.2), and hence to have an integer solution for x_n we take $x_n=(-X_n-1)/10$ for odd n and $x_n=(X_n-1)/10$ for even n. Some of the solutions are:

n	(X_n,y_n)	(x_n,y_n)
1	$(9,\pm 1)$	$(-1,\pm 1)$
2	$(161,\pm 18)$	$(16,\pm 18)$
3	$(2889,\pm 323)$	$(-289,\pm 323)$
4	$(51841,\pm 5796)$	$(5184,\pm 5796)$
5	$(930249,\pm 104005)$	$(-93025,\pm 104005)$
6	$(16692641,\pm 1866294)$	$(1669264,\pm 1866294)$

(**c**) An obvious solution is $(x,y)=(0,0)$. Now, let $xy\neq 0$. If we divide by x and divide by y then we get (respectively):

$$1+y+\frac{y}{x}=0 \qquad\qquad \frac{x}{y}+x+1=0$$

i.e. x divides y and y divides x. Hence, $y=\pm x$ (see rule 9 of § 1.9 of V1) and thus:

$$1+y\pm 1=0 \qquad\qquad \pm 1+x+1=0$$

Now, the $+1$ case leads to $(x,y)=(-2,-2)$ while the -1 case leads to $(x,y)=(0,0)$ which is not acceptable because of the assumption $xy\neq 0$ (noting that this solution is found already).
So in brief, the solutions are $(x,y)=(0,0)$ and $(x,y)=(-2,-2)$.
(**d**) If we write this equation as $x^4+y^4=8^4$ then it should be obvious that this equation has no solution in natural numbers (according to Fermat's last theorem; see § 2.9.5 of V1). Now, if we note that the power (i.e. 4) is even then it should also be obvious that this equation has no solution for any $xy\neq 0$. So, we must have either $x=0$ and $y\neq 0$ (and hence $y=\pm 8$) or $x\neq 0$ and $y=0$ (and hence $x=\pm 8$). So, the only possible solutions are: $(x,y)=(0,\pm 8)$ and $(x,y)=(\pm 8,0)$.
(**e**) We note first that $16807=7^5$ Now, we have 6 cases to consider:
• $x=y=0$: i.e. $0-0=16807$ which is obviously impossible.
• $x,y>0$: if we write this equation as $x^5=y^5+7^5$ then it is obvious that it has no solution (by Fermat's last theorem; see § 2.9.5 of V1).
• $x,y<0$: if we write this equation as $-|x|^5=-|y|^5+7^5$ (which is equivalent to $|y|^5=|x|^5+7^5$) then it is obvious that it has no solution (by Fermat's last theorem).
• $x>0$ and $y<0$: if we write this equation as $x^5+|y|^5=7^5$ then it is obvious that it has no solution (by Fermat's last theorem).
• $x<0$ and $y>0$: if we write this equation as $-|x|^5-y^5=16807$ then it is obvious that it has no solution (noting that the LHS is negative while the RHS is positive).
• $x=0$ and $y\neq 0$ (or $x\neq 0$ and $y=0$): i.e. $-y^5=16807$ and hence $y=-7$ (or $x^5=16807$ and hence $x=7$).
So in brief, we have only two solutions: $(x,y)=(0,-7)$ and $(x,y)=(7,0)$.
(**f**) We have:

$$x^2+4x+y^2-14y+48=0 \qquad \rightarrow \qquad (x+2)^2+(y-7)^2=5 \qquad \rightarrow \qquad X^2+Y^2=5$$

Now, we have 8 solutions for (X,Y), that is:

$$5=(-2)^2+(\pm 1)^2=(-1)^2+(\pm 2)^2=(+1)^2+(\pm 2)^2=(+2)^2+(\pm 1)^2$$

Hence, we have 8 solutions for (x,y), that is:

$(-4,6) \qquad (-4,8) \qquad (-3,5) \qquad (-3,9) \qquad (-1,5) \qquad (-1,9) \qquad (0,6) \qquad (0,8)$

(**g**) If we write this equation as $x^2y - xy^2 = 13$ then we can see that the LHS is always even while the RHS is odd and hence this equation has no solution.
(**h**) The square of an integer is congruent (mod 4) either to 0 or to 1 and hence the LHS is congruent (mod 4) to 0 or 1 or 2. Now, if we note that 43275 is congruent (mod 4) to 3 then it should be obvious that this congruence has no solution.
(**i**) Let us write this equation as $x^2 - 18 = y^5$. Now, the residues of $x^2 - 18$ (mod 11) are: 4, 5, 8, 2, 9, 7, 7, 9, 2, 8, 5 while the residues of y^5 (mod 11) are: 0, 1, 10, 1, 1, 1, 10, 10, 10, 1, 10. Hence, $x^2 - 18 \overset{11}{\neq} y^5$ which implies that the equation has no solution (see § 2.7.6 of V1).

3. Solve the following Diophantine equations (where $x, y \in \mathbb{Z}$):

(**a**) $x^3 + y^3 - x - y = 0$. (**b**) $x^3 + y^3 + x + y = 0$. (**c**) $x^3 + x^2 - y^3 - y^2 = 0$.

(**d**) $x^3 + y^3 + x^2 + y^2 = 0$. (**e**) $x^3 + y^3 - x^2 - y^2 = 0$. (**f**) $x^2 - xy + 6x - y + 2 = 0$.

Solution:
(**a**) We have:

$(x^3 + y^3) - (x + y) = 0 \quad \rightarrow \quad (x + y)(x^2 - xy + y^2) - (x + y) = 0 \quad \rightarrow$

$(x + y)(x^2 - xy + y^2 - 1) = 0$

So, either $x + y = 0$ or $x^2 - xy + y^2 - 1 = 0$. Hence, we have two cases:
• $x + y = 0$ and hence $y = -x$.
• $x^2 - xy + y^2 - 1 = 0$ which is equivalent to $(x - y)^2 + xy - 1 = 0$. Accordingly:
If $(x - y)^2 = 0$ then $x = y$ and hence $xy = x^2 = y^2 = 1$, i.e. $x = y = -1$ or $x = y = 1$.
If $(x - y)^2 = 1$ then $xy = 0$, i.e. $x = y = 0$ (which is inconsistent) or $x = 0$ (and hence $y = \pm 1$) or $y = 0$ (and hence $x = \pm 1$).
If $(x - y)^2 > 1$ then if we write the equation $x^2 - xy + y^2 - 1 = 0$ as $x^2 + y^2 = xy + 1$ then x and y must have the same sign because otherwise the LHS will be greater than 1 (noting that the difference between x and y must be greater than 1 in magnitude) while the RHS will not exceed 1. Now, if we write the equation $(x - y)^2 + xy - 1 = 0$ as $(x - y)^2 - 1 = -xy$ then the LHS must be positive while the RHS must be non-positive (noting that x and y presumably have the same sign). So, this contradiction should lead to the conclusion that there is no solution for $(x - y)^2 > 1$, and hence we have no other solutions.
So in brief, the solutions are (where $k \in \mathbb{Z}$):

$(x, y) = (k, -k) \quad (x, y) = (-1, -1) \quad (x, y) = (1, 1) \quad (x, y) = (0, \pm 1) \quad (x, y) = (\pm 1, 0)$

(**b**) We have:

$(x^3 + y^3) + (x + y) = 0 \quad \rightarrow \quad (x + y)(x^2 - xy + y^2) + (x + y) = 0 \quad \rightarrow$

$(x + y)(x^2 - xy + y^2 + 1) = 0$

So, either $x + y = 0$ or $x^2 - xy + y^2 + 1 = 0$. Hence, we have two cases:
• $x + y = 0$ and hence $y = -x$.
• $x^2 - xy + y^2 + 1 = 0$ which is equivalent to $(x - y)^2 + xy + 1 = 0$. Accordingly:
If $(x - y)^2 = 0$ then $x = y$ and hence $xy = x^2 = y^2 = -1$ which is impossible.
If $(x - y)^2 = 1$ then $x - y = \pm 1$, i.e. $x = y - 1$ or $x = y + 1$ which lead to $y^2 - y + 2 = 0$ or $y^2 + y + 2 = 0$. These equations have no integer solution.
If $(x - y)^2 > 1$ then if we write the equation $x^2 - xy + y^2 + 1 = 0$ as $x^2 + y^2 + 1 = xy$ then x and y must have the same sign because otherwise the LHS will be positive while the RHS cannot be positive. Now, if we write the equation $(x - y)^2 + xy + 1 = 0$ as $(x - y)^2 + 1 = -xy$ then the LHS must be positive while the RHS must be non-positive (noting that x and y presumably have the same sign). So, this contradiction should lead to the conclusion that there is no solution for $(x - y)^2 > 1$.
So in brief, the only solution is: $(x, y) = (k, -k)$ where $k \in \mathbb{Z}$.
(**c**) If we write the equation as $(x^3 - y^3) + (x^2 - y^2) = 0$ then it is obvious that $x = y$ is a solution. So, let us consider the other case, i.e. $x \neq y$:
If $x = 0$ then $y^3 + y^2 = y^2(y + 1) = 0$, i.e. $(x, y) = (0, -1)$.

If $x = 1$ then $y^3 + y^2 - 2 = 0$ which has the solution $y = 1$ (but it is not acceptable because $x \neq y$ although it is included in the previous solution $x = y$).
If $x = -1$ then $y^3 + y^2 = y^2(y + 1) = 0$, i.e. $(x, y) = (-1, 0)$.
Now, we show that $|x| > 1$ is not a possibility except when $x = y$ (which we obtained already). If we write the equation as $x^2(x + 1) = y^2(y + 1)$ then it should be obvious that $(x + 1)$ and $(y + 1)$ must have the same sign (noting that x^2 and y^2 have the same sign and noting as well that $y = 0$ is not a possibility). Now, if we note that x and $(x + 1)$ are consecutive integers and y and $(y + 1)$ are consecutive integers then we must have $x = y$ which is the solution that we obtained already.
So in brief, we have only 3 solutions: $(x, y) = (k, k)$, $(0, -1)$, $(-1, 0)$ where $k \in \mathbb{Z}$.
(**d**) We have 4 (comprehensive) cases: $x = 0$ or $x = \pm 1$ or $|x| > 1$. So, let us consider these cases:
If $x = 0$ then $y^3 + y^2 = y^2(y + 1) = 0$, i.e. $(x, y) = (0, 0)$ and $(x, y) = (0, -1)$.
If $x = 1$ then $y^3 + y^2 + 2 = 0$ which has no solution.
If $x = -1$ then $y^3 + y^2 = y^2(y + 1) = 0$, i.e. $(x, y) = (-1, 0)$ and $(x, y) = (-1, -1)$.
Now, we show that $|x| > 1$ is not a possibility (i.e. it does not lead to new solutions). If we write the equation as $x^2(x+1) = -y^2(y+1)$ then it should be obvious that $(x+1)$ and $(y+1)$ must have opposite signs (noting that x^2 and y^2 have the same sign and noting as well that $y = 0$ is not a possibility). Now, if we note that x and $(x + 1)$ are consecutive integers and y and $(y + 1)$ are consecutive integers then we must have $x^2 = y^2$ (i.e. $x = \pm y$) and $x + 1 = -y - 1$ (i.e. $x = -y - 2$). On substituting $x = \pm y$ in the equation $x^3 + y^3 + x^2 + y^2 = 0$ we get only $(x, y) = (0, 0)$ and $(x, y) = (-1, -1)$ which we obtained already. On substituting $x = -y - 2$ in the equation $x^3 + y^3 + x^2 + y^2 = 0$ we get only $(x, y) = (-1, -1)$ which we obtained already.
So in brief, we have only 4 solutions: $(x, y) = (0, 0)$, $(0, -1)$, $(-1, 0)$, $(-1, -1)$.
(**e**) Let $x = -X$ and $y = -Y$. Now, if we substitute this in the given equation then we get: $-X^3 - Y^3 - X^2 - Y^2 = 0$, i.e. $X^3 + Y^3 + X^2 + Y^2 = 0$. The solutions of this equation (according to part d) are: $(X, Y) = (0, 0)$, $(0, -1)$, $(-1, 0)$, $(-1, -1)$. So, on transforming back to x and y we get: $(x, y) = (0, 0)$, (0,1), (1,0), (1,1).
(**f**) If we write this equation as $x^2 + (6 - y)x + (2 - y) = 0$ then it is a quadratic in x and hence its discriminant must be a perfect square (say k^2), that is:

$$k^2 = (6-y)^2 - 4(2-y) \quad \rightarrow \quad k^2 = y^2 - 8y + 28 \quad \rightarrow \quad k^2 = (y-4)^2 + 12 \quad \rightarrow$$

$$k^2 - (y-4)^2 = 12 \quad \rightarrow \quad \big[k - (y-4)\big]\big[k + (y-4)\big] = 12 \quad \rightarrow \quad (k - y + 4)(k + y - 4) = 12$$

Now, if we factorize 12 as $12 = (\pm 1)(\pm 12) = (\pm 2)(\pm 6) = (\pm 3)(\pm 4)$ and consider all the possibilities of these numeric factors equaling the two factors on the LHS (considering both orders) then by solving the resulting twelve systems of simultaneous equations in k and y (accepting only the integer solutions) we get: $(k, y) = (-4, 2)$, $(-4, 6)$, (4,6), (4,2). Now, if we insert these values of y (i.e. $y = 2$ and $y = 6$) in the given equation we get: $x^2 + 4x = 0$ (whose solutions are $x = 0$ and $x = -4$) and $x^2 - 4 = 0$ (whose solutions are $x = \pm 2$). Hence, the solutions of the given equation are:

$(x, y) = (0, 2)$ $(x, y) = (-4, 2)$ $(x, y) = (-2, 6)$ $(x, y) = (2, 6)$

4. Solve the following Diophantine equations (where $x, y, z \in \mathbb{Z}$):

(**a**) $xy + yz = xyz$. (**b**) $x + y + z = xyz$. (**c**) $x^2yz - 3xy^2z - 2z + 1 = 0$.

(**d**) $x^6 - y^3 + 216z^3 = 0$. (**e**) $x^2 + y^2 + z^2 = 237327$.

Solution:
(**a**) If $y = 0$ then $(x, y, z) = (m, 0, k)$ is a solution where $m, k \in \mathbb{Z}$.
If $y \neq 0$ then we have $x + z = xz$ and hence:
• If $x = 0$ ($z = 0$) then $z = 0$ ($x = 0$) and hence $(x, y, z) = (0, n, 0)$ is a solution where $\mathbb{Z} \ni n \neq 0$.
• If $x \neq 0$ then $x = z(x - 1)$ and hence $z|x$. Similarly, $z = x(z - 1)$ and hence $x|z$. This means $x = z$ (noting that $x = -z$ is not a possibility) and hence we have $2x = xz$, i.e. $z = x = 2$. Thus, we have another solution: $(x, y, z) = (2, n, 2)$ where $\mathbb{Z} \ni n \neq 0$.
So in brief, we have 3 solutions: $(m, 0, k)$, $(0, n, 0)$ and $(2, n, 2)$ where $m, n, k \in \mathbb{Z}$ and $n \neq 0$.
(**b**) If $xyz = 0$ then we have the following solutions: $(x, y, z) = (m, -m, 0)$, $(m, 0, -m)$ and $(0, m, -m)$

where $m \in \mathbb{Z}$. So, in the following we assume $xyz \neq 0$.
Let us first assume that $|x| \leq |y| \leq |z|$. In the following we will show that (with this condition) x must be equal to ± 1. This is because for all the possibilities of $|x| > 1$ we have $|x + y + z| < |xyz|$, e.g.

$$|\pm 2 \pm 2 \pm 2| < |(\pm 2)(\pm 2)(\pm 2)| \qquad |\pm 2 \pm 2 \pm 3| < |(\pm 2)(\pm 2)(\pm 3)| \qquad |\pm 2 \pm 3 \pm 3| < |(\pm 2)(\pm 3)(\pm 3)|$$

Now, we have 2 cases to consider:
• $x = 1$ and hence we have $1 + y + z = yz$, i.e. $y + 1 = z(y - 1)$. This equation means $(y - 1)|(y + 1)$ and hence:

$$\frac{y+1}{y-1} = 1 + \frac{2}{y-1}$$

i.e. $(y - 1)|2$ and hence (noting that $y \neq 0$) $y = 2$ or $y = -1$ or $y = 3$. On substituting $x = 1$ and $y = 2, -1, 3$ in the given equation we get the following solutions: $(x, y, z) = (1, 2, 3)$, $(1, -1, 0)$ and $(1, 3, 2)$. However, because $z \neq 0$ and we are currently assuming $|x| \leq |y| \leq |z|$ we can accept only $(x, y, z) = (1, 2, 3)$.
• $x = -1$ and hence we have $-1 + y + z = -yz$, i.e. $1 - y = z(1 + y)$. This equation means $(1 + y)|(1 - y)$ and hence:

$$\frac{1-y}{1+y} = -1 + \frac{2}{y+1}$$

i.e. $(y + 1)|2$ and hence (noting that $y \neq 0$) $y = -2$ or $y = -3$ or $y = 1$. On substituting $x = -1$ and $y = -2, -3, 1$ in the given equation we get the following solutions: $(x, y, z) = (-1, -2, -3)$, $(-1, -3, -2)$ and $(-1, 1, 0)$. However, because $z \neq 0$ and we are currently assuming $|x| \leq |y| \leq |z|$ we can accept only $(x, y, z) = (-1, -2, -3)$, i.e. $(x, y, z) = -(1, 2, 3)$.
So, assuming that $|x| \leq |y| \leq |z|$ we have only 2 (zero-free) solutions: $(x, y, z) = \pm(1, 2, 3)$. Now, if we lift the condition $|x| \leq |y| \leq |z|$ (noting the symmetry in x, y, z) by permuting x, y, z (and hence permuting the values in these 2 solutions) then we get the following 12 solutions:

$$\pm(1,2,3) \qquad \pm(1,3,2) \qquad \pm(2,1,3) \qquad \pm(2,3,1) \qquad \pm(3,1,2) \qquad \pm(3,2,1)$$

(**c**) If we write this equation as: $z(x^2y - 3xy^2 - 1) = z - 1$ then we can see that $(x^2y - 3xy^2 - 1)$ is always odd and hence if z is odd then the LHS is odd while the RHS is even, while if z is even then the LHS is even while the RHS is odd. Hence, this equation has no solution.
(**d**) If we write this equation as $(x^2)^3 + (6z)^3 = y^3$ then (by Fermat's last theorem)[42] it is obvious that it has no "non-zero" solutions (i.e. solutions with $xyz \neq 0$). Regarding the zero solutions we have three cases:
• $x = 0$ and hence:

$$-y^3 + 216z^3 = 0 \quad \rightarrow \quad y^3 = 216z^3 \quad \rightarrow \quad y^3 = (6z)^3 \quad \rightarrow \quad y = 6z$$

So, the solution in this case is $(x, y, z) = (0, 6k, k)$ where $k \in \mathbb{Z}$.
• $y = 0$ and hence:

$$x^6 + 216z^3 = 0 \quad \rightarrow \quad (x^2)^3 = (-6z)^3 \quad \rightarrow \quad x^2 = -6z \quad \rightarrow \quad (6k)^2 = -6(-6k^2)$$

So, the solution in this case is $(x, y, z) = (6k, 0, -6k^2)$ where $k \in \mathbb{Z}$.
• $z = 0$ and hence:

$$x^6 - y^3 = 0 \quad \rightarrow \quad y^3 = x^6 \quad \rightarrow \quad y^3 = (x^2)^3 \quad \rightarrow \quad y = x^2$$

So, the solution in this case is $(x, y, z) = (k, k^2, 0)$ where $k \in \mathbb{Z}$.
So in brief, we have three main solutions:

$$(x, y, z) = (0, 6k, k) \qquad (x, y, z) = (6k, 0, -6k^2) \qquad (x, y, z) = (k, k^2, 0)$$

(**e**) The number 237327 on the RHS is congruent (mod 8) to 7. Now, the square of an integer is congruent (mod 8) either to 0 or to 1 or to 4 and hence the LHS cannot be congruent (mod 8) to 7. Hence, this equation has no solution (see § 2.7.6 of V1).

[42] Regarding the possibility of y and z being negative, we can exchange their positions and hence we deal with natural solutions. Regarding the possibility of y being positive and z being negative, we can move the z term to the RHS and again dealing with natural solutions. Regarding the possibility of y being negative and z being positive, the equation will obviously have no solution because the LHS is positive while the RHS is negative.

5. Find all $x, y, z \in \mathbb{Z}$ such that $x^2 + y^2 = z^2$ and x, y, z are consecutive integers.
Solution: We have six cases:
• $x < y < z$ and hence $y = x + 1$ and $z = x + 2$. Thus, we have:
$x^2 + (x+1)^2 = (x+2)^2 \quad \rightarrow \quad x^2 - 2x - 3 = 0 \quad \rightarrow \quad (x+1)(x-3) = 0$
i.e. $x = -1$ and $x = 3$. Therefore, we have only two solutions: $(x, y, z) = (-1, 0, 1)$ and $(3, 4, 5)$.
• $x < z < y$ and hence $y = x + 2$ and $z = x + 1$. Thus, we have:
$x^2 + (x+2)^2 = (x+1)^2 \quad \rightarrow \quad x^2 + 2x + 3 = 0$
which has no solution.
• $y < x < z$: this is similar to the first case (with the exchange of x, y which are symmetric). Therefore, we have only two solutions: $(x, y, z) = (0, -1, 1)$ and $(x, y, z) = (4, 3, 5)$.
• $y < z < x$: this is similar to the second case (with the exchange of x, y which are symmetric). Therefore, we have no solution.
• $z < x < y$ and hence $y = x + 1$ and $z = x - 1$. Thus, we have:
$x^2 + (x+1)^2 = (x-1)^2 \quad \rightarrow \quad x^2 + 4x = 0 \quad \rightarrow \quad x(x+4) = 0$
i.e. $x = 0$ and $x = -4$. Therefore, we have only two solutions: $(x, y, z) = (0, 1, -1)$ and $(-4, -3, -5)$.
• $z < y < x$: this is similar to the previous case (with the exchange of x, y which are symmetric). Therefore, we have only two solutions: $(x, y, z) = (1, 0, -1)$ and $(-3, -4, -5)$.
So in brief, we have only eight (x, y, z) solutions which are:
$(-1, 0, 1) \quad (3, 4, 5) \quad (0, -1, 1) \quad (4, 3, 5) \quad (0, 1, -1) \quad (-4, -3, -5) \quad (1, 0, -1) \quad (-3, -4, -5)$
It is worth noting that these results mean that $(3, 4, 5)$ is the only Pythagorean triple with consecutive integers.

6. Solve the following Diophantine equation (where $m, n \in \mathbb{Z}$):

$$3n^3m + 2n^2m - 7m = m^6n + 5m^3n + mn$$

Solution: An obvious solution is $m = 0$ with n being an arbitrary integer, i.e. $(m, n) = (0, k)$ where $k \in \mathbb{Z}$. If $m \neq 0$ then we can divide the two sides by m and obtain:

$$3n^3 + 2n^2 - 7 = n(m^5 + 5m^2 + 1)$$

This equation has no solution due to parity violation, i.e. $(m^5 + 5m^2 + 1)$ is always odd and hence if n is even then we have: odd = even while if n is odd then we have: even = odd.
So in brief, we have only the solution $(m, n) = (0, k)$ where $k \in \mathbb{Z}$.

7. Let $f(x, y) = 120x^5 + 274x^4y + 225x^3y^2 + 85x^2y^3 + 15xy^4 + y^5$. Are there $x, y \in \mathbb{Z}$ such that f is equal to the following integers:
(**a**) 21. (**b**) 27. (**c**) 181. (**d**) 45. (**e**) -105. (**f**) 63.
Solution: In essence, this is a Diophantine equation problem where we are supposed to investigate if there are $x, y \in \mathbb{Z}$ that make f equal to these integers. Now, let us factorize f:

$$\begin{aligned}
f(x,y) &= 120x^5 + (154+120)x^4y + (71+154)x^3y^2 + (14+71)x^2y^3 + (1+14)xy^4 + y^5 \\
&= (120x^5 + 154x^4y + 71x^3y^2 + 14x^2y^3 + xy^4) + (120x^4y + 154x^3y^2 + 71x^2y^3 + 14xy^4 + y^5) \\
&= x(120x^4 + 154x^3y + 71x^2y^2 + 14xy^3 + y^4) + y(120x^4 + 154x^3y + 71x^2y^2 + 14xy^3 + y^4) \\
&= (x+y)\left[120x^4 + 154x^3y + 71x^2y^2 + 14xy^3 + y^4\right] \\
&= (x+y)\left[120x^4 + (94+60)x^3y + (24+47)x^2y^2 + (2+12)xy^3 + y^4\right] \\
&= (x+y)\left[(120x^4 + 94x^3y + 24x^2y^2 + 2xy^3) + (60x^3y + 47x^2y^2 + 12xy^3 + y^4)\right] \\
&= (x+y)\left[2x(60x^3 + 47x^2y + 12xy^2 + y^3) + y(60x^3 + 47x^2y + 12xy^2 + y^3)\right] \\
&= (x+y)(2x+y)\left[60x^3 + 47x^2y + 12xy^2 + y^3\right] \\
&= (x+y)(2x+y)\left[60x^3 + (27+20)x^2y + (3+9)xy^2 + y^3\right] \\
&= (x+y)(2x+y)\left[(60x^3 + 27x^2y + 3xy^2) + (20x^2y + 9xy^2 + y^3)\right]
\end{aligned}$$

$$
\begin{aligned}
&= (x+y)(2x+y)\left[3x(20x^2+9xy+y^2)+y(20x^2+9xy+y^2)\right]\\
&= (x+y)(2x+y)(3x+y)\left[20x^2+9xy+y^2\right]\\
&= (x+y)(2x+y)(3x+y)\left[20x^2+(4+5)xy+y^2\right]\\
&= (x+y)(2x+y)(3x+y)\left[(20x^2+4xy)+(5xy+y^2)\right]\\
&= (x+y)(2x+y)(3x+y)\left[4x(5x+y)+y(5x+y)\right]\\
&= (x+y)(2x+y)(3x+y)(4x+y)(5x+y)
\end{aligned}
$$

As we see:
If $x = y = 0$ then $f = 0$.
If $x = 0$ and $y \neq 0$ then $f = y^5 \neq 0$.
If $x \neq 0$ and $y = 0$ then $f = 120x^5 \neq 0$.
If $x \neq 0$ and $y \neq 0$ and one of these five factors is zero (e.g. when $y = -x$) then $f = 0$.
If $x \neq 0$ and $y \neq 0$ and none of these five factors is zero then $f \neq 0$ is a product of 5 distinct factors.
So in brief, either $f = 0$, or $f = y^5 \neq 0$, or $f = 120x^5 \neq 0$, or $f = abcde$ where a, b, c, d, e are distinct non-zero integers.
(**a**) It is obvious that $21 \neq 0$, $21 \neq y^5$ and $21 \neq 120x^5$. Moreover, if we consider all the possible factorizations of 21 into distinct integer factors then we have:

$$
\begin{aligned}
21 &= (1)(21) = (-1)(-21)\\
&= (3)(7) = (-3)(-7)\\
&= (1)(-1)(-21)\\
&= (1)(3)(7) = (-1)(-3)(7) = (-1)(3)(-7) = (1)(-3)(-7)\\
&= (1)(-1)(-3)(7) = (1)(-1)(3)(-7)
\end{aligned}
$$

As we see, 21 can be factorized only in 2 or 3 or 4 distinct integer factors and hence it cannot be equal to $abcde$. Therefore, f cannot be equal to 21.
(**b**) It is obvious that $27 \neq 0$, $27 \neq y^5$ (noting that $27 = 3^3$) and $27 \neq 120x^5$. Moreover, if we consider all the possible factorizations of 27 into distinct integer factors then we have:

$$
\begin{aligned}
27 &= (1)(27) = (-1)(-27)\\
&= (3)(9) = (-3)(-9)\\
&= (1)(-1)(-27)\\
&= (1)(3)(9) = (-1)(-3)(9) = (-1)(3)(-9) = (1)(-3)(-9)\\
&= (1)(-1)(-3)(9) = (1)(-1)(3)(-9)
\end{aligned}
$$

As we see, 27 can be factorized only in 2 or 3 or 4 distinct integer factors and hence it cannot be equal to $abcde$. Therefore, f cannot be equal to 27.
(**c**) 181 is prime and hence it is obvious that $181 \neq 0$, $181 \neq y^5$ and $181 \neq 120x^5$. Moreover, 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 $p = (1)(-1)(-p)$. Hence, 181 cannot be equal to $abcde$. Therefore, f cannot be equal to 181.
(**d**) $45 \neq 0$, $45 \neq y^5$ and $45 \neq 120x^5$. However, in principle 45 can be equal to $abcde$ because 45 can be factorized into 5 distinct integers, that is:

$$45 = (1)(-1)(3)(-3)(5)$$

Now, $(x + y)$ must be equal to one of these five numeric factors while $(2x + y)$ must be equal to one of the remaining four numeric factors. So, if we consider all the 20 systems of simultaneous equations obtained from the five possibilities of $x+y = (1), (-1), (3), (-3), (5)$ with the four remaining possibilities of $2x+y = (1), (-1), (3), (-3), (5)$ then we can identify x and y values that can potentially make $f = 45$.

These 20 systems with their solutions and the corresponding values of f $\big[$in the form $(x, y, f)\big]$ are given in the following table:

	$\boldsymbol{x+y=1}$	$\boldsymbol{x+y=-1}$	$\boldsymbol{x+y=3}$	$\boldsymbol{x+y=-3}$	$\boldsymbol{x+y=5}$
$\boldsymbol{2x+y=1}$		$(2,-3,-105)$	$(-2,5,-45)$	$(4,-7,-1755)$	$(-4,9,-1155)$
$\boldsymbol{2x+y=-1}$	$(-2,3,105)$		$(-4,7,1755)$	$(2,-5,45)$	$(-6,11,8645)$
$\boldsymbol{2x+y=3}$	$(2,-1,945)$	$(4,-5,-3465)$		$(6,-9,-25515)$	$(-2,7,45)$
$\boldsymbol{2x+y=-3}$	$(-4,5,3465)$	$(-2,1,-945)$	$(-6,9,25515)$		$(-8,13,84645)$
$\boldsymbol{2x+y=5}$	$(4,-3,9945)$	$(6,-7,-21505)$	$(2,1,10395)$	$(8,-11,-118755)$	

As we see, f can take the value 45, i.e. when $(x, y) = (2, -5)$ and when $(x, y) = (-2, 7)$. So, there are $x, y \in \mathbb{Z}$ that make $f = 45$.
(**e**) From the table of part (d) we can see that f can take the value -105, e.g. when $(x, y) = (2, -3)$. So, there are $x, y \in \mathbb{Z}$ that make $f = -105$.
(**f**) $63 \neq 0$, $63 \neq y^5$ and $63 \neq 120x^5$. However, in principle 63 can be equal to $abcde$ because 63 can be factorized into 5 distinct integers, that is:

$$63 = (1)(-1)(3)(-3)(7)$$

Now, if we follow the procedure of part (d) by building a similar table (where $x + y = 5$ and $2x + y = 5$ are replaced by $x + y = 7$ and $2x + y = 7$) then we find that f cannot take the value 63. So, there are no $x, y \in \mathbb{Z}$ that make $f = 63$ (despite the fact that 63 can be factorized into 5 distinct integers, i.e. the possibility of factorization is a necessary but not sufficient condition for f to take the given integer value).

8. Show that if (a, b, c) is a primitive Pythagorean triple then exactly one of a, b, c is divisible by 3, exactly one of a, b, c is divisible by 4, and exactly one of a, b, c is divisible by 5.
Solution: **Regarding the divisibility by 3**, we have $x^2 (x \overset{3}{=} 0, 1, 2) \overset{3}{=} 0, 1, 1$. Thus, either $c^2 \overset{3}{=} 0$ and hence $a^2 \overset{3}{=} 0$ and $b^2 \overset{3}{=} 0$ (which is impossible because this means that all the three numbers are divisible by 3 in contradiction to being primitive) or $c^2 \overset{3}{=} 1$ and hence one of a, b must be congruent (mod 3) to 0 and the other must be congruent (mod 3) to 1 or to 2, i.e. exactly one of a, b, c (i.e. a or b) is divisible by 3.
Regarding the divisibility by 4, it was shown (in Problem 3 of § 4.1.4 of V1) that if (a, b, c) is a primitive Pythagorean triple, then there are coprimes $m, n \in \mathbb{N}$ of opposite parity with $m > n$ such that (a, b, c) is given by Euclid's formula, i.e. $(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$. This means that a is divisible by 4. Moreover, it was shown (in Problem 2 of § 4.1.4 of V1) that if (a, b, c) is a primitive Pythagorean triple then a and b have opposite parity (and hence c is odd). This means that only a is divisible by 4, i.e. exactly one of a, b, c is divisible by 4.
Regarding the divisibility by 5, we have $x^2 (x \overset{5}{=} 0, 1, 2, 3, 4) \overset{5}{=} 0, 1, 4, 4, 1$. Now:
If $c^2 \overset{5}{=} 0$ then one of a^2, b^2 must be congruent (mod 5) to 1 and the other must be congruent (mod 5) to 4 (noting that $a^2 \overset{5}{=} 0$ and $b^2 \overset{5}{=} 0$ is not possible because this contradicts being primitive) and hence exactly one of a, b, c (i.e. c) is divisible by 5.
If $c^2 \overset{5}{=} 1$ then one of a^2, b^2 must be congruent (mod 5) to 0 and the other must be congruent (mod 5) to 1 and hence exactly one of a, b, c (i.e. a or b) is divisible by 5.
If $c^2 \overset{5}{=} 4$ then one of a^2, b^2 must be congruent (mod 5) to 0 and the other must be congruent (mod 5) to 4 and hence exactly one of a, b, c (i.e. a or b) is divisible by 5.
So, in all cases exactly one of a, b, c is divisible by 5.

9. Find all the solutions of the Diophantine equation: $ax + xy + by = c$ where $a, b, c, x, y \in \mathbb{Z}$ and $ab \neq 0$.
Solution: We have $ax + xy + by = c$ and hence $ax + xy + by + ab = ab + c$, i.e. $(x + b)(y + a) = ab + c$. Now, if we consider all the possible 2-factor factorizations of $(ab + c)$ in both orders and equate one factor to $(x + b)$ and the other factor to $(y + a)$ then we get all the possible solutions.
For example, if $a = b = 1$ and $c = 7$ then we have $x + xy + y = 7$ and hence $x + xy + y + 1 = 8$, i.e.

$(x+1)(y+1) = 8$. Thus:

$$(x+1)(y+1) = (-1)(-8) = (-8)(-1) = (1)(8) = (8)(1) = (-2)(-4) = (-4)(-2) = (2)(4) = (4)(2)$$

On considering these eight possibilities we get the following eight (x, y) solutions:
$(-2, -9)$ $(-9, -2)$ $(0, 7)$ $(7, 0)$ $(-3, -5)$ $(-5, -3)$ $(1, 3)$ $(3, 1)$

10. Solve the following Diophantine equations in two variables (where $x, y \in \mathbb{Z}$):
(**a**) $x^2 - 6xy - 3x + 9y + 5 = 0$. (**b**) $3x^3y - 3x^2 + 22x^2y - 7x + 21xy - 3y + 1 = 0$.
(**c**) $7x^2 - x^2y^2 + 13 = 0$. (**d**) $x^2 - xy + 6x - y + 2 = 0$.

Solution: The common feature of these equations is that we can separate the two variables in a way that changes the problem from being a Diophantine equation problem to a polynomial divisibility problem. This essentially converts the problem from being a two-variable Diophantine equation problem to a one-variable divisibility problem (which is generally easier to solve).
(**a**) We have:

$x^2 - 6xy - 3x + 9y + 5 = 0 \quad \rightarrow \quad x^2 - 3x + 5 = 6xy - 9y \quad \rightarrow \quad y = \frac{x^2-3x+5}{6x-9}$

Now, the solutions of the divisibility problem $(6x-9)|(x^2-3x+5)$ are $x = -4, 1, 2, 7$ (see § 6.4 of V1). Hence, the solutions of the given Diophantine equation are: $(x, y) = (-4, -1)$, $(1, -1)$, $(2, 1)$, $(7, 1)$.
(**b**) We have:

$3x^3y - 3x^2 + 22x^2y - 7x + 21xy - 3y + 1 = 0 \quad \rightarrow \quad 3x^3y + 22x^2y + 21xy - 3y = 3x^2 + 7x - 1 \quad \rightarrow$

$y = \frac{3x^2+7x-1}{3x^3+22x^2+21x-3}$

Now, the solution of the divisibility problem $(3x^3 + 22x^2 + 21x - 3)|(3x^2 + 7x - 1)$ is $x = -1$ (see § 6.4 of V1). Hence, the solution of the given Diophantine equation is: $(x, y) = (-1, 1)$.
(**c**) If we write this equation as $x^2 = \frac{13}{y^2-7}$ then we must have $(y^2 - 7)|13$, i.e. $y^2 - 7 = \pm 1, \pm 13$. However, there is no integer solution to any of these four equations. Hence, the given equation has no solution.
(**d**) This equation was solved in Problem 3 by treating it as a quadratic in x. In the present Problem we will solve it as a divisibility problem, that is:

$x^2 - xy + 6x - y + 2 = 0 \quad \rightarrow \quad x^2 - 4 - xy + 6x - y + 6 = 0 \quad \rightarrow \quad x^2 - 4 = xy - 6x + y - 6 \quad \rightarrow$

$x^2 - 4 = (y-6)(x+1) \quad \rightarrow \quad y - 6 = \frac{x^2-4}{x+1}$

Now, the solutions of the divisibility problem $(x+1)|(x^2-4)$ are $x = -4, -2, 0, 2$ (see § 6.4 of V1). Hence, the solutions of the given Diophantine equation are: $(x, y) = (-4, 2)$, $(-2, 6)$, $(0, 2)$, $(2, 6)$.

11. Solve the following Diophantine equations in two variables (where $x, y \in \mathbb{Z}$):
(**a**) $x^2 - y^2 - 12x - 3y + 1 = 0$. (**b**) $x^3 - x^2 - y - 1 = 0$.
(**c**) $x^4 - y^3 + 2y^2 + 3x + 9 = 0$. (**d**) $x^3 - 2y^2 - 7x^2 + 6y - 11 = 0$.

Solution: The common feature of these equations is that we can separate the two variables and hence this Problem is like Problem 10. However, unlike Problem 10 we do not have the luxury of converting a two-variable Diophantine equation problem to a one-variable divisibility problem because we have two equal polynomial expressions in two separate variables. So, we usually need to invent and employ some algebraic (and possibly non-algebraic) tricks (or techniques or considerations). Some of these tricks (or techniques or considerations) are considered in the following solutions.
(**a**) We have:

$x^2 - y^2 - 12x - 3y + 1 = 0 \quad \rightarrow \quad x^2 - 12x = y^2 + 3y - 1 \quad \rightarrow$

$x^2 - 12x + 36 = y^2 + 3y + 35 \quad \rightarrow \quad (x-6)^2 = y^2 + 3y + 35 \quad \rightarrow$

$(2x-12)^2 = (2y)^2 + 12y + 140 \quad \rightarrow \quad (2x-12)^2 = (2y+3)^2 + 131 \quad \rightarrow$

$X^2 - Y^2 = 131 \quad \rightarrow \quad (X-Y)(X+Y) = 131$

where $X = 2x - 12$ and $Y = 2y + 3$. Noting that 131 is prime, we have 4 possibilities of factorization:

$$(X - Y)(X + Y) = (-1)(-131) = (-131)(-1) = (1)(131) = (131)(1)$$

On solving the four 2-equation systems representing these 4 possibilities we get the following solutions:

$$(X, Y) = (-66, -65),\ (-66, 65),\ (66, 65),\ (66, -65)$$

Now, if we use the reverse transformation: $(X, Y) \mapsto (x, y) = \left(\frac{X+12}{2}, \frac{Y-3}{2}\right)$ then we get the following solutions:

$$(x, y) = (-27, -34),\ (-27, 31),\ (39, 31),\ (39, -34)$$

(**b**) If we write this equation as $y = x^3 - x^2 - 1$ then the solutions are: $(x, y) = (k,\ k^3 - k^2 - 1)$ (where $k \in \mathbb{Z}$) and hence we have infinitely many solutions, i.e. one solution for each integer value of x. Some of these solutions are:
$(-3, -37)$ $(-2, -13)$ $(-1, -3)$ $(0, -1)$ $(1, -1)$ $(2, 3)$ $(3, 17)$

(**c**) Let us separate the variables by writing the equation as: $x^4 + 3x = y^3 - 2y^2 - 9$. If we now factorize the two sides we get: $x(x^3 + 3) = (y - 3)(y^2 + y + 3)$. So, we have two possibilities (noting that x and y are free to vary):
• $x = (y - 3)$. Now, if we substitute this in the original equation and simplify we get: $y^4 - 13y^3 + 56y^2 - 105y + 81 = 0$ whose (integer) solution is $y = 3$ and hence $x = 0$.
• $x = (y^2 + y + 3)$. Now, if we substitute this in the original equation and simplify we get:

$$y^8 + 4y^7 + 18y^6 + 40y^5 + 91y^4 + 119y^3 + 167y^2 + 111y + 99 = 0$$

which has no (integer) solution.
So in brief, this equation has only one solution, i.e. $(x, y) = (0, 3)$.
(**d**) If we write this equation as: $x^3 - 7x^2 = 2y^2 - 6y + 11$ then we can see that the LHS is even while the RHS is odd and hence it has no solution.

12. Solve the following Diophantine equations in three variables (where $x, y, z \in \mathbb{Z}$):
(**a**) $14xy - 4x + 12y + z = 10$. (**b**) $x^3 + y^3 + z^3 = 58$. (**c**) $4x^2 + 16y^2 - 9z^2 - 12x + 8y + 10 = 0$.
Solution:
(**a**) If we write this equation as $z = 10 - 14xy + 4x - 12y$ then the solutions are: $(x, y, z) = (k,\ s,\ 10 - 14ks + 4k - 12s)$ (where $k, s \in \mathbb{Z}$) and hence we have infinitely many solutions, i.e. one solution for each pair of integer values of x and y. Some of these solutions are:
$(-5, 0, -10)$ $(-1, 4, 14)$ $(0, 1, -2)$ $(1, 3, -64)$ $(3, -7, 400)$ $(11, 0, 54)$

(**b**) If we reduce this equation modulo 9 we get: $x^3 + y^3 + z^3 \stackrel{9}{=} 4$. Now, the cube of an integer can be congruent (mod 9) only to 0, 1 and 8. Noting that no combination of 3-term sum of these numbers (i.e. 0, 1 and 8) can be congruent (mod 9) to 4, we conclude that this equation has no solution (see § 2.7.6 of V1).
(**c**) We have:

$$\begin{aligned} 4x^2 + 16y^2 - 9z^2 - 12x + 8y + 10 &= (4x^2 - 12x + 9) + (16y^2 + 8y + 1) - (3z)^2 \\ &= (2x - 3)^2 + (4y + 1)^2 - (3z)^2 = 0 \end{aligned}$$

i.e. $(2x-3)^2 + (4y+1)^2 = (3z)^2$. However, the sum of two odd squares cannot be a perfect square (see Problem 17 of § 4). Hence, this equation has no solution.

13. Find a natural number n such that the Diophantine equation $3x + 5y = n$ has exactly 5 solutions in natural numbers (i.e. $x, y \in \mathbb{N}$).
Solution: The simplest approach is to tackle this Problem computationally by searching for the values of n that produce exactly 5 natural solutions. If we do this then we will find (for example) that $n = 68, 71, 73, 74, 76, 77, 90$ solve this Problem. For instance, $3x + 5y = 90$ has the following five natural solutions: $(x, y) = (5, 15),\ (10, 12),\ (15, 9),\ (20, 6),\ (25, 3)$.

14. Find all quadruples of integers whose sum is equal to their product.
Solution: This is a 4-variable Diophantine equation problem, i.e. $x+y+z+w=xyzw$ where $x,y,z,w\in\mathbb{Z}$. Now:
• If $xyzw=0$ then we have the following solutions: $(x,y,z,w)=(0,k,s,-k-s)$, $(k,0,s,-k-s)$, $(k,s,0,-k-s)$, $(k,s,-k-s,0)$ where $k,s\in\mathbb{Z}$.
• If $xyzw\neq 0$ then let assume for the time being that $|x|\leq|y|\leq|z|\leq|w|$. Now, if $|x|>1$ or $|y|>1$ then $|x+y+z+w|<|xyzw|$, e.g.

$$|\pm 2\pm 2\pm 2\pm 2|<|(\pm 2)(\pm 2)(\pm 2)(\pm 2)| \qquad |\pm 1\pm 2\pm 2\pm 2|<|(\pm 1)(\pm 2)(\pm 2)(\pm 2)|$$

Hence, we must have $x=\pm 1$ and $y=\pm 1$.
Similarly, if $|z|>2$ then $|x+y+z+w|<|xyzw|$, e.g.

$$|\pm 1\pm 1\pm 3\pm 3|<|(\pm 1)(\pm 1)(\pm 3)(\pm 3)| \qquad |\pm 1\pm 1\pm 3\pm 4|<|(\pm 1)(\pm 1)(\pm 3)(\pm 4)|$$

Hence, we must have $z=\pm 2$. Now, if we test the 8 combinations of these values of x,y,z (considering the conditions $xyzw\neq 0$ and $|x|\leq|y|\leq|z|\leq|w|$ as well as $x,y,z,w\in\mathbb{Z}$) then we find only 3 solutions which are: $(x,y,z,w)=(1,1,2,4)$, $(1,-1,-2,-2)$, $(-1,1,-2,-2)$. Now, if we lift the condition $|x|\leq|y|\leq|z|\leq|w|$ (noting the symmetry in x,y,z,w) by permuting x,y,z,w (and hence permuting the values in these 3 solutions) then we get 24 solutions in total (i.e. $12+12$ noting that the last two solutions produce the same permutations).

15. Show that the product of every Pythagorean triple is divisible by 60.
Solution: Non-primitive Pythagorean triples are scaled-up versions of primitive Pythagorean triples (because any non-primitive triple can be reduced to primitive by dividing by the common factor)[43] and hence it is enough to prove this proposition for primitive Pythagorean triples. Now, from the result of Problem 8 we can conclude that every Pythagorean triple has factors of 3, 4 and 5 and hence their product must have a factor of $3\times 4\times 5=60$, i.e. every Pythagorean triple is divisible by 60.

16. Show that the Diophantine equation $x^2-y^2+z^2=w$ has a solution (x,y,z) for any w (where $x,y,z,w\in\mathbb{Z}$).
Solution: w is either odd or even. Now, $2n+1=(n+1)^2-n^2+0^2$ (where $n\in\mathbb{Z}$) can represent any odd number, while $2n+2=(n+1)^2-n^2+1^2$ can represent any even number. So, if we choose $z=0$ when w is odd and choose $z=1$ (or $z=-1$) when w is even then we can find $x=n+1$ and $y=n$ (for some $n\in\mathbb{Z}$) that satisfy $x^2-y^2+z^2=w$. The obvious implication of this result is that any integer can be expressed as a sum of two squares (of integers) minus a square (of an integer).

17. Solve the following Diophantine equations (where $x,y\in\mathbb{Z}$):
(**a**) $x^2+xy+2y+2=0$. (**b**) $4x^2+4x-15-y^3=0$. (**c**) $x^3-4y^4+2=0$. (**d**) $x^2+4x=y^2$.
Solution:
(**a**) This is a quadratic equation in x whose discriminant is y^2-8y-8. So, if this equation has a solution then this discriminant must be a perfect square, i.e. $y^2-8y-8=m^2$ (where $m\in\mathbb{Z}$). Hence:
$y^2-8y=m^2+8 \quad\rightarrow\quad y^2-8y+16=m^2+24 \quad\rightarrow\quad (y-4)^2=m^2+24 \quad\rightarrow$
$(y-4)^2-m^2=24 \quad\rightarrow\quad (y-4-m)(y-4+m)=24$
Now, $24=(-1)(-24)=(1)(24)=(-2)(-12)=(2)(12)=(-3)(-8)=(3)(8)=(-4)(-6)=(4)(6)$. So, if we consider equating these 8 factorizations (in both orders) to the factors on the LHS then we obtain 16 systems of simultaneous equations. On solving these systems of equations we find the following integer solutions for y (noting that we ignore the non-integer solutions): $y=-3,11,-1,9$ (corresponding to $m^2=25,25,1,1$). Thus, the solutions (x,y) of the given Diophantine equation are:
$(-1,-3)$ $(4,-3)$ $(-3,11)$ $(-8,11)$ $(0,-1)$ $(1,-1)$ $(-4,9)$ $(-5,9)$
(**b**) We have:

[43] It should be obvious that all non-primitive Pythagorean triples can be obtained from the primitive Pythagorean triples by multiplying the three numbers of the primitive triples by a natural number $k>1$, and hence non-primitive triples can be reduced (or scaled down) to their primitive form by dividing them by this common factor k.

$y^3 = 4x^2 + 4x - 15 \quad \rightarrow \quad y^3 = (2x+1)^2 - 16 \quad \rightarrow \quad y^3 = (2x-3)(2x+5)$

Now, $(2x+5)-(2x-3) = 8$ which means that the gcd of $(2x+5)$ and $(2x-3)$ is a divisor of 8. However, both $(2x+5)$ and $(2x-3)$ are odd and hence the only possible divisor of 8 (and hence a gcd of these factors) is 1. This means $\big[$noting that $y^3 = (2x-3)(2x+5)\big]$ that $(2x+5) = a^3$ and $(2x-3) = b^3$ (where $a, b \in \mathbb{Z}$) and hence:

$$a^3 - b^3 = (a-b)(a^2+ab+b^2) = 8 = (-1)(-8) = (1)(8) = (-2)(-4) = (2)(4)$$

Now, if we consider these 4 factorization possibilities in both orders then we have 8 systems of simultaneous equations (e.g. $a-b=-1$ and $a^2+ab+b^2=-8$). Of these 8 systems the only solvable system in integers is $a-b=2$ and $a^2+ab+b^2=4$ which leads to $(a,b)=(0,-2)$ and $(a,b)=(2,0)$. However, neither of these solutions leads to an acceptable solution for x and y and hence the given Diophantine equation has no solution.

(**c**) If we reduce this equation modulo 4 we get $x^3 + 2 \stackrel{4}{=} 0$ which has no solution and hence the given Diophantine equation has no solution (see § 2.7.6 of V1).

(**d**) We have $x^2 + 4x - y^2 = 0$ which is a quadratic in x and hence:

$$x = \frac{-4 \pm \sqrt{16+4y^2}}{2} = -2 \pm \sqrt{4+y^2}$$

Now, we have two cases:

• $y = 0$ and hence $x = 0, -4$.

• $y \neq 0$ and hence we have no solution. This is because $4+y^2$ must be a perfect square which is impossible because y^2 is a perfect square and hence $4+y^2$ cannot be a perfect square because the difference between two (non-trivial) perfect squares cannot be 4.[44]

So in brief, the given equation has only two solutions: $(x,y) = (0,0)$ and $(x,y) = (-4,0)$.

18. Find the necessary and sufficient conditions for the following Diophantine equation to have a solution:

$$x^2 \pm py + c = 0 \qquad (p \text{ is odd prime coprime to } c)$$

Solution: Regarding the **necessary condition**, if this is solvable then by reducing it in modulo p we get $x^2 + c \stackrel{p}{=} 0$, i.e. $x^2 \stackrel{p}{=} -c$. This means that $-c$ must be a quadratic residue (mod p).

Regarding the **sufficient condition**, we will show that this condition is also sufficient. If $-c$ is a quadratic residue (mod p) then $x^2 + c \stackrel{p}{=} 0$ must be solvable, i.e. we must have some $x \in \mathbb{Z}$ such that $x^2 + c \stackrel{p}{=} 0$. This means that $x^2 + c = \mp py$ (for some $y \in \mathbb{Z}$), i.e. $x^2 \pm py + c = 0$ has an integer solution (x,y) which means $x^2 \pm py + c = 0$ is solvable.

So in brief, the necessary and sufficient condition for the given Diophantine equation to have a solution is that $-c$ is a quadratic residue (mod p).

19. Find all $x, y, z \in \mathbb{Z}$ that satisfy the following equation: $xy + xz + yz = xyz$.

Solution: We have 3 main cases to consider:

• $xyz = 0$ and hence $(x,y,z) = (0,0,k)$ or $(0,k,0)$ or $(k,0,0)$ where $k \in \mathbb{Z}$.

• $xyz \neq 0$ and all x, y, z are positive (i.e. $x, y, z \in \mathbb{N}$). If we divide the two sides by xyz we get $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$ whose solutions were obtained in Problem 7 of § 4.1.10 of V1.

• $xyz \neq 0$ and not all x, y, z are positive (i.e. at least some of them are negative). If we divide the two sides by xyz we get $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$ and hence at least one of x, y, z must be > 0 (because otherwise the LHS will be < 0). In fact, we must have exactly two variables > 0 because otherwise the LHS will be < 1. Now, we have two cases:

One of the positive variables is 1 and hence the other two variables (i.e. the other positive and the negative) must be equal in magnitude and opposite in sign, i.e. $(x,y,z) = (1,k,-k)$ or $(k,1,-k)$ or $(k,-k,1)$.

Both positive variables are > 1 and hence the LHS will be < 1 (i.e. we have no solution). This is

[44] We note that the only solutions to the Diophantine equation $m^2 - n^2 = 4$ are $(m,n) = (\pm 2, 0)$.

because the maximum value of the sum of the terms involving these variables is 1 (i.e. $1/2 + 1/2$) and hence the sum of the three terms must be less than 1.
So in brief, the solutions (x, y, z) are (where $k \in \mathbb{Z}$):

$(0, 0, k)$ $(0, k, 0)$ $(k, 0, 0)$ $(2, 3, 6)$ $(2, 6, 3)$ $(3, 2, 6)$ $(3, 6, 2)$ $(6, 2, 3)$

$(6, 3, 2)$ $(2, 4, 4)$ $(4, 2, 4)$ $(4, 4, 2)$ $(3, 3, 3)$ $(1, k, -k)$ $(k, 1, -k)$ $(k, -k, 1)$

20. Find all $x, y, z \in \mathbb{N}$ such that $x^2 + y^2 - z^2 = 0$ and $60|(xyz)$.
Solution: It is obvious that (x, y, z) is a Pythagorean triple and hence from the result of Problem 15 we conclude that the solutions to this Problem are all the Pythagorean triples.
21. Create a 2-variable polynomial Diophantine equation which has the following solutions: $(x, y) = (3, 5)$, $(-11, 21)$, (1, 12).
Solution: A simple way for solving this type of problems is to use a "graphical approach", e.g. we assume that the equation is a parabola passing through these three points. So, if the parabola is represented by the equation $y = ax^2 + bx + c$ then we have the following system of linear equations in a, b, c:

$$5 = 9a + 3b + c \qquad 21 = 121a - 11b + c \qquad 12 = a + b + c$$

whose solution is $(a, b, c) = (-11/56,\ -19/7,\ 835/56)$. On inserting these values in the equation $y = ax^2 + bx + c$ and multiplying by 56 we get: $56y + 11x^2 + 152x - 835 = 0$. So, this Diophantine equation meets the stated requirement.

5.3 Exponential Diophantine Equations

1. Show that the following Diophantine exponential equations have no solution (where $x, y \in \mathbb{N}^0$):
(**a**) $5^x + 7 = 6^y$. (**b**) $7^x + 3 = 8^y$. (**c**) $8^x + 5 = 9^y$. (**d**) $80^x + 3 = 121^y$. (**e**) $39^x + 2 = 49^y$.
Solution: We note that none of these equations have a solution when $xy = 0$. Hence, in the following we assume $xy \neq 0$.
(**a**) In modulo 5 we have $0 + 2 \stackrel{5}{=} 1$ and hence the given Diophantine equation has no solution.
(**b**) In modulo 7 we have $0 + 3 \stackrel{7}{=} 1$ and hence the given Diophantine equation has no solution.
(**c**) In modulo 8 we have $0 + 5 \stackrel{8}{=} 1$ and hence the given Diophantine equation has no solution.
(**d**) In modulo 4 we have $0 + 3 \stackrel{4}{=} 1$ and hence the given Diophantine equation has no solution.
(**e**) In modulo 13 we have $0 + 2 \stackrel{13}{=} (-3)^y$ which has no solution $\left[\text{noting that } (-3)^{y \stackrel{6}{=} 0,1,2,3,4,5} \stackrel{13}{=} 1, 10, 9, 12, 3, 4\right]$ and hence the given Diophantine equation has no solution.
2. Show that the following Diophantine exponential equations have no solution (where $x, y, z \in \mathbb{N}$):
(**a**) $21^x + 37^y = 46^z$. (**b**) $38^x + 43^y = 79^z$. (**c**) $22^x + 71^y = 83^z$.
Solution:
(**a**) In modulo 5 we have $1 + 2^y \stackrel{5}{=} 1$ (i.e. $2^y \stackrel{5}{=} 0$) and hence the given Diophantine equation has no solution (noting that $2^{y \stackrel{4}{=} 0,1,2,3} \stackrel{5}{=} 1, 2, 4, 3$ and hence $2^y \stackrel{5}{\neq} 0$).
(**b**) In modulo 3 we have $2^x + 1 \stackrel{3}{=} 1$ (i.e. $2^x \stackrel{3}{=} 0$) and hence the given Diophantine equation has no solution (noting that $2^{x \stackrel{2}{=} 0,1} \stackrel{3}{=} 1, 2$ and hence $2^x \stackrel{3}{\neq} 0$).
(**c**) In modulo 7 we have $1 + 1 \stackrel{7}{=} 6^z$ (i.e. $6^z \stackrel{7}{=} 2$) and hence the given Diophantine equation has no solution (noting that $6^{z \stackrel{2}{=} 0,1} \stackrel{7}{=} 1, 6$ and hence $6^z \stackrel{7}{\neq} 2$).
3. Find all $x, y \in \mathbb{N}^0$ such that:
(**a**) $2^x - 3^y = 1$. (**b**) $3^x - 2^y = 1$.
Solution:
(**a**) We have two cases:
• x is odd: if we reduce the equation in modulo 3 we get $2 - 1 \stackrel{3}{=} 1$ (if $y = 0$) or $2 - 0 \stackrel{3}{=} 1$ (if $y > 0$). So, the only solution is $(x, y) = (1, 0)$.
• x is even: i.e. $4^k - 3^y = 1$ (where $x = 2k$ with $k \in \mathbb{N}^0$). The only solution to this equation is $k = y = 1$

(see part a of Problem 3 of § 4.1.7 of V1). So, the only solution is $(x, y) = (2, 1)$.
So in brief, the given equation has only two solutions: $(x, y) = (1, 0)$ and $(2, 1)$.
(**b**) We have two cases:
• x is odd: if we reduce the equation in modulo 8 we get:

$3 - 1 \stackrel{8}{=} 1$ (if $y = 0$) $\quad 3 - 2 \stackrel{8}{=} 1$ (if $y = 1$) $\quad 3 - 4 \stackrel{8}{=} 1$ (if $y = 2$) $\quad 3 - 0 \stackrel{8}{=} 1$ (if $y > 2$)

So, the only solution in this case is $(x, y) = (1, 1)$.
• x is even: i.e. $3^{2k} - 2^y = 1$ (where $x = 2k$ with $k \in \mathbb{N}$ noting that $x = 0$ is impossible). Accordingly:

$$3^{2k} - 1 = 2^y \quad \rightarrow \quad (3^k - 1)(3^k + 1) = 2^y$$

i.e. $3^k - 1 = 2^m$ and $3^k + 1 = 2^n$ (where $m, n \in \mathbb{N}$ with $m < n$ and $m + n = y$). Now, if we subtract the first of the last two equations from the second we get $2 = 2^n - 2^m$, i.e. $2 = 2^m(2^{n-m} - 1)$. The only solution to the last equation is $m = 1$ and $n = 2$ and hence $y = 3$. So, the only solution in this case is $(x, y) = (2, 3)$.
So in brief, the given equation has only two solutions: $(x, y) = (1, 1)$ and $(2, 3)$.

4. Find all $x, y \in \mathbb{N}^0$ such that:
(**a**) $10^x + 7 = 2^y$. (**b**) $4^x - 7 = 9^y$. (**c**) $3^x - 8 = 11^y$. (**d**) $5^x - 9 = 2^y$.
(**e**) $4^x - 3^y = 7$. (**f**) $5^x - 3^y = 2$. (**g**) $3^x - 5^y = 4$.

Solution:
(**a**) We obviously have parity violation unless:
• $x = 0$ and $y \neq 0$ and hence we have $1 + 7 = 2^y$, i.e. $(x, y) = (0, 3)$.
• $x \neq 0$ and $y = 0$ and hence we have $10^x + 7 = 1$ which has no solution.
So, the only solution to the given equation is $(x, y) = (0, 3)$.
(**b**) This equation has no solution if $xy = 0$. Hence, in the following we assume $xy \neq 0$.
If we reduce the equation in modulo 5 we get $(-1)^x - 2 \stackrel{5}{=} (-1)^y$ and hence x must be even (say $x = 2k$ where $k \in \mathbb{N}$) and y must be odd. Hence:

$$4^{2k} - 7 = 9^y \quad \rightarrow \quad 4^{2k} - 7 = 3^{2y} \quad \rightarrow \quad 4^{2k} - 3^{2y} = 7 \quad \rightarrow \quad (4^k - 3^y)(4^k + 3^y) = 7$$

Now, if we consider the factorization of 7 then we can easily conclude that the only possibility is $4^k - 3^y = 1$ and $4^k + 3^y = 7$, i.e. $k = y = 1$.
So, the only possible solution to the given equation is $(x, y) = (2, 1)$.
(**c**) If $xy = 0$ then we have only one solution, i.e. $(x, y) = (2, 0)$. So, in the following we assume $xy \neq 0$.
If we reduce the equation in modulo 3 we get $0 + 1 \stackrel{3}{=} (-1)^y$ and hence y must be even, i.e. $3^x - 8 = 11^{2s}$ (where $s \in \mathbb{N}$).
If we reduce the equation in modulo 4 we get $(-1)^x - 0 \stackrel{3}{=} (-1)^{2s}$ and hence x must be even, i.e. $3^{2k} - 8 = 11^{2s}$ (where $k \in \mathbb{N}$). Accordingly:

$$3^{2k} - 8 = 11^{2s} \quad \rightarrow \quad 3^{2k} - 11^{2s} = 8 \quad \rightarrow \quad (3^k - 11^s)(3^k + 11^s) = 8$$

Now, if we consider the factorization of 8 then we can easily conclude that the only possibility is $3^k - 11^s = 2$ and $3^k + 11^s = 4$, i.e. $k = 1$ and $s = 0$ and hence $(x, y) = (2, 0)$. However, we are currently assuming $xy \neq 0$ (noting that this solution is obtained already).
So, the only solution to this equation is $(x, y) = (2, 0)$.
(**d**) This equation has no solution if $xy = 0$. Hence, in the following we assume $xy \neq 0$.
If we reduce the equation in modulo 3 we get $(-1)^x - 0 \stackrel{3}{=} (-1)^y$ and hence x and y must have the same parity.
If we reduce the equation in modulo 5 we get $0 + 1 \stackrel{5}{=} 2^y$. Now, $2^{y \stackrel{4}{=} 0,1,2,3} \stackrel{5}{=} 1, 2, 4, 3$ and hence we must have $y \stackrel{4}{=} 0$ (say $y = 4s$ where $s \in \mathbb{N}$). But since x and y have the same parity then x must be even (say $x = 2k$ where $k \in \mathbb{N}$). Accordingly:

$$5^{2k} - 9 = 2^{4s} \quad \rightarrow \quad 5^{2k} - 9 = 4^{2s} \quad \rightarrow \quad 5^{2k} - 4^{2s} = 9 \quad \rightarrow \quad (5^k - 4^s)(5^k + 4^s) = 9$$

Now, if we consider the factorization of 9 then we can easily conclude that the only possibility is $5^k - 4^s = 1$ and $5^k + 4^s = 9$, i.e. $k = s = 1$.

So, the only solution to this equation is $(x, y) = (2, 4)$.

(**e**) This equation has no solution if $xy = 0$. Hence, in the following we assume $xy \neq 0$.

If we reduce the equation in modulo 4 we get $0 - (-1)^y \stackrel{4}{=} -1$ and hence y must be even (say $y = 2s$ where $s \in \mathbb{N}$). Accordingly:

$$4^x - 3^{2s} = 7 \quad \rightarrow \quad 2^{2x} - 3^{2s} = 7 \quad \rightarrow \quad (2^x - 3^s)(2^x + 3^s) = 7$$

Now, if we consider the factorization of 7 then we can easily conclude that the only possibility is $2^x - 3^s = 1$ and $2^x + 3^s = 7$, i.e. $x = 2$ and $s = 1$.

So, the only solution to this equation is $(x, y) = (2, 2)$.

(**f**) In modulo 9 we have $5^{x \stackrel{6}{=} 0,1,2,3,4,5} \stackrel{9}{=} 1, 5, 7, 8, 4, 2$. Also:

$$3^y \stackrel{9}{=} 1 \text{ (if } y = 0) \qquad 3^y \stackrel{9}{=} 3 \text{ (if } y = 1) \qquad 3^y \stackrel{9}{=} 0 \text{ (if } y > 1)$$

So, $5^x - 3^y$ can be congruent to 2 (mod 9) only in the following two cases:

- $5^x \stackrel{9}{=} 5$ and $3^y \stackrel{9}{=} 3$: i.e. $5^x - 3^1 = 2$ which has only the solution $(x, y) = (1, 1)$.
- $5^x \stackrel{9}{=} 2$ and $3^y \stackrel{9}{=} 0$: i.e. $x \stackrel{6}{=} 5$ and $y > 1$. Hence, we have (where $k, s \in \mathbb{N}^0$):

$$5^{5+6k} - (9)3^s = 2 \quad \rightarrow \quad 17 - (9)3^s \stackrel{28}{=} 2 \quad \rightarrow \quad (9)3^s \stackrel{28}{=} 15 \quad \rightarrow$$

$$3^s \stackrel{28}{=} 9^* \times 15 \quad \rightarrow \quad 3^s \stackrel{28}{=} 25 \times 15 \quad \rightarrow \quad 3^s \stackrel{28}{=} 11$$

The last congruence has no solution (noting that $3^{s \stackrel{6}{=} 0,1,2,3,4,5} \stackrel{28}{=} 1, 3, 9, 27, 25, 19$). Hence, we have no solution in this case.

So in brief, the given equation has only one solution: $(x, y) = (1, 1)$.

(**g**) In modulo 9 we have $3^{x=0,1,>1} \stackrel{9}{=} 1, 3, 0$ and $5^{y \stackrel{6}{=} 0,1,2,3,4,5} \stackrel{9}{=} 1, 5, 7, 8, 4, 2$. So, $3^x - 5^y$ can be congruent to 4 (modulo 9) only in the following two cases:

- $3^x \stackrel{9}{=} 3$ and $5^y \stackrel{9}{=} 8$: i.e. $3^1 - 5^y = 4$ which has no solution.
- $3^x \stackrel{9}{=} 0$ and $5^y \stackrel{9}{=} 5$: i.e. $x > 1$ and $y \stackrel{6}{=} 1$. Hence, we have (where $k, s \in \mathbb{N}^0$):

$$(9)3^s - 5^{1+6k} = 4 \quad \rightarrow \quad (9)3^s - 5 \stackrel{28}{=} 4 \quad \rightarrow \quad (9)3^s \stackrel{28}{=} 9 \quad \rightarrow$$

$$3^s \stackrel{28}{=} 9^* \times 9 \quad \rightarrow \quad 3^s \stackrel{28}{=} 25 \times 9 \quad \rightarrow \quad 3^s \stackrel{28}{=} 1$$

The last congruence has the solution $s = 6a$ (where $a \in \mathbb{N}^0$). Accordingly:

$$3^x - 5^y = 4 \quad \rightarrow \quad 3^{2+6a} - 5^y = 4 \quad \rightarrow \quad 3^{2+6a} - 4 = 5^y \quad \rightarrow \quad (3^{1+3a} - 2)(3^{1+3a} + 2) = 5^y$$

i.e. $3^{1+3a} - 2 = 5^m$ and $3^{1+3a} + 2 = 5^n$ (where $m, n \in \mathbb{N}^0$ with $m < n$ and $m + n = y$). Now, if we add the last two equations we get:

$$2(3^{1+3a}) = 5^m + 5^n \quad \rightarrow \quad 2(3^{1+3a}) = 5^m(1 + 5^{n-m})$$

Thus, m must be zero (because there is no factor on the LHS that can match a natural power of 5) and hence we have:

$$3^{1+3a} - 2 = 1 \quad \rightarrow \quad 3^{1+3a} = 3 \quad \rightarrow \quad a = 0$$

i.e. $x = 2$ and hence $3^2 - 5^y = 4$ whose solution is $y = 1$.

So in brief, the given equation has only one solution: $(x, y) = (2, 1)$.

5. Find all $x, y, z \in \mathbb{N}^0$ such that:

(**a**) $3^x + 4^y = 8^z$. (**b**) $4^x - 2^y = 15^z$. (**c**) $4^x - 3^y = 15^z$. (**d**) $4^x + 15^y = 2^z$.

(**e**) $4^x + 5^y = 6^z$. (**f**) $13^x + 9^y = 14^z$. (**g**) $3^x + 4^y = 5^z$.

Solution:

(**a**) We obviously have parity violation unless:

- $y = 0$ and $z \neq 0$ and hence we have $3^x + 1 = 8^z$. On reducing this equation in modulo 7 we get $3^x + 1 \stackrel{7}{=} 1$ (i.e. $3^x \stackrel{7}{=} 0$) which has no solution. So, we have no solution in this case.
- $y \neq 0$ and $z = 0$ and hence we have $3^x + 4^y = 1$. The LHS is obviously greater than 1 and hence we have no solution in this case.

So in brief, this equation has no solution.

(**b**) We obviously have parity violation unless:
• $x = 0$ and $y \neq 0$ and hence we have $1 - 2^y = 15^z$ which obviously has no solution because the LHS is negative while the RHS is positive.
• $x \neq 0$ and $y = 0$ and hence we have $4^x - 1 = 15^z$. Now, if we reduce this equation in modulo 5 we get $(-1)^x - 1 \stackrel{5}{=} 0$ and hence x must be even (say $x = 2k$ where $k \in \mathbb{N}$). Accordingly:

$$4^{2k} - 1 = 15^z \qquad \rightarrow \qquad (4^k - 1)(4^k + 1) = 15^z$$

Now, the difference between $(4^k - 1)$ and $(4^k + 1)$ is 2 (noting that $4^k - 1$ and $4^k + 1$ cannot match 15^z in factorization sensibly unless $4^k - 1 = 3$ and $4^k + 1 = 5$) and hence the only possibility is $k = z = 1$. So in brief, the only possible solution to the given equation is $(x, y, z) = (2, 0, 1)$.
(**c**) If both y and z are greater than zero then we have no solution because in modulo 3 we have $1-0 \stackrel{3}{=} 0$ which is nonsensical. Hence, if we have any solution then y or z must be zero. So, we have two cases:
• $y = 0$ and hence $4^x - 1 = 15^z$. This equation was solved in part (b) where we found that the solution is $(x, y, z) = (2, 0, 1)$.
• $z = 0$ and hence $4^x - 3^y = 1$. This equation was solved in Problem 3 of § 4.1.7 of V1 where we found that its only solution is $x = y = 1$. Hence, in this case we have $(x, y, z) = (1, 1, 0)$.
So in brief, the only solutions to the given equation are $(x, y, z) = (2, 0, 1)$ and $(1, 1, 0)$.
(**d**) We obviously have parity violation unless:
• $x \neq 0$ and $z = 0$ and hence $4^x + 15^y = 1$. This case has obviously no solution because the LHS is greater than 1.
• $x = 0$ and $z \neq 0$ and hence $1 + 15^y = 2^z$. Now:
If $y = 0$ then we have $z = 1$ and hence $(x, y, z) = (0, 0, 1)$.
If $y > 0$ then on reducing the equation in modulo 3 we get $1 + 0 \stackrel{3}{=} 2^z$ and hence z must be even (say $z = 2k$ where $k \in \mathbb{N}$) because $2^{z \stackrel{2}{=} 0,1} \stackrel{3}{=} 1, 2$. Therefore, we have:

$$1 + 15^y = 2^{2k} \qquad \rightarrow \qquad 15^y = 2^{2k} - 1 \qquad \rightarrow \qquad 15^y = (2^k - 1)(2^k + 1)$$

Now, the difference between $(2^k - 1)$ and $(2^k + 1)$ is 2 and hence one of these factors must be of magnitude 3 and the other of magnitude 5 (noting that no other possibility can match the factorization of 15^y). Simple inspection will reveal that k must be 2 (i.e. $z = 4$) and hence $y = 1$. So, we have $(x, y, z) = (0, 1, 4)$.
So in brief, the given equation has only two solutions: $(x, y, z) = (0, 0, 1)$ and $(x, y, z) = (0, 1, 4)$.
(**e**) We obviously have parity violation unless:
• $x \neq 0$ and $z = 0$ and hence we have $4^x + 5^y = 1$. The LHS is obviously greater than 1 and hence we have no solution in this case.
• $x = 0$ and $z \neq 0$ and hence we have $1+5^y = 6^z$. On reducing this equation in modulo 4 we get $1+1 \stackrel{4}{=} 2^z$ and hence z must be 1 (because $2^{y=0,1,>1} \stackrel{4}{=} 1, 2, 0$) and so we get the solution $(x, y, z) = (0, 1, 1)$.
So in brief, the given equation has only one solution: $(x, y, z) = (0, 1, 1)$.
(**f**) We have two main cases to consider:
• $xyz = 0$: it is obvious that z must be greater than 0 to avoid parity violation (as well as magnitude violation). Moreover, x and y cannot be both 0 because the LHS will become less than the RHS. So, EITHER:
$x = 0$ and $y \neq 0$ and hence we have $1 + 9^y = 14^z$. If we reduce this equation in modulo 4 we get $1 + 1 \stackrel{4}{=} 2^z$ whose only solution is $z = 1$ (noting that $2^{z=0,1,>1} \stackrel{4}{=} 1, 2, 0$). However, $1 + 9^y = 14^1$ has no solution and hence $x = 0$ and $y \neq 0$ do not lead to a solution to the given Diophantine equation. OR:
$x \neq 0$ and $y = 0$ and hence we have $13^x + 1 = 14^z$. If we reduce this equation in modulo 4 we get $1 + 1 \stackrel{4}{=} 2^z$ whose only solution is $z = 1$ (noting that $2^{z=0,1,>1} \stackrel{4}{=} 1, 2, 0$). Accordingly, we have $13^x + 1 = 14^1$ whose solution is $x = 1$ and hence the given Diophantine equation has the solution $(x, y, z) = (1, 0, 1)$.
• $xyz \neq 0$: in modulo 4 we have $1 + 1 \stackrel{4}{=} 2^z$ and hence z must be 1 (noting that $2^{z=0,1,>1} \stackrel{4}{=} 1, 2, 0$). So, we have $13^x + 9^y = 14^1$ which has no solution because the LHS is greater than the RHS (noting that $x > 0$ and $y > 0$).

So in brief, the given equation has only one solution, i.e. $(x, y, z) = (1, 0, 1)$.
(**g**) We have two main cases to consider:
• $xyz = 0$: it is obvious that $x = y = z = 0$ is not a possibility. Similarly, exactly two of the three variables are zero is not a possibility. Regarding the case of exactly one of the three variables is zero, we have:
$z = 0$ and hence $3^x + 4^y = 1$ which has no solution because the LHS is > 1.
$y = 0$ and hence $3^x + 1 = 5^z$ which is impossible because of parity violation.
$x = 0$ and hence $1 + 4^y = 5^z$. Now, in modulo 3 we have $1 + 1 \stackrel{3}{=} 2^z$ and hence z is odd (say $z = 2t + 1$ where $t \in \mathbb{N}^0$) noting that $2^{z \stackrel{2}{=} 0,1} \stackrel{3}{=} 1, 2$. So we have (see Eq. 12 in V1):

$$1 + 4^y = 5^{2t+1} \quad \rightarrow \quad 4^y = 5^{2t+1} - 1 \quad \rightarrow \quad 4^y = (5-1)\sum_{k=0}^{2t} 5^k \quad \rightarrow \quad 4^y = 4\sum_{k=0}^{2t} 5^k$$

Now, if $y = 1$ then we have $1 = \sum_{k=0}^{2t} 5^k$ and hence $t = 0$, i.e. $z = 1$. So, we have the solution: $(x, y, z) = (0, 1, 1)$. But if $y > 1$ then we have $4^{y-1} = \sum_{k=0}^{2t} 5^k$. On reducing this equation in modulo 4 we get $0 \stackrel{4}{=} \sum_{k=0}^{2t} 1$ which is nonsensical because the sum on the RHS is odd. So, we have no more solutions in this case.
• $xyz \neq 0$: if we reduce the equation $3^x + 4^y = 5^z$ in modulo 3 we get $0 + 1 \stackrel{3}{=} (-1)^z$ and hence z must be even (say $z = 2t$ where $t \in \mathbb{N}$). Also, if we reduce the equation $3^x + 4^y = 5^z$ in modulo 4 we get $(-1)^x + 0 \stackrel{4}{=} 1$ and hence x must be even. So in brief, both x and z are even. Accordingly:

$$3^x + 4^y = 5^z \quad \rightarrow \quad 3^x + 2^{2y} = 5^{2t} \quad \rightarrow \quad 5^{2t} - 2^{2y} = 3^x \quad \rightarrow \quad (5^t - 2^y)(5^t + 2^y) = 3^x$$

i.e. $5^t - 2^y = 3^m$ and $5^t + 2^y = 3^n$ (where $m, n \in \mathbb{N}^0$ with $m < n$ and $m + n = x$). Now, if we add the last two equations we get:

$$2(5^t) = 3^m + 3^n \quad \rightarrow \quad 2(5^t) = 3^m(1 + 3^{n-m})$$

Thus, m must be zero (because there is no factor on the LHS that can match a natural power of 3) and hence we have:

$$5^t - 2^y = 1 \quad \text{and} \quad 5^t + 2^y = 3^x$$

Now, if we reduce the equation $5^t - 2^y = 1$ in modulo 3 we get:

$$(-1)^t - (-1)^y \stackrel{3}{=} 1$$

So, t must be odd and y must be even. Now:
If $y = 2$ then from the equation $5^t - 2^y = 1$ we get $t = 1$ (i.e. $z = 2$) and hence $x = 2$. So, we have the solution $(x, y, z) = (2, 2, 2)$.
If $y > 2$ then if we reduce the equation $5^t + 2^y = 3^x$ in modulo 8 we get $5^t + 0 \stackrel{8}{=} 1$ (since x is even noting that $3^{x \stackrel{2}{=} 0,1} \stackrel{8}{=} 1, 3$) and hence t must be even (noting that $5^{t \stackrel{2}{=} 0,1} \stackrel{8}{=} 1, 5$). But this contradicts what we found earlier that t is odd. So, this contradiction leads to the conclusion that y cannot be greater than 2.
So in brief, the only solutions to the given equation are $(x, y, z) = (0, 1, 1)$ and $(2, 2, 2)$.

5.4 Mixed Polynomial-Exponential Diophantine Equations

1. Find all the solutions of the following Diophantine equations (where $x \in \mathbb{Z}$ and $y \in \mathbb{N}^0$):
(**a**) $x^2 + x + 1 = 3^y$. (**b**) $x^2 + x + 1 = 4^y$. (**c**) $x^2 + x + 1 = 5^y$.

Solution:
(**a**) We have three cases to consider:
• $y = 0$ and hence $x^2 + x = 0$ whose solutions are $x = 0$ and $x = -1$. Hence, $(x, y) = (0, 0)$ and $(x, y) = (-1, 0)$ are solutions.
• $y = 1$ and hence $x^2 + x - 2 = 0$ whose solutions are $x = -2$ and $x = 1$. Hence, $(x, y) = (-2, 1)$ and $(x, y) = (1, 1)$ are solutions.
• $y > 1$ and hence $x^2 + x + 1 = 9(3^{y-2})$. Now, if we reduce this equation in modulo 9 we get $x^2 + x + 1 \stackrel{9}{=} 0$ which has no solution and hence the original equation has no solution.

So in brief, the given Diophantine equation has only those four solutions.
(**b**) We have two cases to consider:
• $y = 0$ and hence (from part a) we get $(x, y) = (0, 0)$ and $(x, y) = (-1, 0)$.
• $y > 0$ and hence on reducing the equation $x^2 + x + 1 = 4^y$ in modulo 4 we get $x^2 + x + 1 \stackrel{4}{=} 0$ which has no solution and hence the original equation has no solution.
So in brief, the given Diophantine equation has only those two solutions.[45]
(**c**) This is exactly like part (b) (but we reduce in modulo 5 instead of modulo 4) and hence the only solutions are $(x, y) = (0, 0)$ and $(x, y) = (-1, 0)$.

2. Let $x, y \in \mathbb{N}^0$. Show that $4^x - 3^y = z$ has no solution for $z = 2, 4, 5, 6, 8, 9, 10, 11, 12$.
Solution: We note first that if $xy = 0$ then there is no solution to $4^x - 3^y = z$ for any one of these values of z (as direct test can easily reveal) and hence in the following we assume $x, y > 0$.
Now, $(4^x - 3^y)$ is odd for all $x, y \in \mathbb{N}$ and hence z cannot be 2, 4, 6, 8, 10, 12. Hence, $4^x - 3^y = z$ has no solution for $z = 2, 4, 6, 8, 10, 12$.
Regarding $4^x - 3^y = 5$, if we reduce this equation modulo 3 we get $1^x \stackrel{3}{=} 2$ which has no solution and hence $4^x - 3^y = 5$ has no solution (see § 2.7.6 of V1). This similarly applies to $4^x - 3^y = 11$ and hence $4^x - 3^y = 11$ has no solution.
Regarding $4^x - 3^y = 9$, if we reduce this equation modulo 3 we get $1^x \stackrel{3}{=} 0$ which has no solution and hence $4^x - 3^y = 9$ has no solution.

3. Solve the following Diophantine equations (where $m, n \in \mathbb{N}^0$ and $k \in \mathbb{Z}$):
(**a**) $7^m = 8^n + 2k$. (**b**) $7^m = 8^n + k$.
Solution:
(**a**) We have 4 main cases:
• $m = n = 0$: the solution is $(m, n, k) = (0, 0, 0)$.
• $m = 0$ and $n > 0$: there is no solution due to parity violation.
• $m > 0$ and $n = 0$: the solutions are $(m, n, k) = \left(m, 0, \frac{7^m-1}{2}\right)$, e.g. $(1, 0, 3)$, $(2, 0, 24)$, $(3, 0, 171)$.
• $m > 0$ and $n > 0$: there is no solution due to parity violation.
(**b**) We have 4 main cases:
• $m = n = 0$: the solution is $(m, n, k) = (0, 0, 0)$.
• $m = 0$ and $n > 0$: the solutions are $(m, n, k) = (0, n, 1 - 8^n)$, e.g. $(0, 1, -7)$, $(0, 2, -63)$, $(0, 3, -511)$.
• $m > 0$ and $n = 0$: the solutions are $(m, n, k) = (m, 0, 7^m - 1)$, e.g. $(1, 0, 6)$, $(2, 0, 48)$, $(3, 0, 342)$.
• $m > 0$ and $n > 0$: the solutions are $(m, n, k) = (m, n, 7^m - 8^n)$, e.g. $(1, 1, -1)$, $(1, 2, -57)$, $(2, 1, 41)$, $(2, 2, -15)$.

4. Find all $x, y \in \mathbb{N}^0$ and $z \in \mathbb{Z}$ such that:
(**a**) $2^x - 3^y = z^2$. (**b**) $2^x + 3^y = z^2$.
Solution:
(**a**) We consider and inspect the following cases:
• $x = 0$: the only solution (by inspection) is $(x, y, z) = (0, 0, 0)$ because the LHS must be non-negative.
• $x = 1$: the only solutions (by inspection) are $(x, y, z) = (1, 0, \pm 1)$ because the LHS must be non-negative.
• $x = 2$: the only solutions (by inspection) are $(x, y, z) = (2, 1, \pm 1)$ because the LHS must be non-negative.
• $x > 2$: there is no solution. This is because in modulo 8 we have $2^x \stackrel{8}{=} 0$ and $3^{y \stackrel{2}{=} 0,1} \stackrel{8}{=} 1, 3$. Accordingly:
$2^x - 3^y = z^2 \quad \rightarrow \quad 0 - 1 \stackrel{8}{=} z^2$ or $0 - 3 \stackrel{8}{=} z^2 \quad \rightarrow \quad 7 \stackrel{8}{=} z^2$ or $5 \stackrel{8}{=} z^2$
Noting that 7 and 5 are quadratic non-residues of 8 (see § 1.6) we conclude that there is no solution to the given Diophantine equation for $x > 2$.
So in brief, the given Diophantine equation has only the above five solutions.
(**b**) We consider and inspect the following cases:

[45] In fact, we can obtain this result more easily by noting that y must be zero (to avoid parity violation) and hence we must have only those two solutions.

• $x = 0$: the only solutions are $(x, y, z) = (0, 1, \pm 2)$. This is because $3^y = z^2 - 1 = (z-1)(z+1)$ which implies (considering the factorization of 3^y noting as well that $y = 0$ is not a possibility) that one of the factors $(z-1)$ and $(z+1)$ must be of unity magnitude (noting that the difference between $z-1$ and $z+1$ is 2) and hence $z = \pm 2$ which leads to the given solutions.

• $x = 1$: there is no solution. This is because in modulo 3 we have $2^1 + 0 \stackrel{3}{=} z^2$ which has no solution since 2 is a quadratic non-residue of 3.

• $x = 2$: there is no solution. This is because in modulo 8 we have $2^2 + 3^y \stackrel{8}{=} z^2$. However, $3^{y \stackrel{2}{=} 0,1} \stackrel{8}{=} 1, 3$ and hence we have either $5 \stackrel{8}{=} z^2$ or $7 \stackrel{8}{=} z^2$ which have no solution because 5 and 7 are quadratic non-residues of 8.

• $x > 2$: the only solutions are $(x, y, z) = (3, 0, \pm 3)$ and $(4, 2, \pm 5)$. This is because in modulo 8 we have $2^x \stackrel{8}{=} 0$ and $3^{y \stackrel{2}{=} 0,1} \stackrel{8}{=} 1, 3$ while $z^2 \stackrel{8}{=} 0, 1, 4$ and this implies that if we have any solution then $y = 2k$ (where $k \in \mathbb{N}^0$). Accordingly, the given Diophantine equation becomes:

$$2^x + 3^{2k} = z^2 \quad \rightarrow \quad 2^x = z^2 - 3^{2k} \quad \rightarrow \quad 2^x = (z - 3^k)(z + 3^k)$$

i.e. $z - 3^k = 2^m$ and $z + 3^k = 2^n$ (where $m, n \in \mathbb{N}$ with $m < n$ and $m + n = x$).[46] Now, if we subtract the first of the last two equations from the second we get:

$$2(3^k) = 2^n - 2^m \quad \rightarrow \quad 3^k = 2^{m-1}(2^{n-m} - 1)$$

Now, 3^k is odd and hence both 2^{m-1} and $(2^{n-m} - 1)$ must be odd, and this implies $m = 1$ and hence $3^k = 2^{n-1} - 1$. Accordingly:

If $n = 1$ then we have $3^k = 2^{1-1} - 1 = 0$ which has no solution (noting that $k \in \mathbb{N}^0$).[47]

If $n = 2$ then we have $3^k = 2^{2-1} - 1 = 1$ which has only one solution, i.e. $k = 0$. As a result, we have $x = m + n = 1 + 2 = 3$ and $y = 2k = 2(0) = 0$ and hence $(x, y, z) = (3, 0, \pm 3)$.

If $n = 3$ then we have $3^k = 2^{3-1} - 1 = 3$ which has only one solution, i.e. $k = 1$. As a result, we have $x = m + n = 1 + 3 = 4$ and $y = 2k = 2(1) = 2$ and hence $(x, y, z) = (4, 2, \pm 5)$.

If $n > 3$ then we have $2^{n-1} \stackrel{8}{=} 0$ and hence we get $3^k \stackrel{8}{=} 0 - 1 \stackrel{8}{=} 7$ which has no solution since the residues of 3^k (modulo 8) are either 1 or 3 and hence $3^k \stackrel{8}{\neq} 7$. This means that there is no solution to the given Diophantine equation for $n > 3$ (i.e. $x > 4$).

So in brief, the given Diophantine equation has only the above six solutions.

5. Find all $x, y \in \mathbb{N}^0$ and $z \in \mathbb{Z}$ such that:

(**a**) $3^x - 4^y = z^2$. (**b**) $4^x - 3^y = z^2$. (**c**) $4^x + 3^y = z^2$. (**d**) $3^x + 5^y = z^2$.

Solution:

(**a**) For $x = 0$ the only solution (by inspection) is $(x, y, z) = (0, 0, 0)$ because the LHS must be non-negative.

For $x > 0$ there is no solution. This is because if we reduce the given equation in modulo 3 we get $-1 \stackrel{3}{=} z^2$ (i.e. $2 \stackrel{3}{=} z^2$) which has no solution because 2 is a quadratic non-residue of 3 (see § 1.6). So, the only solution to the given equation is $(x, y, z) = (0, 0, 0)$.

(**b**) For $x = 0$ the only solution (by inspection) is $(x, y, z) = (0, 0, 0)$ because the LHS must be non-negative.

For $x = 1$ the only solutions (by inspection) are $(x, y, z) = (1, 1, \pm 1)$ because the LHS must be non-negative.

For $x > 1$ there is no solution. This is because if we reduce the given equation in modulo 8 we get $0 - 1 \stackrel{8}{=} z^2$ or $0 - 3 \stackrel{8}{=} z^2$ (i.e. $7 \stackrel{8}{=} z^2$ or $5 \stackrel{8}{=} z^2$) since $3^{y \stackrel{2}{=} 0,1} \stackrel{8}{=} 1, 3$. However, neither of these congruences has a solution because 7 and 5 are quadratic non-residues of 8 (see § 1.6). So, the only solutions are $(x, y, z) = (0, 0, 0)$ and $(1, 1, \pm 1)$.

(**c**) If we write this equation as $2^X + 3^y = z^2$ (where $X = 2x$) then this equation is the same as the

[46] Although $z \in \mathbb{Z}$ we can make $z \in \mathbb{N}$ at this stage noting that z is squared and hence its sign does not matter; moreover within the imposed conditions z cannot be 0. We should also note that $2^x + 3^{2k} = z^2$ implies that z is odd and hence $z - 3^k \neq 1$.

[47] In fact, we can also rule out this possibility by the condition $m < n$ noting that $m = 1$.

equation of part (b) of Problem 4 (with X replacing x). Now, if we note that $X = 2x$ then we can conclude (by using the solutions of part b of Problem 4) that the only solutions to the given equation are $(x, y, z) = (0, 1, \pm 2)$ and $(2, 2, \pm 5)$.
(**d**) We have three cases to consider and inspect:
• $x = 0$: i.e. $5^y = z^2 - 1 = (z-1)(z+1)$. Noting that the difference between $(z-1)$ and $(z+1)$ is 2, we can see that no value of z can make these expressions non-negative powers of 5. Hence, we have no solution in this case.
• $x = 1$: if we reduce the equation in modulo 3 we get $5^y \stackrel{3}{=} z^2$. Now, $5^{y \stackrel{2}{=} 0,1} \stackrel{3}{=} 1, 2$ and hence y must be even (noting that 2 is not a quadratic residue of 3). So, the original equation becomes $3 + 5^{2k} = z^2$ (where $k \in \mathbb{N}^0$), i.e. $3 = z^2 - 5^{2k} = (z - 5^k)(z + 5^k)$. Therefore, one of the factors $(z - 5^k)$ and $(z + 5^k)$ must be of magnitude 1 while the other must be of magnitude 3. Simple algebraic inspection shows that we must have $k = 0$ (and hence $y = 0$) and $z = \pm 2$. So, the only solutions in this case are $(x, y, z) = (1, 0, \pm 2)$.
• $x > 1$: we note first that z must be even (because the LHS is even) and hence z^2 is a multiple of 4. Now, if we reduce the equation in modulo 4 then we get $3^x + 1 \stackrel{4}{=} 0$. So, if we note that $3^{x \stackrel{2}{=} 0,1} \stackrel{4}{=} 1, 3$ then x must be odd (say $x = 2s + 1$ where $s \in \mathbb{N}$). Hence, the given equation becomes $3^{2s+1} + 5^y = z^2$. Now, **EITHER**:
$y = 0$ and hence:
$3^{2s+1} + 1 = z^2 \quad \rightarrow \quad 3^{2s+1} = z^2 - 1 \quad \rightarrow \quad 3^{2s+1} = (z-1)(z+1)$
However, the difference between $(z-1)$ and $(z+1)$ is 2 and this implies that 3^{2s+1} must be made of a factor of magnitude 1 and another factor of magnitude 3, i.e. $s = 0$ which is impossible because we are currently assuming $x > 1$ (i.e. $s \in \mathbb{N}$) although we should note that this will lead to the previous solutions, i.e. $(x, y, z) = (1, 0, \pm 2)$. **OR**:
$y > 0$ and hence if we reduce the equation $3^{2s+1} + 5^y = z^2$ in modulo 5 then we get $3^{2s+1} \stackrel{5}{=} z^2$ which has no solution. This is because $3^{2s+1} \stackrel{5}{=} 2, 3$ (corresponding to s odd and s even) and hence we must have $z^2 \stackrel{5}{=} 2, 3$ which has no solution because 2 and 3 are quadratic non-residues of 5. This means that for $x > 1$ we have no solution.
So in brief, the given Diophantine equation has only the two solutions: $(x, y, z) = (1, 0, \pm 2)$.

5.5 Diophantine Equations Involving Roots

1. Find all $x, y \in \mathbb{Z}$ that satisfy the following equations:
(**a**) $\sqrt{x} + \sqrt{y} = 5$. (**b**) $\sqrt{x} - \sqrt{y} = 5$. (**c**) $x - \sqrt[3]{y} = 5$. (**d**) $\sqrt{x} + \sqrt[3]{y} = 5$.
(**e**) $\sqrt[3]{x} + \sqrt[3]{y} = 13$. (**f**) $\sqrt[3]{x} - \sqrt[3]{y} = 13$. (**g**) $3^x + \sqrt{y} = 21$. (**h**) $5^x + \sqrt[3]{y} = 128$.
Solution:
(**a**) x and y must be perfect squares.[48] So, the easiest way to solve an equation like this is to enumerate over the perfect squares $x, y = 0, 1, 4, 9, 16, 25$ (noting that exceeding 25 will make the LHS greater than 5). If we do so we get the following (x, y) solutions:
$(0, 25) \quad (1, 16) \quad (4, 9) \quad (9, 4) \quad (16, 1) \quad (25, 0)$
(**b**) If we write the equation as $\sqrt{x} = \sqrt{y} + 5$ and square it we get $x = y + 10\sqrt{y} + 25$. Accordingly, y must be a perfect square. So, if $y = s^2$ (where $s \in \mathbb{Z}$) then the solutions are $(x, y) = (s^2 + 10\,|s| + 25,\ s^2)$.
(**c**) y must be a perfect cube (say $y = s^3$ where $s \in \mathbb{Z}$) and hence $x = 5 + s$. So, the solutions are $(x, y) = (5 + s,\ s^3)$.
(**d**) We have two cases:
• $y \geq 0$ and hence the only possible values of $\sqrt{x}$ are $0, 1, 2, 3, 4, 5$ (noting that other values will make the LHS > 5). This leads to the following (x, y) solutions:
$(0, 125) \quad (1, 64) \quad (4, 27) \quad (9, 8) \quad (16, 1) \quad (25, 0)$

[48] Although the algebraic sum of two irrational numbers can be rational (or integer) this does not apply here and hence we can assume here that $\sqrt{x}$ and $\sqrt{y}$ must be integers.

• $y < 0$ and hence if $y = s^3$ (where $s \in \mathbb{Z}$) then $\sqrt{x} - |s| = 5$, i.e. $x = (5 + |s|)^2$. So, the solutions in this case are: $(x, y) = \big([5 + |s|]^2,\ s^3\big)$.

So in brief, the solutions of the given equation are the union of the sets of solutions in these two cases.

(**e**) If $x = k^3$ (where $k \in \mathbb{Z}$) then:

$$\sqrt[3]{x} + \sqrt[3]{y} = 13 \quad \rightarrow \quad k + \sqrt[3]{y} = 13 \quad \rightarrow \quad \sqrt[3]{y} = 13 - k \quad \rightarrow \quad y = (13 - k)^3$$

So, the solutions are: $(x, y) = (k^3,\ [13 - k]^3)$.

(**f**) If we follow the approach of part (e) then we get: $(x, y) = (k^3,\ [k - 13]^3)$.

(**g**) Let $\sqrt{y} = s$ (i.e. $y = s^2$) where $s \in \mathbb{N}^0$ and hence $s = 21 - 3^x$ where $(21 - 3^x) \geq 0$ and $x \in \mathbb{N}^0$. It is obvious that only $x = 0, 1, 2$ satisfy the condition $(21 - 3^x) \geq 0$ and hence the solutions are: $(x, y) = (0, 400)$, $(1, 324)$ and $(2, 144)$.

(**h**) Let $\sqrt[3]{y} = s$ (i.e. $y = s^3$) where $s \in \mathbb{Z}$ and hence $s = 128 - 5^x$ where $x \in \mathbb{N}^0$. Therefore, the solutions are: $(x, y) = (k,\ [128 - 5^k]^3)$ where $k \in \mathbb{N}^0$.

2. Find all $x, y, z \in \mathbb{Z}$ that satisfy the following equations:

(**a**) $\sqrt{x} + \sqrt{y} + \sqrt{z} = 5$. (**b**) $\sqrt{x} - \sqrt{y} - \sqrt{z} = 5$. (**c**) $\sqrt{x} + \sqrt{y} - \sqrt{z} = 5$.

(**d**) $\sqrt{x} + \sqrt{y} + \sqrt[3]{z} = 5$. (**e**) $x\sqrt{y} + y\sqrt{x} = z$. (**f**) $3^x + 5^y - \sqrt[3]{z} = 7$.

Solution:

(**a**) If we do what we did in part (a) of Problem 1 we get the following (x, y, z) solutions:

$(0, 0, 25)$	$(0, 1, 16)$	$(0, 4, 9)$	$(0, 9, 4)$	$(0, 16, 1)$	$(0, 25, 0)$	$(1, 0, 16)$
$(1, 1, 9)$	$(1, 4, 4)$	$(1, 9, 1)$	$(1, 16, 0)$	$(4, 0, 9)$	$(4, 1, 4)$	$(4, 4, 1)$
$(4, 9, 0)$	$(9, 0, 4)$	$(9, 1, 1)$	$(9, 4, 0)$	$(16, 0, 1)$	$(16, 1, 0)$	$(25, 0, 0)$

(**b**) Let $x = k^2$, $y = s^2$ and $z = t^2$ where $k, s, t \in \mathbb{N}^0$. So, we can write the given equation as $k - s - t = 5$, i.e. $k = 5 + s + t$. Accordingly, the solutions are given by: $(x, y, z) = \big([5 + s + t]^2, s^2, t^2\big)$. For example, given $s = 2$ and $t = 7$ we get the solution $(x, y, z) = (196, 4, 49)$.

(**c**) We have 3 cases:

• $x = z$ and hence y must be 25. Thus the solutions are: $(x, y, z) = (k, 25, k)$ where $k \in \mathbb{N}^0$.

• $y = z$ and hence x must be 25. Thus the solutions are: $(x, y, z) = (25, k, k)$ where $k \in \mathbb{N}^0$.

• $x \neq z$ and $y \neq z$ and hence x, y, z are perfect squares. So, let $x = k^2$, $y = s^2$ and $z = t^2$ (where $k, s, t \in \mathbb{N}^0$) and hence we can write the given equation as $k + s - t = 5$, i.e. $t = k + s - 5$. Accordingly, the solutions are given by: $(x, y, z) = \big(k^2, s^2, [k + s - 5]^2\big)$. However, we need to impose the condition that $(k + s) \geq 5$. For example, given $k = 2$ and $s = 7$ we get the solution $(x, y, z) = (4, 49, 16)$.

(**d**) We have two cases to consider:

• $z \geq 0$ and hence if we do what we did in part (a) we get the following (x, y, z) solutions:

$(0, 0, 125)$	$(0, 1, 64)$	$(0, 4, 27)$	$(0, 9, 8)$	$(0, 16, 1)$	$(0, 25, 0)$	$(1, 0, 64)$
$(1, 1, 27)$	$(1, 4, 8)$	$(1, 9, 1)$	$(1, 16, 0)$	$(4, 0, 27)$	$(4, 1, 8)$	$(4, 4, 1)$
$(4, 9, 0)$	$(9, 0, 8)$	$(9, 1, 1)$	$(9, 4, 0)$	$(16, 0, 1)$	$(16, 1, 0)$	$(25, 0, 0)$

• $z < 0$ and hence if $z = t^3$ (where $t \in \mathbb{Z}$) then $\sqrt{x} + \sqrt{y} - |t| = 5$, i.e. $|t| = \sqrt{x} + \sqrt{y} - 5$ where $(\sqrt{x} + \sqrt{y}) > 5$. Therefore, the solutions in this case are: $(x, y, z) = \big(k^2,\ s^2,\ [5 - k - s]^3\big)$ where $k, s \in \mathbb{N}^0$ and $5 < (k + s)$.

So in brief, the solutions of the given equation are the union of the sets of solutions in these two cases.[49]

(**e**) x and y are perfect squares and hence let $x = k^2$ and $y = s^2$ where $k, s \in \mathbb{Z}$. Therefore, the solutions are: $(x, y, z) = \big(k^2,\ s^2,\ k^2|s| + s^2|k|\big)$.

(**f**) Let $\sqrt[3]{z} = t$ (i.e. $z = t^3$) where $t \in \mathbb{Z}$ and hence $t = 3^x + 5^y - 7$ where $x, y \in \mathbb{N}^0$. Therefore, the solutions are: $(x, y, z) = (k,\ s,\ [3^k + 5^s - 7]^3)$ where $k, s \in \mathbb{N}^0$.

[49] We note that the solution in the second case applies even to the solutions of the first case (by keeping the condition $k, s \in \mathbb{N}^0$ and dropping the condition $5 < k + s$) and hence we could have considered only one case. However, we preferred to deal with two separate cases to show the finitely many solutions in the case of $z \geq 0$ and the infinitely many solutions in the case of $z < 0$.

5.6 Diophantine Equations Involving Fractions

1. Find all $x, y \in \mathbb{Z}$ that satisfy the following equations:
(**a**) $\frac{1}{x} + \frac{1}{y} = 1$. (**b**) $\frac{1}{x} + \frac{1}{y} = 5$. (**c**) $\frac{1}{x} + \frac{1}{y} = \frac{2}{3}$. (**d**) $\frac{1}{x} + \frac{2}{y} = \frac{3}{4}$.
Solution:
(**a**) $xy \neq 0$. On multiplying the two sides by xy we get $x + y = xy$, i.e. $xy - x - y + 1 = 1$ and hence $(1 - x)(1 - y) = 1$. So, $1 - x = -1$ and $1 - y = -1$ (i.e. $x = y = 2$) or $1 - x = 1$ and $1 - y = 1$ (i.e. $x = y = 0$ which is not acceptable). Therefore, the only solution is $x = y = 2$. Also see Problem 9 of § 5.2.
(**b**) $xy \neq 0$. The maximum value of the LHS is 2 (i.e. when $x = y = 1$) and hence this equation has no solution.
(**c**) $xy \neq 0$. Also, x and y cannot be both negative. Hence, we have two main cases: both x and y are positive or one negative and one positive. In the following we investigate these cases where we exploit the symmetry in x and y:
• Both positive: $x = 1$ is not possible because the LHS becomes $> 2/3$ (noting that $y > 0$). $x = 2$ leads to the solutions: $(x, y) = (2, 6)$ and $(x, y) = (6, 2)$. $x = 3$ leads to the solution: $(x, y) = (3, 3)$. $x = 4$ and $x = 5$ do not lead to solutions. $x = 6$ was already found by symmetry. $x \geq 7$ do not lead to any solution because the LHS becomes either $> 2/3$ (i.e. if $y = 1$) or $< 2/3$ (i.e. if $y > 1$).
• Only one positive: $x = 1$ leads to the solutions: $(x, y) = (1, -3)$ and $(x, y) = (-3, 1)$. $x > 1$ do not lead to any solution because the LHS becomes $< 2/3$.
So in brief, we have only 5 solutions: $(x, y) = (2, 6)$, $(6, 2)$, $(3, 3)$, $(1, -3)$, $(-3, 1)$.
(**d**) $xy \neq 0$. Let us use a method similar to the method of part (c) and hence we have three main cases:
• Both positive: $y = 1, 2$ are not possible because the LHS becomes $> 3/4$. $y = 3$ leads to $x = 12$. $y = 4$ leads to $x = 4$. $y = 5, 6, 7$ do not lead to solutions. $y = 8$ leads to $x = 2$. $y > 8$ do not lead to any solution because the LHS becomes either $> 3/4$ (i.e. when $x = 1$) or $< 3/4$ (i.e. when $x > 1$).
• Only x positive: $x = 1$ leads to $y = -8$. $x > 1$ do not lead to any solution because the LHS becomes $< 3/4$.
• Only y positive: $y = 1$ is not possible because the LHS becomes $> 3/4$. $y = 2$ leads to $x = -4$. $y > 2$ do not lead to any solution because the LHS becomes $< 3/4$.
So in brief, we have only 5 solutions: $(x, y) = (12, 3)$, (4,4), (2,8), $(1, -8)$, $(-4, 2)$.
2. Find all $x, y, z \in \mathbb{Z}$ that satisfy the following equations:
(**a**) $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$. (**b**) $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2$. (**c**) $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 3$. (**d**) $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 4$.
Solution: We solved these equations in V1 for $x, y, z \in \mathbb{N}$ (see Problem 7 of § 4.1.10 of V1). So, all we need to do here is to consider the possibility of having more solutions with some (but not all) of the variables being negative (noting that none of the variables can be 0, i.e. we must have $xyz \neq 0$).
(**a**) The solutions are the same as the solutions of Problem 19 of § 5.2 (of the present volume) excluding the zero solutions, i.e. any (x, y, z) such that $xyz = 0$.
(**b**) If any one of the variables is negative then the LHS will be less than the RHS. Hence, the solutions are only those with $x, y, z \in \mathbb{N}$ (which we found in V1), i.e. $(x, y, z) = (1, 2, 2), (2, 1, 2), (2, 2, 1)$.
(**c**) As in part (b), no one of the variables can be negative (for the same reason), and hence the solutions are only those with $x, y, z \in \mathbb{N}$ (which we found in V1), i.e. $(x, y, z) = (1, 1, 1)$.
(**d**) This equation has no solution because the LHS cannot be greater than 3, i.e. when $x = y = z = 1$.
3. Investigate the solutions of the following Diophantine equation:

$$\frac{x^2y + x + y}{xy^2 + y + a} = z$$

where $x, y, z \in \mathbb{N}$ and a is a specific natural number.
Solution: We have two categories of solutions for this equation:
(**a**) Solutions of general type, i.e. those solutions that can be inferred from the form of this equation. We can easily identify two solutions of general type:

- $(x, y, z) = (az^2, az, z)$: this is because:

$$\frac{x^2y + x + y}{xy^2 + y + a} = \frac{(az^2)^2(az) + az^2 + az}{(az^2)(az)^2 + az + a} = \frac{a^3z^5 + az^2 + az}{a^3z^4 + az + a} = \frac{a^3z^4 + az + a}{a^3z^4 + az + a}\, z = z$$

- $(x, y, z) = (a^2, 1, a^2 - a + 1)$: this is because:

$$\frac{x^2y + x + y}{xy^2 + y + a} = \frac{(a^2)^2(1) + a^2 + (1)}{(a^2)(1)^2 + (1) + a} = \frac{a^4 + a^2 + 1}{a^2 + a + 1} = \frac{(a^2 + a + 1)(a^2 - a + 1)}{a^2 + a + 1} = a^2 - a + 1 = z$$

(**b**) Solutions of special type, i.e. those solutions that depend (in their existence and nature) on the specific a. For example, if $a = 5$ then $(x, y, z) = (11, 2, 5)$ is also a solution to this equation while if $a = 13$ then $(x, y, z) = (47, 1, 37)$ and $(49, 2, 23)$ are also solutions. These solutions should be investigated within the specific problem (as determined by the specific value of a).

4. Investigate the solutions of the following equations:
(**a**) $\frac{x}{y} + xy = z \quad (x, y, z \in \mathbb{Z})$. (**b**) $\frac{1}{x} + \frac{1}{y} = \frac{1}{z} \quad (x, y, z \in \mathbb{N})$.
Solution:
(**a**) It is obvious that $y \neq 0$ and x must be divisible by y. So, if $y = s$ (where $\mathbb{Z} \ni s \neq 0$) then $x = ks$ (where $k \in \mathbb{Z}$) and hence $z = k + ks^2$. So, the solution of the given equation is $(x, y, z) = (ks, s, k + ks^2)$.
(**b**) Let $x = k$ and $y = s$ where $k, s \in \mathbb{N}$. Hence:
$\frac{1}{x} + \frac{1}{y} = \frac{1}{z} \quad \rightarrow \quad \frac{1}{k} + \frac{1}{s} = \frac{1}{z} \quad \rightarrow \quad \frac{k+s}{ks} = \frac{1}{z} \quad \rightarrow \quad z = \frac{ks}{k+s}$
Now, since $z \in \mathbb{N}$ then we must impose the condition that $(k + s)|(ks)$. So, the general solution of the given equation is: $(x, y, z) = \left(k, s, \frac{ks}{k+s}\right)$ where $k, s \in \mathbb{N}$ and $(k + s)|(ks)$. The following are some of the specific solutions:
$(2, 2, 1) \quad (3, 6, 2) \quad (4, 4, 2) \quad (4, 12, 3) \quad (5, 20, 4) \quad (6, 3, 2) \quad (6, 6, 3)$
It is worth noting that the solution $(x, y, z) = (2n, 2n, n)$ (which is a special case of the above general solution) applies to all $n \in \mathbb{N}$.

5. Find all the solutions of the equation $\frac{x}{y} + xy = a$ (where $x, y \in \mathbb{Z}$) for $a = 0, 1, 2$.
Solution: This equation is the same as the equation of part (a) of Problem 4. So, all we need to do is to find $k, s \in \mathbb{Z}$ such that $k + ks^2 = 0, 1, 2$. Now:
• For $a = 0$ we have $k + ks^2 = k(1 + s^2) = 0$. So, $k = 0$ (noting that $1 + s^2 \neq 0$) and hence the solution of the given equation is $(x, y) = (0, s)$ where $\mathbb{Z} \ni s \neq 0$.
• For $a = 1$ we have $k + ks^2 = 1$ which has no solution for $k = 0$. For $k \neq 0$ we divide the equation by k to obtain $1 + s^2 = 1/k$ which implies that $k|1$ and hence $k = \pm 1$. Now:
If $k = -1$ then we have $s^2 + 2 = 0$ which has no solution.
If $k = 1$ then we have $s^2 = 0$ (i.e. $s = 0$) which is not acceptable.
So in brief, for $a = 1$ the given equation has no solution.[50]
• For $a = 2$ we have $k + ks^2 = 2$ which has no solution for $k = 0$. For $k \neq 0$ we divide the equation by k to obtain $1 + s^2 = 2/k$ which implies that $k|2$ and hence $k = \pm 1, \pm 2$. Now:
For $k = -1$ we have $s^2 + 3 = 0$ which has no solution.
For $k = +1$ we have $s^2 - 1 = 0$ (i.e. $s = \pm 1$) and hence $(x, y) = (1, 1)$ and $(x, y) = (-1, -1)$.
For $k = -2$ we have $s^2 + 2 = 0$ which has no solution.
For $k = +2$ we have $s^2 = 0$ (i.e. $s = 0$) which is not acceptable.
So in brief, for $a = 2$ the given equation has only two solutions: $(x, y) = (1, 1)$ and $(x, y) = (-1, -1)$.

6. Find all $x, y, z \in \mathbb{N}$ such that: $z = \frac{1}{x} + \frac{1}{y} + \frac{2}{xy}$.
Solution: If we multiply the two sides by xy we get $xyz = x + y + 2$. Now, we have two cases:
• $z = 1$ and hence $xy = x + y + 2$. Now, it is obvious that $x = 1$ or $y = 1$ is not a possibility (because we get $0 = 3$). So, we must have $x > 1$ and $y > 1$. However, if $x > 1$ and $y > 1$ then the LHS of

[50] Another (and simpler) approach to reach this conclusion is that x and y must have the same sign (because otherwise the sum will be negative) and hence (whether $x \geq y$ or $x < y$) the LHS must be greater than 1 (noting that $xy = 0$ is not a possibility), i.e. the equation has no solution.

$xy = x + y + 2$ becomes greater than its RHS if $x > 4$ or $y > 4$. So, all we need to do is to test the (nine) combinations of $x = 2, 3, 4$ and $y = 2, 3, 4$ (to see which combinations satisfy the equation $xy = x + y + 2$). On doing so we get only two solutions: $(x, y, z) = (2, 4, 1)$ and $(4, 2, 1)$.

• $z > 1$ and hence the LHS of $xyz = x + y + 2$ becomes greater than its RHS if $x > 3$ or $y > 3$. So, all we need to do is to test the (nine) combinations of $x = 1, 2, 3$ and $y = 1, 2, 3$ (to obtain the values of z corresponding to these combinations). On doing so we get only three solutions: $(x, y, z) = (1, 1, 4)$, $(1, 3, 2)$ and $(3, 1, 2)$.

So in brief, the given equation has only these five solutions.

7. Find all $x, y, z \in \mathbb{N}$ that satisfy the following equations:

(**a**) $\frac{3}{x} + \frac{7}{y} = z$. (**b**) $\frac{1}{x} + \frac{2}{y} + \frac{3}{z} = 4$.

Solution:

(**a**) The LHS cannot exceed 10 (i.e. when $x = y = 1$). Therefore, all we need to do is to solve the equation: $\frac{3}{x} + \frac{7}{y} = z$ for $z = 1, 2, \ldots, 10$. Accordingly:

• $\frac{3}{x} + \frac{7}{y} = 1$: we must have $x > 3$ and $y > 7$ (because otherwise the LHS becomes > 1). We must also have $x < 25$ and $y < 29$ (because otherwise the LHS becomes < 1). So, on testing these possibilities (i.e. $x = 4, 5, \ldots, 24$ and $y = 8, 9, \ldots, 28$) we find the following four solutions: $(x, y, z) = (4, 28, 1)$, $(6, 14, 1)$, $(10, 10, 1)$ and $(24, 8, 1)$.

• $\frac{3}{x} + \frac{7}{y} = 2$: by a similar argument to that in the previous point we must have $1 < x < 13$ and $3 < y < 15$, and hence on testing these possibilities we find the following four solutions: $(x, y, z) = (2, 14, 2)$, $(3, 7, 2)$, $(5, 5, 2)$ and $(12, 4, 2)$.

• For $z = 3, 6, 7, 9$ we find no solution.

• For $z = 4, 5, 8, 10$ we find the following five solutions: $(x, y, z) = (1, 7, 4)$, $(6, 2, 4)$, $(2, 2, 5)$, $(3, 1, 8)$ and $(1, 1, 10)$.

So in brief, this equation has only these 13 solutions.

(**b**) If $z > 3$ then the LHS becomes less then 4. So, we must have $z = 1, 2, 3$ and hence:

• $z = 1$ and hence $\frac{1}{x} + \frac{2}{y} = 1$. Now, we must have $x > 1$ and $y > 2$. However, if $y > 2$ then we must have $x < 4$. So in brief, we must have $x = 2, 3$ that is: $\frac{2}{y} = \frac{1}{2}$ (i.e. $y = 4$) and $\frac{2}{y} = \frac{2}{3}$ (i.e. $y = 3$). So, we found the following two solutions: $(x, y, z) = (2, 4, 1)$ and $(3, 3, 1)$.

• $z = 2$ and hence $\frac{1}{x} + \frac{2}{y} = \frac{5}{2}$, i.e. $\frac{2}{x} + \frac{4}{y} = 5$. Now, we must have $y = 1$ and hence $x = 2$. So, we found the following solution: $(x, y, z) = (2, 1, 2)$.

• $z = 3$ and hence $\frac{1}{x} + \frac{2}{y} = 3$. The only possibility in this case is $x = y = 1$. So, we found the following solution: $(x, y, z) = (1, 1, 3)$.

So in brief, this equation has only these 4 solutions.

8. Find all $x, y, z \in \mathbb{N}$ that satisfy the following equations:

(**a**) $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 1$. (**b**) $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 2$. (**c**) $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 3$.

Solution:[51]

(**a**) The LHS of this equation is greater than 1 because at least one of the variables is greater than or equal to another variable and hence one term at least is greater than or equal to 1 and thus the sum of the three terms must be greater than 1 (noting that the sum of the other two terms is greater than 0).[52] Hence, this equation has no solution.

(**b**) We have two cases to consider:

• The triple equality $x = y = z$ does hold and hence the LHS of the equation is 3, i.e. there is no solution.

• The triple equality $x = y = z$ does not hold and hence one of the variables x, y, z must be greater than another variable. So, let assume (without loss of generality since it is a matter of labeling) that x is the greater variable. Hence, (with a proper labeling of y and z) we have one of the following three situations:

⋆ $x = y > z$ and hence $\frac{x}{y} = 1$ while $\frac{y}{z} > 1$. So, the LHS is greater than 2, i.e. there is no solution.

[51] We refer the reader to Problem 8 of § 7.3 for another method for solving this Problem.

[52] For example, if $x \geq y \geq z$ then $(x/y) \geq 1$ while if $x \leq y \leq z$ then $(z/x) \geq 1$.

$\star$ $x > y = z$ and hence $\frac{x}{y} > 1$ while $\frac{y}{z} = 1$. So, the LHS is greater than 2, i.e. there is no solution.
$\star$ $x > y > z$ and hence $\frac{x}{y} > 1$ and $\frac{y}{z} > 1$. So, the LHS is greater than 2, i.e. there is no solution.
So in brief, this equation has no solution.
(**c**) We have two cases to consider:
• The triple equality $x = y = z$ does hold and hence the LHS of the equation is 3. So, in this case we have the solution $(x, y, z) = (k, k, k)$ where $k \in \mathbb{N}$.
• The triple equality $x = y = z$ does not hold and hence one of the variables x, y, z must be greater than another variable. So, let assume (without loss of generality) that x is the greater variable. Hence, we have one of the following three situations:
$\star$ $x = y > z$ and hence we have:

$$1 + \tfrac{x}{z} + \tfrac{z}{x} = 3 \quad \rightarrow \quad \tfrac{x}{z} + \tfrac{z}{x} = 2 \quad \rightarrow \quad x^2 - 2xz + z^2 = 0 \quad \rightarrow \quad (x - z)^2 = 0$$

i.e. $x = z$ which is a contradiction. Hence, there is no solution.
$\star$ $x > y = z$ and hence we have:

$$\tfrac{x}{y} + 1 + \tfrac{y}{x} = 3 \quad \rightarrow \quad \tfrac{x}{y} + \tfrac{y}{x} = 2 \quad \rightarrow \quad x^2 - 2xy + y^2 = 0 \quad \rightarrow \quad (x - y)^2 = 0$$

i.e. $x = y$ which is a contradiction. Hence, there is no solution.
$\star$ $x > y > z$ and hence $x = z + a$ and $y = z + b$ where $2 \leq a$ and $1 \leq b$ with $a > b$. Accordingly:

$$\begin{aligned}
\frac{x}{y} + \frac{y}{z} + \frac{z}{x} &= \frac{z+a}{z+b} + \frac{z+b}{z} + \frac{z}{z+a} \\
&= \frac{a^2z + ab^2 + 2abz + 3az^2 + b^2z + 3bz^2 + 3z^3}{abz + az^2 + bz^2 + z^3} \\
&= \frac{2(abz + az^2 + bz^2 + z^3)}{abz + az^2 + bz^2 + z^3} + \frac{a^2z + ab^2 + az^2 + b^2z + bz^2 + z^3}{abz + az^2 + bz^2 + z^3} \\
&= 2 + \frac{a^2z + ab^2 + az^2 + b^2z + bz^2 + z^3}{abz + az^2 + bz^2 + z^3} \\
&= 2 + \frac{a^2z + ab^2 + b^2z + (az^2 + bz^2 + z^3)}{abz + (az^2 + bz^2 + z^3)}
\end{aligned}$$

Now, $(a^2z + ab^2 + b^2z) > abz$ (noting that $a^2z > abz$ since $a > b$) and hence the last term in the last equation is greater than 1, i.e. the LHS of the given equation is greater than 3 and hence there is no solution.
So in brief, the only solution of this equation is $(x, y, z) = (k, k, k)$ where $k \in \mathbb{N}$.

5.7 Diophantine Equations Involving Roots and Fractions

1. Find all $x, y \in \mathbb{N}$ that satisfy the following equations:
(**a**) $\frac{1}{\sqrt{x}} + \frac{1}{\sqrt{y}} = \frac{1}{2}$. (**b**) $\frac{1}{\sqrt{x}} + \frac{1}{\sqrt{y}} = \frac{1}{3}$. (**c**) $\frac{1}{\sqrt{x}} - \frac{1}{\sqrt{y}} = \frac{1}{2}$. (**d**) $\frac{1}{\sqrt{x}} - \frac{1}{\sqrt{y}} = \frac{1}{3}$.
Solution: We note first that the square roots of all positive integers (excluding perfect squares) are irrational, and hence if a square root of an integer is rational then the integer is a perfect square (i.e. the square root is an integer).
(**a**) We have:

$$\tfrac{1}{\sqrt{x}} + \tfrac{1}{\sqrt{y}} = \tfrac{1}{2} \quad \rightarrow \quad \tfrac{1}{\sqrt{x}} = \tfrac{1}{2} - \tfrac{1}{\sqrt{y}} \quad \rightarrow \quad \tfrac{1}{\sqrt{x}} = \tfrac{\sqrt{y}-2}{2\sqrt{y}} \quad \rightarrow$$

$$\left(\tfrac{1}{\sqrt{x}}\right)^2 = \left(\tfrac{\sqrt{y}-2}{2\sqrt{y}}\right)^2 \quad \rightarrow \quad \tfrac{1}{x} = \tfrac{y-4\sqrt{y}+4}{4y} \quad \rightarrow \quad \sqrt{y} = \tfrac{xy+4x-4y}{4x}$$

Therefore, y must be a perfect square (say $y = s^2$ where $s \in \mathbb{N}$) noting that the RHS is rational. By a similar argument (or by symmetry) x must also be a perfect square. Hence:

$$\tfrac{1}{x} = \tfrac{y-4\sqrt{y}+4}{4y} \quad \rightarrow \quad x = \tfrac{4y}{y-4\sqrt{y}+4} \quad \rightarrow \quad x = \tfrac{4s^2}{s^2-4s+4} \quad \rightarrow \quad x = \left(\tfrac{2s}{s-2}\right)^2$$

Therefore, $s - 2$ must divide $2s$ (since x is a perfect square noting as well that $\frac{2s}{s-2}$ is rational). Now, $s - 2$ divides $2s - 4$ and $s - 2$ supposedly divides $2s$ and hence $s - 2$ divides their difference which is 4.

So, $s-2=\pm1,\pm2,\pm4$ and hence $s=1,3,4,6$ (where we take only the positive values of s). On trying these values of s on the equation $x=\left(\frac{2s}{s-2}\right)^2$ we find that only $s=3,4,6$ produce valid solutions to the original equation.
So in brief, the solutions of the given Diophantine equation are: $(x,y)=(36,9)$, $(16,16)$ and $(9,36)$.
(**b**) If we repeat the argument of part (a) with replacing 2 by 3 we get $x=\left(\frac{3s}{s-3}\right)^2$ and hence $s-3$ divides 9. So, $s-3=\pm1,\pm3,\pm9$ and hence $s=2,4,6,12$ (where we take only the positive values of s). On trying these values of s on the equation $x=\left(\frac{3s}{s-3}\right)^2$ we find that only $s=4,6,12$ produce valid solutions to the original equation.
So in brief, the solutions of the given Diophantine equation are: $(x,y)=(144,16)$, $(36,36)$ and $(16,144)$.
(**c**) We choose to solve this part (more simply) by a logical argument (rather than by a mathematical argument as we did in part a), that is: $1/\sqrt{x}$ must be 1 because otherwise the LHS will be less than $1/2$ (noting that the highest magnitude that $1/\sqrt{x}$ can assume if it is not 1 is $1/2$ since x must be a perfect square). So, $\sqrt{x}$ must be 1 (i.e. $x=1$) and hence $\sqrt{y}$ must be 2 (i.e. $y=4$).
So in brief, we have only one possible solution, i.e. $(x,y)=(1,4)$.
(**d**) We argue logically (similar to what we did in part c) that is:
• $1/\sqrt{x}$ cannot be 1 because otherwise the LHS will be either 0 (i.e. if $1/\sqrt{y}$ is 1) or greater than $1/3$ (i.e. if $1/\sqrt{y}$ is less than 1 noting that the highest magnitude that $1/\sqrt{y}$ can assume if it is less than 1 is $1/2$ since y must be a perfect square).
• $1/\sqrt{x}$ cannot be less than $1/2$ because otherwise the LHS will be less than $1/3$ (noting that the highest magnitude that $1/\sqrt{x}$ can assume if it is less than $1/2$ is $1/3$ since x must be a perfect square).
Therefore, $1/\sqrt{x}$ must be $1/2$ (i.e. $x=4$) and hence $1/\sqrt{y}$ must be $1/6$ (i.e. $y=36$).
So in brief, we have only one possible solution, i.e. $(x,y)=(4,36)$.

2. Find all $x,y,z\in\mathbb{N}$ that satisfy the following equations:
(**a**) $\frac{1}{\sqrt{x}}+\frac{1}{\sqrt{y}}+\frac{1}{\sqrt{z}}=2$. (**b**) $\frac{1}{\sqrt{x}}+\frac{1}{\sqrt{y}}=\frac{1}{\sqrt{z}}$.
Solution:
(**a**) x,y,z must be perfect squares (for reasons explained earlier). Now:
If all the square roots are greater than 1 then the LHS will be less than 2, and this implies that *at least* one of the square roots must be 1 (i.e. *at least* one of the variables must be 1).
If more than one of the square roots are 1 then the LHS will be greater than 2, and this implies that *exactly* one of the square roots must be 1 (i.e. *exactly* one of the variables must be 1).
If one of the remaining square roots is greater than 2 then the LHS will be less than 2, and this implies that one of the remaining square roots must be 2 (i.e. one of the remaining variables must be 4). Accordingly, the other remaining variable must be 4.
So in brief, the solutions of the given equation are: $(x,y,z)=(1,4,4)$, $(4,1,4)$ and $(4,4,1)$.
We finally note that a simpler approach is to use the solutions of part (b) of Problem 2 of § 5.6 by squaring the variables since the given equation is equivalent to $\frac{1}{X}+\frac{1}{Y}+\frac{1}{Z}=2$ where X,Y,Z represent the square roots of x,y,z. However, we preferred the above approach for the sake of diversity and because it is not dependent on having the solutions of another equation (noting that we use the method of comparison occasionally; see part b).
(**b**) If we write this equation as $\frac{1}{X}+\frac{1}{Y}=\frac{1}{Z}$ (where these capital symbols represent radicals of their corresponding variables) then we can obtain the solutions of the given equation from the solutions of the equation of part (b) of Problem 4 of § 5.6 by squaring the values of the variables of those solutions. The following are some solutions (corresponding to the sample solutions given in Problem 4 of § 5.6):
$(4,4,1)$ $(9,36,4)$ $(16,16,4)$ $(16,144,9)$ $(25,400,16)$ $(36,9,4)$ $(36,36,9)$

5.8 Diophantine Equations Involving Factorials

1. Show that the following equations have no solutions (where $x\in\mathbb{Z}$ and $y\in\mathbb{N}^0$):
(**a**) $11x-y!=13$. (**b**) $15x-19y!=538$. (**c**) $x^3+13y!=31$.

Solution:
(**a**) By inspection, this equation has no solution for $y < 13$. For $y \geq 13$ we have $11x \stackrel{13}{=} 0$ whose only solution is $x = 13k$ where $k \in \mathbb{Z}$. On substituting this in the given equation we get:

$$11(13k) - y! = 13 \qquad \rightarrow \qquad k = \tfrac{y!+13}{11\times 13} \qquad \rightarrow \qquad k = \tfrac{(y!/13)+1}{11}$$

Now, 11 divides $y!/13$ (noting that $y \geq 13$) but it does not divide 1 and hence 11 does not divide $(y!/13)+1$. This means that there is no integer k that satisfies the given equation and hence the given equation has no solution.

(**b**) By inspection, this equation has no solution for $y < 7$. For $y \geq 7$ we have $x \stackrel{7}{=} 6$, i.e. $x = 6 + 7k$ where $k \in \mathbb{Z}$. On substituting this in the given equation we get:

$$15(6 + 7k) - 19y! = 538 \qquad \rightarrow \qquad k = \tfrac{19y!+448}{105}$$

Now, 105 divides $19y!$ (noting that $105 = 3 \times 5 \times 7$ and $y \geq 7$) but it does not divide 448 and hence 105 does not divide $19y! + 448$. This means that there is no integer k that satisfies the given equation and hence the given equation has no solution.

(**c**) By inspection, this equation has no solution for $y < 7$. For $y \geq 7$ we have $x^3 \stackrel{7}{=} 3$ which has no solution. Hence, the given equation has no solution.

2. Find all the solutions of the following equations (where $x \in \mathbb{Z}$ and $y \in \mathbb{N}^0$):
(**a**) $x^2 - y! = 2$. (**b**) $x^2 - y! = 3$. (**c**) $x^2 - y! = 1$. (**d**) $16x + 9y! = 121$.
Solution:
(**a**) For $y > 2$ we have $x^2 \stackrel{3}{=} 2$. However, $x^2 \stackrel{3}{=} 2$ has no solution (because 2 is quadratic non-residue of 3; see § 1.6). So, if there is any solution then we must have $y = 0$ (and hence $x^2 - 1 = 2$ which has no solution) or $y = 1$ (and hence $x^2 - 1 = 2$ which has no solution) or $y = 2$ (and hence $x^2 - 2 = 2$, i.e. $x = \pm 2$). So, the solutions are: $(x, y) = (\pm 2, 2)$.
(**b**) For $y > 3$ we have $x^2 \stackrel{4}{=} 3$. However, $x^2 \stackrel{4}{=} 3$ has no solution (because 3 is quadratic non-residue of 4). So, if there is any solution then we must have $y = 0$ (and hence $x^2 - 1 = 3$, i.e. $x = \pm 2$) or $y = 1$ (and hence $x^2 - 1 = 3$, i.e. $x = \pm 2$) or $y = 2$ (and hence $x^2 - 2 = 3$ which has no solution) or $y = 3$ (and hence $x^2 - 6 = 3$, i.e. $x = \pm 3$). So, the solutions are: $(x, y) = (\pm 2, 0), (\pm 2, 1), (\pm 3, 3)$.
(**c**) This is known as Brocard's problem. The only known solutions are: $(x, y) = (\pm 5, 4), (\pm 11, 5), (\pm 71, 7)$. It is unknown if the problem can have more solutions (so the problem is in the research domain and hence it deserves the attention of the young ambitious mathematicians).
(**d**) For $y = 0$ and $y = 1$ we have $x = 7$. For $y > 1$ the LHS is even while the RHS is odd and hence there is no solution. So, the only solutions to this equation are: $(x, y) = (7, 0)$ and $(x, y) = (7, 1)$.

3. Find all the solutions of the following equations (where $x, y \in \mathbb{Z}$ and $z \in \mathbb{N}^0$):
(**a**) $2x + 3y - 6z! = 222$. (**b**) $3x + 5y + 15z! = 17$. (**c**) $x^2 + y^2 + z! = 24$. (**d**) $x^2 + y^2 - z! = 3$.
Solution:
(**a**) On reducing the equation in modulo 3 we get $2x \stackrel{3}{=} 0$, i.e. $x = 3k$ where $k \in \mathbb{Z}$.
On reducing the equation in modulo 2 we get $y \stackrel{2}{=} 0$, i.e. $y = 2s$ where $s \in \mathbb{Z}$.
On substituting these into the original equation we get:
$2(3k) + 3(2s) - 6z! = 222 \quad \rightarrow \quad 6k + 6s - 6z! = 222 \quad \rightarrow \quad k + s - z! = 37 \quad \rightarrow \quad s = z! + 37 - k$
So, the solutions are: $(x, y, z) = (3k,\ 2t! + 74 - 2k,\ t)$ where $k \in \mathbb{Z}$ and $t \in \mathbb{N}^0$.
(**b**) On reducing the equation in modulo 5 we get $3x \stackrel{5}{=} 2$, i.e. $x = 4 + 5k$ where $k \in \mathbb{Z}$.
On reducing the equation in modulo 3 we get $2y \stackrel{3}{=} 2$, i.e. $y = 1 + 3s$ where $s \in \mathbb{Z}$.
On substituting these into the original equation we get:
$3(4 + 5k) + 5(1 + 3s) + 15z! = 17 \qquad \rightarrow \qquad 12 + 15k + 5 + 15s + 15z! = 17 \qquad \rightarrow \qquad s = -k - z!$
So, the solutions are: $(x, y, z) = (4 + 5k,\ 1 - 3k - 3t!,\ t)$ where $k \in \mathbb{Z}$ and $t \in \mathbb{N}^0$.
(**c**) z cannot be greater than 4 because otherwise the LHS will be greater than 24. So, all we need to do is to consider $z = 0, 1, 2, 3, 4$. On doing so we get the following five solutions:

$$(x, y, z) = (-3, \pm 3, 3) \qquad (x, y, z) = (0, 0, 4) \qquad (x, y, z) = (3, \pm 3, 3)$$

(**d**) For $z > 3$ we have $x^2+y^2 \stackrel{4}{=} 3$ which has no solution. So, all we need to do is to consider $z = 0, 1, 2, 3$. On doing so we get the following twenty solutions:

$(\pm 3, 0, 3)$ $(\pm 2, -1, 2)$ $(\pm 2, 0, 0)$ $(\pm 2, 0, 1)$ $(\pm 2, 1, 2)$

$(\pm 1, -2, 2)$ $(\pm 1, 2, 2)$ $(0, \pm 3, 3)$ $(0, \pm 2, 0)$ $(0, \pm 2, 1)$

5.9 Trigonometric Diophantine Equations

1. Find all $x, y \in \mathbb{Z}$ that satisfy the following equations:

(**a**) $3\sin\left(\frac{x\pi}{2}\right) - 4\sin\left(\frac{y\pi}{2}\right) = 1.$ (**b**) $5\sin\left(\frac{x\pi}{2}\right) + \cos(y\pi) = 3.$ (**c**) $2\sin\left(\frac{x\pi}{2}\right) + 3\cos\left(\frac{y\pi}{2}\right) = 2.$

Solution:

(**a**) The sine function of integer multiples of $\pi/2$ takes the values $0, 1, 0, -1$ corresponding to $x \stackrel{4}{=} 0, 1, 2, 3$ (and similarly for y). So, the only possibility for the LHS of this equation to be equal to 1 is when $\sin\left(\frac{x\pi}{2}\right) = \sin\left(\frac{y\pi}{2}\right) = -1$ so that the LHS becomes $3(-1) - 4(-1) = 1$. So, the solutions of the given equation are $(x, y) = (3 + 4k,\ 3 + 4s)$ where $k, s \in \mathbb{Z}$.

(**b**) The sine function of integer multiples of $\pi/2$ takes the values $0, 1, -1$ while the cosine function of integer multiples of π takes the values $1, -1$. Accordingly, the term $5\sin\left(\frac{x\pi}{2}\right)$ takes the values $0, 5, -5$ while the term $\cos(y\pi)$ takes the values $1, -1$. As we see there is no combination of these values that can make the sum of the terms on the LHS to be equal to 3. So, the given equation has no solution.

(**c**) If we argue as in the previous parts then $2\sin\left(\frac{x\pi}{2}\right) = 0, 2, 0, -2$ corresponding to $x \stackrel{4}{=} 0, 1, 2, 3$ while $3\cos\left(\frac{y\pi}{2}\right) = 3, 0, -3, 0$ corresponding to $y \stackrel{4}{=} 0, 1, 2, 3$. So, their sum is equal to 2 when $(x, y) \stackrel{4}{=} (1, 1)$ and $(x, y) \stackrel{4}{=} (1, 3)$. Hence, the solutions of the given equation are $(x, y) = (1 + 4k,\ 1 + 2s)$ where $k, s \in \mathbb{Z}$.

2. Find all $x, y, z \in \mathbb{Z}$ that satisfy the following equations:

(**a**) $\sin\left(\frac{x\pi}{2}\right) + 5\cos(y\pi) = 6\cos(z\pi).$ (**b**) $\tan\left(x\pi + \frac{\pi}{3}\right) + 2\sin\left(y\pi + \frac{2\pi}{3}\right) = 2\cos\left(\frac{z\pi}{6}\right).$

Solution:

(**a**) We have:

$$\sin\left(\tfrac{x\pi}{2}\right) = 0, 1, 0, -1 \quad \text{for} \quad x \stackrel{4}{=} 0, 1, 2, 3$$

$$5\cos(y\pi) = 5, -5 \quad \text{for} \quad y \stackrel{2}{=} 0, 1$$

$$6\cos(z\pi) = 6, -6 \quad \text{for} \quad z \stackrel{2}{=} 0, 1$$

So, the two sides become equal in the following two cases (where $k, s, t \in \mathbb{Z}$):

$$(x, y, z) = (1 + 4k,\ 2s,\ 2t) \qquad (x, y, z) = (3 + 4k,\ 1 + 2s,\ 1 + 2t)$$

So, these are the solutions of the given equation.

(**b**) We have:

$$\tan\left(x\pi + \tfrac{\pi}{3}\right) = \sqrt{3} \quad \text{for all } x \in \mathbb{Z}$$

$$2\sin\left(y\pi + \tfrac{2\pi}{3}\right) = \sqrt{3}, -\sqrt{3} \quad \text{for} \quad y \stackrel{2}{=} 0, 1$$

$$2\cos\left(\tfrac{z\pi}{6}\right) = 2, \sqrt{3}, 1, 0, -1, -\sqrt{3}, -2, -\sqrt{3}, -1, 0, 1, \sqrt{3} \quad \text{for} \quad z \stackrel{12}{=} 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$$

So, the two sides become equal in the following two cases (where $k, s, t \in \mathbb{Z}$):

$$(x, y, z) = (k,\ 1 + 2s,\ 3 + 12t) \qquad (x, y, z) = (k,\ 1 + 2s,\ 9 + 12t)$$

These cases can be combined in the following single formula (which represents all the solutions of the given equation): $(x, y, z) = (k,\ 1 + 2s,\ 3 + 6t)$.

Chapter 6
Diophantine Systems

In this chapter we investigate some examples of systems of Diophantine equations of various types and how they are solved. In fact, this chapter should be regarded as continuation to the previous chapter as both chapters are essentially about solving Diophantine equations (i.e. individually or collectively).[53]

6.1 General Issues about Diophantine Systems

1. What we mean by "the solution of a system of Diophantine equations"?
   Solution: A solution of a system of Diophantine equations is a solution that satisfies all the equations in the system simultaneously, and hence the solution of a system of Diophantine equations is the set of all such solutions. Accordingly, the set of solutions of a system of Diophantine equations (which is "the solution of a system of Diophantine equations") is the intersection of the sets of solutions of its individual equations. So, when we tackle a problem of a system of Diophantine equations we are actually trying to find the intersection of the sets of solutions of its individual equations.
2. What we mean by "solving a system of Diophantine equations"?
   Solution: "Solving" (or "finding the solution") of a system of Diophantine equations should mean *proving* (by an irrefutable logical/mathematical argument) that there is no solution (i.e. when there is no solution) or *finding* all solutions of the system (either explicitly or through a sort of closed form formula or formulae) with an irrefutable argument that there are no other solutions to the system. So, a system of Diophantine equations is not solved, for instance, by finding a number of solutions (e.g. through inspection or through computational search) even if we are absolutely certain that there are no other solutions to the system.
3. Outline the criterion for the solvability of a system of Diophantine equations.
   Solution: As we already said, the set of solutions of a system of Diophantine equations is the intersection of the sets of solutions of its individual equations. As a result, a system of Diophantine equations is solvable only if its individual equations are solvable, although the converse is not true in general. This means that a system of Diophantine equations has no solution if some of its equations have no solution, but a system may not have a solution even though all its individual equations have solutions (i.e. when the intersection of these solutions is the empty set). In other words, the solvability (i.e. having solution) of the individual equations of a system is a necessary but not sufficient condition for the solvability of the system itself.
4. Outline the main methods for solving a system of Diophantine equations.
   Solution: There are two main methods for solving a system of Diophantine equations in number theory:
   • The first method employs a "collective approach" (i.e. by solving the system as a whole) which is based on using the traditional methods of solving systems of multivariate equations (as investigated in algebra and linear algebra for instance) such as by substitution or comparison or use of the techniques of matrices (see for instance § 4.3 of V1).
   • The second method employs an "individual approach", i.e. by solving the individual equations of the system separately (either by the general methods of algebra or by the special methods and techniques of number theory as seen for instance in chapter 5) and selecting the solutions that satisfy the system as a whole (i.e. by accepting only the solutions which are common to all the equations). In this context, we should pay special attention to the method of having (or obtaining) the solution of one equation and test it on the other equations in the system (see the last point of Problem 6).
   It should be obvious that any solution found by these methods is acceptable only if it is an integer

[53] In fact, it is also continuation to the material about this topic which we investigated in the first volume of this book.

solution (or sub-integer solution if there are extra conditions imposed on the system by the given problem such as being positive or non-negative or within certain range as demanded for instance by physical requirements).

5. Discuss briefly "linear" and "non-linear" systems of Diophantine equations.
   Solution: We note the following:
   • Systems of Diophantine equations can be classified into two main categories: linear (when all the equations of the system are linear) and non-linear (when some or all of the equations of the system are non-linear).
   • Systems of linear Diophantine equations can be easily solved by the well known (and standard) methods of linear algebra where only the integer (or sub-integer such as positive integer) solutions are accepted. Other methods (including the methods used for solving systems of non-linear equations) are also possible to use in general for solving systems of linear equations (as will be discussed later).
   • Non-linear systems of Diophantine equations can be solved usually by the well known algebraic methods of solving systems of equations (which are not restricted to Diophantine equations) such as by elimination, comparison and substitution where only integer (or sub-integer) solutions are accepted. However, it should be noted that certain methods (which are mostly investigated in linear algebra) are not applicable in solving non-linear Diophantine systems since these methods are specific to linear systems.
6. Outline some general recommendations or guidelines that should be followed in solving systems of Diophantine equations (especially the non-linear ones).
   Solution: For example:
   • Initial sensibility checks (such as parity or modularity or sign or magnitude checks) are strongly recommended (if not required) as the first step in tackling and solving Diophantine systems as well as in tackling and solving individual Diophantine equations (see Problem 5 of § 5.1 as well as Problem 7 of the present section). In many cases, solving the given system of equations does not need more than these initial sensibility checks since these checks can reveal that the system either has no solution (e.g. because one of the equations has no solution due to parity violation or modularity inconsistency or because some of the equations require conditions that contradict the conditions required by the other equations) or because the solution becomes so obvious by these initial sensibility checks.
   • It is recommended to test all the obtained solutions on the given system of equations. This is because some of the algebraic manipulations which are (usually) required during the process of solving systems of non-linear equations (such as raising to powers or multiplication or division by a variable) can introduce foreign solutions and hence by testing the obtained solutions we make sure that no foreign solution is introduced during these manipulations.
   • Systems of linear equations can be considered as a special case of systems of non-linear equations and hence they can be solved by the methods of systems of non-linear equations (when applicable) as well as by the methods and techniques which are specific to systems of linear equations (such as by the methods of matrices of linear algebra).
   • Unlike linear systems of Diophantine equations, there is no standard (or systematically applicable) method or technique for solving non-linear systems of Diophantine equations and hence solving these systems is a mix of art and science (where the art is required for selecting the main approach or strategy for solving the system while the science is needed for employing and applying the technicalities of the selected approach). Therefore, it is recommended to investigate various potential methods or strategies before setting off and making the choice of the best (or even applicable) strategy to use. Investing some time and effort in this initial investigation can be very rewarding and beneficial and can save considerable amounts of time and effort in trying to solve the system in a rather random approach and chaotic manner (i.e. by a "hit-and-miss" approach).
   • If the system of Diophantine equations contains an equation whose solution is known (or can be obtained easily or more easily) then the best approach for solving the system is to test the solutions of that equation on the other equations where only the common solutions (if any) to all equations are accepted.[54] This is particularly true when some of the equations in the (non-linear) system are linear.

[54] This is based on the obvious fact that the solution of the system is the intersection of the solutions of the individual

This approach usually saves considerable amounts of time and effort in trying to solve the system by other methods. In fact, in some cases this can be the only viable method for solving the system.

7. Discuss (briefly) initial sensibility checks and the importance of applying them when tackling a Diophantine system problem.

Solution: Conducting initial sensibility checks as a first step in dealing with Diophantine problems applies not only to single Diophantine equations (which we investigated in Problem 5 of § 5.1) but also to systems of Diophantine equations. So, if a system contains a non-solvable equation then the system is not solvable. Therefore, it is worthwhile to inspect the individual equations of the system (to check if they are solvable or not) before trying to solve the system. For example, if we are given the following system:

$$x^2 + y^3 - z^4 = 3 \qquad 2x + y^2 - 3y - 6z^2 = 75 \qquad (x, y, z \in \mathbb{Z})$$

then a quick initial inspection should reveal that the second equation has no solution (due to parity violation) and hence the system has no solution (with no need for inspecting the first equation or the system as a whole).

It is also worthwhile to inspect the characteristics of the system as a whole (i.e. not only its individual equations separately) to see if it is sensible for the system to have a solution or not. For example, if we are given the following system of Diophantine equations:

$$3x^4 + 7y^2 + z^2 = 0 \qquad x^2 + y^4 = 37 \qquad (x, y, z \in \mathbb{Z})$$

then a quick initial inspection should reveal that the first equation has only the trivial solution (i.e. $x = y = z = 0$), while the second equation can have only non-trivial solutions (i.e. it cannot accept the trivial solution). This means that the two equations cannot have a common solution and hence the system has no solution (although both equations are solvable individually). Initial inspection to the system as a whole should also reveal that the following system:

$$3x^2 + 5y^2 - z = 0 \qquad 2x^2 + 7y^4 + z^3 + 9 = 0 \qquad x + y + z + 1 = 0 \qquad (x, y, z \in \mathbb{Z})$$

has no solution because if the first equation has a solution then z must be non-negative, while if the second equation has a solution then z must be negative. So, the two equations cannot have a common solution and hence this system cannot have a solution (although each equation in the system is solvable).

Also see Problem 5 of § 5.1.

6.2 Systems of Diophantine Equations

1. Solve the following systems of Diophantine equations in the unknowns $x, y \in \mathbb{Z}$:

(**a**) $3x^2 + 4y = 19$	$5x - 2y = 3$.	
(**b**) $\sqrt{x} - 11y^2 = 8$	$4xy - 1033y^2 = 411$.	
(**c**) $x^3y + y^3x - xy = 0$	$x^2 + y^2 - 2xy - x = 0$.	
(**d**) $x^3 + y + 2xy = 0$	$y^3 + x + 2xy = 0$.	
(**e**) $x^2 - 2x + 4 + y = 0$	$x^2 + y^2 + 6x - 10y + 30 = 0$.	
(**f**) $15x + 13xy - 20y = 0$	$3x^4 + 2y^3 + 202 = 0$	$7x^5 - 4y^2 - 9x^3y = 484$.
(**g**) $x^2 - 3y = 19$	$13y^3 + 6x = 11$	$x^2 + y^2 = 17$.
(**h**) $3xy + x^2 - 5y = 33$	$5x^3 + 10xy + 11y^2 = 23$	$17x + 4xy^2 = 147$.

Solution:

(**a**) From the second equation we get $2y = 5x - 3$. On substituting this into the first equation and simplifying we get $3x^2 + 10x - 25 = 0$ whose only (integer) solution is $x = -5$ (and hence $y = -14$).

---

equations (see Problem 1) and hence the set of solutions of the system cannot exceed the set of solutions of any one of the equations in the system, i.e. the set of solutions of the system is a (proper or improper) subset of the set of solutions of any one of the equations in the system.

So, the only solution to this system is $(x, y) = (-5, -14)$. Also see part (a) of Problem 1 of § 6.3.
(**b**) From the first equation we get $x = (11y^2 + 8)^2$. On substituting this into the second equation and simplifying we get $484y^5 + 704y^3 - 1033y^2 + 256y = 411$ whose only (integer) solution is $y = 1$ (and hence $x = 19^2 = 361$). So, the only solution to this system is $(x, y) = (361, 1)$.
(**c**) We have two cases:
• $x = 0$ and hence (from the second equation) we get $y = 0$.
• $x \neq 0$ and hence:
If $y = 0$ then (from the second equation) we get $x^2 - x = 0$ whose solution is $x = 1$ (noting that $x \neq 0$).
If $y \neq 0$ then (from the first equation) we get:

$$x^3y + y^3x - xy = 0 \qquad \rightarrow \qquad x^3y + y^3x = xy \qquad \rightarrow \qquad x^2 + y^2 = 1$$

The last equation has no solution (noting that $x \neq 0$ and $y \neq 0$).
So in brief, the given system has only two solutions: $(x, y) = (0, 0)$ and $(x, y) = (1, 0)$.
(**d**) If $xy = 0$ then $(x, y) = (0, 0)$ is a solution.
If $xy \neq 0$ then on dividing the first equation by x and the second equation by y we get:

$$x^2 + \tfrac{y}{x} + 2y = 0 \qquad \text{and} \qquad y^2 + \tfrac{x}{y} + 2x = 0$$

This implies that $y = \pm x$. On substituting these into the first equation we get:[55]

$$x^3 + x + 2x^2 = 0 \qquad \text{and} \qquad x^3 - x - 2x^2 = 0$$

On solving these equations we get $x = -1$ from the first equation (and no integer solution $\neq 0$ from the second equation). On substituting $x = -1$ in any one of the given equations and solving for y we get $y = -1$.
So in brief, the given system has only two solutions: $(x, y) = (0, 0)$ and $(x, y) = (-1, -1)$.
(**e**) Someone with modest knowledge in mathematics should immediately realize that the first equation represents a parabola while the second equation represents a circle, and hence the problem can be solved "graphically" (possibly with no need to make any plot). If we put these equations in their standard forms (so that we can easily identify the shape and position of the graphs they represent) then we have:

$$y + 3 = -(x - 1)^2 \qquad\qquad (x + 3)^2 + (y - 5)^2 = 4$$

So, now it is obvious that the first equation represents a parabola which concaves down with vertex at $(x, y) = (1, -3)$ while the second equation represents a circle with radius 2 and center at $(x, y) = (-3, 5)$ and hence they cannot have a common point. Therefore, this system obviously has no solution. Also see part (d) of Problem 1 of § 6.3.
(**f**) In part (j) of Problem 1 of § 4.1.5 of V1 we obtained the solutions of $15x + 13xy - 20y = 0$ which are: $(x, y) = (2, -5)$, $(0, 0)$, $(-10, -1)$. So, the easiest approach for solving this system is to test the solutions of this equation on the other equations in the system where we accept only the solutions which are common to all the equations in the system.[56] If we do so we will find out that only the solution $(x, y) = (2, -5)$ satisfies all the equations of the system and hence this is the only solution to the system.
(**g**) We note that the last equation in this system is easy to solve (since we have a few possibilities for x and y to satisfy this equation). The solutions of the last equation are: $(x, y) = (\pm 1, 4)$, $(\pm 1, -4)$, $(\pm 4, 1)$ and $(\pm 4, -1)$. On testing these eight solutions on the other two equations in the system we find that only the solution $(x, y) = (4, -1)$ satisfies the other two equations. Hence, this system has only one solution, i.e. $(x, y) = (4, -1)$. Also see part (c) of Problem 1 of § 6.3.
(**h**) Initial inspection should reveal that the second equation has no solution because in modulo 5 this equation becomes $y^2 \overset{5}{=} 3$ which has no solution since 3 is not a quadratic residue of 5. So, this system has no solution although the other two equations in the system have a common solution, i.e. $(x, y) = (7, -1)$.

[55] The same result will be obtained from substitution into the second equation.
[56] The justification of this approach is that the solution of the system is the intersection of the solutions of the individual equations and hence the set of solutions of the system cannot exceed the set of solutions of any one of the equations in the system, i.e. the set of solutions of the system is a (proper or improper) subset of the set of solutions of any one of the equations in the system. Also see Problem 6 of § 6.1.

2. Solve the following systems of Diophantine equations in the unknowns $x, y, z \in \mathbb{Z}$:

(**a**) $\sqrt{x} - y^2 - z^2 + 13 = 0$ $\quad 2y^2 + z^2 - x = 22.$

(**b**) $x^2 - x + 3y^2 + 14z^3 = 34$ $\quad 6x^3 + 4xy + 5y^3 - 2z = 13.$

(**c**) $7\sqrt{x} + 3\sqrt{y} + 2\sqrt{z} = 66$ $\quad 3\sqrt{x} + 5\sqrt{y} - \sqrt{z} = 19.$

(**d**) $2x + 8y^2 + 4^z = 77$ $\quad x^3 + 3y^2 - 5^z = 34.$

(**e**) $x^3 - y^3 + 3xy + z^3 = 103$ $\quad 3x + 8y^2 - z^3 = 191$ $\quad 3y^3 - 8xy - 3z^3 = 101.$

(**f**) $9x^2 + z^2 = 90$ $\quad 13x + 11y + 2\sqrt{z} = 15$ $\quad 2x^2 + 5y^2 + 3z = 49.$

Solution:

(**a**) x must be a perfect square (because of $\sqrt{x}$) and hence let $x = X^2$ where $X \in \mathbb{N}^0$. So, the equations become:

$$X - y^2 - z^2 + 13 = 0 \qquad 2y^2 + z^2 - X^2 = 22$$

Now, if we add these equations side by side we get:

$y^2 - X^2 + X = 9 \quad \rightarrow \quad 4y^2 - 4X^2 + 4X = 36 \quad \rightarrow \quad 4y^2 - (4X^2 - 4X) = 36 \quad \rightarrow$

$4y^2 - (4X^2 - 4X + 1) = 35 \quad \rightarrow \quad 4y^2 - (2X - 1)^2 = 35$

So, by factoring the two sides of the last equation we get:

$$(2y - 2X + 1)(2y + 2X - 1) = (-1)(-35) = (1)(35) = (-5)(-7) = (5)(7)$$

Now, if we consider all these eight possibilities (by comparing the factors on the two sides in both orders) then we get eight systems of simultaneous equations. On solving these eight systems (accepting only the solutions with $X \geq 0$) we get the following solutions:

$\boldsymbol{(X, y) =}$	$(9, -9)$	$(9, 9)$	$(0, -3)$	$(1, -3)$	$(1, 3)$	$(0, 3)$
$\boldsymbol{(x, y) =}$	$(81, -9)$	$(81, 9)$	$(0, -3)$	$(1, -3)$	$(1, 3)$	$(0, 3)$

On inserting these values in the original equations and solving for z (accepting only the consistent solutions) we get: $(x, y, z) = (0, \pm 3, 2)$ and $(x, y, z) = (0, \pm 3, -2)$. So, these four solutions are the only solutions to the given system.

(**b**) If the first equation has any solution then y must be even, while if the second equation has any solution then y must be odd. This parity inconsistency of the system makes the given system non-solvable, i.e. it has no solution in integers.

(**c**) x, y, z must be perfect squares. If we add twice the second equation to the first equation and simplify we get:

$$\sqrt{x} + \sqrt{y} = 8 \tag{27}$$

Now, it is obvious that $\sqrt{x}$ and $\sqrt{y}$ cannot exceed 8 (because otherwise the LHS of Eq. 27 will be > 8). So, it is obvious that only the following nine pairs satisfy Eq. 27:

$\boldsymbol{(x, y) =}$ $(0, 64)$ $(1, 49)$ $(4, 36)$ $(9, 25)$ $(16, 16)$ $(25, 9)$ $(36, 4)$ $(49, 1)$ $(64, 0)$

Now, if we try these nine pairs on the equations of the given system we find that all these pairs produce valid solutions. So, the solutions of the given system are: $(x, y, z) = (0, 64, 441)$, $(1, 49, 361)$, $(4, 36, 289)$, $(9, 25, 225)$, $(16, 16, 169)$, $(25, 9, 121)$, $(36, 4, 81)$, $(49, 1, 49)$, $(64, 0, 25)$.

Finally, it is worth noting that this system can be treated as a system of linear equations in $\sqrt{x}, \sqrt{y}, \sqrt{z}$ (where the domain of these roots is the set of non-negative integers) and hence it is solved as such (where the final x, y, z solutions are obtained by squaring the values of the variables in the solutions of the system of linear equations).

(**d**) We must have $z \geq 0$. From the first equation, z must be zero (due to parity requirement). So, the system becomes:

$$2x + 8y^2 = 76 \qquad x^3 + 3y^2 = 35$$

Now, from the first of these equations we get $x = 38 - 4y^2$. On substituting this into the second equation and simplifying we get: $64y^6 - 1824y^4 + 17325y^2 = 54837$ whose only (integer) solutions are $y = \pm 3$

(and hence $x = 2$). So, the given system has only two solutions, i.e. $(x, y, z) = (2, \pm 3, 0)$.
(**e**) We have:

$$\begin{aligned} 3\left(x^3 - y^3 + 3xy + z^3\right) + \left(3y^3 - 8xy - 3z^3\right) &= (3 \times 103) + 101 \\ 3x^3 + xy &= 410 \\ y &= \frac{410}{x} - 3x^2 \end{aligned}$$

i.e. x is a divisor of 410. Now, the divisors of 410 are 1, 2, 5, 10, 41, 82, 205, 410 and their negatives (i.e. 16 divisors in total). So, from the last equation we obtain the value of y corresponding to each one of these 16 divisors (which represent the values of x) and hence we get 16 (x, y) pairs. On trying these 16 pairs on the three equations of the system and solving for z we find that only the pair $(x, y) = (5, 7)$ produces a consistent result (where z corresponding to this pair is 6). Hence, the only solution of the given system is $(x, y, z) = (5, 7, 6)$.
(**f**) The second equation implies $z \geq 0$ while the third equation implies $z \leq 16$. So, all we need to do is to try the values $z = 0, 1, \ldots, 16$ in the first equation to get the corresponding values of x and hence obtaining 34 pairs of $(\pm|x|,\ z)$. On trying these 34 pairs[57] in the second and third equations we get the corresponding values of y. On doing this we find that only the pair $(x, z) = (-1, 9)$ produces a consistent result (where y corresponding to this pair is 2). Hence, the only solution of the given system is $(x, y, z) = (-1, 2, 9)$.

3. Find all $x, y \in \mathbb{Z}$ such that $f_1 = f_2 = f_3 = f_4$ where:

$$\begin{aligned} f_1(x, y) &= x^2 - y^3 + 3xy + 7788 \\ f_2(x, y) &= x^3 - 2y^3 + 51x^2 - 5y - 5652 \\ f_3(x, y) &= x^2 - 22y + 3xy + 1347 \\ f_4(x, y) &= xy^2 + y^3 + 55y + 4146 \end{aligned}$$

Solution: If $f_1 = f_2 = f_3 = f_4$ then: $f_1 = f_2$, $f_1 = f_3$ and $f_1 = f_4$. So, this Problem can be solved as a system of multivariate Diophantine equations, i.e.

$$f_1 - f_2 = 0 \qquad f_1 - f_3 = 0 \qquad f_1 - f_4 = 0$$

On solving this system[58] we find that $f_1 = f_2 = f_3 = f_4$ for $(x, y) = (-33, 19)$.

4. Class A, B, C of orange cost \$1.71, \$1.63, \$1.51 per kg, while class A, B, C of apple cost \$1.57, \$1.49, \$1.42 per kg. An 11% (9%) discount is offered to anyone who buys more than \$1000 of orange (apple) with the condition that he should buy at least 100 kg of any class he buys in multiples of 100's (i.e. $100, 200, 300, \ldots$). We bought 1000 kg of orange and 1000 kg of apple and paid \$2753.55 where we benefited from both discounts on the entire deal. How many kilograms of each class of orange and apple we bought?
Solution: Let a be the cost of 1000 kg of orange before discount and b be the cost of 1000 kg of apple before discount. It should be obvious that a and b are integers (noting the 100 kg condition in multiples of 100's). Now, from the discount offer we get:

$$0.89a + 0.91b = 2753.55 \tag{28}$$

Also, from the price limits and the purchased quantities we get the following inequalities:

$$1510 \leq a \leq 1710 \qquad \text{and} \qquad 1420 \leq b \leq 1570$$

Now, if we solve Eq. 28 considering the restrictions imposed by these inequalities we get only one acceptable integer solution which is $(a, b) = (1598, 1463)$.[59] Accordingly:

[57] Actually, we try only the integers of these pairs.
[58] The easiest way to solve this system is by solving the equation $f_1 - f_3 = 0$, i.e. $22y - y^3 + 6441 = 0$. The only (integer) solution of this equation is $y = 19$ and hence $x = -33$ (where this can be obtained, for instance, from $f_1 - f_2 = 0$).
[59] From Eq. 28 we have $a = (2753.55 - 0.91b)/0.89$. So, on trying $1420 \leq b \leq 1570$ we get only two integer solutions: $(a, b) = (1598, 1463)$ and $(1507, 1552)$. However, the latter solution is not acceptable because $1510 \leq a \leq 1710$.

• Regarding the orange deal we have the following system of simultaneous equations:

$$1.71x + 1.63y + 1.51z = 1598 \qquad \text{and} \qquad x + y + z = 1000$$

where x, y, z are the numbers of kilograms of class A, B, C of orange which we bought. On solving this system[60] we get: $(x, y, z) = (1.5z - 400,\ 1400 - 2.5z,\ z)$. Now, we must have:

$$x \geq 100 \quad \rightarrow \quad 1.5z - 400 \geq 100 \quad \rightarrow \quad z \geq 500/1.5 \quad \rightarrow \quad z \geq 334$$

$$y \geq 100 \quad \rightarrow \quad 1400 - 2.5z \geq 100 \quad \rightarrow \quad z \leq 1300/2.5 \quad \rightarrow \quad z \leq 520$$

So, $z = 400$ $\big[$and thus $(x, y, z) = (200, 400, 400)\big]$ or $z = 500$ $\big[$and thus $(x, y, z) = (350, 150, 500)\big]$. However, the latter solution is not acceptable because it violates the condition of multiples of 100's. So, $(x, y, z) = (200, 400, 400)$.

• Regarding the apple deal we have the following system of simultaneous equations:

$$1.57X + 1.49Y + 1.42Z = 1463 \qquad \text{and} \qquad X + Y + Z = 1000$$

where X, Y, Z are the numbers of kilograms of class A, B, C of apple which we bought. On solving this system[61] we get: $(X, Y, Z) = (0.875Z - 337.5,\ 1337.5 - 1.875Z,\ Z)$. Now, we must have:

$$X \geq 100 \quad \rightarrow \quad 0.875Z - 337.5 \geq 100 \quad \rightarrow \quad Z \geq 437.5/0.875 \quad \rightarrow \quad Z \geq 500$$

$$Y \geq 100 \quad \rightarrow \quad 1337.5 - 1.875Z \geq 100 \quad \rightarrow \quad Z \leq 1237.5/1.875 \quad \rightarrow \quad Z \leq 660$$

So, $Z = 500$ $\big[$and thus $(X, Y, Z) = (100, 400, 500)\big]$ or $Z = 600$ $\big[$and thus $(X, Y, Z) = (187.5, 212.5, 600)\big]$. However, the latter solution is obviously not acceptable. So, $(X, Y, Z) = (100, 400, 500)$.

6.3 Solving Systems of Diophantine Equations Graphically

Many systems of Diophantine equations lend themselves to a graphic approach where their solutions can be identified and obtained graphically by using graphic tools, considerations and reasoning (possibly without need for plotting and creating actual graphs). This is particularly true when we deal with 2-variable systems of Diophantine equations of various types (such as polynomials and exponentials).

The idea of using graphic approach should be obvious, i.e. we plot the graphs (possibly in our mind) representing the equations of the system to see where (or if) they meet and hence in most cases we can easily see graphically the solutions (if exist) as well as the impossibility of having more solutions (noting that graphs of different equations usually meet only in a few points in a certain region of their domain space and they depart from each other in all other regions making the impossibility of having more solutions definite and certain and hence it is a "graphic proof").

Problems

1. Find (graphically) all the solutions of the following systems of Diophantine equations:

(**a**) $3x^2 + 4y = 19$	$5x - 2y = 3.$		$(x, y \in \mathbb{Z})$
(**b**) $3^x - 5^y = 2$	$x^2 + y^2 = 13.$		$(x, y \in \mathbb{N}^0)$
(**c**) $x^2 - 3y = 19$	$13y^3 + 6x = 11$	$x^2 + y^2 = 17.$	$(x, y \in \mathbb{Z})$
(**d**) $x^2 - 2x + 4 + y = 0$	$x^2 + y^2 + 6x - 10y + 30 = 0.$		$(x, y \in \mathbb{Z})$

Solution:

(**a**) If we plot these equations we get what we see in the left frame of Figure 1. From this Figure it is obvious that this system has a maximum of two solutions. Now, if we zoom on the point at the upper right (see the middle frame of Figure 1) we see that it is not a possible (integer) solution. If we zoom on the point at the bottom left (see the right frame of Figure 1) we see that it is a possible (integer)

[60] We have:

$$1.71x + 1.63y + 1.51z - 1.63(x + y + z) = 1598 - 1.63(1000) \quad \rightarrow \quad 0.12z - 0.08x = 32 \quad \rightarrow \quad x = 1.5z - 400$$
$$1.71x + 1.63y + 1.51z - 1.71(x + y + z) = 1598 - 1.71(1000) \quad \rightarrow \quad 0.08y + 0.20z = 112 \quad \rightarrow \quad y = 1400 - 2.5z$$

[61] We have:

$$1.57X + 1.49Y + 1.42Z - 1.49(X + Y + Z) = 1463 - 1.49(1000) \quad \rightarrow \quad X = 0.875Z - 337.5$$
$$1.57X + 1.49Y + 1.42Z - 1.57(X + Y + Z) = 1463 - 1.57(1000) \quad \rightarrow \quad Y = 1337.5 - 1.875Z$$

solution. On testing $(x, y) = (-5, -14)$ on the system we find this is a solution. Hence, we conclude *graphically* that $(x, y) = (-5, -14)$ is the only solution of this system (which is a conclusion that we obtained *algebraically* in part a of Problem 1 of § 6.2).

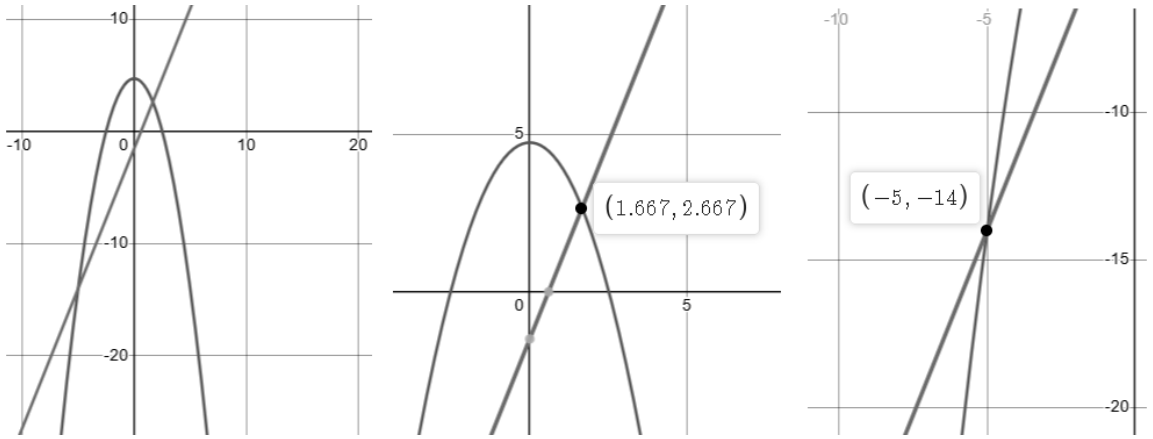


Figure 1: The plot of part (a) of Problem 1 of § 6.3.

(**b**) If we plot these equations we get what we see in Figure 2. From this Figure it is obvious that this system has only one possible solution (noting that $x, y \in \mathbb{N}^0$ because of the exponential equation) which (by graphic inspection and verification) is $(x, y) = (3, 2)$.

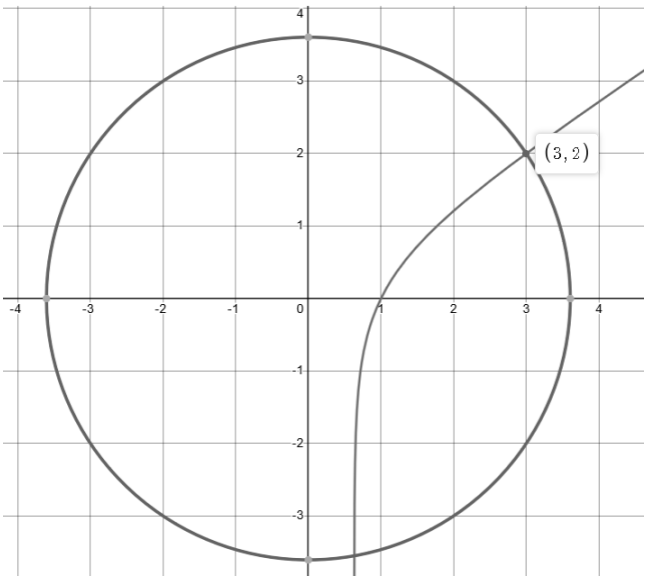


Figure 2: The plot of part (b) of Problem 1 of § 6.3. The parts of the curves outside the first quadrant should be ignored.

(**c**) If we plot these equations we get what we see in Figure 3. This Figure (associated with the awareness that all the "potential solutions" that belong to the circle are within the plotted area) should lead to the definite conclusion that the only solution to this system is $(x, y) = (4, -1)$. This conclusion was obtained *algebraically* in part (g) of Problem 1 of § 6.2).
(**d**) In part (e) of Problem 1 of § 6.2, this system was "solved graphically" without visualization (i.e. we used a "graphic argument" without plotting any graph). In the present Problem we plot the graphs

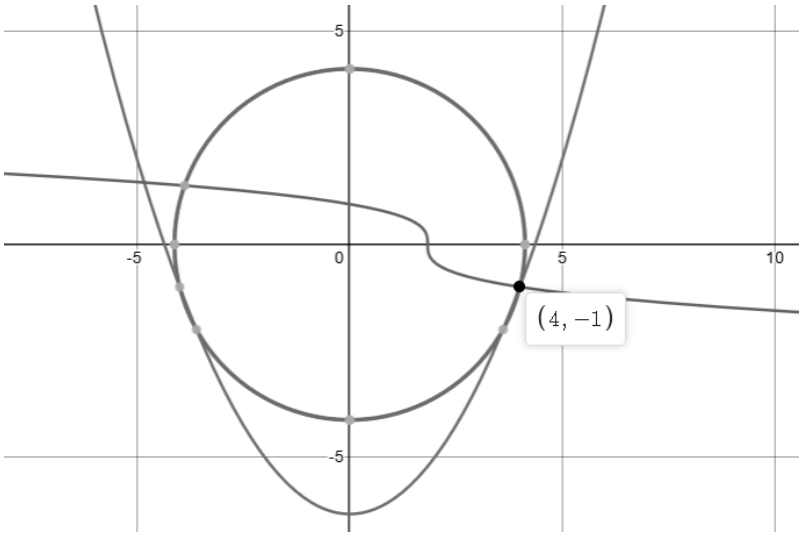


Figure 3: The plot of part (c) of Problem 1 of § 6.3.

representing the two equations of this system to confirm our solution in that Problem (see Figure 4).

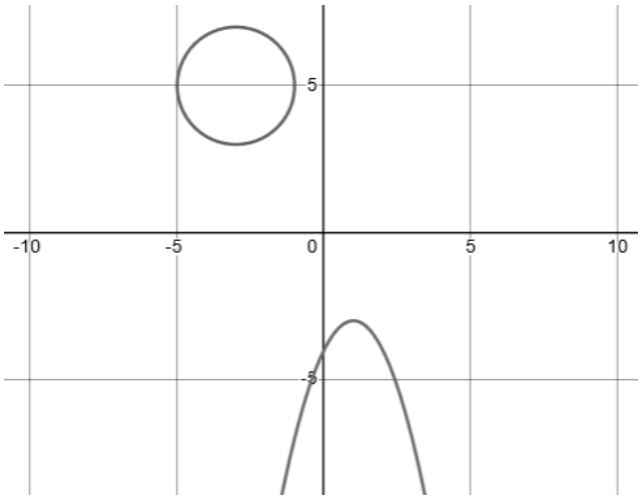


Figure 4: The plot of part (d) of Problem 1 of § 6.3.

6.4 Final Thought about how to Solve Diophantine Problems

Solving Diophantine problems (whether individual equations or systems of equations) is usually a big task. In this final section of this chapter[62] we present a list of recommendations and guidelines that can (and should) be used as a reference in tackling Diophantine problems. In fact, most of these recommendations are based on (and extracted from) our experience (in the present and previous chapter as well as in V1) related to the methods and techniques used in solving Diophantine problems.

1. Conduct an initial (and basic) sensibility checks (or tests) such as parity consistency checks, simple divisibility tests, primality/composity tests, sign tests, and so on (see for instance § 1.11 and § 4.1 of

[62] We note that this section is mostly about the previous chapter but it was deferred to this position because it is about systems as well as equations.

V1 for some recommendations and guidelines; also see Problem 5 of § 5.1 and Problem 6 of § 6.1 of the present volume). Many Diophantine problems do not need in their solution more than an informed inspection based on these initial and simple checks and tests and hence it is worthwhile to spend a few minutes on doing this sort of initial inspection and tests which can save a considerable amount of time and effort in trying to solve the given problem by the use of sophisticated approaches and techniques (which may or may not lead to the required result).

2. Use computational tools (such as coding or spreadsheets or software packages) to give you an initial impression and insight about the nature of the expected (and sought-after) solution(s). In fact, this initial computational inspection can be a great help in identifying and producing a theoretical and general argument (or proof or formulation or ...) that solves the problem completely and unequivocally.
3. Use graphic tools (when possible and applicable) for initial inspection of systems of Diophantine equations by plotting the equations on the same graph to see if and where they have points of intersection (see § 6.3). In fact, the use of these tools can lead to the final solution of the problem without further inspection or work.
4. Classify the problem such as linear or non-linear, exponential or polynomial (involving quadratic or/and cubic or ...), 2- or 3- $\cdots$ or n-variable problem, etc.
5. Recall the standard methods of solution for the specific type (as identified according to the recommendation of the previous point). Use previously-solved problems (related to the identified specific type) as prototypes and models to see if it is possible to apply their methods of solution to the problem at hand.
6. Consider comparing the given Diophantine equation to a similar equation whose solutions are known or whose solutions are easier to obtain and hence obtain the solutions of the given equation with minimal effort (or with no effort). See for instance Problem 3 of § 5.1.
7. Look for symmetry in the variables which can be exploited (for instance) in assuming temporarily that the variables have a certain increasing or decreasing order. This should facilitate the search for a solution (where the final and complete solution can be obtained eventually by permuting the solution obtained on the base of ordering assumption). Also look for cyclic pattern in the variables where this pattern can be exploited similarly (e.g. by assuming certain ordering in the variables).
8. Consider reducing the domain of solution temporarily until a solution is found (for the reduced domain) where this solution can be extended and generalized later on to reach the final and complete solution for the entire domain. For example, if we are dealing with a Diophantine equation in the domain of integers $\mathbb{Z}$ involving variables with even powers then we can start by considering its solution in the domain of natural numbers $\mathbb{N}$ (instead of $\mathbb{Z}$) where the final and complete solution can be obtained trivially later on by extending the domain to the negative integers (noting that even powers do not distinguish between positive and negative bases).
9. Consider producting a factored expression involving variables (on the LHS) that is equal to a specific number (on the RHS) where the factors involving variables (on the LHS) can be matched with numeric factors (on the RHS) to produce systems of simultaneous equations that can be solved to produce the solution(s) of the given problem. The number of the possible factors on the two sides should also be considered in some problems since it can eliminate certain possibilities for the solution (see for instance Problem 7 of § 5.2). Also consider employing divisibility arguments of one side (or of factors of one side) by the other side (or by factors of the other side).
10. Consider employing modular arithmetic to reduce the given equation in certain moduli where the relationship between ordinary and congruence equations (see § 2.7.6 of V1) can be exploited to infer the solutions of the given equation (or to conclude that the given equation has no solution).
11. Recall basic rules and principles (such as ordering rules and principles). Examples of these rules and principles are:
    No (perfect) square can be between consecutive squares, no (perfect) cube can be between consecutive cubes, and so on.
    No (perfect) square can be the sum of two odd squares.
    Any (perfect) cube can be expressed as a difference of two squares.
    Fermat's last theorem can also be considered in this regard since it eliminates certain possibilities of

solution.

12. Remember Pell's equation (see § 1.2) when dealing with quadratic polynomial equations in 2-variables. Consider manipulating the equation (if necessary) to put it in a standard Pell's form (e.g. by scaling the equation and completing squares to simplify the expressions and reducing the number of terms as well as organizing the equation to identify and recognize the pattern). Also consider the generalized form of Pell's equation (not only its standard form). As soon as we solve the obtained Pell equation we can try obtaining the solutions of the original equation by the reverse transformation (where we accept only the integer solutions). However, we should keep in mind that the existence of solution to the transformed Pell equation does not guarantee the existence of solution to the original equation (see § 1.2) since the reverse transformation may not produce integer solutions.
13. Remember Pythagorean triple rules and theorems when dealing with quadratic equations in 3 variables. As in the previous point, consider manipulating the equation (if necessary) to put it in a standard Pythagorean triple equation form (e.g. by completing the squares or/and by transforming the variables).
14. Consider upper and lower bounds on the potential solutions (e.g. when dealing with equations involving fractions).
15. Consider sign bounds and bounding inequalities (e.g. when dealing with polynomials and exponentials).
16. Recall Wilson's theorem when the equation involves factorial.
17. Consider special (or limiting or obvious or eccentric or ...) cases and instances such as when one (or more) of the variables is 0 or ± 1 or goes to infinity. Such considerations can give an insight in the solution (or reduce the possibilities or organize the approach of solution or ...).
    Give special attention to the dominating terms which can (for instance) impose limits or determine the eventual tendency of the equation.
18. Use computational tools (such as coding or spreadsheets or software packages) to check the final answer (if necessary) especially when you have some doubt or when the produced argument (or proof or formulation or ...) is very messy and susceptible to errors and mistakes.

Chapter 7
Inequalities

7.1 General Issues about Inequalities

1. Outline some basic rules that govern inequalities and hence they can (and should) be used to solve inequality problems in number theory (as well as in other mathematical branches like analysis).
Solution: For example:
• We can add and subtract the same quantity to both sides.
• We can multiply and divide each side by the same (non-zero) quantity but the sense of inequality should be reversed if the quantity is negative.
• The factorial function $n!$ grows faster than the corresponding exponential function a^n (where $a > 1$ is constant) and hence $n!$ becomes $> a^n$ eventually (i.e. at high values of n).
• The exponential function a^n $(a > 1, n > 0)$ grows faster than the corresponding polynomial function (e.g. n^5) and hence a^n becomes $> n^5$ eventually.
• Higher order polynomials (e.g. n^3) grows faster than the corresponding lower order polynomials (e.g. $n + 99$) and hence the higher order becomes bigger (in magnitude) than the lower order eventually. In particular, any (non-constant) polynomial will eventually exceed (in magnitude) any constant (polynomial) function.
• An inequality involving absolute value represents double inequality. For example, $|n| < 3$ means $-3 < n < 3$ while $|n| > 3$ means $n < -3$ and $n > 3$.
• Taking the absolute value of the two sides of an inequality whose both sides are negative should reverse the sense of inequality (because it is equivalent to multiplication by -1). For example, if $m, n < 0$ and $m < n$ then $|m| > |n|$.
2. List some tools and techniques that can (and should) be used (at least as a first step) in inspecting and investigating inequality problems.
Solution: The most common tools and techniques are:
• Graphs (whether in 1D or 2D or 3D depending on the nature of the problem and the number of variables).[63]
• Tables of values (such as spreadsheets) where the sense of inequality can be observed as a function of the value of variable(s).
• Tables of sign (see for instance Problem 3 of § 2).
• Coding and programming by using computer languages for systematic search and inspection. In fact, this tool is usually more powerful than graphs and tables (especially in multivariate inequalities and could be the only viable choice in such cases) since it can inspect a huge amount of possibilities and values in reasonable time and with maximum reliability (if vigilance and caution are observed).
3. Which of the following inequalities is correct/incorrect:
(**a**) $9279^{3284} > 3979^{4729}$. (**b**) $4321! > 17^{11251}$. (**c**) $C_{991}^{2388} < C_{1397}^{2388}$. (**d**) $P_{528}^{1127} < P_{444}^{1324}$.
Solution: All these inequalities are incorrect because:
(**a**) The number of digits of 9279^{3284} is (see Problem 10 of § 2):

$$\lfloor 3284 \log_{10} 9279 \rfloor + 1 = \lfloor 13029.274 \rfloor + 1 = 13030$$

while the number of digits of 3979^{4729} is:

$$\lfloor 4729 \log_{10} 3979 \rfloor + 1 = \lfloor 17023.331 \rfloor + 1 = 17024$$

[63] 1D graph refers to the common technique of using number line (possibly truncated) to mark the critical values for the inequality. 2D and 3D graphs should be obvious (e.g. the x, y and the x, y, z plots which are commonly used in calculus and analysis).

(**b**) The number of digits of 4321! is (see Problem 9 of § 2):

$$\left\lfloor \sum_{k=1}^{4321} \log_{10}(k) \right\rfloor + 1 = \lfloor 13834.990 \rfloor + 1 = 13835$$

while the number of digits of 17^{11251} is (see Problem 10 of § 2):

$$\lfloor 11251 \log_{10} 17 \rfloor + 1 = \lfloor 13843.781 \rfloor + 1 = 13844$$

(**c**) We have $C_{991}^{2388} = C_{1397}^{2388}$ because $1397 = 2388 - 991$.
(**d**) The number of digits of P_{528}^{1127} is (see Problem 11 of § 2):

$$\left\lfloor \sum_{k=1127-528+1}^{1127} \log_{10}(k) \right\rfloor + 1 = \left\lfloor \sum_{k=600}^{1127} \log_{10}(k) \right\rfloor + 1 = \lfloor 1546.669 \rfloor + 1 = 1547$$

while the number of digits of P_{444}^{1324} is:

$$\left\lfloor \sum_{k=1324-444+1}^{1324} \log_{10}(k) \right\rfloor + 1 = \left\lfloor \sum_{k=881}^{1324} \log_{10}(k) \right\rfloor + 1 = \lfloor 1349.497 \rfloor + 1 = 1350$$

7.2 Univariate Inequalities

1. Find all $n \in \mathbb{N}^0$ such that $n^6 + 3n^4 + 2 > n!$.
Solution: The factorial function grows faster than the polynomial functions and hence we expect $n!$ to become bigger than $(n^6 + 3n^4 + 2)$ at high values of n (see Problem 1 of § 7.1). On inspecting the low values of n (say up to $n = 10$) we find that $n^6 + 3n^4 + 2 > n!$ is true only for $n = 0, 1, \ldots, 9$. To make sure that this does not hold for any $n > 9$ we can use induction. So, for $n = 10$ we have $n^6 + 3n^4 + 2 < n!$. Now, let assume that this is true for a given $n \geq 10$ (as it is the case for $n = 10$) and hence we will prove that if so then it must also be true for $n+1$, i.e. $(n+1)^6 + 3(n+1)^4 + 2 < (n+1)!$. On multiplying both sides of $n^6 + 3n^4 + 2 < n!$ by $n + 1$ we get:

$$\begin{aligned} (n+1)(n^6 + 3n^4 + 2) &< (n+1)! \\ (n^7 + n^6 + 3n^5 + 3n^4 + 2n + 2) &< (n+1)! \\ (n^7 + 3n^5 + 2n) + (n^6 + 3n^4 + 2) &< (n+1)! \end{aligned} \tag{29}$$

Also, on substituting $(n + 1)$ in the polynomial $(n^6 + 3n^4 + 2)$ we get:

$$\begin{aligned} (n+1)^6 + 3(n+1)^4 + 2 &= n^6 + 6n^5 + 18n^4 + 32n^3 + 33n^2 + 18n + 6 \\ &= (6n^5 + 15n^4 + 32n^3 + 33n^2 + 18n + 4) + (n^6 + 3n^4 + 2) \end{aligned} \tag{30}$$

So, to prove that $(n + 1)^6 + 3(n + 1)^4 + 2 < (n + 1)!$ we need (by comparing Eqs. 29 and 30) to show that:

$$(n^7 + 3n^5 + 2n) \geq (6n^5 + 15n^4 + 32n^3 + 33n^2 + 18n + 4) \tag{31}$$

Now:

$$\begin{aligned} \frac{n^7 + 3n^5 + 2n}{6n^5 + 15n^4 + 32n^3 + 33n^2 + 18n + 4} &= \frac{1 + 3n^{-2} + 2n^{-6}}{6n^{-2} + 15n^{-3} + 32n^{-4} + 33n^{-5} + 18n^{-6} + 4n^{-7}} \\ &> 1 + 3n^{-2} + 2n^{-6} \end{aligned}$$

where the last inequality is justified by the fact that for $n \geq 10$ the denominator of the last fraction is < 1 (as well as positive). Now, since $(1 + 3n^{-2} + 2n^{-6}) > 1$ the inequality of Eq. 31 is true and hence $(n + 1)^6 + 3(n + 1)^4 + 2 < (n + 1)!$. So, by mathematical induction we conclude that $n^6 + 3n^4 + 2 < n!$ for all $n \geq 10$ and hence $n^6 + 3n^4 + 2 > n!$ is true only for $n = 0, 1, \ldots, 9$.

2. Find all $n \in \mathbb{N}^0$ such that $5^n > n!$.
   Solution: The factorial function grows faster than the exponential function and hence we expect $n!$ to become bigger than 5^n at high values of n (see Problem 1 of § 7.1). On inspecting the low values of n (say up to $n = 15$) we find that $5^n > n!$ is true only for $n = 1, 2, \ldots, 11$. To make sure that this does not hold for any $n > 11$ we can use induction (as we did in Problem 1). In brief, if $5^n < n!$ for a given $n > 11$ (as it is the case for $n = 12$) then on multiplying the two sides of this inequality by $n + 1$ we get:
   $$(n5^n + 5^n) < (n + 1)! \tag{32}$$
   Also, on substituting $(n + 1)$ in the exponential we get:
   $$5^{n+1} = 5 \times 5^n = (4 \times 5^n) + 5^n \tag{33}$$
   Now, for all $n > 11$ we have $(4 \times 5^n) < n5^n$ and hence (from Eqs. 32 and 33) we get:
   $$5^{n+1} = (4 \times 5^n) + 5^n < (n5^n + 5^n) < (n + 1)!$$
   So, $5^n > n!$ is true only for $n = 1, 2, \ldots, 11$.
3. Find all values of $n \in \mathbb{N}^0$ such that $n! > 5^n + n^5 - 10$.
   Solution: We note that this inequality is true for $n = 0$ and $n = 1$. Moreover, because at high values of n the factorial function ($n!$) grows faster than the exponential and polynomial functions (i.e. 5^n and $n^5 - 10$), we know that $n!$ will eventually exceed both 5^n and $n^5 - 10$ and their sum. So, we need to test the low values of n (i.e. which are > 1) until we reach a "critical" value of n at which $n!$ becomes bigger than $5^n + n^5 - 10$ and hence we conclude that all values of n equal and bigger than this critical value should also satisfy this inequality. On doing this we find that the critical value is $n = 12$. Hence, we conclude that $n! > 5^n + n^5 - 10$ for all $n \in \mathbb{N}^0$ excluding $2 \leq n \leq 11$.
4. Find all $n \in \mathbb{Z}$ such that $P_1 > P_2 > P_3 > P_4$ where:
   $$\begin{aligned} P_1(n) &= n^4 - 164n^3 + 8106n^2 - 119804n + 416245 \\ P_2(n) &= n^4 - 155n^3 + 7850n^2 - 144520n + 616704 \\ P_3(n) &= -n^4 + 145n^3 - 6321n^2 + 88119n - 211302 \\ P_4(n) &= -10n^3 + 1480n^2 - 53450n - 54940 \end{aligned}$$
   Solution: If $P_1 > P_2 > P_3 > P_4$ then:
   $$P_1 > P_2 \;\;\&\;\; P_2 > P_3 \;\;\&\;\; P_3 > P_4 \qquad \rightarrow \qquad P_1 - P_2 > 0 \;\;\&\;\; P_2 - P_3 > 0 \;\;\&\;\; P_3 - P_4 > 0$$
   Now, if we solve the last three inequalities we get:
   • $P_1 - P_2 > 0$ for $n < -44$ and $7 < n < 66$.
   • $P_2 - P_3 > 0$ for $n < 5$ and $25 < n < 44$ and $n > 75$.
   • $P_3 - P_4 > 0$ for $1 < n < 78$.
   These three inequalities are satisfied simultaneously for $n = 26, 27, \ldots, 43$.
5. Show that $n^n > n!$ for all $\mathbb{N} \ni n > 1$.
   Solution: We prove this by induction. It is obvious that this inequality is true for $n = 2$. Now, if we assume that it is true for a given $\mathbb{N} \ni n > 1$ then we have:
   $$(n + 1)^{n+1} = (n + 1)^n(n + 1) > n^n(n + 1) > n!(n + 1) = (n + 1)!$$
   i.e. $(n + 1)^{n+1} > (n + 1)!$. Hence, by mathematical induction this inequality is true for all $\mathbb{N} \ni n > 1$.
6. Find $n \in \mathbb{N}$ such that $10^n < 5^{6^7} < 10^{n+1}$.
   Solution: We have:
   $$\log_{10} 5^{6^7} = 279936 \log_{10} 5 \qquad \rightarrow \qquad 5^{6^7} = 10^{\log_{10} 5^{6^7}} = 10^{279936 \log_{10} 5} \simeq 10^{195666.867}$$
   Hence, $n = 195666$.

7.3 Multivariate Inequalities

1. Find the condition(s) for the validity of the following relations (where $x, y, z \in \mathbb{N}$):
   (**a**) $x^2z \le xy \le y^2z$. (**b**) $x^3y^2 - x^3y + x^2y - 7xy \ge 0$. (**c**) $x^2 - 2xy - 3y^2 \ge 0$.
   Solution:
   (**a**) If we start with $x^2 \le xy \le y^2$ then it is obvious that the condition for the validity of the given relation without z (or rather with $z = 1$) is $x \le y$ because both $x^2 \le xy$ and $xy \le y^2$ lead (by division by x and y respectively) to $x \le y$. Now, if we multiply y^2 by z (i.e. $x^2 \le xy \le y^2z$) then the validity of the relation is not affected (i.e. it is still valid for any z as long as $x \le y$) because the y^2 side represents the higher (and hence "open" or unbounded) end and hence multiplying by z does not impose a new restriction. So, a new restriction is imposed only when we multiply x^2 (which is the lower and "closed" or bounded end) by z (noting that $z \ge 1$). In other words, the restriction is imposed only on the relation $x^2z \le xy$. This relation obviously leads (by dividing by x) to $xz \le y$.
   So in brief, the condition for the validity of the given relation is $xz \le y$ or $x \le (y/z)$.
   (**b**) If we write the given relation as $x^3y^2 + x^2y \ge x^3y + 7xy$ and compare the terms on the two sides then it is obvious that $x^3y^2 \ge x^3y$ for all x, y. So, any potential violation to the validity of this relation should originate only from the last terms on the two sides. Now, it is obvious that $x^2y \ge 7xy$ is valid for all $x \ge 7$ (regardless of y). So, all we need is to investigate the cases $x = 1, 2, \ldots, 6$ with correspondingly low values of y. On doing this we find that this relation is violated only in the following cases: $x = 1, 2, \ldots, 6$ with $y = 1$, $x = 1, 2$ with $y = 2$, and $x = 1$ with $y = 3, 4, 5, 6$.
   So in brief, the conditions for the validity of the given relation are: $(x, y) \ne (m, 1)$, $(x, y) \ne (n, 2)$, and $(x, y) \ne (1, k)$ where $m = 1, 2, \ldots, 6$, $n = 1, 2$ and $k = 3, 4, 5, 6$.
   (**c**) We have:
   $$x^2 - 2xy - 3y^2 \ge 0 \quad \to \quad x^2 - 2xy + y^2 - 4y^2 \ge 0 \quad \to \quad (x-y)^2 - 4y^2 \ge 0 \quad \to$$
   $$\big[(x-y) - 2y\big]\big[(x-y) + 2y\big] \ge 0 \quad \to \quad (x-3y)(x+y) \ge 0$$
   Now, $(x + y) > 0$ and hence we must have $(x - 3y) \ge 0$, i.e. $(x/3) \ge y$.
   So in brief, the condition for the validity of the given relation is $(x/3) \ge y$.
2. Find all $m \in \mathbb{N}$ such that $m^n - n^m \ge 0$ for all $n \in \mathbb{N}^0$.
   Solution: Only $m = 3$ meets this requirement.
   For $m = 1$, $m^n - n^m < 0$ for all $n > 1$.
   For $m = 2$, $m^n - n^m < 0$ for $n = 3$.
   For $m > 3$, $m^n - n^m < 0$ for some $n < m$.
3. Find all $x, y, z, w \in \mathbb{N}$ such that $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} \ge w$.
   Solution: The maximum value of the LHS is 3 (i.e. when $x = y = z = 1$). So, we have only three cases to consider:
   • $w = 3$: we have only one possibility, i.e. $(x, y, z) = (1, 1, 1)$.
   • $w = 2$: at least one of x, y, z must be 1 (say $x = 1$), while at least one of the remaining variables must be < 3 (say $y < 3$). Now, if $y = 1$ then z can take any value while if $y = 2$ then $z < 3$. Hence, the following (x, y, z) triplets and their permutations (due to the symmetry in x, y, z) are valid solutions in this case: $(x, y, z) = (1, 1, a)$ and $(1, 2, b)$ $\big[$where $a \in \mathbb{N}$ and $\mathbb{N} \ni b < 3\big]$.
   • $w = 1$: at least one of x, y, z must be < 4 (say $x < 4$).
   If $x = 1$ then y and z can take any value.
   If $x = 2$ then at least one of y, z must be < 5 (say $y < 5$). If $y = 1$ or 2 then z can take any value. If $y = 3$ then z can take any value < 7. If $y = 4$ then z can take any value < 5.
   If $x = 3$ then at least one of y, z must be < 4 (say $y < 4$). If $y = 1$ then z can take any value. If $y = 2$ then z can take any value < 7. If $y = 3$ then z can take any value < 4.
   Hence, the following (x, y, z) triplets and their permutations are valid solutions in this case:[64]
   $(1, a, b)$ $(2, 1, a)$ $(2, 2, a)$ $(2, 3, c)$ $(2, 4, d)$ $(3, 1, a)$ $(3, 3, e)$

[64] We ignored the triplet $(3, 2, c)$ because it is included by permutation.

where $a, b \in \mathbb{N}$, $\mathbb{N} \ni c < 7$, $\mathbb{N} \ni d < 5$, $\mathbb{N} \ni e < 4$.

4. Find all $x, y, z, w \in \mathbb{N}$ such that $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} < w$.
   Solution: We do not need to solve this Problem independently because the solutions of this Problem can be obtained from the solutions of Problem 3 (i.e. the solutions of this Problem are the complement of the solutions of Problem 3).
5. Let $x, y \in \mathbb{N}$ and $x < y$. Find all (x, y) pairs such that $x^y < y^x$.
   For $x = 1$ and $y \geq 2$ we have: $1^y < y^1$ for all $y \geq 2$.
   For $x = 2$ and $y \geq 3$ we have $2^y < y^2$ only for $y = 3$.
   Regarding $x \geq 3$, it is shown in calculus that if $2 < x < y$ then $\sqrt[x]{x} > \sqrt[y]{y}$. Now, if we raise both sides of the last inequality to xy we get $x^y > y^x$.
   So in brief, if $x < y$ then $x^y < y^x$ only when $(x, y) = (1, y)$ and $(x, y) = (2, 3)$. Also see Problem 14 of § 2.
6. Let $z = \frac{x^2+x+y^2+y}{xy}$ where $x, y \in \mathbb{N}$. Show that if z is to be an integer then $z > 2$.
   Solution: If z is an integer then it must be a natural number (noting that $x, y \in \mathbb{N}$). So, all we need to do is to prove that z cannot be 1 or 2. Thus, we have two cases to consider:
   • $z = 1$, i.e. $xy = x^2 + x + y^2 + y$ which is impossible because if (we assume with no loss of generality that) $x \leq y$ then $xy \leq y^2$ and hence $xy < x^2 + x + y^2 + y$.
   • $z = 2$, i.e. $2xy = x^2 + x + y^2 + y$. Now, $x = y$ is not a possibility (because it implies $x + y = 0$) and hence let assume (with no loss of generality) that $x < y$. So, from $2xy = x^2 + x + y^2 + y$ we get:
   $xy - x^2 + xy - y^2 = x + y \quad \rightarrow \quad x(y - x) + y(x - y) = x + y \quad \rightarrow \quad x(y - x) = x + y + y(y - x)$
   The last equation is nonsensical because $x(y - x) < y(y - x)$.
7. Show that for all $x, y, z \in \mathbb{N}$ the following relation holds: $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} \geq 3$.
   Solution: If μ_a is the arithmetic mean of a set of positive numbers and μ_g is their geometric mean then the following relation holds:
   $$\mu_a \geq \mu_g \tag{34}$$
   where the equality holds *iff* all the numbers in the set are identical (noting that in this case both the arithmetic mean and the geometric mean are equal to that "identical" number). Now, μ_a and μ_g for the set $\left\{\frac{x}{y}, \frac{y}{z}, \frac{z}{x}\right\}$ are:
   $$\mu_a = \frac{\frac{x}{y} + \frac{y}{z} + \frac{z}{x}}{3} \qquad \mu_g = \sqrt[3]{\frac{x}{y} \times \frac{y}{z} \times \frac{z}{x}} = \sqrt[3]{\frac{xyz}{xyz}} = \sqrt[3]{1} = 1$$
   On substituting these in Eq. 34 we get:
   $$\frac{\frac{x}{y} + \frac{y}{z} + \frac{z}{x}}{3} \geq 1 \qquad \rightarrow \qquad \frac{x}{y} + \frac{y}{z} + \frac{z}{x} \geq 3$$
8. Repeat Problem 8 of § 5.6 using this time the result of Problem 7.
   Solution:
   (**a**) According to Problem 7, $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} \geq 3$ and hence $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 1$ has no solution.
   (**b**) According to Problem 7, $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} \geq 3$ and hence $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 2$ has no solution.
   (**c**) According to Problem 7, $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} \geq 3$ where the equality holds *iff* $\frac{x}{y} = \frac{y}{z} = \frac{z}{x}$, i.e. $x = y = z$ (see Problem 16 of § 2). This means that we have solution only when $x = y = z$. Hence, the only solution to the equation $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 3$ is $(x, y, z) = (k, k, k)$ where $k \in \mathbb{N}$ (noting that $x, y, z \in \mathbb{N}$).

Chapter 8
Congruence Equations

8.1 General Issues about Congruence Equations

1. What is the number of solutions a congruence equation can have?
   Solution: A congruence equation can have no solution, or a single solution, or finitely many solutions (i.e. in modular arithmetic sense).
2. Show that $m^2 \overset{p}{=} n^2$ *iff* $m \overset{p}{=} \pm n$ (where $m, n \in \mathbb{Z}$ and $p \in \mathbb{P}$).
   Solution: If $m \overset{p}{=} \pm n$ then by squaring both sides (according to the power rule of congruence) we get $m^2 \overset{p}{=} n^2$.
   If $m^2 \overset{p}{=} n^2$ then $m^2 - n^2 \overset{p}{=} 0$, i.e. $(m-n)(m+n) \overset{p}{=} 0$ which means that p divides $(m-n)(m+n)$. So, either p divides $(m-n)$ or p divides $(m+n)$, i.e. either $m \overset{p}{=} +n$ or $m \overset{p}{=} -n$.
3. Show that if n is a quadratic residue of an odd prime $p = 4k-1$ (where $k \in \mathbb{N}$) then the solutions of the congruence equation $x^2 \overset{p}{=} n$ are $x \overset{p}{=} \pm n^{(p+1)/4}$.
   Solution: We have:

$$x^2 \overset{p}{=} n = n \times 1 \overset{p}{=} n \times n^{(p-1)/2} = n^{(p+1)/2} = \left[\pm n^{(p+1)/4}\right]^2$$

   where we used Euler's criterion in step 3 (see § 1.9). It is worth noting that since $p = 4k-1$ then $(p+1)/4$ is integer.
4. Let $m = a\mu$ and $n = a\nu$ where $m, a, \mu, n, \nu \in \mathbb{Z}$. Show that if $m \overset{k}{=} n$ then $\mu \overset{k/g}{=} \nu$ where $g = \gcd(a, k)$.
   Solution: We have:

$m \overset{k}{=} n$	(given)
$a\mu \overset{k}{=} a\nu$	($m = a\mu$, $n = a\nu$)
$\mu \overset{k/g}{=} \nu$	(rule 8 of § 2.7 of V1; see Problem 5 of § 2.7 of V1)

   Note: the result of this Problem implies that we can divide the two sides of a congruence equation by an integer a (which is a common factor of the two sides) without affecting the validity of the congruence *iff* a is coprime to the modulo k.
5. Show that $m = n$ *iff* $m \overset{p}{=} n$ for every $p \in \mathbb{P}$ (where $m, n \in \mathbb{Z}$).[65]
   Solution: Regarding **the if part**, $m \overset{p}{=} n$ means $p|(m-n)$. Now, whatever the magnitude of $(m-n)$ there should be some p whose magnitude is bigger than the magnitude of $m-n$ (due to the fact that there are infinitely many primes). Noting that 0 is the only integer that is divisible by an integer which is bigger in magnitude, we conclude that $m-n=0$, i.e. $m=n$.
   Regarding **the only if part**, $m = n$ means $m-n=0$ and hence $p|(m-n)$ for any $p \in \mathbb{P}$ since 0 is divisible by any other integer. The result will follow from the fact that $p|(m-n)$ is equivalent to $m \overset{p}{=} n$.
   Note: "the only if part" of this proposition is straightforward because if $m = n$ then $m \overset{p}{=} n$ for every $p \in \mathbb{P}$. However, "the if part" of this proposition requires some clarification to avoid potential misunderstanding. In the above proof of "the if part" we are implicitly assuming that $(m-n)$ has a

[65] In a sense, this proposition is a stronger version of the proposition that we stated in § 2.7.6 of V1 (with minor differences in symbolism), that is: $x = y$ *iff* $x \overset{m}{=} y$ for *all* m (where $x, y \in \mathbb{Z}$ and $\mathbb{N} \ni m > 1$). This is because m should have a certain prime factorization where the divisibility by m depends on the divisibility by its prime factors. We did not use this stronger version in V1 for the sake of simplicity noting that the version of V1 was sufficient for our purposes.

given magnitude and this should suggest that m and n are fixed integers. So, "the if part" is essentially about m and n as *fixed* integers and not about them as integers *in whatever shape or form.*
For instance, if $n = 0$ while m is a function $\big[\text{say } m \equiv f(x)\big]$ such that for every $p \in \mathbb{P}$ we have $f(x) = kp$ (for some $x, k \in \mathbb{Z}$ and $k \neq 0$) then we have $f(x) \stackrel{p}{=} 0$ for every $p \in \mathbb{P}$ (i.e. $m \stackrel{p}{=} n$ for every $p \in \mathbb{P}$) although $f(x) \neq 0$ (i.e. $m \neq n$). The explanation of this is that the meaning of zero in a congruence is not the same as the meaning of zero in an ordinary equality (and this should shed more light on the meaning of zero in the above proof).
In this regard, we should mention the function $f(x) = 6x^2 + 5x + 1$ which is proved in the literature to be congruent to 0 for every $p \in \mathbb{P}$ (i.e. $6x^2 + 5x + 1 \stackrel{p}{=} 0$ has an integer solution for every $p \in \mathbb{P}$) although $6x^2 + 5x + 1 = 0$ has no integer solution. In other words, $m \stackrel{p}{=} n$ for every $p \in \mathbb{P}$ while $m \neq n$ (where $\stackrel{p}{=}$ and $\neq$ indicate the existence and non-existence of an integer solution x).

6. Find the number of (modular) solutions of the exponential congruence equation $a^x \stackrel{k}{=} b$ (where $a, b \in \mathbb{Z}$ are given constants, $x \in \mathbb{N}^0$ and k is a modulo that possesses a primitive root and it is coprime to a and b).
Solution: Let r be a primitive root of k. Now, if we take the index of both sides of the given congruence equation (see § 1.5) then we get:

$$I_{k,r}(a^x) \stackrel{\phi(k)}{=} I_{k,r}(b) \qquad \rightarrow \qquad x\, I_{k,r}(a) \stackrel{\phi(k)}{=} I_{k,r}(b)$$

This is a linear congruence equation which (according to the LCE theorem; see § 3.2.1 of V1) has either no solution if $d \nmid I_{k,r}(b)$ or has d modular solutions $\big[\text{in mod } \phi(k)\big]$ if $d | I_{k,r}(b)$ $\big[$where d is the gcd of $I_{k,r}(a)$ and $\phi(k)\big]$.

7. Find the necessary and sufficient conditions for the following congruence quadratic equation to have solutions:

$$ax^2 + bx + c \stackrel{p}{=} 0 \qquad\qquad (a, b, c, x \in \mathbb{Z},\ a \neq 0,\ p \text{ is odd prime coprime to } a)$$

Solution: Regarding the **necessary condition**, let assume that the given congruence is solvable and hence we have some $X \in \mathbb{Z}$ such that $aX^2 + bX + c \stackrel{p}{=} 0$, i.e. $aX^2 + bX \stackrel{p}{=} -c$. Now:

$$(2aX + b)^2 = 4a^2X^2 + 4abX + b^2 = 4a(aX^2 + bX) + b^2 \stackrel{p}{=} 4a(-c) + b^2 = b^2 - 4ac \equiv \Delta \qquad (35)$$

i.e. we have an integer $(2aX + b)$ such that $(2aX + b)^2 \stackrel{p}{=} \Delta$. This means that the necessary condition for the given congruence quadratic equation to have solutions is that its discriminant is a quadratic residue of p (where "quadratic residue" here includes 0; see the preamble of § 1.6).
Regarding the **sufficient condition**, we will show that this condition is also sufficient, i.e. if the discriminant is a quadratic residue of p then the given congruence is solvable. So, let us verify this claim by proving that if there is some $Y \in \mathbb{Z}$ such that $\Delta \stackrel{p}{=} Y^2$ then the given congruence is solvable. Now, according to the LCE theorem (noting that $2a$ and p are coprime; see § 3.2.1 of V1) $Y \stackrel{p}{=} 2ax + b$ is solvable, i.e. there is some $X \in \mathbb{Z}$ such that $Y \stackrel{p}{=} 2aX + b$. Moreover, from Eq. 35 (read in the reverse direction) $\Delta \stackrel{p}{=} Y^2$ means that the existence of such X is equivalent to the solvability of the given congruence. So, we conclude that if the discriminant is a quadratic residue of p then the given congruence is solvable. This means that the sufficient condition for the given congruence quadratic equation to have solutions is that its discriminant is a quadratic residue of p.

8. Prove the following proposition using modular arithmetic: an integer is divisible by 3 (9) *iff* the sum of its digits is divisible by 3 (9).
Solution: Let $n = d_k \ldots d_2 d_1 d_0$ (where $d_k, \ldots, d_2, d_1, d_0$ are digits) and $m = 3$ (9). So, we have:

$$\begin{aligned} n &= d_k \ldots d_2 d_1 d_0 = d_k \times 10^k + \ldots + d_2 \times 10^2 + d_1 \times 10^1 + d_0 \\ &\stackrel{m}{=} d_k \times 1^k + \ldots + d_2 \times 1^2 + d_1 \times 1^1 + d_0 = d_k + \ldots + d_2 + d_1 + d_0 \end{aligned}$$

This (read in both directions) should prove the equivalence between the divisibility of an integer by 3 (9) and the divisibility of the sum of its digits by 3 (9).

9. Prove the following using modular arithmetic: an integer is divisible by 11 *iff* the alternating sum of its digits is divisible by 11.
   Solution: Let $n = d_k \dots d_3 d_2 d_1 d_0$ (where $d_k, \dots, d_3, d_2, d_1, d_0$ are digits). So, we have:

$$\begin{aligned} n &= d_k \dots d_3 d_2 d_1 d_0 = d_k \times 10^k + \dots + d_3 \times 10^3 + d_2 \times 10^2 + d_1 \times 10^1 + d_0 \\ &\overset{11}{=} d_k \times (-1)^k + \dots + d_3 \times (-1)^3 + d_2 \times (-1)^2 + d_1 \times (-1)^1 + d_0 \\ &= (-1)^k d_k + \dots - d_3 + d_2 - d_1 + d_0 \end{aligned}$$

   This (read in both directions) should prove the equivalence between the divisibility of an integer by 11 and the divisibility of the alternating sum of its digits by 11 (noting that the sign does not affect divisibility since divisibility is an attribute of the magnitude).
10. Show that the congruence equation $ax^2 \overset{p}{=} b$ (where p is an odd prime) is solvable *iff* a and b are both quadratic residues of p or both quadratic non-residues of p.
    Solution: $ax^2 \overset{p}{=} b$ implies $x^2 \overset{p}{=} a^*b$ and hence (see Problem 13 of § 1.8)[66] a^*b is a quadratic residue of p (i.e. $x^2 \overset{p}{=} a^*b$ is solvable and hence $ax^2 \overset{p}{=} b$ is solvable) *iff* a^* and b are either both quadratic residues of p or both quadratic non-residues of p. Now, a and a^* are either both quadratic residues or both quadratic non-residues (see Problem 14 of § 1.8). Therefore, $ax^2 \overset{p}{=} b$ is solvable *iff* a and b are both quadratic residues of p or both quadratic non-residues of p.
11. Show that the congruence equation $x^2 \overset{p}{=} mn$ is solvable *iff* $x^2 \overset{p}{=} m$ and $x^2 \overset{p}{=} n$ are both solvable or both non-solvable (where p is an odd prime and mn is coprime to p).
    Solution: This is a corollary of Problem 13 of § 1.8 (noting the connection between solvability and quadratic residue).
12. One of the practical applications of congruence equations is in random number generation which is widely used in many branches and disciplines of computer science (and computing in general) and its many applications (in theories as well as in real life). In this Problem we outline the basic idea of using modular arithmetic in the generation of sequences of (pseudo) random numbers.
    So, let us create a simple modular arithmetic "model" to generate (pseudo) random numbers r_i between 0 and 10000, i.e. $0 \leq r_i \leq 9999$ where $i = 1, 2, \dots$. This model is based on the following congruence equation:

$$r_i \overset{k}{=} mr_{i-1} + d$$

    where r_0 (i.e. r_{1-1}) is the seed (which determines the progress of the sequence), k (which is equal to 10000 in our case) is the upper limit of the generated random numbers, m is a natural number between 1 and k (i.e. $2 \leq m \leq 9999$), and d is a given integer increment (e.g. $d = 713$).
    For example, if $r_0 = 93$, $m = 381$ and $d = 11$ then our random number generation model will generate the following sequence of random numbers:

$$5444, 4175, 686, 1377, 4648, 899, 2530, 3941, 1532, 3703, 854, 5385, 1696, 6187, 7258, 5309, 2740, 3951, \dots$$

    This random number generation model (or "device") can be easily implemented in a few lines of computer code or in a simple spreadsheet. It is obvious that if the random numbers are required to be between 0 and 1 (instead of being between 0 and k) then we simply divide these numbers by k.
    Also see Problem 2 of § 18.1.
13. Discuss the difference between Legendre's symbol and Jacobi's symbol as metrics for determining the solvability of quadratic congruence equations.
    Solution: From point 8 in the preamble of § 1.11, we can see that Legendre's symbol is a full metric for solvability of quadratic congruence equations since it can determine its solvability and non-solvability, while Jacobi's symbol is a partial metric for solvability of quadratic congruence equations since it can determine only its non-solvability.
    For instance, we can conclude that $x^2 \overset{71}{=} 2$ is solvable and $x^2 \overset{101}{=} 2$ is non-solvable because $\left(\frac{2}{71}\right) = 1$ and

[66] It is obvious that we are assuming a and p are coprime (noting that otherwise the case is trivial and obvious and can be excluded or included according to the convention about quadratic residue; see § 1.6).

$\left(\frac{2}{101}\right) = -1$.

On the other hand, we can conclude that $x^2 \overset{21}{=} 2$ is non-solvable because $\left(\frac{2}{21}\right) = -1$, but we cannot conclude that $x^2 \overset{21}{=} 16$ and $x^2 \overset{21}{=} 5$ are solvable (or non-solvable) from the fact that $\left(\frac{16}{21}\right) = 1$ and $\left(\frac{5}{21}\right) = 1$ (noting that the first is solvable while the second is not).

8.2 Univariate Congruence Equations

1. Consider the congruence equation $ax \overset{m}{=} 1$ (where $a, x, m \in \mathbb{Z}$ with $1 \leq a \leq m$ and $m > 1$). How many values of a make this congruence equation solvable?
   Solution: According to the LCE theorem (see § 3.2.1 of V1) we must have $\gcd(a, m)|1$ if $ax \overset{m}{=} 1$ is to be solvable. This means that $\gcd(a, m) = 1$, i.e. a and m are coprime. Now, the number of integer values between 1 and m (inclusive) which are coprime to m is given by $\phi(m)$. So, the number of values of a (where $1 \leq a \leq m$) that make the congruence $ax \overset{m}{=} 1$ solvable is $\phi(m)$.
2. Let $p \in \mathbb{P}$ and $x \in \mathbb{Z}$. Show that $x^p \overset{p}{=} x$ has exactly p modular solutions.
   Solution: This is no more than (the essence of) Fermat's little theorem (see § 2.9.3 of V1), i.e. the congruence $x^p \overset{p}{=} x$ is satisfied by the entire residue system of p and hence this congruence has exactly p modular solutions (noting that a complete residue system modulo p contains p residue classes, i.e. $x \overset{p}{=} 0, 1, 2, \ldots, p-1$).
3. Let $x \in \mathbb{Z}$ and $q, p \in \mathbb{P}$ with $q < p$. Show that the congruence equation $x^q \overset{p}{=} x$ cannot be satisfied by all the residue classes of p, i.e. we must have some $x \in \mathbb{Z}$ such that $x^q \overset{p}{\neq} x$.
   Solution: In fact, this is an implication (or requirement or instance) of Lagrange's polynomial roots theorem. However, let us establish it in a different way.
   p must have a primitive root (see point 5 in the preamble of § 1.4). Now, "$x^q \overset{p}{=} x$ for every $x \in \mathbb{Z}$" means that all the residue classes of p satisfy this congruence with natural powers of x (i.e. x^q) which are less than $(p-1)$. This implies that p has no primitive root (noting that the order of a primitive root of p is $p-1$). So, this contradiction should lead to the conclusion that the congruence $x^q \overset{p}{=} x$ cannot be satisfied by all the residue classes of p.
   Note: the implication of this Problem is that if $x^q \overset{p}{=} x$ for all $x \in \mathbb{Z}$ then $q \geq p$.
4. Show that the only (distinct modular) solutions to the congruence equation $x^2 \overset{p}{=} 1$ are $x \overset{p}{=} 1$ and $x \overset{p}{=} p-1$ (where p is an odd prime).
   Solution: The congruence $x^2 \overset{p}{=} 1$ has obviously one solution (which is $x \overset{p}{=} 1$ since $1^2 \overset{p}{=} 1$) and hence it must have exactly two distinct modular solutions (see Problem 1 of § 1.6). We also have:

$$(p-1)^2 = p^2 - 2p + 1 \overset{p}{=} 1$$

   i.e. $x \overset{p}{=} p-1$ is the other solution. It should be obvious that $1 \overset{p}{\neq} (p-1)$ because otherwise:

$$1 \overset{p}{=} (p-1) \quad \rightarrow \quad p \overset{p}{=} 2 \quad \rightarrow \quad p|(p-2)$$

   which is nonsensical since $p > (p-2)$ and $(p-2) \neq 0$ noting that p is an odd prime.[67] So, $x \overset{p}{=} 1$ and $x \overset{p}{=} p-1$ are the only (distinct modular) solutions to the congruence equation $x^2 \overset{p}{=} 1$.
   Note: we may also prove the given proposition (more easily) by noting that $(\pm 1)^2 = 1$ and hence the distinct modular solutions of $x^2 \overset{p}{=} 1$ are $x \overset{p}{=} 1$ and $x \overset{p}{=} -1 \overset{p}{=} p-1$ (noting that modular distinction is because p is an odd prime). We may also prove it by using Problem 2 of § 8.1, i.e. if $x^2 \overset{p}{=} 1^2$ then $x \overset{p}{=} \pm 1$ (where $x \overset{p}{=} -1 \overset{p}{=} p-1$ noting again that modular distinction is because p is an odd prime).
5. Show that if $n \in \mathbb{Z}$ is a solution of the congruence equation $n^3 + 6n^2 + n + 6 \overset{4}{=} 0$ then n cannot be the difference of two squares.
   Solution: The only solution to $n^3 + 6n^2 + n + 6 \overset{4}{=} 0$ is $n \overset{4}{=} 2$ (see § 3.2.1 of V1). Now, if n is the

[67] We may similarly say: $p \overset{p}{=} 2$ means $0 \overset{p}{=} 2$ which is nonsensical because p is an odd prime.

difference between two squares then we have 4 possibilities regarding the parity of the squares (where $m, k \in \mathbb{Z}$):

$$n = (2m+1)^2 - (2k+1)^2 \stackrel{4}{=} 0 \qquad n = (2m)^2 - (2k)^2 \stackrel{4}{=} 0$$

$$n = (2m+1)^2 - (2k)^2 \stackrel{4}{=} 1 \qquad n = (2m)^2 - (2k+1)^2 \stackrel{4}{=} 3$$

As we see, there is no n which is a difference between two squares that is congruent (mod 4) to 2, and hence if n is a difference between two squares then it cannot be a solution to $n^3 + 6n^2 + n + 6 \stackrel{4}{=} 0$.

6. Let $P(x)$ (where $x \in \mathbb{Z}$) be an n^{th} degree polynomial none of its coefficients is zero. Create examples for the following:[68]

(**a**) $n = 2$ and $P \stackrel{k}{=} 0$ $(k = 3, 5, 7, 11)$ has root 0 for all these moduli.

(**b**) $n = 3$ and $P \stackrel{k}{=} 0$ $(k = 2, 6, 9, 13, 15)$ has root 1 for all these moduli.

(**c**) $n = 3$ and $P \stackrel{12}{=} 0$ has the following roots (and possibly other roots): 1, 3, 4, 7, 10.

Solution:

(**a**) If we start with a quadratic whose constant coefficient is 0 (say $x^2 - x$) then it is obvious that $x^2 - x \stackrel{k}{=} 0$ $(k = 3, 5, 7, 11)$ has root 0 for all these moduli. Now, if we add to this polynomial the least common multiple of these moduli (i.e. their product which is 1155) then $P = x^2 - x + 1155$ should meet all the given conditions.

(**b**) If we start with the linear polynomial $(x - 1)$ then it is obvious that $x - 1 \stackrel{k}{=} 0$ $(k = 2, 6, 9, 13, 15)$ has root 1 for all these moduli. Now, if we multiply $(x - 1)$ by a quadratic polynomial with non-zero coefficients (say $x^2 - 4x + 3$) then we get a cubic that meet all the given conditions, i.e. $P = (x - 1)(x^2 - 4x + 3) = x^3 - 5x^2 + 7x - 3$.

(**c**) Let the congruence equation be $ax^3 + bx^2 + cx + d \stackrel{12}{=} 0$ (where $a, b, c, d \in \mathbb{Z}$). Now, if this equation has the given roots (i.e. 1, 3, 4, 7, 10) then we must have:

$$\begin{aligned} a(1)^3 + b(1)^2 + c(1) + d &\stackrel{12}{=} 0 \\ a(3)^3 + b(3)^2 + c(3) + d &\stackrel{12}{=} 0 \\ a(4)^3 + b(4)^2 + c(4) + d &\stackrel{12}{=} 0 \\ a(7)^3 + b(7)^2 + c(7) + d &\stackrel{12}{=} 0 \\ a(10)^3 + b(10)^2 + c(10) + d &\stackrel{12}{=} 0 \end{aligned}$$

On solving this system of congruences for the variables a, b, c, d (see § 4.4.1 of V1 as well as chapter 9 of the present volume) we get: $(a, b, c, d) \stackrel{12}{=} (2, 2, 8, 12)$. Hence, $P = 2x^3 + 2x^2 + 8x + 12$ should meet all the given conditions.

7. Show that the congruence equation $n^6 - 11n^4 + 36n^2 - 36 \stackrel{p}{=} 0$ is always solvable (where $p \in \mathbb{P}$ and $n \in \mathbb{Z}$).

Solution: We have three (comprehensive) cases to consider:

- $p = 2$: the polynomial $n^6 - 11n^4 + 36n^2 - 36$ is even and hence the given congruence is solvable.
- $p = 3$: we have $n^6 - 11n^4 + 36n^2 - 36 \stackrel{3}{=} 0$ which has the solution $n = 3k$ $(k \in \mathbb{Z})$.
- $p > 3$: we have:

$$n^6 - 11n^4 + 36n^2 - 36 = (n^2 - 2)(n^2 - 3)(n^2 - 6)$$

Now, from Problem 3 of § 1.8 at least one of $2, 3, 6$ must be a quadratic residue (mod p) which means that at least one of the three congruences: $n^2 - a \stackrel{p}{=} 0$ $(a = 2, 3, 6)$ is solvable. Therefore, the given congruence equation is solvable.

So, in all three cases the given congruence equation is solvable and hence it is always solvable.

[68] This Problem (and its alike) is about obtaining polynomial congruences with given conditions. The purpose of it is to improve the skill of constructing such congruences when needed during investigating and solving some number theory problems.

8. Show that $98^n - 68^n - 31^n + 1 \overset{2010}{=} 0$ for all $n \in \mathbb{N}$.
Solution: We have $2010 = 2 \times 3 \times 5 \times 67$. Now:
• $98^n - 68^n - 31^n + 1$ is even and hence $98^n - 68^n - 31^n + 1 \overset{2}{=} 0$ for all $n \in \mathbb{N}$.
• $98^n - 68^n - 31^n + 1 \overset{3}{=} 2^n - 2^n - 1^n + 1 = 0$ for all $n \in \mathbb{N}$.
• $98^n - 68^n - 31^n + 1 \overset{5}{=} 3^n - 3^n - 1^n + 1 = 0$ for all $n \in \mathbb{N}$.
• $98^n - 68^n - 31^n + 1 \overset{67}{=} 31^n - 1^n - 31^n + 1 = 0$ for all $n \in \mathbb{N}$.
Hence, $98^n - 68^n - 31^n + 1 \overset{2010}{=} 0$ for all $n \in \mathbb{N}$ (see rule 14 of § 2.7 of V1).
9. Which of the following quadratic congruence equations are solvable:
(**a**) $3x^2 - 15x + 221 \overset{3797}{=} 0$. (**b**) $11x^2 + 4x + 311 \overset{5281}{=} 0$.
(**c**) $x^2 - 19x - 52 \overset{7171}{=} 0$. (**d**) $26x^4 + 31x^3 - 85x^2 - 111x - 5 \overset{199}{=} 0$.
Solution: We use the proposition of Problem 7 of § 8.1 (where Legendre's symbol criterion is used to determine if the discriminant Δ is a quadratic residue of the modulo or not).[69]
(**a**) 3797 is prime. We have $\Delta = (-15)^2 - 4 \times 3 \times 221 = -2427$. Now, $\left(\frac{-2427}{3797}\right) = 1$ (i.e. Δ is a quadratic residue of 3797) and hence the given congruence equation is solvable.
(**b**) 5281 is prime. We have $\Delta = (4)^2 - 4 \times 11 \times 311 = -13668$. Now, $\left(\frac{-13668}{3797}\right) = -1$ (i.e. Δ is a quadratic non-residue of 5281) and hence the given congruence equation is not solvable.
(**c**) $7171 = 71 \times 101$. If the given congruence equation is solvable then we must have $x^2 - 19x - 52 \overset{71}{=} 0$ and $x^2 - 19x - 52 \overset{101}{=} 0$. We have $\Delta = (-19)^2 - 4 \times (-52) = 569$. Now, $\left(\frac{569}{71}\right) = 1$ and $\left(\frac{569}{101}\right) = 1$ and hence the given congruence is solvable.
(**d**) 199 is prime. Also, $26x^4 + 31x^3 - 85x^2 - 111x - 5 = (2x^2 - x - 5)(13x^2 + 22x + 1)$. So, if the given congruence equation is solvable then we must have $2x^2 - x - 5 \overset{199}{=} 0$ or/and $13x^2 + 22x + 1 \overset{199}{=} 0$.
For $2x^2 - x - 5$ we have $\Delta = (-1)^2 - 4 \times 2 \times (-5) = 41$. Now, $\left(\frac{41}{199}\right) = -1$ and hence $2x^2 - x - 5 \overset{199}{=} 0$ is not solvable.
For $13x^2 + 22x + 1$ we have $\Delta = (22)^2 - 4 \times 13 \times 1 = 432$. Now, $\left(\frac{432}{199}\right) = -1$ and hence $13x^2 + 22x + 1 \overset{199}{=} 0$ is not solvable.
Therefore, the given congruence equation is not solvable.
10. Find the number of (modular) solutions of the following exponential congruence equations (where $n \in \mathbb{N}$):
(**a**) $5^n \overset{7}{=} 6$. (**b**) $3^n \overset{10}{=} 1$. (**c**) $4^n \overset{27}{=} 7$. (**d**) $7^n \overset{25}{=} 1$. (**e**) $3^n \overset{22}{=} 5$.
Solution: We use the proposition of Problem 6 of § 8.1 (noting that all these congruences meet the required conditions of that proposition where we take $r = 5, 3, 2, 2, 7$ for $k = 7, 10, 27, 25, 22$).
(**a**) The congruence $5^n \overset{7}{=} 6$ has one solution (mod 6) because $I_{7,5}(5) = 1$ and $\phi(7) = 6$ and hence their gcd is 1.
(**b**) The congruence $3^n \overset{10}{=} 1$ has one solution (mod 4) because $I_{10,3}(3) = 1$ and $\phi(10) = 4$ and hence their gcd is 1.
(**c**) The congruence $4^n \overset{27}{=} 7$ has two solutions (mod 18) because $I_{27,2}(4) = 2$ and $\phi(27) = 18$ and hence their gcd is 2 (noting that 2 divides $I_{27,2}7$ which is 16).
(**d**) The congruence $7^n \overset{25}{=} 1$ has five solutions (mod 20) because $I_{25,2}(7) = 5$ and $\phi(25) = 20$ and hence their gcd is 5 (noting that 5 divides $I_{25,2}1$ which is 20).
(**e**) The congruence $3^n \overset{22}{=} 5$ has two solutions (mod 10) because $I_{22,7}(3) = 4$ and $\phi(22) = 10$ and hence their gcd is 2 (noting that 2 divides $I_{22,7}5$ which is 2).
11. Find the solutions of the congruence equations of Problem 10 using the index of integer method.
Solution: According to Problem 6 of § 8.1, the congruence equation $a^n \overset{k}{=} b$ can be solved by the index of integer method using the equation:

$$n\, I_{k,r}(a) \overset{\phi(k)}{=} I_{k,r}(b) \tag{36}$$

[69] For how to evaluate Legendre symbols we refer the reader to § 1.8 (see for instance Problem 8 of § 1.8).

(**a**) From Eq. 36 we have $n \times 1 \overset{6}{=} 3$. So, the solution is $n \overset{6}{=} 3$.
(**b**) From Eq. 36 we have $n \times 1 \overset{4}{=} 4$. So, the solution is $n \overset{4}{=} 0$.
(**c**) From Eq. 36 we have $n \times 2 \overset{18}{=} 16$. So, the solutions are $n \overset{18}{=} 8, 17$ (i.e. $n \overset{9}{=} 8$).
(**d**) From Eq. 36 we have $n \times 5 \overset{20}{=} 20$. So, the solutions are $n \overset{20}{=} 0, 4, 8, 12, 16$ (i.e. $n \overset{4}{=} 0$).
(**e**) From Eq. 36 we have $n \times 4 \overset{10}{=} 2$. So, the solutions are $n \overset{10}{=} 3, 8$ (i.e. $n \overset{5}{=} 3$).

12. Find all primes p such that the following congruences have solutions:

(**a**) $x^2 - 1 \overset{p}{=} 0$. (**b**) $x^2 + 1 \overset{p}{=} 0$. (**c**) $x^2 - 2 \overset{p}{=} 0$.

(**d**) $x^2 + 2 \overset{p}{=} 0$. (**e**) $x^2 - 4 \overset{p}{=} 0$. (**f**) $x^2 + 4 \overset{p}{=} 0$.

Solution: We note first that all these congruences are solvable for $p = 2$ and hence in the following we consider only odd primes.
(**a**) We have $x^2 \overset{p}{=} 1$, i.e. 1 is a quadratic residue of p. Now, 1 is a quadratic residue for all odd primes and hence the given congruence is solvable for all p (see Problem 2 of § 1.6).
(**b**) We have $x^2 \overset{p}{=} -1$, i.e. -1 is a quadratic residue of p. Now, the Legendre symbol $\left(\frac{-1}{p}\right)$ is $+1$ for all $p = 4k + 1$ and -1 for all $p = 4k - 1$ (see Problem 9 of § 1.8). So, the given congruence is solvable for all $p = 4k + 1$ and non-solvable for all $p = 4k - 1$.
(**c**) We have $x^2 \overset{p}{=} 2$, i.e. 2 is a quadratic residue of p. So, from Eq. 7 we conclude that the given congruence is solvable for all $p \overset{8}{=} \pm 1$ and non-solvable for all $p \overset{8}{=} \pm 3$.
(**d**) We have $x^2 \overset{p}{=} -2$, i.e. -2 is a quadratic residue of p. Now, form Eq. 8 we have $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$, i.e. $\left(\frac{-2}{p}\right) = 1$ if $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ have the same sign. So, from parts (b) and (c) we conclude that the given congruence is solvable if $p = 4k+1$ and $p \overset{8}{=} \pm 1$ (i.e. $p \overset{8}{=} 1$) or $p = 4k - 1$ and $p \overset{8}{=} \pm 3$ (i.e. $p \overset{8}{=} 3$) and non-solvable otherwise.
(**e**) We have $x^2 \overset{p}{=} 4$, i.e. 4 is a quadratic residue of p. Now, 4 is a quadratic residue for all odd primes and hence the given congruence is solvable for all p (see Problem 2 of § 1.6).
(**f**) We have $x^2 \overset{p}{=} -4$, i.e. -4 is a quadratic residue of p. Now, form Eqs. 8 and 9 we have:

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

So, as in part (b) the given congruence is solvable for all $p = 4k+1$ and non-solvable for all $p = 4k-1$.

13. Let $x \in \mathbb{N}$ and $\mathbb{P} \ni p > 3$. Find all the solutions of the following congruence equation: $\sum_{k=0}^{p-2} x^k \overset{p}{=} 0$.

Solution: We note first that $x \overset{p}{=} 1$ is not a possible solution because $\sum_{k=0}^{p-2} 1^k = p - 1 \overset{p}{=} -1 \overset{p}{\neq} 0$. Similarly, $x \overset{p}{=} p$ is not a possible solution because $\sum_{k=0}^{p-2} p^k \overset{p}{=} 1 \overset{p}{\neq} 0$. So, any potential solution must be among $x \overset{p}{=} 2, 3, \ldots, p-1$.
We have (see Eq. 12 in V1):

$(x-1)\left(\sum_{k=0}^{p-2} x^k\right) = x^{p-1} - 1 \quad \rightarrow \quad (x-1)\left(\sum_{k=0}^{p-2} x^k\right) \overset{p}{=} x^{p-1} - 1 \quad \rightarrow$

$(x-1)\left(\sum_{k=0}^{p-2} x^k\right) \overset{p}{=} 0 \quad (x \overset{p}{=} 2, 3, \ldots, p-1)$

where we used Fermat's little theorem in the last step (noting that $p \not| x$ for $x \overset{p}{=} 2, 3, \ldots, p-1$). The last congruence means that p divides $(x-1)\left(\sum_{k=0}^{p-2} x^k\right)$. Now, for $x \overset{p}{=} 2, 3, \ldots, p-1$ we have $p \not| (x-1)$ and hence we must have $p \Big| \left(\sum_{k=0}^{p-2} x^k\right)$, i.e. $\sum_{k=0}^{p-2} x^k \overset{p}{=} 0$ for $x \overset{p}{=} 2, 3, \ldots, p-1$. So, the solutions of the congruence $\sum_{k=0}^{p-2} x^k \overset{p}{=} 0$ are $x \overset{p}{=} 2, 3, \ldots, p-1$.

14. Show that the following congruence equation has no solution: $4x^4 + 4 \overset{323}{=} 0$.

Solution: If $4x^4 + 4 \overset{323}{=} 0$ then $x^4 + 1 \overset{323}{=} 0$ (because 4 and 323 are coprime; see rule 7 of § 2.7 of V1). Noting that $323 = 17 \times 19$, $x^4 + 1 \overset{323}{=} 0$ means that $x^4 + 1$ is divisible by 17 and divisible by 19, i.e.

$x^4+1 \overset{17}{=} 0$ and $x^4+1 \overset{19}{=} 0$. It is fairly obvious that $x^4+1 \overset{17}{=} 0$ has a solution (e.g. $x \overset{17}{=} 2$) and hence $x^4+1 \overset{323}{=} 0$ has a solution *iff* $x^4+1 \overset{19}{=} 0$ has a solution. So, let us see if $x^4+1 \overset{19}{=} 0$ has a solution (where from now on we can assume that x and 19 are coprime noting that $0+1 \overset{19}{\neq} 0$).

$x^4+1 \overset{19}{=} 0$ implies $x^4 \overset{19}{=} -1$ and hence $x^8 \overset{19}{=} 1$. Now, from Problem 1 of § 1.3 we conclude that $O_{19}x|8$, i.e. $O_{19}x = 1$ or $O_{19}x = 2$ or $O_{19}x = 4$ or $O_{19}x = 8$. Now:

• If $O_{19}x = 1$ then $x^1 \overset{19}{=} 1$ and hence $x^4 \overset{19}{=} 1$ which contradicts $x^4 \overset{19}{=} -1$.

• If $O_{19}x = 2$ then $x^2 \overset{19}{=} 1$ and hence $x^4 \overset{19}{=} 1$ which contradicts $x^4 \overset{19}{=} -1$.

• If $O_{19}x = 4$ then $x^4 \overset{19}{=} 1$ which contradicts $x^4 \overset{19}{=} -1$.

So, we must have $O_{19}x = 8$. Now, from Problem 3 of § 1.3 we must have $8|\phi(19)$, i.e. $8|18$ which is untrue. This means that $x^4+1 \overset{19}{=} 0$ has no solution and hence $x^4+1 \overset{323}{=} 0$ (as well as $4x^4+4 \overset{323}{=} 0$) has no solution.

15. Find all the solutions of the following exponential congruence equations (where $x \in \mathbb{N}$):

(**a**) $13^x \overset{33}{=} 1$. (**b**) $7^x \overset{9}{=} 4$. (**c**) $22^x \overset{15}{=} 13$.

Solution: We use points 1 and 2 in the preamble of § 1.3.

(**a**) We have $O_{33}13 = 10$ and hence the solutions are $x \overset{10}{=} 0$ (i.e. $x = 10, 20, 30, \ldots$).

(**b**) We have $O_9 7 = 3$ and $7^2 \overset{9}{=} 4$ and hence the solutions are $x \overset{3}{=} 2$ (i.e. $x = 2, 5, 8, \ldots$).

(**c**) We have $O_{15}22 = 4$ and $22^3 \overset{15}{=} 13$ and hence the solutions are $x \overset{4}{=} 3$ (i.e. $x = 3, 7, 11, \ldots$).

16. Find an integer a such that:

(**a**) The congruence equation $ax^2 \overset{107}{=} 5$ has the solutions $x \overset{107}{=} 4$ and $x \overset{107}{=} 103$ (where $0 < a < 107$).

(**b**) The congruence equation $ax^{19} \overset{29}{=} 43$ has the solution $x \overset{29}{=} 21$ (where $0 < a < 29$).

Solution:

(**a**) A primitive root of 107 is 2. Taking the index of both sides of the given congruence equation (see § 1.5) we have:

$$I_{107,2}\left(ax^2\right) \overset{\phi(107)}{=} I_{107,2}(5) \quad \rightarrow \quad I_{107,2}(a) + 2I_{107,2}(x) \overset{106}{=} I_{107,2}(5) \quad \rightarrow$$

$$I_{107,2}(a) \overset{106}{=} I_{107,2}(5) - 2I_{107,2}(x) \quad \rightarrow \quad I_{107,2}(a) \overset{106}{=} 47 - 2I_{107,2}(x)$$

Now, if $x \overset{107}{=} 4$ then $I_{107,2}(4) = 2$ and hence:

$$I_{107,2}(a) \overset{106}{=} 47 - 2 \times 2 \qquad \text{that is} \qquad I_{107,2}(a) \overset{\phi(107)}{=} 43$$

Thus, $a \overset{107}{=} 2^{43} \overset{107}{=} 7$, i.e. $a = 7$ (noting that $0 < a < 107$).

Similarly, if $x \overset{107}{=} 103$ then $I_{107,2}(103) = 55$ and hence:

$$I_{107,2}(a) \overset{106}{=} 47 - 2 \times 55 \qquad \text{that is} \qquad I_{107,2}(a) \overset{\phi(107)}{=} 43$$

i.e. we get the same result as for $x \overset{107}{=} 4$. Therefore, $a = 7$.

(**b**) A primitive root of 29 is 2. Taking the index of both sides of the given congruence equation (see § 1.5) we have:

$$I_{29,2}\left(ax^{19}\right) \overset{\phi(29)}{=} I_{29,2}(43) \quad \rightarrow \quad I_{29,2}(a) + 19I_{29,2}(x) \overset{28}{=} I_{29,2}(43) \quad \rightarrow$$

$$I_{29,2}(a) \overset{28}{=} I_{29,2}(43) - 19I_{29,2}(x) \quad \rightarrow \quad I_{29,2}(a) \overset{28}{=} 13 - 19I_{29,2}(x)$$

Now, if $x \overset{29}{=} 21$ then $I_{29,2}(21) = 17$ and hence:

$$I_{29,2}(a) \overset{28}{=} 13 - 19 \times 17 \qquad \text{that is} \qquad I_{29,2}(a) \overset{\phi(29)}{=} 26$$

Thus, $a \overset{29}{=} 2^{26} \overset{29}{=} 22$, i.e. $a = 22$ (noting that $0 < a < 29$).

17. Solve the following congruence equations (where $n \in \mathbb{N}^0$):

(**a**) $n! \overset{11}{=} 10$. (**b**) $(n+1)! - n! \overset{263}{=} 0$. (**c**) $6n! + 7(n-3)! \overset{13}{=} 0$.

Solution:

(**a**) For all $n > 10$ we have $n! \overset{11}{=} 0$. So, we need only to test $n = 0, 1, \ldots, 10$. On doing this we find that $n! \overset{11}{=} 10$ is only for $n = 5$ and $n = 10$. Hence, the only solutions of $n! \overset{11}{=} 10$ are $n = 5$ and $n = 10$.

(**b**) We have:

$$(n+1)! - n! \overset{263}{=} 0 \quad \rightarrow \quad n!\big[(n+1) - 1\big] \overset{263}{=} 0 \quad \rightarrow \quad n!(n) \overset{263}{=} 0$$

Now, we have two obvious cases in which this congruence is satisfied: $n = 0$ and $n > 262$. For $1 \leq n \leq 262$ we note that 263 is prime and hence it can divide neither n nor $n!$. Hence, the solutions of the given congruence are $n = 0, 263, 264, \ldots$.

(**c**) Because the factorial is defined only for non-negative integers, we must have $n \geq 3$. Now, for $(n-3) \geq 13$ (i.e. $n \geq 16$) we have $n! \overset{13}{=} 0$ and $(n-3)! \overset{13}{=} 0$ and hence the given congruence is satisfied. So, all we need to do is to test $3 \leq n \leq 15$. On doing this we find out that this congruence has no solution for any value of $3 \leq n \leq 15$. So, the solutions of the given congruence are $n \geq 16$.

8.3 Multivariate Congruence Equations

In § 4.2 of V1 we investigated multivariate congruence equations of various types (such as polynomials and exponentials) and how they are solved (giving sufficient examples of them with their solutions). So, in the following Problems we just do a little more investigation to this type of congruence equations (so that we keep the space for other issues which were less investigated).

Problems

1. Find all $\mathbb{P} \ni p < 1000$ such that $x^7 + y^{19} \overset{p}{=} 153$ has no solution (where $x, y \in \mathbb{Z}$).

Solution: If $p \overset{19}{\neq} 1$ then y^{19} will cycle over all the residue classes of p and hence we must have a solution. So, all we need to do is to test the p's which are equal to 1 (mod 19), i.e. $p \overset{19}{=} 1$. Now, the only $p < 1000$ which meet this condition are: 191, 229, 419, 457, 571, 647, 761. On testing $x^7 + y^{19} \overset{p}{=} 153$ for these values of p we find that this congruence has solutions for all these values of p. So, there is no $\mathbb{P} \in p < 1000$ such that $x^7 + y^{19} \overset{p}{=} 153$ has no solution. Also see Problem 2 of § 18.3.

2. Show that the following congruence equation has no solution: $x^5 + y^6 \overset{11}{=} 7$.

Solution: The residues of x^5 (mod 11) are $0, 1, 10$ while the residues of y^6 (mod 11) are $0, 1, 3, 4, 5, 9$. Hence, no combination of these residues can add up to 7 (mod 11). Therefore, this congruence equation has no solution.

3. Solve the following linear polynomial congruence equations (where $x, y, z \in \mathbb{Z}$):

(**a**) $2x + y \overset{3}{=} 0$. (**b**) $x - 2y \overset{5}{=} 3$. (**c**) $x - 4y \overset{5}{=} 2$.

(**d**) $5x + y \overset{7}{=} 1$. (**e**) $x + y - z \overset{2}{=} 0$. (**f**) $2x + y + z \overset{3}{=} 1$.

Solution: All these congruences can be easily solved by considering all the modular combinations of x, y, z (as we did in parts a, b and c of Problem 1 of § 4.2.1 of V1).

(**a**) $(\boldsymbol{x, y}) \overset{\mathbf{3}}{=}$ $(0,0)$ $(1,1)$ $(2,2)$

(**b**) $(\boldsymbol{x, y}) \overset{\mathbf{5}}{=}$ $(0,1)$ $(1,4)$ $(2,2)$ $(3,0)$ $(4,3)$

(**c**) $(\boldsymbol{x, y}) \overset{\mathbf{5}}{=}$ $(0,2)$ $(1,1)$ $(2,0)$ $(3,4)$ $(4,3)$

(**d**) $(\boldsymbol{x, y}) \overset{\mathbf{7}}{=}$ $(0,1)$ $(1,3)$ $(2,5)$ $(3,0)$ $(4,2)$ $(5,4)$ $(6,6)$

(**e**) $(\boldsymbol{x, y, z}) \overset{\mathbf{2}}{=}$ $(0,0,0)$ $(0,1,1)$ $(1,0,1)$ $(1,1,0)$

(**f**) $(\boldsymbol{x, y, z}) \overset{\mathbf{3}}{=}$ $(0,0,1)$ $(0,1,0)$ $(0,2,2)$ $(1,0,2)$ $(1,1,1)$ $(1,2,0)$ $(2,0,0)$ $(2,1,2)$ $(2,2,1)$

4. Solve the following non-linear polynomial congruence equations (where $x, y, z \in \mathbb{Z}$):

(**a**) $x^3 + y \stackrel{2}{=} 0$. (**b**) $x^2 + y^3 \stackrel{3}{=} 1$. (**c**) $3x^2 + 4y^4 \stackrel{5}{=} 1$. (**d**) $x^2 + 2y + 3z \stackrel{5}{=} 1$.

Solution: All these congruences can be easily solved by considering all the modular combinations of x, y, z (as we did in parts d, e and f of Problem 1 of § 4.2.1 of V1).

(**a**) $(\boldsymbol{x, y}) \stackrel{\mathbf{2}}{=}$ $(0,0)$ $(1,1)$

(**b**) $(\boldsymbol{x, y}) \stackrel{\mathbf{3}}{=}$ $(0,1)$ $(1,0)$ $(2,0)$

(**c**) $(\boldsymbol{x, y}) \stackrel{\mathbf{5}}{=}$ $(2,1)$ $(2,2)$ $(2,3)$ $(2,4)$ $(3,1)$ $(3,2)$ $(3,3)$ $(3,4)$

(**d**) $(\boldsymbol{x, y, z}) \stackrel{\mathbf{5}}{=}$ $(0,0,2)$ $(0,1,3)$ $(0,2,4)$ $(0,3,0)$ $(0,4,1)$ $(1,0,0)$ $(1,1,1)$ $(1,2,2)$ $(1,3,3)$
$(1,4,4)$ $(2,0,4)$ $(2,1,0)$ $(2,2,1)$ $(2,3,2)$ $(2,4,3)$ $(3,0,4)$ $(3,1,0)$ $(3,2,1)$
$(3,3,2)$ $(3,4,3)$ $(4,0,0)$ $(4,1,1)$ $(4,2,2)$ $(4,3,3)$ $(4,4,4)$

5. Solve the following exponential congruence equations (where $x, y, z \in \mathbb{N}^0$):

(**a**) $3^x + 4^y \stackrel{5}{=} 2$. (**b**) $3^x + 5^y \stackrel{7}{=} 1$. (**c**) $5^x + 7^y \stackrel{11}{=} 10$.

(**d**) $2^x + 3^y + 5^z \stackrel{7}{=} 4$. (**e**) $3^x + 4^y + 7^z \stackrel{11}{=} 5$. (**f**) $2^x + 3^y + 5^z \stackrel{11}{=} 4$.

Solution: All these congruences can be easily solved by considering all the modular combinations of the exponentials (as we did in § 4.2.2 of V1).

(**a**) $(\boldsymbol{x \stackrel{4}{=},\ y \stackrel{2}{=}})$ $(0,0)$ $(1,1)$

(**b**) $(\boldsymbol{x \stackrel{6}{=},\ y \stackrel{6}{=}})$ $(1,1)$ $(2,3)$ $(3,4)$ $(4,2)$ $(5,5)$

(**c**) $(\boldsymbol{x \stackrel{5}{=},\ y \stackrel{10}{=}})$ $(0,8)$ $(1,2)$ $(2,1)$ $(3,7)$ $(4,0)$

(**d**) $(\boldsymbol{x \stackrel{3}{=},\ y \stackrel{6}{=},\ z \stackrel{6}{=}})$ $(0,0,4)$ $(0,2,0)$ $(0,3,2)$ $(0,4,3)$ $(0,5,1)$ $(1,0,0)$ $(1,1,3)$ $(1,3,5)$
$(1,4,1)$ $(1,5,2)$ $(2,0,3)$ $(2,1,2)$ $(2,2,1)$ $(2,3,0)$ $(2,4,5)$ $(2,5,4)$

(**e**) $(\boldsymbol{x \stackrel{5}{=},\ y \stackrel{5}{=},\ z \stackrel{10}{=}})$ $(0,0,4)$ $(0,2,5)$ $(0,3,7)$ $(0,4,0)$ $(1,0,0)$ $(1,1,8)$ $(1,2,9)$ $(1,3,6)$
$(1,4,5)$ $(2,0,7)$ $(2,1,4)$ $(2,2,3)$ $(2,3,8)$ $(2,4,6)$ $(3,0,5)$ $(3,1,1)$
$(3,2,7)$ $(3,3,3)$ $(3,4,9)$ $(4,1,9)$ $(4,2,1)$ $(4,3,4)$ $(4,4,8)$

(**f**) $(\boldsymbol{x \stackrel{10}{=},\ y \stackrel{5}{=},\ z \stackrel{5}{=}})$ $(0,2,1)$ $(0,3,4)$ $(1,0,0)$ $(1,2,3)$ $(1,4,4)$ $(3,1,3)$ $(3,2,4)$ $(3,4,2)$
$(4,0,4)$ $(4,2,0)$ $(4,3,1)$ $(5,0,3)$ $(5,4,0)$ $(6,0,1)$ $(6,1,2)$ $(6,3,0)$
$(7,1,1)$ $(7,3,2)$ $(7,4,3)$ $(8,1,4)$ $(8,2,2)$ $(9,3,3)$ $(9,4,1)$

6. Solve the following congruence equations (where $m, n \in \mathbb{N}^0$ and $x \in \mathbb{Z}$):

(**a**) $x^2 + n! \stackrel{7}{=} 0$. (**b**) $7^m + n! \stackrel{11}{=} 1$. (**c**) $2x^2 + 3^m + n! \stackrel{5}{=} 0$.

Solution:

(**a**) We have five main cases to consider:

- $n = 0, 1, 2, 5$ and hence $x^2 + a \stackrel{7}{=} 0$ (where $a = 1, 1, 2, 120$ respectively) which has no solution.
- $n = 3$ and hence $x^2 + 6 \stackrel{7}{=} 0$ whose solutions are $x \stackrel{7}{=} 1, 6$.
- $n = 4$ and hence $x^2 + 24 \stackrel{7}{=} 0$ whose solutions are $x \stackrel{7}{=} 2, 5$.
- $n = 6$ and hence $x^2 + 720 \stackrel{7}{=} 0$ whose solutions are $x \stackrel{7}{=} 1, 6$.
- $n > 6$ and hence $x^2 \stackrel{7}{=} 0$ whose solution is $x \stackrel{7}{=} 0$.

So in brief, the solutions of the given congruence equation are (where $\mathbb{N} \ni b > 6$ and $k \in \mathbb{Z}$):

$\boldsymbol{(n, x) =}$ $(3, 1 + 7k)$ $(3, 6 + 7k)$ $(4, 2 + 7k)$ $(4, 5 + 7k)$ $(6, 1 + 7k)$ $(6, 6 + 7k)$ $(b, 7k)$

(**b**) We have:

$7^{m \stackrel{10}{=} 0,1,2,3,4,5,6,7,8,9} \stackrel{11}{=} 1, 7, 5, 2, 3, 10, 4, 6, 9, 8$ and

$n!(n = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, > 10) \stackrel{11}{=} 1, 1, 2, 6, 2, 10, 5, 2, 5, 1, 10, 0$.

On considering all the possible combinations we get the following solutions (noting that m is in modulo 10 while n is in ordinary arithmetic):

$\boldsymbol{(m, n) =}$ $(0, > 10)$ $(1, 6)$ $(1, 8)$ $(3, 5)$ $(3, 10)$ $(5, 2)$ $(5, 4)$ $(5, 7)$ $(7, 3)$

(**c**) We have:
$2x^2(x \overset{5}{=} 0, 1, 2, 3, 4) \overset{5}{=} 0, 2, 3, 3, 2$ and
$3^{m \overset{4}{=} 0,1,2,3} \overset{5}{=} 1, 3, 4, 2$ and
$n!(n = 0, 1, 2, 3, 4, > 4) \overset{5}{=} 1, 1, 2, 1, 4, 0.$
On considering all the possible combinations we get the following solutions (noting that x is in modulo 5 and m is in modulo 4 while n is in ordinary arithmetic):

$\boldsymbol{(x, m, n) =}$	$(0, 0, 4)$	$(0, 1, 2)$	$(0, 2, 0)$	$(0, 2, 1)$	$(0, 2, 3)$	$(1, 0, 2)$	$(1, 1, > 4)$
	$(1, 2, 4)$	$(1, 3, 0)$	$(1, 3, 1)$	$(1, 3, 3)$	$(2, 0, 0)$	$(2, 0, 1)$	$(2, 0, 3)$
	$(2, 1, 4)$	$(2, 3, > 4)$	$(3, 0, 0)$	$(3, 0, 1)$	$(3, 0, 3)$	$(3, 1, 4)$	$(3, 3, > 4)$
	$(4, 0, 2)$	$(4, 1, > 4)$	$(4, 2, 4)$	$(4, 3, 0)$	$(4, 3, 1)$	$(4, 3, 3)$	

Chapter 9
Congruence Systems

In this chapter we investigate some examples of systems of congruence equations of various types and how they are solved. In fact, this chapter should be regarded as continuation to the previous chapter as both chapters are essentially about solving congruence equations (i.e. individually or collectively).[70]

9.1 General Issues about Congruence Systems

1. Define the meaning of "solving a system of congruence equations".
   Solution: It means finding the intersection of solutions of the individual congruence equations (whether this intersection is the empty set or not).
2. What is the number of solutions a system of congruence equations can have?
   Solution: A system of congruence equations can have no solution, or a single solution, or finitely many solutions (i.e. in modular arithmetic sense).
3. Investigate the solvability of the congruence equations of the following system as well as the solvability of the system itself:
   $$x^2 \overset{p}{=} m \qquad x^2 \overset{p}{=} n \qquad x^2 \overset{p}{=} mn$$
   where p is an odd prime, and $m, n \in \mathbb{Z}$ are coprime to p.
   Solution: We have four cases to consider (noting that we use Problem 11 of § 8.1):
   • m is a quadratic residue and n is a quadratic non-residue of p and hence only the first congruence is solvable, i.e. the second and third congruences (as well as the system) are non-solvable.
   • n is a quadratic residue and m is a quadratic non-residue of p and hence only the second congruence is solvable, i.e. the first and third congruences (as well as the system) are non-solvable.
   • Both m and n are quadratic non-residues of p and hence only the third congruence is solvable, i.e. the first and second congruences (as well as the system) are non-solvable.
   • Both m and n are quadratic residues of p and hence all the three congruences are solvable. Regarding the solvability of the system, it is potentially solvable (noting that the solvability of the individual equations of a system is a necessary but not sufficient condition for the solvability of the system).[71]
4. Propose a criterion for the solvability of a system of univariate linear congruence equations.
   Solution: We use the following proposition (which may be regarded as an "addendum" or extension[72] to the Chinese remainder theorem and can be used as a criterion for solvability): the following system of simultaneous linear congruence equations in the unknown $x \in \mathbb{Z}$:
   $$x \overset{m_1}{=} n_1 \qquad x \overset{m_2}{=} n_2 \qquad \cdots \qquad x \overset{m_k}{=} n_k$$
   (where $\mathbb{N} \ni m_1, m_2, \ldots, m_k > 1$ and $n_1, n_2, \ldots, n_k \in \mathbb{Z}$) is solvable *iff* $n_i - n_j$ $(i, j = 1, 2, \ldots, k)$ is divisible by $\gcd(m_i, m_j)$ for every i and j (where $i \neq j$). When the system meets this criterion (i.e. it is solvable) then the general solution of the system is represented by a single congruence $x \overset{m}{=} n$ where $m = \operatorname{lcm}(m_1, m_2, \ldots, m_k)$ and $n \in \mathbb{Z}$.

[70] In fact, it is also continuation to the material about this topic which we investigated in the first volume of this book.
[71] In fact, there are some details about the nature of m and n and if they belong to different residue classes or not. In general, such a system is solvable in trivial cases like $x^2 \overset{7}{=} 8$, $x^2 \overset{7}{=} 15$, $x^2 \overset{7}{=} 120$ (noting that 8, 15, 120 belong to the same residue class modulo 7, i.e. 1).
[72] See Problem 3 of § 9.2.2 and Problem 5 of § 9.3.2 for more details about this issue.

9.2 Univariate Congruence Systems

9.2.1 Single Modulo

1. Solve the following systems of non-linear polynomial congruence equations (where $x \in \mathbb{Z}$):

   (**a**) $15x^2 - x - 2 \overset{70}{=} 0$ $\quad$ $x^3 + 2x^2 + 5 \overset{70}{=} 0$.

   (**b**) $x^3 - x^2 + 12 \overset{2210}{=} 0$ $\quad$ $x^3 + 305x^2 - 612x - 226 \overset{2210}{=} 0$.

   (**c**) $14x^2 - 32 \overset{166}{=} 0$ $\quad$ $x^3 - 50x^2 - 69x - 18 \overset{166}{=} 0$.

   Solution:[73]

   (**a**) The solutions of the first congruence are: $x \overset{70}{=} 13, 23, 48, 58$ while the solutions of the second congruence are: $x \overset{70}{=} 23, 65$. So, the solution of the system is $x \overset{70}{=} 23$.

   (**b**) Both these congruences have the following solutions: $x \overset{2210}{=} 24$, 219, 778, 908, 999, 1103, 1129, 1324, 1883, 2013, 2104, 2208. So, these are the solutions of this system.

   (**c**) The solutions of the first congruence are: $x \overset{166}{=} 21, 62, 104, 145$ while the solutions of the second congruence are: $x \overset{166}{=} 62, 72, 82, 145, 155, 165$. So, the solutions of the system are $x \overset{166}{=} 62, 145$.

2. Solve the following systems of exponential congruence equations (where $x \in \mathbb{N}^0$):

   (**a**) $3^x + 4^x \overset{11}{=} 3$ $\quad$ $2^x + 5^x \overset{11}{=} 7$.

   (**b**) $5^x + 7^x + 8^x \overset{17}{=} 10$ $\quad$ $2^x + 4^x + 9^x \overset{17}{=} 16$.

   (**c**) $11^x + 17^x + 31^x \overset{164}{=} 3$ $\quad$ $13^x + 19^x + 23^x \overset{164}{=} 155$.

   Solution:

   (**a**) The solutions of the first congruence are: $x \overset{5}{=} 2, 3$ (i.e. $x \overset{10}{=} 2, 3, 7, 8$) while the solutions of the second congruence are: $x \overset{10}{=} 1, 2, 8$. So, the solutions of the system are $x \overset{10}{=} 2, 8$.

   (**b**) The solutions of the first congruence are: $x \overset{16}{=} 11, 14, 15$ while the solutions of the second congruence are: $x \overset{8}{=} 2, 4, 6$. Now, if we try all the 9 combinations of $x \overset{16}{=} 11, 14, 15$ with $x \overset{8}{=} 2, 4, 6$ (using the Chinese remainder theorem) we find that the only solution to this system is $x \overset{16}{=} 14$.[74]

   (**c**) The solutions of the first congruence are: $x \overset{40}{=} 0, 21, 31$ while the solutions of the second congruence are: $x \overset{40}{=} 21$. Hence, the only solution to this system is $x \overset{40}{=} 21$.

3. Solve the following systems of mixed polynomial-exponential congruence equations (where $x \in \mathbb{N}^0$):

   (**a**) $2x^3 + 5x^2 + 8x + 1 \overset{124}{=} 0$ $\quad$ $5^x + 7^x \overset{124}{=} 12$.

   (**b**) $x^4 + 12x^2 + 7x + 22 \overset{77}{=} 0$ $\quad$ $13^x + 25^x \overset{77}{=} 2$.

   (**c**) $6x^3 + 33x^2 + 13x \overset{69}{=} 0$ $\quad$ $19^x + 35^x + 41^x \overset{69}{=} 38$.

   Solution:

   (**a**) The solutions of the first congruence are: $x \overset{124}{=} 3, 17, 55, 65, 79, 117$ while the solutions of the second congruence are: $x \overset{30}{=} 1, 17$. Now, if we try the 12 combinations of $x \overset{124}{=} 3, 17, 55, 65, 79, 117$ with $x \overset{30}{=} 1, 17$ (using the Chinese remainder theorem) we find that the solutions of this system are: $x \overset{1860}{=} 17, 241, 437, 451, 737, 871, 947, 1171, 1367, 1381, 1667, 1801$.

   (**b**) The solutions of the first congruence are: $x \overset{77}{=} 22, 55$ while the solutions of the second congruence are: $x \overset{30}{=} 0, 12$. Now, if we try the 4 combinations of $x \overset{77}{=} 22, 55$ with $x \overset{30}{=} 0, 12$ we find that the solutions

[73] For how to obtain the solutions of the individual congruence equations (in this and other Problems), we refer the reader to the previous chapter (as well as V1).

[74] Alternatively (and more simply), if we convert modulo 8 to modulo 16 (similar to what we did in part a by converting modulo 5 to modulo 10) then the solutions of the second congruence are: $x \overset{16}{=} 2, 4, 6, 10, 12, 14$ and hence we obtain the same result.

of this system are: $x \overset{2310}{=} 132, 330, 792, 1980$.

(**c**) The solutions of the first congruence are: $x \overset{69}{=} 0, 33, 42$ while the solutions of the second congruence are: $x \overset{22}{=} 13, 17, 19$. Now, if we try the 9 combinations of $x \overset{69}{=} 0, 33, 42$ with $x \overset{22}{=} 13, 17, 19$ we find that the solutions of this system are: $x \overset{1518}{=} 171, 387, 525, 585, 723, 897, 1311, 1449, 1491$.

9.2.2 Multiple Moduli

1. Solve the following system of non-linear polynomial congruence equations:

$$33x^8 \overset{21}{=} 27 \qquad\qquad x^3 - 4x^2 + 3x + 5 \overset{19}{=} 0$$

Solution: The solutions of these equations (respectively) are (see for example § 3.2.1 of V1):

$$x \overset{21}{=} 2, 5, 9, 12, 16, 19 \qquad\qquad x \overset{19}{=} 6, 8, 9$$

The first of these congruences can be simplified to $x \overset{7}{=} 2, 5$.[75] Now, if we consider the 6 combinations of $x \overset{7}{=} 2, 5$ with $x \overset{19}{=} 6, 8, 9$ then we obtain 6 systems of linear congruence equations which can be solved (for instance) by the Chinese remainder theorem. These solutions are given in the following table:

	$\boldsymbol{x \overset{19}{=} 6}$	$\boldsymbol{x \overset{19}{=} 8}$	$\boldsymbol{x \overset{19}{=} 9}$
$\boldsymbol{x \overset{7}{=} 2}$	44	65	9
$\boldsymbol{x \overset{7}{=} 5}$	82	103	47

So, the solutions of the given system of congruences are: $x \overset{133}{=} 9, 44, 47, 65, 82, 103$.

2. Which of the following systems of simultaneous linear congruence equations is solvable (giving their solutions when they are solvable):

(**a**) $x \overset{3}{=} 2 \qquad x \overset{9}{=} 5 \qquad x \overset{23}{=} 8.$

(**b**) $x \overset{8}{=} 5 \qquad x \overset{6}{=} 11 \qquad x \overset{31}{=} 19.$

(**c**) $x \overset{11}{=} 1 \qquad x \overset{16}{=} 7 \qquad x \overset{99}{=} 18.$

(**d**) $x \overset{29}{=} 19 \qquad x \overset{34}{=} 14 \qquad x \overset{48}{=} 13.$

(**e**) $x \overset{7}{=} 5 \qquad x \overset{21}{=} 12 \qquad x \overset{35}{=} 19 \qquad x \overset{49}{=} 33.$

Solution: We use the criterion of Problem 4 of § 9.1.

(**a**) We have:

$$\gcd(3, 9) | (5 - 2) \qquad \gcd(3, 23) | (8 - 2) \qquad \gcd(9, 23) | (8 - 5)$$

Hence, the system is solvable. Its solution is $x \overset{207}{=} 77$ noting that $207 = \operatorname{lcm}(3, 9, 23)$.

(**b**) We have:

$$\gcd(8, 6) | (11 - 5) \qquad \gcd(8, 31) | (19 - 5) \qquad \gcd(6, 31) | (19 - 11)$$

Hence, the system is solvable. Its solution is $x \overset{744}{=} 701$ noting that $744 = \operatorname{lcm}(8, 6, 31)$.

(**c**) We have:

$$\gcd(11, 16) | (7 - 1) \qquad \gcd(11, 99) \nmid (18 - 1) \qquad \gcd(16, 99) | (18 - 7)$$

Hence, the system is not solvable.

(**d**) We have:

$$\gcd(29, 34) | (19 - 14) \qquad \gcd(29, 48) | (19 - 13) \qquad \gcd(34, 48) \nmid (14 - 13)$$

Hence, the system is not solvable.

(**e**) We have:

---

[75] Instead, we could have simplified the congruence $33x^8 \overset{21}{=} 27$ to $11x^8 \overset{7}{=} 9$ (by using rule 9 of § 2.7 of V1) and hence obtain the solution $x \overset{7}{=} 2, 5$.

$\gcd(7,21)|(12-5)$ $\gcd(7,35)|(19-5)$ $\gcd(7,49)|(33-5)$

$\gcd(21,35)|(19-12)$ $\gcd(21,49)|(33-12)$ $\gcd(35,49)|(33-19)$

Hence, the system is solvable. Its solution is $x \overset{735}{=} 474$ noting that $735 = \text{lcm}(7,21,35,49)$.

3. Discuss the extensions (or generalizations) that we introduced in the previous Problems on the (original) Chinese remainder theorem (as given in § 2.7.3 of V1).
Solution: We can identify two extensions:
• The extension that was introduced (implicitly) in Problem 1 by lifting the restriction of linearity,[76] i.e. when the system contains non-linear congruences then we "decompose" the non-linear congruences to their linear solutions and consider the possible combinations of solutions (as we did in Problem 1). Although this is not an extension to the Chinese remainder theorem itself, it is an extension that enables the employment of the Chinese remainder theorem to solve non-linear systems (i.e. systems that include non-linear congruences).[77]
• The extension that was introduced in Problem 4 of § 9.1 by lifting the restriction of coprimality of moduli, i.e. the condition of pairwise coprimality of the moduli $m_1, m_2, \ldots, m_k$ (which we imposed earlier in the statement of the Chinese remainder theorem; see § 2.7.3 of V1) does not appear in this proposition and hence this proposition is an extension or generalization to the (original) Chinese remainder theorem.
Also see Problem § 5 of § 9.3.2.

4. Solve the following systems of non-linear polynomial congruence equations (where $x \in \mathbb{Z}$):

(**a**) $15x^2 - x - 2 \overset{70}{=} 0$ $x^3 + 2x^2 + 21 \overset{99}{=} 0$.

(**b**) $2x^4 + 3x^2 + 18x + 9 \overset{372}{=} 0$ $x^4 - 33x^3 - 28 \overset{524}{=} 0$.

(**c**) $x^3 + 7x^2 - x + 1 \overset{422}{=} 0$ $3x^2 + 27x + 6 \overset{621}{=} 0$.

Solution:
(**a**) The solutions of the first congruence are: $x \overset{70}{=} 13, 23, 48, 58$ while the solutions of the second congruence are: $x \overset{99}{=} 40, 58, 76$. Now, if we try the 12 combinations of $x \overset{70}{=} 13, 23, 48, 58$ with $x \overset{99}{=} 40, 58, 76$ (as we did in Problem 1) we find that the solutions of this system are: $x \overset{6930}{=}$ 58, 373, 2218, 2533, 2848, 3208, 3523, 3838, 5683, 5998, 6313, 6673.
(**b**) The solutions of the first congruence are: $x \overset{372}{=} 69, 105, 255, 291$ while the solutions of the second congruence are: $x \overset{524}{=} 18, 149, 280$. Now, if we try the 12 combinations of $x \overset{372}{=} 69, 105, 255, 291$ with $x \overset{524}{=} 18, 149, 280$ we find only the following two solutions: $x \overset{48732}{=} 29493, 35781$.
(**c**) The solutions of the first congruence are: $x \overset{422}{=} 77, 361, 399$ while the solutions of the second congruence are: $x \overset{207}{=} 31, 77, 121, 167$. Now, if we try the 12 combinations of $x \overset{422}{=} 77, 361, 399$ with $x \overset{207}{=} 31, 77, 121, 167$ we find that the solutions of this system are: $x \overset{87354}{=}$ 77, 7573, 19489, 26663, 29057, 46075, 48469, 48929, 55643, 68341, 75055, 75515.

5. Solve the following systems of exponential congruence equations (where $x \in \mathbb{N}^0$):

(**a**) $3^x + 4^x \overset{11}{=} 3$ $2^x + 5^x \overset{19}{=} 7$.

(**b**) $5^x + 7^x + 8^x \overset{17}{=} 2$ $2^x + 4^x + 9^x \overset{31}{=} 7$.

(**c**) $11^x + 17^x + 31^x \overset{164}{=} 3$ $13^x + 19^x + 23^x \overset{175}{=} 3$.

Solution:
(**a**) The solutions of the first congruence are: $x \overset{5}{=} 2, 3$ while the solutions of the second congruence are: $x \overset{18}{=} 1$. On trying these two combinations (using the Chinese remainder theorem) we get the following

[76] In fact, this extension is also present in the upcoming Problems of this subsection.
[77] Actually, this extension normally deals with non-linear systems of polynomial type (although the idea is applicable to other types of non-linear systems).

two solutions: $x \overset{90}{=} 37, 73$.

(**b**) The solutions of the first congruence are: $x \overset{16}{=} 2$ while the solutions of the second congruence are: $x \overset{15}{=} 8, 10$. On trying these two combinations we get the following two solutions: $x \overset{240}{=} 98, 130$.

(**c**) The solutions of the first congruence are: $x \overset{40}{=} 0, 21, 31$ while the solutions of the second congruence are: $x \overset{60}{=} 0$. Hence, the only solution to this system is $x \overset{120}{=} 0$.

6. Solve the following systems of mixed polynomial-exponential congruence equations (where $x \in \mathbb{N}^0$):

(**a**) $2x^3 + 5x^2 + 8x + 1 \overset{124}{=} 0$ $\quad$ $5^x + 7^x \overset{144}{=} 12$.

(**b**) $x^4 + 12x^2 + 7x + 22 \overset{77}{=} 0$ $\quad$ $13^x + 25^x \overset{101}{=} 2$.

(**c**) $6x^3 + 33x^2 + 13x \overset{69}{=} 0$ $\quad$ $19^x + 35^x + 41^x \overset{117}{=} 3$.

Solution:

(**a**) The solutions of the first congruence are: $x \overset{124}{=} 3, 17, 55, 65, 79, 117$ while the solutions of the second congruence are: $x \overset{12}{=} 1$. On trying the 6 combinations of $x \overset{124}{=} 3, 17, 55, 65, 79, 117$ with $x \overset{12}{=} 1$ (using the Chinese remainder theorem) we find that the only solutions of this system are: $x \overset{372}{=} 241, 265, 313$.

(**b**) The solutions of the first congruence are: $x \overset{77}{=} 22, 55$ while the solutions of the second congruence are: $x \overset{50}{=} 0$. On trying the two combinations of $x \overset{77}{=} 22, 55$ with $x \overset{50}{=} 0$ we find that the solutions of this system are: $x \overset{3850}{=} 1100, 2750$.

(**c**) The solutions of the first congruence are: $x \overset{69}{=} 0, 33, 42$ while the solutions of the second congruence are: $x \overset{12}{=} 0$. On trying these three combinations of $x \overset{69}{=} 0, 33, 42$ with $x \overset{12}{=} 0$ we find that the solutions of this system are: $x \overset{276}{=} 0, 180, 240$.

9.3 Multivariate Congruence Systems

9.3.1 Single Modulo

In § 4.4.1 of V1 we discussed systems of multivariate linear congruence equations with a single modulo and how they are solved (giving some examples of them with their solutions). So, in the following Problems we restrict our attention to systems of multivariate non-linear congruence equations with a single modulo.

Problems

1. Solve the following systems of non-linear polynomial congruences (where $x, y, z \in \mathbb{Z}$):

(**a**) $x^3 + y \overset{17}{=} 0$ $\quad$ $3x^2 + 4y^4 \overset{17}{=} 1$.

(**b**) $x^2 + y^3 \overset{41}{=} 1$ $\quad$ $4x^2 + 2y \overset{41}{=} 3$.

(**c**) $x^3 + y^2 + 2z^2 \overset{88}{=} 1$ $\quad$ $x^2 + 2y + 3z \overset{88}{=} 1$.

Solution:

(**a**) The solutions of these equations are (see § 8.3):

$(\boldsymbol{x, y}) \overset{\mathbf{17}}{=}$ $(0,0)$ $(1,16)$ $(2,9)$ $(3,7)$ $(4,4)$ $(5,11)$ $(6,5)$ $(7,14)$ $(8,15)$ $(9,2)$
$(10,3)$ $(11,12)$ $(12,6)$ $(13,13)$ $(14,10)$ $(15,8)$ $(16,1)$

$(\boldsymbol{x, y}) \overset{\mathbf{17}}{=}$ $(0,3)$ $(0,5)$ $(0,12)$ $(0,14)$ $(4,1)$ $(4,4)$ $(4,13)$ $(4,16)$ $(8,2)$ $(8,8)$
$(8,9)$ $(8,15)$ $(9,2)$ $(9,8)$ $(9,9)$ $(9,15)$ $(13,1)$ $(13,4)$ $(13,13)$ $(13,16)$

As we see, what is common between these two sets of solutions (i.e. their intersection) are the following 4 solutions: $(x, y) \overset{17}{=} (4,4)$, $(8,15)$, $(9,2)$ and $(13,13)$. So, these are the solutions of the system.

Alternatively, we can solve this system more simply by just looping over x and y (e.g. by a simple code or a spreadsheet) between 0 and 16 (considering all the 17×17 combinations) to get these 4 solutions.

(**b**) By looping (or by following a similar approach to that of part a) we get the following two solutions: $(x, y) \overset{41}{=} (2,14)$ and $(39,14)$.

(**c**) By looping we get the following 32 solutions in modulo 88 [i.e. $(x, y, z) \overset{88}{=}$]:

$(1, 0, 0)$	$(1, 44, 0)$	$(9, 12, 24)$	$(9, 28, 72)$	$(9, 56, 24)$	$(9, 72, 72)$	$(17, 28, 32)$
$(17, 72, 32)$	$(21, 6, 84)$	$(21, 38, 4)$	$(21, 50, 84)$	$(21, 82, 4)$	$(33, 20, 64)$	$(33, 40, 80)$
$(33, 64, 64)$	$(33, 84, 80)$	$(45, 22, 44)$	$(45, 66, 44)$	$(53, 6, 28)$	$(53, 34, 68)$	$(53, 50, 28)$
$(53, 78, 68)$	$(61, 6, 76)$	$(61, 50, 76)$	$(65, 16, 48)$	$(65, 28, 40)$	$(65, 60, 48)$	$(65, 72, 40)$
$(77, 18, 36)$	$(77, 42, 20)$	$(77, 62, 36)$	$(77, 86, 20)$			

2. Solve the following systems of exponential congruence equations (where $x, y, z \in \mathbb{N}^0$):

(**a**) $3^x + 4^y \overset{19}{=} 2$ $\quad$ $3^x + 5^y \overset{19}{=} 1$.

(**b**) $3^x + 4^y \overset{41}{=} 2$ $\quad$ $5^x + 7^y \overset{41}{=} 10$.

(**c**) $2^x + 3^y + 5^z \overset{11}{=} 4$ $\quad$ $3^x + 4^y + 7^z \overset{11}{=} 5$.

Solution:

(**a**) The solutions of these equations are (see § 8.3):

$\boldsymbol{(x \overset{18}{=}, y \overset{9}{=})}$	$(0, 0)$	$(4, 2)$	$(5, 7)$	$(10, 8)$	$(11, 6)$	$(13, 3)$	$(14, 5)$	$(15, 4)$	$(16, 1)$
$\boldsymbol{(x \overset{18}{=}, y \overset{9}{=})}$	$(1, 4)$	$(2, 3)$	$(5, 1)$	$(10, 8)$	$(12, 5)$	$(13, 2)$	$(14, 7)$	$(17, 6)$	

As we see, what is common between these two sets of solutions (i.e. their intersection) is only one solution, i.e. $x \overset{18}{=} 10$ and $y \overset{9}{=} 8$. So, this is the only solution to this system.

(**b**) The solutions of these equations are:

$\boldsymbol{(x \overset{8}{=}, y \overset{10}{=})}$	$(0, 0)$	$(1, 5)$	$(3, 2)$					
$\boldsymbol{(x \overset{20}{=}, y \overset{40}{=})}$	$(0, 10)$	$(1, 18)$	$(2, 23)$	$(3, 2)$	$(5, 0)$	$(6, 39)$	$(7, 12)$	$(8, 22)$
	$(9, 14)$	$(10, 37)$	$(11, 3)$	$(12, 19)$	$(13, 13)$	$(14, 6)$	$(15, 31)$	$(16, 15)$
	$(17, 17)$	$(18, 29)$	$(19, 24)$					

Now, we form the following 57 systems of linear congruence equations in x (where the rows represent x in mod 8 and the columns represent x in mod 20 while the entries represent x in mod 40 noting that the empty entries mean no solution) and solve them (by the Chinese remainder theorem):

	0	**1**	**2**	**3**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
0	**0**							8				32				16			
1		1			25				9				33						
3				**3**			**27**				11				35				19

We also form the following 57 systems of linear congruence equations in y (where the rows represent y in mod 10 and the columns represent y in mod 40 while the entries represent y in mod 40 noting that the empty entries mean no solution) and solve them:

	10	**18**	**23**	**2**	**0**	**39**	**12**	**22**	**14**	**37**	**3**	**19**	**13**	**6**	**31**	**15**	**17**	**29**	**24**
0	**10**				0														
5																15			
2				**2**			**12**	22											

On comparing the two tables we can see that we have only 3 solutions: $(x, y) \overset{40}{=} (0, 10)$, $(3, 2)$ and $(27, 12)$.

(**c**) The solutions of these equations are given in Problem 5 of § 8.3. Now if we consider the 529 (i.e. 23×23) combinations we can eliminate most of them and obtain the solutions as follows:

• For $x \overset{5}{=} 0$: we have a solution only for $x \overset{10}{=} 0, 5$. Moreover, because y must be identical (since it is in mod 5 in both sets of solutions) then we have only the following 5 potentially solvable combinations (noting that these combinations are one-to-one):

$\boldsymbol{(x \overset{5}{=}, y \overset{5}{=}, z \overset{10}{=})}$	$(0, 0, 4)$	$(0, 2, 5)$	$(0, 3, 7)$	$(0, 4, 0)$
$\boldsymbol{(x \overset{10}{=}, y \overset{5}{=}, z \overset{5}{=})}$	$(5, 0, 3)$	$(0, 2, 1)$	$(0, 3, 4)$	$(5, 4, 0)$

However, considering the solvability of the z system, only the last combination has a solution, i.e. $(x \overset{10}{=},\ y \overset{5}{=},\ z \overset{10}{=}) = (5, 4, 0)$.

• For $x \overset{5}{=} 1$: following the procedure of the previous point we get the following 6 combinations:

$(\boldsymbol{x \overset{5}{=},\ y \overset{5}{=},\ z \overset{10}{=}})$	$(1,0,0)$	$(1,0,0)$	$(1,1,8)$	$(1,2,9)$	$(1,3,6)$	$(1,4,5)$
$(\boldsymbol{x \overset{10}{=},\ y \overset{5}{=},\ z \overset{5}{=}})$	$(1,0,0)$	$(6,0,1)$	$(6,1,2)$	$(1,2,3)$	$(6,3,0)$	$(1,4,4)$

However, only the first combination has a solution, i.e. $(x \overset{10}{=},\ y \overset{5}{=},\ z \overset{10}{=}) = (1, 0, 0)$.

• For $x \overset{5}{=} 2$: we get the following 3 combinations:

$(\boldsymbol{x \overset{5}{=},\ y \overset{5}{=},\ z \overset{10}{=}})$	$(2,1,4)$	$(2,3,8)$	$(2,4,6)$
$(\boldsymbol{x \overset{10}{=},\ y \overset{5}{=},\ z \overset{5}{=}})$	$(7,1,1)$	$(7,3,2)$	$(7,4,3)$

However, none of these combination has a solution.

• For $x \overset{5}{=} 3$: we get the following 5 combinations:

$(\boldsymbol{x \overset{5}{=},\ y \overset{5}{=},\ z \overset{10}{=}})$	$(3,1,1)$	$(3,1,1)$	$(3,2,7)$	$(3,2,7)$	$(3,4,9)$
$(\boldsymbol{x \overset{10}{=},\ y \overset{5}{=},\ z \overset{5}{=}})$	$(3,1,3)$	$(8,1,4)$	$(3,2,4)$	$(8,2,2)$	$(3,4,2)$

However, only the fourth combination has a solution, i.e. $(x \overset{10}{=},\ y \overset{5}{=},\ z \overset{10}{=}) = (8, 2, 7)$.

• For $x \overset{5}{=} 4$: we get the following 4 combinations:

$(\boldsymbol{x \overset{5}{=},\ y \overset{5}{=},\ z \overset{10}{=}})$	$(4,2,1)$	$(4,3,4)$	$(4,3,4)$	$(4,4,8)$
$(\boldsymbol{x \overset{10}{=},\ y \overset{5}{=},\ z \overset{5}{=}})$	$(4,2,0)$	$(4,3,1)$	$(9,3,3)$	$(9,4,1)$

However, none of these combinations has a solution.

So in brief, this system has only three solutions, i.e. $(x \overset{10}{=},\ y \overset{5}{=},\ z \overset{10}{=}) = (1, 0, 0)$, $(5, 4, 0)$ and $(8, 2, 7)$.

3. Solve the following system of mixed polynomial-exponential congruences (where $x, y \in \mathbb{N}^0$):

$$x^3 + y \overset{11}{=} 0 \qquad\qquad 3^x + 4^y \overset{11}{=} 2.$$

Solution: The solutions of these equations are (see § 8.3):

$\boldsymbol{(x,y) \overset{11}{=}}$	$(0,0)$	$(1,10)$	$(2,3)$	$(3,6)$	$(4,2)$	$(5,7)$	$(6,4)$	$(7,9)$	$(8,5)$	$(9,8)$	$(10,1)$
$\boldsymbol{(x,y) \overset{5}{=}}$	$(0,0)$	$(2,1)$	$(4,3)$								

Now, we form the following 33 systems of linear congruence equations in x and the corresponding 33 systems of linear congruence equations in y and solve them where the solutions are shown in the third and sixth columns:

$\boldsymbol{x \overset{11}{=}}$	$\boldsymbol{x \overset{5}{=}}$	$\boldsymbol{x \overset{55}{=}}$	$\boldsymbol{y \overset{11}{=}}$	$\boldsymbol{y \overset{5}{=}}$	$\boldsymbol{y \overset{55}{=}}$
0	0,2,4	0,22,44	0	0,1,3	0,11,33
1	0,2,4	45,12,34	10	0,1,3	10,21,43
2	0,2,4	35,2,24	3	0,1,3	25,36,3
3	0,2,4	25,47,14	6	0,1,3	50,6,28
4	0,2,4	15,37,4	2	0,1,3	35,46,13
5	0,2,4	5,27,49	7	0,1,3	40,51,18
6	0,2,4	50,17,39	4	0,1,3	15,26,48
7	0,2,4	40,7,29	9	0,1,3	20,31,53
8	0,2,4	30,52,19	5	0,1,3	5,16,38
9	0,2,4	20,42,9	8	0,1,3	30,41,8
10	0,2,4	10,32,54	1	0,1,3	45,1,23

So, these are the solutions of the given system, i.e. $(x, y) \overset{55}{=} (0, 0), (22, 11), (44, 33) \ldots, (32, 1), (54, 23)$.

9.3.2 Multiple Moduli

1. Solve the following systems of linear congruence equations (where $x, y, z \in \mathbb{Z}$):

(**a**) $2x + y \overset{3}{=} 0$ $\quad x - 2y \overset{5}{=} 3.$

(**b**) $x - 4y \overset{5}{=} 2$ $\quad 5x + y \overset{7}{=} 1.$

(**c**) $6x - 3y \overset{9}{=} 1$ $\quad 5x + 2y \overset{11}{=} 3.$

(**d**) $x + y - z \overset{2}{=} 0$ $\quad 2x + y + z \overset{3}{=} 1.$

Solution:

(**a**) The solutions of these equations are (see Problem 3 of § 8.3):

$\boldsymbol{(x, y) \overset{3}{=}}$ $(0,0)$ $(1,1)$ $(2,2)$

$\boldsymbol{(x, y) \overset{5}{=}}$ $(0,1)$ $(1,4)$ $(2,2)$ $(3,0)$ $(4,3)$

Now, we form the following 15 systems of linear congruence equations in x and the corresponding 15 systems of linear congruence equations in y and solve them (using for instance the Chinese remainder theorem) where the solutions are shown in the third and sixth rows:

$\boldsymbol{x \overset{3}{=}}$	0	0	0	0	0	1	1	1	1	1	2	2	2	2	2
$\boldsymbol{x \overset{5}{=}}$	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
$\boldsymbol{x \overset{15}{=}}$	**0**	**6**	**12**	**3**	**9**	**10**	**1**	**7**	**13**	**4**	**5**	**11**	**2**	**8**	**14**
$\boldsymbol{y \overset{3}{=}}$	0	0	0	0	0	1	1	1	1	1	2	2	2	2	2
$\boldsymbol{y \overset{5}{=}}$	1	4	2	0	3	1	4	2	0	3	1	4	2	0	3
$\boldsymbol{y \overset{15}{=}}$	**6**	**9**	**12**	**0**	**3**	**1**	**4**	**7**	**10**	**13**	**11**	**14**	**2**	**5**	**8**

So, these are the solutions of the given system, i.e. $(x, y) \overset{15}{=} (0,6), (6,9), \ldots, (14,8)$.

(**b**) The solutions of these equations are (see Problem 3 of § 8.3):

$\boldsymbol{(x, y) \overset{5}{=}}$ $(0,2)$ $(1,1)$ $(2,0)$ $(3,4)$ $(4,3)$

$\boldsymbol{(x, y) \overset{7}{=}}$ $(0,1)$ $(1,3)$ $(2,5)$ $(3,0)$ $(4,2)$ $(5,4)$ $(6,6)$

On forming 35 systems of linear congruence equations in x and the corresponding 35 systems of linear congruence equations in y (as we did in part a) and solving them we get the following 35 solutions:

$\boldsymbol{(x, y) \overset{35}{=}}$ $(0,22)$ $(1,31)$ $(2,5)$ $(3,14)$ $(4,23)$ $(5,32)$ $(6,6)$ $(7,15)$ $(8,24)$
$(9,33)$ $(10,7)$ $(11,16)$ $(12,25)$ $(13,34)$ $(14,8)$ $(15,17)$ $(16,26)$ $(17,0)$
$(18,9)$ $(19,18)$ $(20,27)$ $(21,1)$ $(22,10)$ $(23,19)$ $(24,28)$ $(25,2)$ $(26,11)$
$(27,20)$ $(28,29)$ $(29,3)$ $(30,12)$ $(31,21)$ $(32,30)$ $(33,4)$ $(34,13)$

(**c**) The first equation has no solution[78] and hence this system has no solution.

(**d**) The solutions of these equations are (see Problem 3 of § 8.3):

$\boldsymbol{(x, y, z) \overset{2}{=}}$ $(0,0,0)$ $(0,1,1)$ $(1,0,1)$ $(1,1,0)$

$\boldsymbol{(x, y, z) \overset{3}{=}}$ $(0,0,1)$ $(0,1,0)$ $(0,2,2)$ $(1,0,2)$ $(1,1,1)$ $(1,2,0)$ $(2,0,0)$ $(2,1,2)$ $(2,2,1)$

On forming 36 systems of linear congruence equations in x (and the corresponding 36 systems in y and 36 systems in z as we did in parts a and b) and solving them we get the following 36 solutions:

[78] If we multiply the congruence by 3 we get $18x - 9y \overset{9}{=} 3$, i.e. $0 \overset{9}{=} 3$ which is nonsensical.

$(\boldsymbol{x, y}) \overset{\mathbf{6}}{=}$ $(0,0,4)$ $(0,1,3)$ $(0,2,2)$ $(0,3,1)$ $(0,4,0)$ $(0,5,5)$ $(1,0,5)$ $(1,1,4)$ $(1,2,3)$
$(1,3,2)$ $(1,4,1)$ $(1,5,0)$ $(2,0,0)$ $(2,1,5)$ $(2,2,4)$ $(2,3,3)$ $(2,4,2)$ $(2,5,1)$
$(3,0,1)$ $(3,1,0)$ $(3,2,5)$ $(3,3,4)$ $(3,4,3)$ $(3,5,2)$ $(4,0,2)$ $(4,1,1)$ $(4,2,0)$
$(4,3,5)$ $(4,4,4)$ $(4,5,3)$ $(5,0,3)$ $(5,1,2)$ $(5,2,1)$ $(5,3,0)$ $(5,4,5)$ $(5,5,4)$

2. Solve the following systems of non-linear polynomial congruence equations (where $x, y, z \in \mathbb{Z}$):

(**a**) $x^3 + y \overset{2}{=} 0$ $3x^2 + 4y^4 \overset{5}{=} 1.$

(**b**) $x^2 + y^3 \overset{3}{=} 1$ $4x^2 - 5y \overset{7}{=} 3.$

(**c**) $x^3 - 2y^2 + 2z^2 \overset{3}{=} 1$ $x^2 + 2y + 3z \overset{5}{=} 1.$

Solution:

(**a**) The solutions of these equations are (see Problem 4 of § 8.3):

$(\boldsymbol{x, y}) \overset{\mathbf{2}}{=}$ $(0,0)$ $(1,1)$

$(\boldsymbol{x, y}) \overset{\mathbf{5}}{=}$ $(2,1)$ $(2,2)$ $(2,3)$ $(2,4)$ $(3,1)$ $(3,2)$ $(3,3)$ $(3,4)$

On forming 16 systems of linear congruence equations in x and the corresponding 16 systems of linear congruence equations in y (as we did in Problem 1) and solving them we get the following 16 solutions:

$(\boldsymbol{x, y}) \overset{\mathbf{10}}{=}$ $(2,2)$ $(2,4)$ $(2,6)$ $(2,8)$ $(3,1)$ $(3,3)$ $(3,7)$ $(3,9)$
$(7,1)$ $(7,3)$ $(7,7)$ $(7,9)$ $(8,2)$ $(8,4)$ $(8,6)$ $(8,8)$

(**b**) The solutions of these equations are (see Problem 4 of § 8.3 as well as Problem 1 of 4.2.1 of V1):

$(\boldsymbol{x, y}) \overset{\mathbf{3}}{=}$ $(0,1)$ $(1,0)$ $(2,0)$

$(\boldsymbol{x, y}) \overset{\mathbf{7}}{=}$ $(0,5)$ $(1,3)$ $(2,4)$ $(3,1)$ $(4,1)$ $(5,4)$ $(6,3)$

On forming 21 systems of linear congruence equations in x and the corresponding 21 systems of linear congruence equations in y (as we did in Problem 1) and solving them we get the following 21 solutions:

$(\boldsymbol{x, y}) \overset{\mathbf{21}}{=}$ $(0,19)$ $(1,3)$ $(2,18)$ $(3,1)$ $(4,15)$ $(5,18)$ $(6,10)$
$(7,12)$ $(8,3)$ $(9,4)$ $(10,15)$ $(11,15)$ $(12,4)$ $(13,3)$
$(14,12)$ $(15,10)$ $(16,18)$ $(17,15)$ $(18,1)$ $(19,18)$ $(20,3)$

(**c**) The solutions of these equations are (see Problem 4 of § 8.3 as well as Problem 1 of 4.2.1 of V1):

$(\boldsymbol{x, y, z}) \overset{\mathbf{3}}{=}$ $(0,1,0)$ $(0,2,0)$ $(1,0,0)$ $(1,1,1)$ $(1,1,2)$ $(1,2,1)$ $(1,2,2)$ $(2,0,1)$ $(2,0,2)$

$(\boldsymbol{x, y, z}) \overset{\mathbf{5}}{=}$ $(0,0,2)$ $(0,1,3)$ $(0,2,4)$ $(0,3,0)$ $(0,4,1)$ $(1,0,0)$ $(1,1,1)$ $(1,2,2)$ $(1,3,3)$
$(1,4,4)$ $(2,0,4)$ $(2,1,0)$ $(2,2,1)$ $(2,3,2)$ $(2,4,3)$ $(3,0,4)$ $(3,1,0)$ $(3,2,1)$
$(3,3,2)$ $(3,4,3)$ $(4,0,0)$ $(4,1,1)$ $(4,2,2)$ $(4,3,3)$ $(4,4,4)$

On forming 225 systems of linear congruence equations in x (and the corresponding 225 systems in y and 225 systems in z as we did in the previous Problems) and solving them we get the following 225 solutions (in modulo 15):

$(x$							$y, z)$						
0	1,3	2,9	4,6	5,12	7,9	8,0	10,12	11,3	13,0	14,6			
1	0,0	1,1	1,11	2,2	2,7	3,3	4,4	4,14	5,5	5,10	6,6	7,2	7,7
	8,8	8,13	9,9	10,5	10,10	11,1	11,11	12,12	13,8	13,13	14,4	14,14	
2	0,4	0,14	3,2	3,7	6,5	6,10	9,8	9,13	12,1	12,11			
3	1,0	2,6	4,3	5,9	7,6	8,12	10,9	11,0	13,12	14,3			
4	0,0	1,1	1,11	2,2	2,7	3,3	4,4	4,14	5,5	5,10	6,6	7,2	7,7
	8,8	8,13	9,9	10,5	10,10	11,1	11,11	12,12	13,8	13,13	14,4	14,14	
5	0,2	0,7	3,5	3,10	6,8	6,13	9,1	9,11	12,4	12,14			
6	1,6	2,12	4,9	5,0	7,12	8,3	10,0	11,6	13,3	14,9			
7	0,9	1,5	1,10	2,1	2,11	3,12	4,8	4,13	5,4	5,14	6,0	7,1	7,11
	8,2	8,7	9,3	10,4	10,14	11,5	11,10	12,6	13,2	13,7	14,8	14,13	
8	0,4	0,14	3,2	3,7	6,5	6,10	9,8	9,13	12,1	12,11			
9	1,6	2,12	4,9	5,0	7,12	8,3	10,0	11,6	13,3	14,9			
10	0,12	1,8	1,13	2,4	2,14	3,0	4,1	4,11	5,2	5,7	6,3	7,4	7,14
	8,5	8,10	9,6	10,2	10,7	11,8	11,13	12,9	13,5	13,10	14,1	14,11	
11	0,5	0,10	3,8	3,13	6,1	6,11	9,4	9,14	12,2	12,7			
12	1,0	2,6	4,3	5,9	7,6	8,12	10,9	11,0	13,12	14,3			
13	0,9	1,5	1,10	2,1	2,11	3,12	4,8	4,13	5,4	5,14	6,0	7,1	7,11
	8,2	8,7	9,3	10,4	10,14	11,5	11,10	12,6	13,2	13,7	14,8	14,13	
14	0,5	0,10	3,8	3,13	6,1	6,11	9,4	9,14	12,2	12,7			

3. Solve the following systems of exponential congruence equations (where $x, y, z \in \mathbb{N}^0$):

(**a**) $3^x + 4^y \overset{5}{=} 2$ $\qquad$ $3^x + 5^y \overset{7}{=} 1.$

(**b**) $3^x + 4^y \overset{5}{=} 2$ $\qquad$ $5^x + 7^y \overset{11}{=} 10.$

(**c**) $2^x + 3^y + 5^z \overset{7}{=} 4$ $\qquad$ $3^x + 4^y + 7^z \overset{11}{=} 5.$

Solution:

(**a**) The solutions of these equations are (see Problem 5 of § 8.3):

$(\boldsymbol{x \overset{4}{=}, y \overset{2}{=}})$ $(0,0)$ $(1,1)$

$(\boldsymbol{x \overset{6}{=}, y \overset{6}{=}})$ $(1,1)$ $(2,3)$ $(3,4)$ $(4,2)$ $(5,5)$

Now, we form the following 10 systems of linear congruence equations in x and the corresponding 10 systems of linear congruence equations in y and solve them (using for instance the Chinese remainder theorem) where the solutions (if exist) are shown in the third and sixth rows (noting that blank means there is no solution):

$\boldsymbol{x \overset{4}{=}}$	0	0	0	0	0	1	1	1	1	1
$\boldsymbol{x \overset{6}{=}}$	1	2	3	4	5	1	2	3	4	5
$\boldsymbol{x \overset{12}{=}}$		8		**4**		**1**		9		**5**
$\boldsymbol{y \overset{2}{=}}$	0	0	0	0	0	1	1	1	1	1
$\boldsymbol{y \overset{6}{=}}$	1	3	4	2	5	1	3	4	2	5
$\boldsymbol{y \overset{6}{=}}$			4	**2**		**1**	3			**5**

So, the solutions are (noting that only some combinations produce solutions for both x and y):

$(\boldsymbol{x \overset{12}{=}, y \overset{6}{=}})$ $(1,1)$ $(4,2)$ $(5,5)$

(**b**) The solutions of these equations are (see Problem 5 of § 8.3):

$(\boldsymbol{x} \overset{\mathbf{4}}{=}, \boldsymbol{y} \overset{\mathbf{2}}{=})$	$(0,0)$	$(1,1)$			
$(\boldsymbol{x} \overset{\mathbf{5}}{=}, \boldsymbol{y} \overset{\mathbf{10}}{=})$	$(0,8)$	$(1,2)$	$(2,1)$	$(3,7)$	$(4,0)$

Now, we form the following 10 systems of linear congruence equations in x and the corresponding 10 systems of linear congruence equations in y and solve them where the solutions (if exist) are shown in the third and sixth rows (noting that blank means there is no solution):

$\boldsymbol{x} \overset{\mathbf{4}}{=}$	0	0	0	0	0	1	1	1	1	1
$\boldsymbol{x} \overset{\mathbf{5}}{=}$	0	1	2	3	4	0	1	2	3	4
$\boldsymbol{x} \overset{\mathbf{20}}{=}$	**0**	**16**	12	8	**4**	5	1	**17**	**13**	9
$\boldsymbol{y} \overset{\mathbf{2}}{=}$	0	0	0	0	0	1	1	1	1	1
$\boldsymbol{y} \overset{\mathbf{10}}{=}$	8	2	1	7	0	8	2	1	7	0
$\boldsymbol{y} \overset{\mathbf{10}}{=}$	**8**	**2**			**0**			**1**	**7**	

So, the solutions are (noting that only some combinations produce solutions for both x and y):

$(\boldsymbol{x} \overset{\mathbf{20}}{=}, \boldsymbol{y} \overset{\mathbf{10}}{=})$	$(0,8)$	$(4,0)$	$(13,7)$	$(16,2)$	$(17,1)$

(**c**) The solutions of these equations are given in Problem 5 of § 8.3. We can form 368 combinations and search for solutions (as we did in the previous parts). However, because of limitation of space we will form and inspect only 12 of these combinations (noting that blank means there is no solution), that is:

$\boldsymbol{x} \overset{\mathbf{3}}{=}$	0	0	0	0	1	1	1	1	2	2	2	2
$\boldsymbol{x} \overset{\mathbf{5}}{=}$	0	0	4	1	1	0	2	3	3	4	1	3
$\boldsymbol{x} \overset{\mathbf{15}}{=}$	**0**	0	9	**6**	1	**10**	**7**	13	**8**	14	11	8
$\boldsymbol{y} \overset{\mathbf{6}}{=}$	0	0	4	5	1	3	4	5	0	3	4	5
$\boldsymbol{y} \overset{\mathbf{5}}{=}$	0	2	4	4	1	2	0	1	4	2	0	2
$\boldsymbol{y} \overset{\mathbf{30}}{=}$	**0**	12	4	**29**	1	**27**	**10**	11	**24**	27	10	17
$\boldsymbol{z} \overset{\mathbf{6}}{=}$	4	4	3	1	3	5	1	2	3	0	5	4
$\boldsymbol{z} \overset{\mathbf{10}}{=}$	4	5	8	5	8	5	7	1	9	1	0	7
$\boldsymbol{z} \overset{\mathbf{30}}{=}$	**4**			**25**		**5**	**7**		**9**			

So, the solutions among these 12 combinations are:

$(\boldsymbol{x} \overset{\mathbf{15}}{=}, \boldsymbol{y} \overset{\mathbf{30}}{=}, \boldsymbol{z} \overset{\mathbf{30}}{=})$	$(0,0,4)$	$(6,29,25)$	$(10,27,5)$	$(7,10,7)$	$(8,24,9)$

4. Solve the following system of mixed polynomial-exponential congruence equations (where $x, y \in \mathbb{N}^0$):

$x^3 + y \overset{7}{=} 0$ $\qquad\qquad$ $3^x + 4^y \overset{11}{=} 2.$

Solution: The solutions of these equations are (see § 8.3):

$(\boldsymbol{x}, \boldsymbol{y}) \overset{\mathbf{7}}{=}$	$(0,0)$	$(1,6)$	$(2,6)$	$(3,1)$	$(4,6)$	$(5,1)$	$(6,1)$
$(\boldsymbol{x}, \boldsymbol{y}) \overset{\mathbf{5}}{=}$	$(0,0)$	$(2,1)$	$(4,3)$				

Now, we form the following 21 systems of linear congruence equations in x and the corresponding 21 systems of linear congruence equations in y and solve them where the solutions are shown in the third and sixth rows:

$$
\begin{array}{lllllllllllllllllllll}
\boldsymbol{x} \overset{\mathbf{7}}{=} & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 & 4 & 4 & 4 & 5 & 5 & 5 & 6 & 6 & 6 \\
\boldsymbol{x} \overset{\mathbf{5}}{=} & 0 & 2 & 4 & 0 & 2 & 4 & 0 & 2 & 4 & 0 & 2 & 4 & 0 & 2 & 4 & 0 & 2 & 4 & 0 & 2 & 4 \\
\boldsymbol{x} \overset{\mathbf{35}}{=} & 0 & 7 & 14 & 15 & 22 & 29 & 30 & 2 & 9 & 10 & 17 & 24 & 25 & 32 & 4 & 5 & 12 & 19 & 20 & 27 & 34 \\
\boldsymbol{y} \overset{\mathbf{7}}{=} & 0 & 0 & 0 & 6 & 6 & 6 & 6 & 6 & 6 & 1 & 1 & 1 & 6 & 6 & 6 & 1 & 1 & 1 & 1 & 1 & 1 \\
\boldsymbol{y} \overset{\mathbf{5}}{=} & 0 & 1 & 3 & 0 & 1 & 3 & 0 & 1 & 3 & 0 & 1 & 3 & 0 & 1 & 3 & 0 & 1 & 3 & 0 & 1 & 3 \\
\boldsymbol{y} \overset{\mathbf{35}}{=} & 0 & 21 & 28 & 20 & 6 & 13 & 20 & 6 & 13 & 15 & 1 & 8 & 20 & 6 & 13 & 15 & 1 & 8 & 15 & 1 & 8
\end{array}
$$

So, these are the solutions of the given system, i.e. $(x, y) \overset{35}{=} (0, 0), (7, 21), \ldots, (34, 8)$. Also see part (b) of Problem 3 of § 18.3.

5. Comment on the contents and results of the present subsection.
Solution: We can claim that our investigation in the present subsection is essentially a generalization (or extension) to the Chinese remainder theorem from univariate to multivariate systems of congruence equations. Now, if we look back to Problem 3 of § 9.2.2 we can say: so far we essentially made three main generalizations (or extensions) to the Chinese remainder theorem:
• The extension of lifting the restriction of linearity.[79]
• The extension of lifting the restriction of coprimality of moduli.
• The extension of lifting the restriction of univariability.
So in brief, we can now solve (with the help of the humble Chinese remainder theorem and similar methods) non-linear systems or/and with non-coprime moduli (subject to the conditions given earlier) or/and with multiple variables.

[79] In fact, this extension is not limited to what we did in Problem 1 of § 9.2.2 (and its alike), but it should include what we did in the present subsection with regard to solving non-linear systems of various types.

Chapter 10
Common Functions

1. Find all $n \in \mathbb{N}$ such that $\sigma(n) = 960$ and $\tau(n) = 4$.
   Solution: Let the second and third divisors of n be a and b (respectively). Hence, $n = ab$ and we have

$$1 + a + b + ab = 960 \qquad \rightarrow \qquad b = \frac{959 - a}{1 + a}$$

   Now, if we note that $1 < a < \sqrt{960} \simeq 30.98$ and a and b must be primes (noting that $1+p+p^2+p^3 = 960$ has no solution) then on trying the primes $a = 2, 3, 5, \ldots, 29$ accepting only the corresponding primes of b we obtain only 4 legitimate values of b (i.e. $b = 239, 79, 47, 31$ corresponding to $a = 3, 11, 19, 29$). The corresponding values of n are: 717, 869, 893, 899. So, these 4 values represent all $n \in \mathbb{N}$ such that $\sigma(n) = 960$ and $\tau(n) = 4$.
2. Solve the following "Diophantine" equations (where $x, y, z \in \mathbb{N}$):
   (**a**) $\phi(2^x 13^y 19^z) = 216$. (**b**) $\phi(2^x 3^y 5^z 7^w) = 4032$.
   Solution:
   (**a**) We have (see Eq. 44 in V1):

$$216 = \phi(2^x 13^y 19^z) = 2^x 13^y 19^z \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{13}\right)\left(1 - \frac{1}{19}\right) = 2^x 13^y 19^z \frac{108}{247}$$

   Hence:

$$2^x 13^y 19^z \tfrac{108}{247} = 216 \qquad \rightarrow \qquad 2^x 13^y 19^z = \tfrac{247}{108} \times 216 = 494 = 2^1 \times 13^1 \times 19^1$$

   So, the solution is $(x, y, z) = (1, 1, 1)$, i.e. $\phi(494) = 216$.
   (**b**) We have (see Eq. 44 in V1):

$$4032 = \phi(2^x 3^y 5^z 7^w) = 2^x 3^y 5^z 7^w \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 2^x 3^y 5^z 7^w \frac{8}{35}$$

   Hence:

$$2^x 3^y 5^z 7^w \tfrac{8}{35} = 4032 \qquad \rightarrow \qquad 2^x 3^y 5^z 7^w = \tfrac{35}{8} \times 4032 = 17640 = 2^3 \times 3^2 \times 5^1 \times 7^2$$

   So, the solution is $(x, y, z, w) = (3, 2, 1, 2)$, i.e. $\phi(17640) = 4032$.
3. Find a formula for $\phi(n^m)$ in terms of n, m and $\phi(n)$ where $m, n \in \mathbb{N}$.
   Solution: From Eq. 44 in V1 (with n replaced by n^m) we have:

$$\phi(n^m) = n^m \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) = n^{m-1}\left[n \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)\right] = n^{m-1}\phi(n)$$

4. Show that $\phi(m)\,\phi(n) = \phi(g)\,\phi(l)$ where $m, n \in \mathbb{N}$, $g = \gcd(m, n)$ and $l = \text{lcm}(m, n)$.
   Solution: This can be obtained by comparing Eq. 46 in V1 to Eq. 47 in V1.
5. Find the number of integers between 1 and 1000 (inclusive) which are divisible neither by 2 nor by 5?
   Solution: We note that $1000 = 10^3 = (2 \times 5)^3 = 2^3 \times 5^3$. So, if a number between 1 and 1000 is not divisible by 2 and 5 then it must be coprime to 1000. This means that we want to find the number of integers between 1 and 1000 which are coprime to 1000. In fact, this is the same as $\phi(1000)$ since by definition $\phi(n)$ is the number of positive integers which are less than or equal to n and are relatively prime to n. Thus, the number of integers between 1 and 1000 which are divisible neither by 2 nor by 5 is $\phi(1000) = 400$.

Note: a different approach (for solving this problem and its alike) is to argue as follows: we have 500 integers (between 1 and 1000) which are divisible by 2, and 200 integers which are divisible by 5 and hence we have $500 + 200 = 700$ integers which are divisible by 2 or/and 5. However, we have 100 integers (i.e. the multiples of 10) which are divisible by both 2 and 5 and hence they are counted twice. So, (by the rules of cardinality of sets) we have $700 - 100 = 600$ integers which are divisible by 2 or 5. Therefore, we must have $1000 - 600 = 400$ integers which are divisible neither by 2 nor by 5 (noting that "integers divisible neither by 2 nor by 5" is the complement of "integers divisible by 2 or 5").

6. A natural number n is called abundant if $\sigma(n) > 2n$ $\big[$or equivalently $s(n) > n\big]$. Show the following:
(**a**) n is abundant when $n = 2^{k-1}(2^k - 1)$ where $(2^k - 1)$ is composite and $k \in \mathbb{N}$.
(**b**) There are infinitely many abundant numbers.
(**c**) There are infinitely many even abundant numbers.
(**d**) Natural multiples of abundant numbers are also abundant.
(**e**) Natural multiples (> 1) of perfect numbers are abundant.
Solution:
(**a**) 2^{k-1} is a natural power of 2 (noting that $2^k - 1$ is composite) and $(2^k - 1)$ is odd and hence they are coprime (since they have no common factor). Hence:

$$\sigma(n) = \sigma\left[2^{k-1}(2^k - 1)\right] = \sigma(2^{k-1})\,\sigma(2^k - 1) = (2^k - 1)\,\sigma(2^k - 1) \tag{37}$$

where we used the multiplicativity of the divisor function in step 2 and used Eq. 34 of V1 in step 3. Now, since $(2^k - 1)$ is composite then it must have at least three positive divisors, i.e. 1 and itself as well as another positive divisor. Accordingly, $\sigma(2^k - 1) > 2^k$ and hence from Eq. 37 we get:

$$\sigma(n) = (2^k - 1)\,\sigma(2^k - 1) > (2^k - 1)\,2^k = 2\left[2^{k-1}(2^k - 1)\right] = 2n$$

(**b**) This is implied by part (c).
(**c**) The proof of part (a) should be sufficient noting that we have infinitely many numbers $n = 2^{k-1}(2^k - 1)$ where $(2^k - 1)$ is composite, e.g. when k is even greater than 2 (i.e. $k = 2\kappa$ where $\kappa > 1$) since $2^k - 1 = (2^\kappa - 1)(2^\kappa + 1)$. However, let us prove it in a different way. So, let $n = 2^k p$ where $\mathbb{N} \ni k > 1$ and p is an odd prime. It is obvious that 2^k and p are coprime and hence:

$$\begin{aligned}\sigma(n) &= \sigma(2^k)\,\sigma(p) = (2^{k+1} - 1)(p + 1) = 2^{k+1}(p + 1) - (p + 1) = 2^{k+1}p + 2^{k+1} - (p + 1)\\ &= 2(2^k p) + 2^{k+1} - (p + 1) = 2n + 2^{k+1} - (p + 1)\end{aligned}$$

Now, for any p we have some k such that $\left[2^{k+1} - (p + 1)\right] > 0$ and hence $\sigma(n) > 2n$. This means that we have infinitely many even numbers $n = 2^k p$ such that $\left[2^{k+1} - (p + 1)\right] > 0$ and hence we have infinitely many even abundant numbers. This proof also shows that the smallest even (and actually the smallest unconditionally) abundant number is 12 (which is obvious by inspecting the divisor function of the small natural numbers).
(**d**) Let n be an abundant number and kn is its natural multiple (i.e. $k \in \mathbb{N}$). Hence, we have:

$$\sigma(kn) \geq \sum_{d|n} kd$$

This is because[80] the set S representing the divisors of kn are the divisors of k and the divisors of n as well as the (product) combinations of these divisors, while the set s representing kd (where d is a divisor of n) is just a subset (whether proper or improper) of S, and hence $\sigma(kn)$ cannot be smaller than $\sum_{d|n} kd$. Accordingly:

$$\sigma(kn) \geq \left(\sum_{d|n} kd\right) = \left(k\sum_{d|n} d\right) = k\,\sigma(n) > k\,2n = 2(kn)$$

[80] Although this argument is not rigorous, it should be convincing.

i.e. kn (which is the natural multiple of n) is abundant (like n itself).
(**e**) Let n be a perfect number and kn is its natural multiple > 1 (i.e. $\mathbb{N} \ni k > 1$). Hence, we have:

$$\sigma(kn) > \left(\sum_{d|n} kd\right) = \left(k \sum_{d|n} d\right) = k\,\sigma(n) = k\,2n = 2(kn)$$

where the justification of $>$ is similar to what is given in part (d) noting that in this case $k > 1$.

7. Show that n is prime *iff* $\phi(n) = n - 1$.
Solution: If $\phi(n) = n - 1$ then all positive integers $< n$ are coprime to n and hence n must be prime (because this means that the only divisor of n among the positive integers which are less than n is 1). If n is prime then all positive integers $< n$ are coprime to n (since none of these integers, except 1, can divide n) and hence $\phi(n) = n - 1$ (as required by the definition of ϕ).
8. Show that n is composite *iff* $\phi(n) < (n - 1)$.
Solution: If we note that for all $n > 1$ we have $\phi(n) \leq (n - 1)$ (see point 7 in the preamble of § 2.6.4 of V1), then the proposition of the present Problem is essentially the contrapositive of the proposition of Problem 7.
9. Impose a lower and upper bound on $\phi(n)$ where $n \in \mathbb{N}$.
Solution: The lower bound is obviously 1 while the upper bound is $n - 1$ (see Problems 7 and 8), i.e. $1 \leq \phi(n) \leq (n - 1)$.
10. Find all $n \in \mathbb{N}$ such that (noting that $1 = d_1 < d_2 < \ldots < d_\tau = n$):
(**a**) n has $\tau = 9$ (positive) divisors with $d_5 - d_3 = 22$ and $d_8 - d_5 = 312$.
(**b**) n has $\tau = 24$ (positive) divisors with $d_2 + d_3 + d_4 + d_5 = 15$ and $d_{20} + d_{21} + d_{22} + d_{23} = 1080$.
(**c**) n has $\tau = 3$ (positive) divisors.
(**d**) n has $\tau = 5$ (positive) divisors and $s(n) = n$.
(**e**) n has $\tau = 10$ (positive) divisors and $\sigma(n) < 200$.
Solution:
(**a**) n must be a perfect square and hence $n = d_5^2$ (see Problem 18 of § 1.9 of V1 and Problem 3 of § 2.6.3 of V1). Now, we have two possibilities:
• If n is even then d_2 must be 2 and hence d_3 must be either 3 or 4 (noting that 4 must be a divisor since n is an even perfect square and hence it must have a factor of 2^2). However, $d_3 = 3$ is not a possibility because in this case $d_5 = 25$ and $d_8 = 337$ and hence $n = d_5^2 = 625$ which is not divisible by 337. So, we must have $d_3 = 4$ and hence $d_5 = 26$ and $d_8 = 338$ which is consistent with $n = d_5^2 = 26^2 = 676$ (noting that the divisors of 676 are 1, 2, 4, 13, 26, 52, 169, 338, 676). This means that $n = 676$ is a solution (and indeed the only possible solution if n is even because d_3 is fixed).
• If n is odd then d_2 must be an odd prime. This is because 2 (and its multiples) is not a possibility for d_2 since n is odd; moreover d_2^2 must also be a divisor since n is a perfect square. Now, if we note that $d_5^2 = d_2 d_8$ then we must conclude that d_2 divides d_5 and hence d_2 must also divide d_8. So, we have:

$$d_8 - d_5 = 312 \qquad \rightarrow \qquad d_2(\delta_8 - \delta_5) = 312 \qquad\qquad (d_8 = d_2\delta_8 \text{ and } d_5 = d_2\delta_5)$$

This means that d_2 divides 312. Now, the only odd prime divisors of 312 are 3 and 13. So:
If $d_2 = 3$ then $d_2^2 = 9$ must also be a divisor of n. Now, since $d_2^2 = 9$ is a divisor then d_3 can only be 5 or 7 or 9. However, none of these possibilities produce consistent results.[81]
If $d_2 = 13$ then $d_2^2 = 169$ must also be a divisor of n since n is a perfect square. Now, since $d_2^2 = 169$ is a divisor then d_3 can only be one of the primes between 17 and 167 (inclusive) or 169. However, none of these possibilities produce consistent results.[82]
So, we conclude that the only solution to this problem is $n = 676$.

[81] $d_3 = 5, 7, 9$ lead (noting that $d_5 - d_3 = 22$ and $n = d_5^2$) to $n = 729, 841, 961$. Now, the number of divisors of $729, 841, 961$ is $7, 3, 3$ and hence they are not acceptable.
[82] If we follow a similar procedure to the one outlined in the previous footnote then we will find that all these possibilities of n (except $n = 1521, 4225$ corresponding to $d_3 = 17, 43$ and $d_5 = 39, 65$) are not divisible by 169. Regarding 1521, its d_2 is 3. Regarding 4225, its d_2 is 5.

(**b**) From the relation $d_2 + d_3 + d_4 + d_5 = 15$ (noting that $1 < d_2 < d_3 < d_4 < d_5$) we conclude that $d_2 = 2$, $d_3 = 3$ and $d_4 = 4$ (because otherwise $d_2 + d_3 + d_4 + d_5 > 15$), and hence d_5 must be 6. We must also have:

$$n = d_2 d_{23} = d_3 d_{22} = d_4 d_{21} = d_5 d_{20} \qquad \text{i.e.} \qquad n = 2d_{23} = 3d_{22} = 4d_{21} = 6d_{20}$$

Now, if we substitute from these relations into the relation $d_{20} + d_{21} + d_{22} + d_{23} = 1080$ we get:

$$\frac{n}{6} + \frac{n}{4} + \frac{n}{3} + \frac{n}{2} = 1080 \qquad \rightarrow \qquad n = 864$$

So, $n = 864$ is the required (and the only) solution to this problem.
(**c**) This applies to all squares of primes (e.g. 4, 9, 25) since their divisors are only 1, p and p^2 (where $p \in \mathbb{P}$; see part e of Problem 13 of § 2).
(**d**) $\tau = 5$ means n is a perfect square (see Problem 18 of § 1.9 of V1 and Problem 3 of § 2.6.3 of V1), while $s(n) = n$ means n is a perfect number (see § 2.8 of V1). These conditions are incompatible because no perfect number is a perfect square (see Problem 7 of § 2.8 of V1). Hence, there is no such n.
(**e**) $\sigma(n) < 200$ means $n < 200$. On inspecting the natural numbers which are less than 200 (using for instance tables of divisors) we find that only 48 and 80 satisfy the given conditions (noting that although 112, 162 and 176 satisfy $\tau = 10$ they do not satisfy $\sigma < 200$).

11. Justify why $\phi(n) \neq 391,454$ for any $n \in \mathbb{N}$.
Solution: $\phi(n) \neq 391$ because the totient function is even for all integers greater than 2.
Regarding $\phi(n) \neq 454$, we have three (comprehensive) cases:
• n is prime and $\phi(n) = 454$. This is impossible because 455 is not prime (see Problem 7).
• n is a natural power (> 1) of prime and $\phi(n) = 454$. This is also impossible because there is no $p \in \mathbb{P}$ and $a \in \mathbb{N}$ that satisfy $454 = p^a - p^{a-1}$ (see Eq. 42 in V1).
• n is composite (but not a natural power of prime) and $\phi(n) = 454$. This is also impossible because the prime factorization of 454 is 2×227, and this means that $227 = (p^a - p^{a-1})$ for some $p \in \mathbb{P}$ and $a \in \mathbb{N}$ (see Eq. 43 in V1). However, there is no such p and a that satisfy this equation because 227 is odd while $(p^a - p^{a-1})$ is even (noting that $p = 2$ and $a = 1$ is not a possibility).
So, in each one of the three comprehensive cases we have $\phi(n) \neq 454$ and hence $\phi(n) \neq 454$ for any $n \in \mathbb{N}$.

12. Find all $n \in \mathbb{N}$ such that $\phi(n)$ divides $(n-1)$.
Solution: We have three cases:
• $n = 1$ and hence $\phi(n) = 1$ which divides $n - 1 = 0$.
• n is prime and hence $\phi(n) = n - 1$ which divides $n - 1$.
• n is composite. This is an open problem known as Lehmer's totient problem (and hence it deserves the attention of young mathematicians). No composite n is known such that $\phi(n)$ divides $(n-1)$.
So in brief, $\phi(n)$ divides $(n-1)$ for $n = 1$ and for all $n \in \mathbb{P}$; moreover it is believed (according to Lehmer's totient conjecture) that there is no composite n with this property.

13. Find all $n \in \mathbb{N}$ such that (noting that $m \in \mathbb{N}$):
(**a**) $\phi(2n) = \phi(n)$. (**b**) $\phi(2n) = 2\phi(n)$. (**c**) $\phi(2^m n) = 2^{m-1}\phi(n)$. (**d**) $\phi(2^m n) = 2^m \phi(n)$.
Solution:
(**a**) This applies to all odd n because if n is odd then 2 and n are coprime and hence:

$$\phi(2n) = \phi(2)\,\phi(n) = 1 \times \phi(n) = \phi(n)$$

(**b**) This applies to all even n because if n is even then $n = 2^k \nu$ (where $k \in \mathbb{N}$ and ν is odd) and hence:

$$\begin{aligned} \phi(2n) &= \phi(2^{k+1}\nu) = \phi(2^{k+1})\,\phi(\nu) = (2^{k+1} - 2^k)\,\phi(\nu) = 2\,(2^k - 2^{k-1})\,\phi(\nu) \\ &= 2\,\phi(2^k)\,\phi(\nu) = 2\,\phi(2^k\nu) = 2\,\phi(n) \end{aligned}$$

(**c**) This applies to all odd n because if n is odd then 2^m and n are coprime and hence:

$$\phi(2^m n) = \phi(2^m)\phi(n) = (2^m - 2^{m-1})\,\phi(n) = 2^{m-1}(2-1)\,\phi(n) = 2^{m-1}\phi(n)$$

It is obvious that part (a) is an instance of this identity (corresponding to $m = 1$).
(**d**) This applies to all even n because if n is even then $n = 2^k\nu$ (where $k \in \mathbb{N}$ and ν is odd) and hence:

$$\begin{aligned}\phi(2^m n) &= \phi(2^{m+k}\nu) = \phi(2^{m+k})\,\phi(\nu) = (2^{m+k} - 2^{m+k-1})\,\phi(\nu) = 2^m\,(2^k - 2^{k-1})\,\phi(\nu) \\ &= 2^m\,\phi(2^k)\,\phi(\nu) = 2^m\,\phi(2^k\nu) = 2^m\,\phi(n)\end{aligned}$$

It is obvious that part (b) is an instance of this identity (corresponding to $m = 1$).

14. Calculate $\mu(453627^{21998})$, $\mu(4662!)$, $\mu(\widehat{13})$, and $\mu(6280786)$.
Solution: 453627^{21998}, $4662!$, and $\widehat{13}$ are obviously not square free and hence their Mobius function is 0. Regarding $\mu(6280786)$ we have: $6280786 = 2 \times 17 \times 31 \times 59 \times 101$ and hence $\mu(6280786) = (-1)^5 = -1$.
15. Define the "summatory function" with some examples.
Solution: The summatory function $F(n)$ of an arithmetic function $f(d)$ is defined as:

$$F(n) = \sum_{d \le n} f(d)$$

where d is a positive divisor of n.[83] For example, the divisor function $\sigma(n)$ is the summatory function of $f(d) = d$ because (see Eq. 33 in V1):

$$\sigma(n) = \sum_{d \le n} f(d) = \sum_{d|n} d$$

Similarly, the tau function $\tau(n)$ is the summatory function of $f(d) = 1$ because (see Eq. 37 in V1):

$$\tau(n) = \sum_{d \le n} f(d) = \sum_{d|n} 1$$

16. Show that if f is a multiplicative function, then its summatory function F is also multiplicative.
Solution: Let $n_1, n_2 \in \mathbb{N}$ be coprime and hence (according to the definition of summatory function which was given in Problem 15) we have:

$$F(n_1 n_2) = \sum_{d|(n_1 n_2)} f(d) \tag{38}$$

Now, since n_1 and n_2 are coprime then each divisor (i.e. d) of their product can be written as $d = d_1 d_2$ where d_1 and d_2 are coprime. Accordingly, Eq. 38 can be written as:

$$\begin{aligned}F(n_1 n_2) &= \sum_{d|(n_1 n_2)} f(d) = \sum_{d_1|n_1,\, d_2|n_2} f(d_1 d_2) = \sum_{d_1|n_1,\, d_2|n_2} f(d_1)\, f(d_2) \\ &= \left[\sum_{d_1|n_1} f(d_1)\right]\left[\sum_{d_2|n_2} f(d_2)\right] = F(n_1)\, F(n_2)\end{aligned}$$

Note: the result of this Problem may be used to prove that $\sigma(n)$ and $\tau(n)$ are multiplicative because:
• $\sigma(n)$ is the summatory function of $f(d) = d$ (i.e. the identity function) and hence:

$$f(mn) = mn = f(m)\, f(n)$$

i.e. f is a completely multiplicative function[84] (and hence it is multiplicative).
• $\tau(n)$ is the summatory function of $f(d) = 1$ (i.e. the unity function) and hence:

$$f(mn) = 1 = 1 \times 1 = f(m)\, f(n)$$

i.e. f is a completely multiplicative function (and hence it is multiplicative).

[83] This definition (which should be "sufficient and necessary" to us for the time being) is rather limited. Therefore, the readers should be careful about the terminology used in the literature in this regard where the domain of f (and hence the "summatory function" F) could vary. These issues should be elaborated and clarified further in the future.
[84] A "completely multiplicative function" f means: $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$ (i.e. regardless of m, n being coprime or not).

17. Show that the summatory function of the totient function is n, i.e.

$$\sum_{d|n} \phi(d) = n$$

Solution: This was shown in Problem 1 of § 2.6.4 of V1.

18. Show that the summatory function of the Mobius function is 0, i.e.

$$\sum_{d|n} \mu(d) = 0 \qquad (n > 1)$$

Solution: This was shown in Problem 3 of § 2.6.5 of V1.

Chapter 11
Interesting Theorems

Despite the importance of the subject of this chapter (i.e. "interesting theorems"), we decided to make it short and brief. The main reason is that most of these "interesting theorems" can be found and met in many places and within many contexts in this book (as well as in the general literature of number theory) since they represent some of the most common principles and foundations of elementary number theory. In fact, the applications of these "interesting theorems" are very broad and abundant and this makes dedicating a chapter (or section or part) of any book to them is a matter of formality and organized structure.

11.1 Wilson's Theorem

1. Use Wilson's theorem to find r:

   (**a**) $2727! \overset{2731}{=} r$. (**b**) $37! \overset{1763}{=} r$.

   Solution:[85]

   (**a**) We note that 2731 is prime. We have:

   $2727! \overset{2731}{=} r \quad \rightarrow \quad 2730! \overset{2731}{=} (2728)(2729)(2730)\,r \quad \rightarrow \quad (2731-1)! \overset{2731}{=} 20324063760\,r \quad \rightarrow$

   $-1 \overset{2731}{=} 2725\,r \quad \rightarrow \quad r \overset{2731}{=} (-1)2725^{*} \quad \rightarrow \quad r \overset{2731}{=} -455 \overset{2731}{=} 2276$

   (**b**) We note that $1763 = 41 \times 43$. Now, we have:

   $37! \overset{41}{=} r \quad \rightarrow \quad 40! \overset{41}{=} (38)(39)(40)\,r \quad \rightarrow \quad -1 \overset{41}{=} 59280\,r \quad \rightarrow \quad r \overset{41}{=} 7$

   $37! \overset{43}{=} r \quad \rightarrow \quad 42! \overset{43}{=} (38)(39)(40)(41)(42)\,r \quad \rightarrow \quad -1 \overset{43}{=} 102080160\,r \quad \rightarrow \quad r \overset{43}{=} 19$

   So, we have the following system of linear congruence equations: $r \overset{41}{=} 7$ and $r \overset{43}{=} 19$. On solving this system (e.g. by the Chinese remainder theorem) we get $r \overset{1763}{=} 1524$.

2. Show that (where $k \in \mathbb{N}$):

$$\big[1 \times 3 \times \cdots \times (p-2)\big]^2 \overset{p}{=} \begin{cases} -1 & (\text{when } p = 4k+1) \\ +1 & (\text{when } p = 4k-1) \end{cases}$$

   Solution: By Wilson's theorem we have:

$$\begin{aligned} -1 &\overset{p}{=} (p-1)! = 1 \times 2 \times 3 \times \cdots \times (p-3) \times (p-2) \times (p-1) \\ &\overset{p}{=} 1 \times \big[-(p-2)\big] \times 3 \times \cdots \times (-3) \times (p-2) \times (-1) \\ &= (-1)^{(p-1)/2}\big[1 \times (p-2)\big] \times 3 \times \cdots \times (3) \times (p-2) \times (1)\big] \\ &= (-1)^{(p-1)/2}\big[1 \times 3 \times \cdots \times (p-2)\big]^2 \end{aligned}$$

   Now, if $p = 4k+1$ then $(p-1)/2 = 2k$ and hence we have $(-1)^{2k}\big[1 \times 3 \times \cdots \times (p-2)\big]^2 \overset{p}{=} -1$, i.e. $\big[1 \times 3 \times \cdots \times (p-2)\big]^2 \overset{p}{=} -1$. On the other hand, if $p = 4k-1$ then $(p-1)/2 = 2k-1$ and hence we have $(-1)^{2k-1}\big[1 \times 3 \times \cdots \times (p-2)\big]^2 \overset{p}{=} -1$, i.e. $\big[1 \times 3 \times \cdots \times (p-2)\big]^2 \overset{p}{=} +1$.

[85] The code CongLargeFactorial.cpp (see Problem 3 of § 18.1) can be used to verify the results of this Problem. We should also note that r in these Problems represents the least non-negative residue of the given congruences.

3. Show that (where $k \in \mathbb{N}$):

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \overset{p}{=} \begin{cases} -1 & (\text{when } p = 4k+1) \\ +1 & (\text{when } p = 4k-1) \end{cases}$$

Solution: In Problem 3 of § 2.9.1 of V1 we proved (by using Wilson's theorem) that $(q!)^2 + (-1)^q$ is divisible by $p \in \mathbb{P}$ where $p = 2q+1$, i.e.

$$(q!)^2 + (-1)^q \overset{p}{=} 0 \qquad \rightarrow \qquad (q!)^2 \overset{p}{=} -(-1)^q \qquad \rightarrow \qquad (q!)^2 \overset{p}{=} (-1)^{q+1}$$

Now, if $p = 4k+1$ then $q \equiv \frac{p-1}{2}$ is even (i.e. $q = 2k$) and hence:

$$(q!)^2 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \overset{p}{=} (-1)^{q+1} = (-1)^{2k+1} = -1$$

while if $p = 4k-1$ then $q \equiv \frac{p-1}{2}$ is odd (i.e. $q = 2k-1$) and hence:

$$(q!)^2 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \overset{p}{=} (-1)^{q+1} = (-1)^{2k-1+1} = (-1)^{2k} = +1$$

11.2 Euler's Theorem

1. Show that for all $n \in \mathbb{N}$ we have $n | \phi(2^n - 1)$.
Solution: According to Euler's theorem we have:

$$2^{\phi(2^n-1)} \overset{2^n-1}{=} 1 \qquad \rightarrow \qquad (2^n-1) \Big| \left(2^{\phi(2^n-1)} - 1\right)$$

Hence, from Problem 6 of § 6.7 of V1 we get $n | \phi(2^n - 1)$.

2. Use Euler's theorem to find r:
(**a**) $33^{3061} \overset{1019}{=} r$. (**b**) $97^{15705} \overset{5237}{=} r$.
Solution:[86]
(**a**) We have:

$$33^{3061} \overset{1019}{=} r \qquad \rightarrow \qquad \left(33^{1018}\right)^3 33^7 \overset{1019}{=} r \qquad \rightarrow \qquad 1^3\, 33^7 \overset{1019}{=} r \qquad \rightarrow \qquad r \overset{1019}{=} 967$$

(**b**) We have:

$$97^{15705} \overset{5237}{=} r \qquad \rightarrow \qquad 97^{15708} \overset{5237}{=} 97^3\, r \qquad \rightarrow \qquad \left(97^{5236}\right)^3 \overset{5237}{=} 97^3\, r \qquad \rightarrow$$

$$1^3 \overset{5237}{=} 97^3\, r \qquad \rightarrow \qquad r \overset{5237}{=} \left(97^3\right)^* \qquad \rightarrow \qquad r \overset{5237}{=} 354$$

3. Prove the following (where $x \in \mathbb{Z}$ and $p, q \in \mathbb{P}$ with $p \neq q$):
(**a**) $x^{(p-1)(q-1)} \overset{pq}{=} 1$ (x and pq are coprime). (**b**) $x^{p^2-p} \overset{p^2}{=} 1$ (x and p^2 are coprime).
Solution:
(**a, b**) These congruences are just instances of Euler's theorem noting that $\phi(pq) = (p-1)(q-1)$ and $\phi(p^2) = p^2 - p$ (see § 2.6.4 and § 2.9.2 of V1).

11.3 Fermat's Little Theorem

1. Let $x \in \mathbb{Z}$ and p be an odd prime. Show that the congruence equation $x^2 + 1 \overset{p}{=} 0$ has a solution *iff* $p = 4k+1$.
Solution: We note first that $x^2 + 1 \overset{p}{=} 0$ is equivalent to $x^2 \overset{p}{=} -1$.
Regarding **the if part**, it is obvious (from Problem 3 of § 11.1) that this congruence has a solution

[86] The code CongLargeExponential.cpp (see Problem 4 of § 18.1) can be used to verify the results of this Problem.

$\left[\text{i.e. } x = \left(\frac{p-1}{2}\right)!\right]$ when $p = 4k+1$.

Regarding **the only if part**, let assume that $x^2+1 \overset{p}{=} 0$ has a solution with $p \neq 4k+1$ (i.e. $p = 4k-1$). This implies that x and p are coprime (because otherwise we will have $0+1 \overset{p}{=} 0$). So, by Fermat's little theorem we have:

$$x^{p-1} \overset{p}{=} 1 \quad \rightarrow \quad x^{4k-1-1} \overset{p}{=} 1 \quad \rightarrow \quad x^{4k-2} \overset{p}{=} 1 \quad \rightarrow \quad \left(x^2\right)^{2k-1} \overset{p}{=} 1 \quad \rightarrow \quad (-1)^{2k-1} \overset{p}{=} 1$$

i.e. $-1 \overset{p}{=} 1$ which is nonsensical noting that p is an odd prime. So, this contradiction implies (by contraposition) that $x^2+1 \overset{p}{=} 0$ has no solution when $p \neq 4k+1$.

2. Show that the congruence $x^{45} \overset{30}{=} x$ is true identically (i.e. it is satisfied by all $x \in \mathbb{Z}$).

Solution: We note that $30 = 2 \times 3 \times 5$. So, we need to show that $x^{45} \overset{2}{=} x$, $x^{45} \overset{3}{=} x$ and $x^{45} \overset{5}{=} x$ are true identically.

Regarding $x^{45} \overset{2}{=} x$, this congruence is equivalent to $x^{45} - x \overset{2}{=} 0$ which is true identically because the LHS is always even.

Regarding $x^{45} \overset{3}{=} x$, we use Fermat's little theorem (repeatedly), that is:

$$x^{45} = \left(x^3\right)^{15} \overset{3}{=} x^{15} = \left(x^3\right)^5 \overset{3}{=} x^5 = \left(x^3\right)^2 x^{-1} \overset{3}{=} x^2 x^{-1} = x$$

Similarly:

$$x^{45} = \left(x^5\right)^9 \overset{5}{=} x^9 = \left(x^5\right)^2 x^{-1} \overset{5}{=} x^2 x^{-1} = x$$

So, $x^{45} \overset{2}{=} x$, $x^{45} \overset{3}{=} x$ and $x^{45} \overset{5}{=} x$ are true identically and hence $x^{45} \overset{30}{=} x$ is true identically.

3. Use Fermat's little theorem to find r:

(**a**) $17^{2804} \overset{401}{=} r$. (**b**) $13^{2455} \overset{2703}{=} r$.

Solution:

(**a**) We have:

$$r \overset{401}{=} 17^{2804} = \left(17^{401}\right)^7 17^{-3} \overset{401}{=} 17^7 \times 17^{-3} = 17^4 \overset{401}{=} 113$$

(**b**) We note that $2703 = 3 \times 17 \times 53$. Now, we have:

$$r \overset{3}{=} 13^{2455} \overset{3}{=} 1^{2455} = 1$$

$$r \overset{17}{=} 13^{2455} = \left(13^{17}\right)^{144} 13^7 \overset{17}{=} 13^{144} \times 13^7 = 13^{151} = \left(13^{17}\right)^9 13^{-2} \overset{17}{=} 13^9 \times 13^{-2} = 13^7 \overset{17}{=} 4$$

$$r \overset{53}{=} 13^{2455} = \left(13^{53}\right)^{47} 13^{-36} \overset{53}{=} 13^{47} \times 13^{-36} = 13^{11} \overset{53}{=} 16$$

So, we have the following system of linear congruence equations: $r \overset{3}{=} 1$, $r \overset{17}{=} 4$ and $r \overset{53}{=} 16$. On solving this system (e.g. by the Chinese remainder theorem) we get $r \overset{2703}{=} 2401$.

11.4 Lagrange's Polynomial Roots Theorem

1. Show that the polynomial congruence equation $x^{49} - 3x^{26} + 2 \overset{13}{=} 0$ (where $x \in \mathbb{Z}$) cannot have more than two roots.

Solution: By Fermat's little theorem we have:

$$x^{49} - 3x^{26} + 2 = \left(x^{13}\right)^4 x^{-3} - 3\left(x^{13}\right)^2 + 2 \overset{13}{=} x^4 x^{-3} - 3x^2 + 2 = x - 3x^2 + 2 \overset{13}{=} 10x^2 + x + 2 \overset{13}{=} 0$$

So, what we actually have is a quadratic congruence equation (i.e. $10x^2 + x + 2 \overset{13}{=} 0$) and hence by Lagrange's polynomial roots theorem it has at most two roots.

2. Despite the fact that 17 is prime, the quadratic congruence equation $102x^2+68x+136 \overset{17}{=} 0$ is identically true, i.e. it has 17 (modular) solutions. Can you explain this "contradiction" to Lagrange's polynomial roots theorem which (seemingly) requires that this quadratic congruence equation should have at most two roots.

Solution: If we inspect the coefficients (i.e. 102, 68, 136) we find that all of them are divisible by 17 and hence what we actually have is not an n degree polynomial (i.e. quadratic) congruence but a "zero

polynomial" congruence (i.e. $0 \overset{17}{=} 0$) which is always true regardless of the value of x.

11.5 Other Theorems

1. Show that Fermat's last theorem is true for all $\mathbb{N} \ni n > 2$ if it is true for $n = 4$ and it is true for all $\mathbb{P} \ni n > 2$ (where n is the exponent in the statement of Fermat's last theorem; see § 2.9.5 of V1).
   Solution: From the result of Problem 16 of § 4, every exponent $\mathbb{N} \ni n > 2$ can be written as $n = 4k$ or as $n = pk$ (where p is an odd prime and $k \in \mathbb{N}$). Accordingly, $a^n + b^n = c^n$ (where $a, b, c \in \mathbb{N}$) can be written as $\left(a^k\right)^4 + \left(b^k\right)^4 = \left(c^k\right)^4$ or as $\left(a^k\right)^p + \left(b^k\right)^p = \left(c^k\right)^p$. Now, $a^k, b^k, c^k \in \mathbb{N}$ (since $a, b, c, k \in \mathbb{N}$) and hence if the theorem is true for $n = 4$ and it is true for all $\mathbb{P} \ni n > 2$ then it must be true for all $\mathbb{N} \ni n > 2$.
2. Which of the following integers can be expressed as a sum of two (perfect) squares:
   (**a**) 57. (**b**) 481. (**c**) 1762. (**d**) 11858.
   Solution: We use the well-known two square theorem which states (see § 2.9.5 of V1): a natural number n can be expressed as a sum of two squares *iff* every prime of the form $4k + 3$ occurs an even number of times in the prime factorization of n.
   (**a**) We have $57 = 3^1 \times 19^1$. As we see, both 3 and 19 (which are of the form $4k + 3$) occur an odd number of times in the prime factorization of 57 and hence 57 cannot be expressed as a sum of two squares.
   (**b**) We have $481 = 13 \times 37$. As we see, both 13 and 37 are of the form $4k + 1$ which means that "every prime of the form $4k + 3$ (if exists) occurs an even number of times".[87] So, 481 can be expressed as a sum of two squares, i.e. $481 = 9^2 + 20^2 = 15^2 + 16^2$.
   (**c**) We have $1762 = 2 \times 881$. As in part (b), we have no prime of the form $4k + 3$ in the factorization of 1762 and hence 1762 can be expressed as a sum of two squares, i.e. $1762 = 9^2 + 41^2$.
   (**d**) We have $11858 = 2 \times 7^2 \times 11^2$. As we see, both 7 and 11 (which are of the form $4k + 3$) occur an even number of times in the prime factorization of 11858 and hence 11858 can be expressed as a sum of two squares, i.e. $11858 = 77^2 + 77^2$.
3. Show that no integer of the form $n = 4k + 3$ (where $k \in \mathbb{Z}$) can be expressed as a sum of two (perfect) squares.
   Solution: We simply prove this theorem by showing that no sum of two perfect squares of integers can be of the form $4k + 3$. So, if $n = 4k + 3$ then it must be odd and hence if it is the sum of two squares then it must be the sum of an odd square $\left[\text{say } (2a + 1)^2 \text{ where } a \in \mathbb{Z}\right]$ plus an even square $\left[\text{say } (2b)^2 \text{ where } b \in \mathbb{Z}\right]$. Therefore:

$$(2a + 1)^2 + (2b)^2 = 4a^2 + 4a + 1 + 4b^2 \overset{4}{=} 1 \overset{4}{\neq} 3 \overset{4}{=} 4k + 3 = n$$

   As we see, the sum of two squares is incongruent (mod 4) to $n = 4k+3$ and hence n cannot be expressed as a sum of two squares.
4. Show that no integer of the form $n = 8k + 7$ (where $k \in \mathbb{Z}$) can be expressed as a sum of three (perfect) squares.
   Solution: We simply prove this theorem by showing that no sum of three perfect squares of integers can be of the form $8k + 7$. Now, n is odd and hence it cannot be the sum of three even integers. Also, n cannot be the sum of two odd integers plus an even integer. So, we have only two possibilities:
   • All the three squares are odd $\left[\text{say } (2a + 1)^2, (2b + 1)^2 \text{ and } (2c + 1)^2 \text{ where } a, b, c \in \mathbb{Z}\right]$ and hence:

$$\begin{aligned}(2a + 1)^2 + (2b + 1)^2 + (2c + 1)^2 &= 4(a^2 + a) + 4(b^2 + b) + 4(c^2 + c) + 3 = 8A + 8B + 8C + 3 \\ &\overset{8}{=} 3 \overset{8}{\neq} 7 \overset{8}{=} 8k + 7 = n\end{aligned}$$

[87] In fact, this "interpretation" of the two square theorem dictates an improvement to the phrasing of this theorem (to avoid misunderstanding), that is: "a natural number n can be expressed as a sum of two perfect squares *iff* the prime factorization of n contains no odd power of any prime factor of the form $4k + 3$". This means that n either contains no prime of the form $4k + 3$ or it contains only even (natural) powers of primes of the form $4k + 3$.

where step 2 is because $(a^2 + a)$, $(b^2 + b)$ and $(c^2 + c)$ are all even.
• Two of the squares are even and the third is odd $\left[\text{say } (2a)^2, (2b)^2 \text{ and } (2c+1)^2 \text{ where } a, b, c \in \mathbb{Z}\right]$ and hence:

$$(2a)^2 + (2b)^2 + (2c + 1)^2 = 4a^2 + 4b^2 + 4c^2 + 4c + 1 = 4(a^2 + b^2) + 8C + 1$$

Now:
If a and b are of the same parity then $(a^2 + b^2)$ is even (say $a^2 + b^2 = 2D$) and hence we have:

$$4(a^2 + b^2) + 8C + 1 = 4(2D) + 8C + 1 = 8D + 8C + 1 \overset{8}{=} 1 \overset{8}{\neq} 7 \overset{8}{=} 8k + 7 = n$$

Similarly, if a and b are of opposite parity then $(a^2 + b^2)$ is odd (say $a^2 + b^2 = 2D + 1$) and hence we have:

$$4(a^2 + b^2) + 8C + 1 = 4(2D + 1) + 8C + 1 = 8D + 8C + 5 \overset{8}{=} 5 \overset{8}{\neq} 7 \overset{8}{=} 8k + 7 = n$$

So, in all cases the sum of three squares is incongruent (mod 8) to $n = 8k + 7$ and hence n cannot be expressed as a sum of three squares.

Chapter 12
Floors and Ceilings

1. Solve the following equation (where $x \in \mathbb{Z}$): $\left\lfloor \frac{x^2+2x-1}{7} \right\rfloor = \frac{x^2+2x-1}{7}$.
Solution: The floor of a real number is equal to the number *iff* the number is an integer. So, the given equation is a statement that $(x^2+2x-1)/7$ is an integer, and hence it is equivalent to the congruence equation $x^2+2x-1 \stackrel{7}{=} 0$. Thus, the solutions of the given equation are: $x = 2+7k$ and $x = 3+7k$ (where $k \in \mathbb{Z}$).
2. Solve the following equations (where $x \in \mathbb{R}$):
(**a**) $\lceil 7\lfloor x \rfloor + 12x \rceil = 39$. (**b**) $25\lfloor x \rfloor - 18\lceil x \rceil = 91$. (**c**) $\lceil x^2+12x-4 \rceil = 22$.
Solution:
(**a**) Let $\lfloor x \rfloor = X$ and hence we have $\lceil 7X+12x \rceil = 39$. This means:
$38 < 7X+12x \leq 39 \quad \rightarrow \quad 38-7X < 12x \leq 39-7X \quad \rightarrow \quad \frac{38-7X}{12} < x \leq \frac{39-7X}{12}$
Also, $\lfloor x \rfloor = X$ means $X \leq x < (X+1)$. So, we need to solve the following system of inequalities:
$$\frac{38-7X}{12} < x \leq \frac{39-7X}{12} \qquad \text{and} \qquad X \leq x < (X+1)$$
This system implies:
$\frac{38-7X}{12} < (X+1) \quad \rightarrow \quad (38-7X) < (12X+12) \quad \rightarrow \quad 26 < 19X \quad \rightarrow \quad X > \frac{26}{19}$
$X \leq \frac{39-7X}{12} \quad \rightarrow \quad 12X \leq (39-7X) \quad \rightarrow \quad 19X \leq 39 \quad \rightarrow \quad X \leq \frac{39}{19}$
On combining these results we get $\frac{26}{19} < X \leq \frac{39}{19}$, i.e. $X = 2$ (noting that X is an integer). Now, on substituting this into the equation $\frac{38-7X}{12} < x \leq \frac{39-7X}{12}$ we get $\frac{24}{12} < x \leq \frac{25}{12}$ (i.e. $2 < x \leq \frac{25}{12}$).
(**b**) We have two cases to consider:
• x is an integer and hence $\lfloor x \rfloor = \lceil x \rceil = x$, that is:
$25\lfloor x \rfloor - 18\lceil x \rceil = 91 \quad \rightarrow \quad 25x-18x = 91 \quad \rightarrow \quad 7x = 91 \quad \rightarrow \quad x = 13$
• x is not an integer. Now, if $\lfloor x \rfloor = x_f$ then $\lceil x \rceil = x_f + 1$ and hence:
$25\lfloor x \rfloor - 18\lceil x \rceil = 91 \quad \rightarrow \quad 25x_f - 18(x_f+1) = 91 \quad \rightarrow \quad 7x_f = 109 \quad \rightarrow \quad x_f = \frac{109}{7} \simeq 15.57$
which is nonsensical because x_f is integer.
So, the only solution to $25\lfloor x \rfloor - 18\lceil x \rceil = 91$ is $x = 13$.
(**c**) $\lceil x^2+12x-4 \rceil = 22$ means $21 < x^2+12x-4 \leq 22$. So, we have two inequalities to consider:
• $21 < x^2+12x-4$ and hence:
$25 < x^2+12x \quad \rightarrow \quad 61 < x^2+12x+36 \quad \rightarrow \quad 61 < (x+6)^2$
So, either $-\sqrt{61} > (x+6)$ or $\sqrt{61} < (x+6)$, i.e. $x < -6-\sqrt{61}$ or $x > -6+\sqrt{61}$.
• $x^2+12x-4 \leq 22$ and hence:
$x^2+12x \leq 26 \quad \rightarrow \quad x^2+12x+36 \leq 62 \quad \rightarrow \quad (x+6)^2 \leq 62$
So, $-\sqrt{62} \leq (x+6) \leq \sqrt{62}$, i.e. $-6-\sqrt{62} \leq x \leq -6+\sqrt{62}$.
So, the solution is the intersection of the inequalities:
$$x < -6-\sqrt{61} \qquad x > -6+\sqrt{61} \qquad -6-\sqrt{62} \leq x \leq -6+\sqrt{62}$$
which is:
$$-6-\sqrt{62} \leq x < -6-\sqrt{61} \qquad \text{and} \qquad -6+\sqrt{61} < x \leq -6+\sqrt{62}$$
3. Solve the following equation $\left\lceil \frac{x^3+2x^2-35x+1}{x} \right\rceil = 0$ (where $\mathbb{Z} \ni x \neq 0$).

Solution: We have:

$$\left\lceil \frac{x^3+2x^2-35x+1}{x} \right\rceil = \left\lceil x^2+2x-35+\frac{1}{x} \right\rceil = x^2+2x-35+\left\lceil \frac{1}{x} \right\rceil = 0$$

Now, we have three cases to consider:
• $x < -1$ and hence $\lceil \frac{1}{x} \rceil = 0$. So, we have $x^2+2x-35=0$ whose only solution (noting that $x<-1$) is $x=-7$.
• $x = -1$ and hence $\lceil \frac{1}{x} \rceil = -1$. So, we have $x^2+2x-36=0$ which has no solution.
• $x \geq 1$ and hence $\lceil \frac{1}{x} \rceil = 1$. So, we have $x^2+2x-34=0$ which has no solution.
So, the only solution to the given equation is $x=-7$.

4. Show that $\lfloor \frac{x}{2} \rfloor + \lceil \frac{x}{2} \rceil = x$ for all $x \in \mathbb{Z}$.
Solution: If x is even then we have $\lfloor \frac{x}{2} \rfloor = \lceil \frac{x}{2} \rceil = \frac{x}{2}$ and hence $\lfloor \frac{x}{2} \rfloor + \lceil \frac{x}{2} \rceil = \frac{x}{2}+\frac{x}{2} = x$.
If x is odd then we have $\lfloor \frac{x}{2} \rfloor = \frac{x}{2}-\frac{1}{2}$ and $\lceil \frac{x}{2} \rceil = \frac{x}{2}+\frac{1}{2}$ and hence $\lfloor \frac{x}{2} \rfloor + \lceil \frac{x}{2} \rceil = \frac{x}{2}-\frac{1}{2}+\frac{x}{2}+\frac{1}{2} = x$.

5. Show that the expression $\left\lfloor \frac{x+1}{2} \right\rfloor^2 + 3\left\lceil \frac{x}{2}+2 \right\rceil$ is always even (where $x \in \mathbb{Z}$).
Solution: This is because:
• If x is even (say $x = 2k$ where $k \in \mathbb{Z}$) then we have:

$$\left\lfloor \frac{x+1}{2} \right\rfloor^2 + 3\left\lceil \frac{x}{2}+2 \right\rceil = \left\lfloor \frac{2k+1}{2} \right\rfloor^2 + 3\left\lceil \frac{2k}{2}+2 \right\rceil = \left\lfloor k+\frac{1}{2} \right\rfloor^2 + 3\lceil k+2 \rceil = k^2+3k+6$$

which is even.
• If x is odd (say $x = 2k+1$) then we have:

$$\begin{aligned} \left\lfloor \frac{x+1}{2} \right\rfloor^2 + 3\left\lceil \frac{x}{2}+2 \right\rceil &= \left\lfloor \frac{2k+2}{2} \right\rfloor^2 + 3\left\lceil \frac{2k+1}{2}+2 \right\rceil = \lfloor k+1 \rfloor^2 + 3\left\lceil k+\frac{1}{2}+2 \right\rceil \\ &= (k+1)^2 + 3(k+3) = k^2+2k+1+3k+9 = k^2+5k+10 \end{aligned}$$

which is even.
So, the given expression is even in both cases and hence it is always even.

6. Solve the following equation (where $x \in \mathbb{N}^0$): $\lfloor \frac{x}{2} \rfloor + 4\lceil \frac{x}{3} \rceil = 329$.
Solution: We have six cases to consider (where $k \in \mathbb{N}^0$):
• $x = 6k$ and hence we have $3k+4(2k) = 329$ which has no solution.
• $x = 6k+1$ and hence we have $3k+4(2k+1) = 329$ which has no solution.
• $x = 6k+2$ and hence we have $3k+1+4(2k+1) = 329$ which has no solution.
• $x = 6k+3$ and hence we have $3k+1+4(2k+1) = 329$ which has no solution.
• $x = 6k+4$ and hence we have $3k+2+4(2k+2) = 329$ whose solution is $k=29$ and hence $x=178$.
• $x = 6k+5$ and hence we have $3k+2+4(2k+2) = 329$ whose solution is $k=29$ and hence $x=179$.
So, the only solutions to the given equation are: $x=178$ and $x=179$.

7. Solve the following series equations (where $x \in \mathbb{N}$):
(**a**) $\sum_{k=1}^{x} \lfloor \frac{25}{k} \rfloor = 87$. (**b**) $\sum_{k=1}^{x} \lceil \frac{25}{k} \rceil = 109$.
Solution:
(**a**) We have $\sum_{k=1}^{25} \lfloor \frac{25}{k} \rfloor = 87$. Now, for all $k > 25$ we have $\lfloor \frac{25}{k} \rfloor = 0$, and hence the sum remains 87 for all $x > 25$. So, the solution of the given equation is $x = 25, 26, 27, \ldots$.
(**b**) We have $\sum_{k=1}^{25} \lceil \frac{25}{k} \rceil = 109$. Now, for all $k > 25$ we have $\lceil \frac{25}{k} \rceil = 1$, and hence the sum keeps increasing. So, the solution of the given equation is $x = 25$.

8. Solve the following inequality (where $x \in \mathbb{Z}$): $\left\lfloor \frac{3x^2}{37} \right\rfloor < 5x$.
Solution: If $\left\lfloor \frac{3x^2}{37} \right\rfloor < 5x$ then we must have $\frac{3x^2}{37} < 5x$, i.e. $3x^2 - 185x < 0$. This is because if $\left\lfloor \frac{3x^2}{37} \right\rfloor < 5x$ then $5x$ is greater than $\left\lfloor \frac{3x^2}{37} \right\rfloor$ by at least 1 (noting that the two sides are integers) while $\frac{3x^2}{37}$ cannot be greater than $\left\lfloor \frac{3x^2}{37} \right\rfloor$ by 1 (i.e. if it is greater then it is greater by less than 1). The solution of this

inequality (i.e. $3x^2 - 185x < 0$) is $1 \le x \le 61$. So, the solutions of the inequality $\left\lfloor \frac{3x^2}{37} \right\rfloor < 5x$ are: $x = 1, 2, \ldots, 61$. It is worth noting that this Problem can be easily solved computationally (e.g. by a computer code or a spreadsheet).

9. Let us define $f(x, y)$ as follows (where $x, y \in \mathbb{N}$):

$$f(x,y) = \begin{cases} 1 & \left(\left\lfloor \frac{xy}{12} \right\rfloor = 1\right) \\ 0 & \left(\left\lfloor \frac{xy}{12} \right\rfloor \ne 1\right) \end{cases}$$

Find the following sum:

$$\sum_{x=1}^{\infty} \sum_{y=1}^{\infty} f(x,y)$$

Solution: If $x \ge 24$ or $y \ge 24$ then we have (where $r \in \mathbb{N}^0$ and $m \in \mathbb{N}$):

$$\frac{xy}{12} = \frac{(24+r)m}{12} = \frac{24m + rm}{12} = 2m + \frac{rm}{12}$$

Hence:

$$\left\lfloor \frac{xy}{12} \right\rfloor = \left\lfloor 2m + \frac{rm}{12} \right\rfloor = \left(2m + \left\lfloor \frac{rm}{12} \right\rfloor\right) > 1$$

So, we need only to consider the sum $\sum_{x=1}^{23} \sum_{y=1}^{23} f(x,y)$.[88] Accordingly, we have only 47 pairs of (x, y) such that $f(x, y) = 1$, i.e.

(1,12)	(1,13)	(1,14)	(1,15)	(1,16)	(1,17)	(1,18)	(1,19)	(1,20)	(1,21)	(1,22)	(1,23)
(2,6)	(2,7)	(2,8)	(2,9)	(2,10)	(2,11)	(3,4)	(3,5)	(3,6)	(3,7)	(4,3)	(4,4)
(4,5)	(5,3)	(5,4)	(6,2)	(6,3)	(7,2)	(7,3)	(8,2)	(9,2)	(10,2)	(11,2)	
(12,1)	(13,1)	(14,1)	(15,1)	(16,1)	(17,1)	(18,1)	(19,1)	(20,1)	(21,1)	(22,1)	(23,1)

Hence, the given sum is 47.

10. Solve the following equations (where $m \in \mathbb{N}^0$):

(**a**) $n = \left\lfloor \frac{m}{2} \right\rfloor + \left\lfloor \frac{m}{3} \right\rfloor$. (**b**) $n = \left\lfloor \frac{2m}{3} \right\rfloor + \left\lfloor \frac{4m}{5} \right\rfloor$.

Solution:

(**a**) Let $m = 6k + r$ (where $k, r \in \mathbb{N}^0$ and $0 \le r \le 5$). Accordingly:

$$n = \left\lfloor \frac{6k+r}{2} \right\rfloor + \left\lfloor \frac{6k+r}{3} \right\rfloor = 3k + \left\lfloor \frac{r}{2} \right\rfloor + 2k + \left\lfloor \frac{r}{3} \right\rfloor = 5k + \left\lfloor \frac{r}{2} \right\rfloor + \left\lfloor \frac{r}{3} \right\rfloor$$

Now:

$r = 0 \ \rightarrow \ n = 5k$ $r = 1 \ \rightarrow \ n = 5k$ $r = 2 \ \rightarrow \ n = 5k + 1$

$r = 3 \ \rightarrow \ n = 5k + 2$ $r = 4 \ \rightarrow \ n = 5k + 3$ $r = 5 \ \rightarrow \ n = 5k + 3$

So, the solutions (m, n) are:

$(6k, 5k)$ $(6k+1, 5k)$ $(6k+2, 5k+1)$ $(6k+3, 5k+2)$ $(6k+4, 5k+3)$ $(6k+5, 5k+3)$

(**b**) Let $m = 15k + r$ (where $k, r \in \mathbb{N}^0$ and $0 \le r \le 14$). Accordingly:

$$n = \left\lfloor \frac{30k+2r}{3} \right\rfloor + \left\lfloor \frac{60k+4r}{5} \right\rfloor = 10k + \left\lfloor \frac{2r}{3} \right\rfloor + 12k + \left\lfloor \frac{4r}{5} \right\rfloor = 22k + \left\lfloor \frac{2r}{3} \right\rfloor + \left\lfloor \frac{4r}{5} \right\rfloor$$

Now:

$r = 0 \rightarrow n = 22k$ $r = 1 \rightarrow n = 22k$ $r = 2 \rightarrow n = 22k + 2$ $r = 3 \rightarrow n = 22k + 4$

$r = 4 \rightarrow n = 22k + 5$ $r = 5 \rightarrow n = 22k + 7$ $r = 6 \rightarrow n = 22k + 8$ $r = 7 \rightarrow n = 22k + 9$

$r = 8 \rightarrow n = 22k + 11$ $r = 9 \rightarrow n = 22k + 13$ $r = 10 \rightarrow n = 22k + 14$ $r = 11 \rightarrow n = 22k + 15$

$r = 12 \rightarrow n = 22k + 17$ $r = 13 \rightarrow n = 22k + 18$ $r = 14 \rightarrow n = 22k + 20$

[88] In fact, because of symmetry we need to consider only half of this.

So, the solutions (m, n) are:

$(15k, 22k)$ $(15k+1, 22k)$ $(15k+2, 22k+2)$ $(15k+3, 22k+4)$

$(15k+4, 22k+5)$ $(15k+5, 22k+7)$ $(15k+6, 22k+8)$ $(15k+7, 22k+9)$

$(15k+8, 22k+11)$ $(15k+9, 22k+13)$ $(15k+10, 22k+14)$ $(15k+11, 22k+15)$

$(15k+12, 22k+17)$ $(15k+13, 22k+18)$ $(15k+14, 22k+20)$

11. Solve the following series equation: $n = \sum_{k=1}^{m} \left\lfloor 7\left(\frac{100}{101}\right)^k \right\rfloor$.

Solution: We have:

- $7\left(\frac{100}{101}\right)^k \simeq 6 \rightarrow k = \frac{\log(6/7)}{\log(100/101)} \simeq 15.49 \rightarrow \left\lfloor 7\left(\frac{100}{101}\right)^k \right\rfloor = 6 \quad (1 \leq k \leq 15).$
- $7\left(\frac{100}{101}\right)^k \simeq 5 \rightarrow k = \frac{\log(5/7)}{\log(100/101)} \simeq 33.82 \rightarrow \left\lfloor 7\left(\frac{100}{101}\right)^k \right\rfloor = 5 \quad (16 \leq k \leq 33).$
- $7\left(\frac{100}{101}\right)^k \simeq 4 \rightarrow k = \frac{\log(4/7)}{\log(100/101)} \simeq 56.24 \rightarrow \left\lfloor 7\left(\frac{100}{101}\right)^k \right\rfloor = 4 \quad (34 \leq k \leq 56).$
- $7\left(\frac{100}{101}\right)^k \simeq 3 \rightarrow k = \frac{\log(3/7)}{\log(100/101)} \simeq 85.15 \rightarrow \left\lfloor 7\left(\frac{100}{101}\right)^k \right\rfloor = 3 \quad (57 \leq k \leq 85).$
- $7\left(\frac{100}{101}\right)^k \simeq 2 \rightarrow k = \frac{\log(2/7)}{\log(100/101)} \simeq 125.90 \rightarrow \left\lfloor 7\left(\frac{100}{101}\right)^k \right\rfloor = 2 \quad (86 \leq k \leq 125).$
- $7\left(\frac{100}{101}\right)^k \simeq 1 \rightarrow k = \frac{\log(1/7)}{\log(100/101)} \simeq 195.56 \rightarrow \left\lfloor 7\left(\frac{100}{101}\right)^k \right\rfloor = 1 \quad (126 \leq k \leq 195).$
- $7\left(\frac{100}{101}\right)^k < 1 \rightarrow \left\lfloor 7\left(\frac{100}{101}\right)^k \right\rfloor = 0 \quad (196 \leq k).$

Accordingly:

- For $m = 1, 2, \ldots, 15$ we have $n = 6m$.
- For $m = 16, 17, \ldots, 33$ we have $n = 5(m-15) + 90 = 5m + 15$.
- For $m = 34, 35, \ldots, 56$ we have $n = 4(m-33) + 180 = 4m + 48$.
- For $m = 57, 58, \ldots, 85$ we have $n = 3(m-56) + 272 = 3m + 104$.
- For $m = 86, 87, \ldots, 125$ we have $n = 2(m-85) + 359 = 2m + 189$.
- For $m = 126, 127, \ldots, 195$ we have $n = (m-125) + 439 = m + 314$.
- For $m \geq 196$ we have $n = 509$.

12. Solve the following equation (where $x, y \in \mathbb{N}^0$): $\left\lfloor \frac{x+1}{2} \right\rfloor + \left\lfloor \frac{y}{3} \right\rfloor = x$.

Solution: If x is even then $x = 2a$ and if x is odd then $x = 2a+1$ (where $a \in \mathbb{N}^0$). Similarly, $y = 3b$ or $y = 3b+1$ or $y = 3b+2$ (where $b \in \mathbb{N}^0$). So, if $\left\lfloor \frac{x+1}{2} \right\rfloor + \left\lfloor \frac{y}{3} \right\rfloor = x$ then we have 6 possibilities:

$$\left\lfloor \frac{2a+1}{2} \right\rfloor + \left\lfloor \frac{3b}{3} \right\rfloor = 2a \qquad \left\lfloor \frac{2a+2}{2} \right\rfloor + \left\lfloor \frac{3b}{3} \right\rfloor = 2a+1$$

$$\left\lfloor \frac{2a+1}{2} \right\rfloor + \left\lfloor \frac{3b+1}{3} \right\rfloor = 2a \qquad \left\lfloor \frac{2a+2}{2} \right\rfloor + \left\lfloor \frac{3b+1}{3} \right\rfloor = 2a+1$$

$$\left\lfloor \frac{2a+1}{2} \right\rfloor + \left\lfloor \frac{3b+2}{3} \right\rfloor = 2a \qquad \left\lfloor \frac{2a+2}{2} \right\rfloor + \left\lfloor \frac{3b+2}{3} \right\rfloor = 2a+1$$

Now, from the first three possibilities (left column) we get $a + b = 2a$ (i.e. $b = a$), and similarly from the second three possibilities (right column) we get: $a + 1 + b = 2a + 1$ (i.e. also $b = a$). Hence, the solutions are:

$(x, y) = (2a, 3a)$ $(x, y) = (2a, 3a+1)$ $(x, y) = (2a, 3a+2)$

$(x, y) = (2a+1, 3a)$ $(x, y) = (2a+1, 3a+1)$ $(x, y) = (2a+1, 3a+2)$

13. Investigate (with some examples) the solutions of the following equation (where $x, y \in \mathbb{R}$):

$$\left\lfloor \frac{xy+2}{y-1} \right\rfloor = \left\lceil \frac{xy+2}{y-1} \right\rceil$$

Solution: $\left\lfloor \frac{xy+2}{y-1} \right\rfloor = \left\lceil \frac{xy+2}{y-1} \right\rceil$ *iff* $\frac{xy+2}{y-1}$ is an integer. This means that we are actually dealing with the following equation: $\frac{xy+2}{y-1} = z$ where $x, y \in \mathbb{R}$ and $z \in \mathbb{Z}$. So, any (x, y) pair that makes the LHS of the last equation an integer is a solution to the given equation. The following are some examples of these solutions: $(x, y) = (1, 2)$, $(-1, 2)$, $(3, 0)$, $(0.5, 2)$, $(1, -0.5)$, $(7.2, 1.25)$.

14. Solve the following equation (where $x \in \mathbb{N}^0$): $y = \left\lfloor \frac{x}{3} \right\rfloor + \left\lceil \frac{x}{3} \right\rceil$.

Solution: We have three cases to consider (where $k \in \mathbb{N}^0$):

- $x = 3k$ and hence we have: $y = k + k = 2k$.
- $x = 3k + 1$ and hence we have: $y = k + k + 1 = 2k + 1$.
- $x = 3k + 2$ and hence we have: $y = k + k + 1 = 2k + 1$.

So, the solutions are: $(x, y) = (3k, 2k)$, $(3k + 1, 2k + 1)$ and $(3k + 2, 2k + 1)$.

15. Solve the following equation: $x - \lfloor \sqrt{y} \rfloor = 0$ where $x, y \in \mathbb{R}$.
Solution: y (and hence x) must be a non-negative real number. Now, if we write the equation as $x = \lfloor \sqrt{y} \rfloor$ then it is obvious that x is a non-negative integer, i.e. $x = 0, 1, 2, \ldots$. So, if $k \in \mathbb{N}^0$ and $s \in \mathbb{R}$ then the solutions of the given equation are: $(x, y) = (k, s)$ where $k^2 \leq s < (k + 1)^2$.
16. Solve the following inequality (where $x, y \in \mathbb{N}^0$): $2x < \left\lfloor \frac{xy}{5} \right\rfloor < 3y$.
Solution: For $x = 0$, the inequality is untrue. For $x > 0$ we have:

$$2x < \left\lfloor \frac{xy}{5} \right\rfloor \qquad \text{and} \qquad \left\lfloor \frac{xy}{5} \right\rfloor < 3y$$

The solutions (x, y) of these simultaneous inequalities are:

$(1, \geq 15)$	$(2, \geq 13)$	$(3, \geq 12)$	$(4, \geq 12)$	$(5, \geq 11)$	$(6, \geq 11)$	$(7, \geq 11)$
$(8, \geq 11)$	$(9, \geq 11)$	$(10, \geq 11)$	$(11, \geq 11)$	$(12, \geq 11)$	$(13, \geq 11)$	$(14, \geq 11)$

Chapter 13
GCD and LCM

1. Let $m = 8^s + 1$ and $n = 35^t + 1$ (where $s, t \in \mathbb{N}$). State a sufficient condition for $\gcd(m, n)$ to be greater than 1.
   Solution: A sufficient condition is that s and t are odd. This is because either $m = 9$ (i.e. when $s = 1$) or it has a factor of 9 (i.e. when $\mathbb{O} \ni s > 1$ according to Eq. 11 in V1). Similarly, either $n = 36$ (i.e. when $t = 1$) or it has a factor of 36 (i.e. when $\mathbb{O} \ni t > 1$ according to Eq. 11 in V1). So, m and n have always a common divisor greater than 1 if s and t are odd.
2. Show that $\gcd(k^m - 1, k^n - 1) = k^{\gcd(m,n)} - 1$ (where $m, n, k \in \mathbb{N}$ and $k > 1$).
   Solution: Let $g = \gcd(m, n)$ and $G = \gcd(k^m - 1, k^n - 1)$. Now:
   • Since $g = \gcd(m, n)$ then $g|m$ and $g|n$ and hence (by the result of Problem 6 of § 6.7 of V1) we have $(k^g - 1)|(k^m - 1)$ and $(k^g - 1)|(k^n - 1)$ which means $(k^g - 1)|G$ (since G is the greatest common divisor of $k^m - 1$ and $k^n - 1$ and hence G must be divisible by any of their common divisors; see Problem 10 of § 2.4 of V1).
   • Since $G = \gcd(k^m - 1, k^n - 1)$ then $G|(k^m - 1)$ and $G|(k^n - 1)$ and this is equivalent to $(k^m - 1) \overset{G}{=} 0$ and $(k^n - 1) \overset{G}{=} 0$, i.e. $k^m \overset{G}{=} 1$ and $k^n \overset{G}{=} 1$. Now (noting that $g = sm + tn$ by Bezout theorem):

$$k^g = k^{sm+tn} = (k^m)^s (k^n)^t \overset{G}{=} 1^s 1^t = 1$$

   i.e. $G|(k^g - 1)$.
   So in brief, we proved in these two points that $(k^g - 1)|G$ and $G|(k^g - 1)$ and hence by rule 9 of § 1.9 of V1 $\left[\text{noting that } G \in \mathbb{N} \text{ and } (k^g - 1) \in \mathbb{N}\right]$ we have $G = (k^g - 1)$, i.e. $\gcd(k^m - 1, k^n - 1) = k^{\gcd(m,n)} - 1$ (as required).
3. Find the greatest common divisor (gcd) of the following polynomials (where $n \in \mathbb{Z}$):
   (**a**) $P_1(n) = n^4 - 10n^3 + 22n^2 - 10n + 21 \qquad P_2(n) = n^3 + 5n^2 - 73n - 77.$
   (**b**) $P_1(n) = n^2 - 3n - 10 \qquad P_2(n) = 2n^3 - n + 6 \qquad P_3(n) = n^2 - 22n + 85.$
   Solution:
   (**a**) If we factorize these polynomials we get:

$$P_1(n) = (n - 7)(n^2 + 1)(n - 3) \qquad P_2(n) = (n - 7)(n + 1)(n + 11)$$

   So, the gcd of these polynomials is $(n - 7)$.
   (**b**) $P_2(n)$ does not factorize and hence it cannot have a common factor with $P_1(n)$ and $P_3(n)$. Therefore, the gcd of these polynomials is 1.
4. Are the following propositions correct:
   (**a**) If $\gcd(m, n) = 1$ and $m \overset{k}{=} n$ then $\gcd(n, k) = 1$.
   (**b**) If $\gcd(m, k) = 1$ and $m \overset{k}{=} n$ then $\gcd(n, k) = 1$.
   Solution:
   (**a**) This is correct and can be proved by various ways. In the following we prove it by using contradiction (which is the easiest way).
   So, let us assume that $g \equiv \gcd(n, k) > 1$ and hence $n = g\nu$ and $k = g\kappa$ and thus (from $m \overset{k}{=} n$) we have $m = sk + n = g(s\kappa + \nu)$ which means that $g|m$ and hence g is a common factor of m and n which contradicts the condition that $\gcd(m, n) = 1$. So, we must have $\gcd(n, k) = 1$.
   (**b**) This is correct and can be proved by various ways. In the following we prove it by using contradiction (which is the easiest way).

So, let us assume that $g \equiv \gcd(n,k) > 1$ and hence $n = g\nu$ and $k = g\kappa$ and thus (from $m \overset{k}{=} n$) we have $m = sk + n = g(s\kappa + \nu)$ which means that $g|m$ and hence g is a common factor of m and k which contradicts the condition that $\gcd(m,k) = 1$. So, we must have $\gcd(n,k) = 1$.

5. Find $\gcd(n, n+2)$ for all $n \in \mathbb{N}$.
Solution: For even n (say $n = 2m$ where $m \in \mathbb{N}$) we have:
$$\gcd(n, n+2) = \gcd(2m, 2m+2) = 2\gcd(m, m+1) = 2$$
where the last step is because m and $m+1$ are coprime.
For odd n we have (see the rules of gcd in the preamble of § 2.4 of V1):
$$\gcd(n, n+2) = \gcd(2m+1, 2m+3) = \gcd(2m+1, [2m+3] - [2m+1]) = \gcd(2m+1, 2) = 1$$
where the last step is because $2m+1$ is odd and hence it is coprime to 2.
So in brief, two natural numbers which differ by 2 are either coprime (i.e. when they are odd) or their greatest common divisor is 2 (i.e. when they are even).

6. Let $a, b, c, d \in \mathbb{Z}$. Show that if $ab + cd = 1$ then a is coprime to both c and d (and similarly b is coprime to both c and d).
Solution: If a is not coprime to one of them (say a is not coprime to c) then they must have a common factor $g > 1$ and hence if $a = g\alpha$ and $c = g\gamma$ $(\alpha, \gamma \in \mathbb{Z})$ then we have:
$$ab + cd = 1 \qquad \rightarrow \qquad g(\alpha b + \gamma d) = 1$$
Now, $(\alpha b + \gamma d)$ is an integer which is either 0 $\big[$and hence $g(\alpha b + \gamma d) = 0 \neq 1\big]$ or not 0 $\big[$and hence $|g(\alpha b + \gamma d)| > 1\big]$. So, these contradictory results (which are based on the assumption that a and c are not coprime) should imply that a and c must be coprime. By the same argument, a and d must also be coprime (and this similarly applies to b with regard to c and d).

7. Show that the following fractions are irreducible for all $m \in \mathbb{N}$:
$$\frac{3m-1}{5m-2} \qquad\qquad \frac{9m+1}{6m+1}$$
Solution: For a fraction to be irreducible, the gcd of its numerator and denominator must be 1. Now, from Bezout theorem we have:
$$\gcd(3m-1, 5m-2) = 5(3m-1) - 3(5m-2) = 1 \qquad \gcd(9m+1, 6m+1) = -2(9m+1) + 3(6m+1) = 1$$
Thus, these fractions are irreducible.

8. Find the gcd and lcm of the following numbers:
(**a**) $m = 3^{290} + 1$ and $n = 3^{70} + 1$. (**b**) $m = 5^{330} + 1$ and $n = 125^{130} + 1$.
Solution:
(**a**) If $x = 3^{10}$ then $m = x^{29} + 1$ and $n = x^7 + 1$. The gcd of $x^{29} + 1$ and $x^7 + 1$ is $x + 1$. Hence, $\gcd(m,n) = 3^{10} + 1 = 59050$.
Regarding the lcm, we have $mn = \gcd(m,n) \times \text{lcm}(m,n)$ and hence:
$$\text{lcm}(m,n) = \frac{mn}{\gcd(m,n)} = \frac{(3^{290}+1)(3^{70}+1)}{3^{10}+1} = 9827\ldots4650$$
which is a 167-digit integer.
(**b**) If $x = 5^{10}$ then $m = x^{33} + 1$ and $n = x^{39} + 1$. The gcd of $x^{33} + 1$ and $x^{39} + 1$ is $x^3 + 1$. Hence, $\gcd(m,n) = 5^{30} + 1 = 931322574615478515626$.
Regarding the lcm, we have:
$$\text{lcm}(m,n) = \frac{mn}{\gcd(m,n)} = \frac{(5^{330}+1)(125^{130}+1)}{5^{30}+1} = 1946\ldots5626$$
which is a 483-digit integer.

9. Show that if m, n, k are integers (which are not all zero) then there are $s, t, u \in \mathbb{Z}$ such that $\gcd(m, n, k) = sm + tn + uk$.
Solution: We note first that in the following we use the rules of gcd which we stated in § 2.4 of V1 without detailed reference to these rules because of their obviousness.
If (exactly) two of m, n, k are 0 (say $n = k = 0$) then we have $\gcd(m, 0, 0) = \gcd(m, 0) = (\pm 1)m + t0 + u0$ (where plus for $m > 0$ and minus for $m < 0$).
If (exactly) one of m, n, k is 0 (say $k = 0$) then we have $\gcd(m, n, 0) = \gcd(m, n) = sm + tn + u0$.
If none of m, n, k is 0 then we have:

$$\gcd(m, n, k) = \gcd\big[m, \gcd(n, k)\big] = sm + \alpha \gcd(n, k) = sm + \alpha(\beta n + \gamma k) = sm + tn + uk$$

where $t = \alpha\beta$ and $u = \alpha\gamma$.
Note: the above (induction-like) argument can be easily extended to the gcd of any number of integers (which are not all zero).

10. Express $\gcd(275, 1430, 374)$ as a linear combination of $275, 1430, 374$.
Solution: The procedure (or "algorithm") for doing this can be easily inferred from the argument of Problem 9, that is:

$$\begin{aligned}
\gcd(275, 1430, 374) &= \gcd\big[275, \gcd(1430, 374)\big] = \gcd\big[275, 22\big] = (1)275 + (-12)22 \\
&= (1)275 + (-12)\gcd(1430, 374) = (1)275 + (-12)\big[(-6)1430 + (23)374\big] \\
&= (1)275 + (72)1430 + (-276)374
\end{aligned}$$

11. Express $\gcd(60, 105, 70, 385)$ as a linear combination of $60, 105, 70, 385$.
Solution: The procedure (or "algorithm") for doing this can be easily inferred from the argument of Problem 9, that is:

$$\begin{aligned}
\gcd(60, 105, 70, 385) &= \gcd\big[\gcd(60, 105), \gcd(70, 385)\big] = \gcd\big[15, 35\big] = (-2)15 + (1)35 \\
&= (-2)\gcd(60, 105) + (1)\gcd(70, 385) \\
&= (-2)\big[(2)60 + (-1)105\big] + (1)\big[(-5)70 + (1)385\big] \\
&= (-4)60 + (2)105 + (-5)70 + (1)385
\end{aligned}$$

12. Show that if $m \overset{k}{=} n$ then $\gcd(m, k) = \gcd(n, k)$.
Solution: $m \overset{k}{=} n$ means $m = n + bk$ (where $b \in \mathbb{Z}$) and hence $\gcd(m, k) = \gcd(n + bk, k)$. Now, if k is a factor of n then we have:

$$\gcd(m, k) = \gcd(n + bk, k) = k \gcd(\nu + b, 1) = k = \gcd(n, k) \qquad (n = k\nu)$$

On the other hand, if k is not a factor of n then let $g = \gcd(n, k)$ and hence we have:

$$\gcd(m, k) = \gcd(n + bk, k) = g \gcd(n' + bk', k') = g = \gcd(n, k) \qquad (n = gn',\ k = gk')$$

where the third step is justified by the fact that n' and k' are coprime and hence $\gcd(n' + bk', k') = 1$. So, in both cases we have $\gcd(m, k) = \gcd(n, k)$.

13. Let m, n be coprime integers. Find the following:
(**a**) $\gcd(2m + n, 3m + 5n)$. (**b**) $\gcd(7m + 3n, 3m + 4n)$.
Solution:
(**a**) Let $S = 5(2m + n) - (3m + 5n) = 7m$ and $D = 2(3m + 5n) - 3(2m + n) = 7n$. Now, if d is any common factor of $(2m + n)$ and $(3m + 5n)$ then d should divide both S and D [i.e. $d|(7m)$ and $d|(7n)$] and hence d should divide their gcd [i.e. $d|\gcd(7m, 7n)$; see Problem 10 of § 2.4 of V1]. Now:

$$\gcd(7m, 7n) = 7 \gcd(m, n) = 7$$

where the second step is because m and n are coprime. Accordingly, $d|7$ which means that d is either ± 1 or ± 7 and hence $\gcd(2m + n, 3m + 5n) = 1$ or $\gcd(2m + n, 3m + 5n) = 7$.

(**b**) Let $S = 4(7m + 3n) - 3(3m + 4n) = 19m$ and $D = 7(3m + 4n) - 3(7m + 3n) = 19n$. Now, if d is any common factor of $(7m + 3n)$ and $(3m + 4n)$ then d should divide both S and D [i.e. $d|(19m)$ and $d|(19n)$] and hence d should divide their gcd, i.e. $d|\gcd(19m, 19n)$. Now:

$$\gcd(19m, 19n) = 19\gcd(m, n) = 19$$

Accordingly, $d|19$ which means that d is either ± 1 or ± 19 and hence $\gcd(7m + 3n, 3m + 4n) = 1$ or $\gcd(7m + 3n, 3m + 4n) = 19$.

14. Propose an "efficient algorithm" for computing the gcd of a large number of (distinct) positive integers greater than 1.[89]

Solution: This "algorithm" is outlined in the following points:

• Take the smallest of these numbers (noting that the gcd cannot exceed in magnitude its operands).

• If anyone of the remaining numbers is prime then the gcd is 1 (because the smallest cannot be divisible by the prime which is divisible only by itself and 1).

• If the smallest is prime (and none of the remaining numbers is prime) then order the remaining numbers increasingly and start dividing the remaining numbers by the smallest. If anyone of the remaining numbers is not divisible by the smallest then the gcd is 1; otherwise the gcd is the smallest.

• If the smallest is composite (and none of the remaining numbers is prime) then:

Order the remaining numbers increasingly and calculate the gcd of the smallest with the second smallest (say gcd_1).

Calculate the gcd of the third smallest with the gcd_1 and hence find their gcd (say gcd_2).

Continue this process [i.e. calculating the gcd of the $(n+2)^{th}$ smallest with the gcd_n to obtain gcd_{n+1}] until you get a gcd that is equal to 1 (and hence the gcd of the given numbers is 1) or you reach the last remaining numbers (and hence the gcd of the given numbers is the last obtained gcd).

15. Find the gcd of the following integers using the "algorithm" of Problem 14:

(**a**) $2135, 1152, 5531, 789, 7105, 3329, 1287, 105, 69917, 7709, 11679, 33219, 4727, 2752$.

(**b**) $1261, 679, 8536, 5917, 97, 2910, 388, 1843, 2619, 9797, 5238$.

Solution:

(**a**) The smallest of these numbers is 105 which is composite. On testing the remaining numbers one by one (say in their increasing order to simplify the process) we find that 3329 is prime. Hence, the gcd of these numbers is 1.

(**b**) The smallest of these numbers is 97 which is prime. On inspecting the remaining numbers one by one we find that they are all divisible by 97. Hence, the gcd of these numbers is 97.

16. Find the lcm of the following integers:

$$7907, 178, 2315, 443, 6682, 2971, 55349, 16728, 1291, 5681, 22100, 3607, 5641, 19996$$

Solution: The following numbers are prime: $7907, 443, 2971, 1291, 3607, 5641$. The prime-factorizations of the remaining numbers are:

$178 = 2 \times 89$ $\quad 2315 = 5 \times 463$ $\quad 6682 = 2 \times 13 \times 257$ $\quad 55349 = 7 \times 7907$

$16728 = 2^3 \times 3 \times 17 \times 41$ $\quad 5681 = 13 \times 19 \times 23$ $\quad 22100 = 2^2 \times 5^2 \times 13 \times 17$ $\quad 19996 = 2^2 \times 4999$

So, the lcm of these numbers is:

$$7907 \times 443 \times 2971 \times 1291 \times 3607 \times 5641 \times 2^3 \times 3 \times 5^2 \times 7 \times 13 \times 17 \times 19 \times 23 \times 41 \times 89 \times 257 \times 463 \times 4999 =$$

$$2406803955976581700443615921802365295158 00$$

17. Find the gcd of all the elements of the following sets (where $x \in \mathbb{Z}$):

(**a**) $\{x^7 - x\}$. $\qquad$ (**b**) $\{x^{11} - x\}$.

[89] If one of the numbers is 0 then we simply ignore it (noting that the gcd of the rest is the same as the gcd of the numbers including 0). If one of the numbers is 1 then the gcd of the numbers is 1. If the numbers include negatives then we take their absolute value (noting that the gcd is not affected by sign). We note that "efficient algorithm" is because the traditional methods for calculating the gcd of a large number of integers are not efficient especially when the given numbers are large in magnitude.

Solution:
(**a**) According to Problem 3 of § 8.2, any prime number that divides $(x^7 - x)$ for all $x \in \mathbb{Z}$ must be less than or equal to 7. So, the gcd of $\{x^7 - x\}$ can contain only the following primes: $p = 2, 3, 5, 7$. On testing these primes on the congruence $x^7 \stackrel{p}{=} x$ we find that only $p = 2, 3, 7$ satisfy this congruence identically (i.e. for all $x \in \mathbb{Z}$). So, the prime factors of the gcd of the elements of $\{x^7 - x\}$ are only $2, 3, 7$. Moreover, p^2 (and hence any higher natural power of p) of these primes does not divide $x^7 - x$ identically because:

$$2^7 - 2 \stackrel{2^2}{=} 2 \qquad 3^7 - 3 \stackrel{3^2}{=} 6 \qquad 7^7 - 7 \stackrel{7^2}{=} 42$$

So, the gcd of the elements of the set $\{x^7 - x\}$ for all $x \in \mathbb{Z}$ is $2 \times 3 \times 7 = 42$.
(**b**) As in part (a), any prime number that divides $(x^{11} - x)$ for all $x \in \mathbb{Z}$ must be less than or equal to 11. So, the gcd of $\{x^{11} - x\}$ can contain only the following primes: $p = 2, 3, 5, 7, 11$. On testing these primes on the congruence $x^{11} \stackrel{p}{=} x$ we find that only $p = 2, 3, 11$ satisfy this congruence identically (i.e. for all $x \in \mathbb{Z}$). So, the prime factors of the gcd of the elements of $\{x^{11} - x\}$ are only $2, 3, 11$. Moreover, p^2 (and hence any higher natural power of p) of these primes does not divide $x^{11} - x$ identically because:

$$2^{11} - 2 \stackrel{2^2}{=} 2 \qquad 3^{11} - 3 \stackrel{3^2}{=} 6 \qquad 11^{11} - 11 \stackrel{11^2}{=} 110$$

So, the gcd of the elements of the set $\{x^{11} - x\}$ for all $x \in \mathbb{Z}$ is $2 \times 3 \times 11 = 66$.

18. Find the gcd of $17! + 17$ and $18! + 17$.
Solution: No prime < 17 can divide $17! + 17$ because such a prime divides $17!$ but not 17. So, no prime < 17 can be a factor in the gcd of $17! + 17$ and $18! + 17$.
Also, no prime > 17 can divide both $17! + 17$ and $18! + 17$ because if such a prime can divide both then it should divide their difference, that is:

$$(18! + 17) - (17! + 17) = 18! - 17! = 17!(18 - 1) = 17! \times 17$$

As we see, any prime > 17 can divide neither $17!$ nor 17 and hence it cannot divide their product. This implies that no prime > 17 can divide both $17! + 17$ and $18! + 17$. So, no prime > 17 can be a factor in the gcd of $17! + 17$ and $18! + 17$.
Thus, the only possible prime that can divide both $17! + 17$ and $18! + 17$ (and hence it can be a factor in their gcd) is 17. So, the gcd of $17! + 17$ and $18! + 17$ must be a natural power of 17. Now if we try 17^2 and 17^3 we find that only 17^2 divides both $17! + 17$ and $18! + 17$. Hence, we conclude that the gcd of $17! + 17$ and $18! + 17$ is $17^2 = 289$.

Chapter 14
Last Digits

1. Find the last 6 digits of the following (where $n \in \mathbb{N}$):

   (**a**) $3412378234699945612 \times 7562988712348990246$.

   (**b**) 999999^n.

   (**c**) 1001^n.

   (**d**) 19^{230}.

   Solution:

   (**a**) The last 6 digits of this product are determined by the product of the last ~ 6 digits of the multiplicands (noting that the higher rank digits of the multiplicands contribute only to the higher rank digits of the product). Accordingly:

$$\begin{aligned} 45612 \times 90246 &= 4116\mathbf{300552} \\ 945612 \times 990246 &= 936388\mathbf{500552} \\ 9945612 \times 8990246 &= 89413498\mathbf{500552} \end{aligned}$$

   As we see, the last 6 digits of the product do not change in the last two equalities (where we take the last 6 and 7 digits only) and hence the last 6 digits of the given product are 500552.

   (**b**) The last 6 digits x are given by $x \overset{10^6}{=} 999999^n$ which is equivalent to $x \overset{10^6}{=} (-1)^n$. Now, for n odd we have $x \overset{10^6}{=} (-1)^n = -1 \overset{10^6}{=} 999999$ while for n even we have $x \overset{10^6}{=} (-1)^n = 1 \overset{10^6}{=} 000001$. So, the last 6 digits of 999999^n are 999999 for odd n and 000001 for even n.

   (**c**) We have:

$$\begin{aligned} 1001^n &= (1000+1)^n \\ &= 1 + C_1^n 1000^1 + C_2^n 1000^2 + \cdots \\ &\overset{10^6}{=} 1 + n1000 \end{aligned}$$

   where line 2 is justified by the binomial theorem (see Eq. 13 in V1), and line 3 is because all the $(C_2^n 1000^2 + \cdots)$ terms have a factor of 10^6. Now, if $n = \cdots d_2 d_1 d_0$ (where the d's stand for digits and where $\cdots d_2 d_1$ could be totally or partially 0) then the last 6 digits x of 1001^n are:

$$x = 1 + d_2 d_1 d_0 000 = d_2 d_1 d_0 001$$

   For example, for $n = 6, 84, 892, 4574$ we have $x = 006001, 084001, 892001, 574001$.

   (**d**) $19^5 = 2476099$ and hence:

$$\begin{aligned} 19^{230} = (19^5)^{46} &= (2476000 + 99)^{46} \\ &= C_0^{46}\, 2476000^0 \times 99^{46} + C_1^{46}\, 2476000^1 \times 99^{45} + \cdots \\ &= 99^{46} + 46 \times 2476000 \times 99^{45} + \cdots \\ &\overset{10^6}{=} 99^{46} + 46 \times 2476000 \times 99^{45} \\ &= (99 + 46 \times 2476000)\, 99^{45} \\ &= 113896099 \times 99^{45} \\ &= 113896099\, (100-1)^{45} \\ &= 113896099 \left[C_0^{45}\, 100^0 (-1)^{45} + C_1^{45}\, 100^1 (-1)^{44} + C_2^{45}\, 100^2 (-1)^{43} + \cdots \right] \\ &= 113896099 \left[-1 + 4500 - 9900000 + \cdots \right] \end{aligned}$$

$$\stackrel{10^6}{=} \quad 113896099 \times (-9895501)$$
$$\stackrel{10^6}{=} \quad 449401$$

So, the last 6 digits of 19^{230} are 449401.

2. Find the last 3 digits of the following:

(**a**) $2003^{2002^{2001}}$. (**b**) $301^{37^{63^{45}}}$.

Solution: We note first that if $m \stackrel{\phi(k)}{=} n$ then $s^m \stackrel{k}{=} s^n$ (where k and s are coprime; see rule 12 of § 2.7 of V1).

(**a**) $\phi(1000) = 400$ and $2002 \stackrel{400}{=} 2$ and hence:

$2002^{2001} \stackrel{\phi(1000)}{=} n \quad \rightarrow \quad 2002^{2001} \stackrel{400}{=} n \quad \rightarrow \quad 2^{2001} \stackrel{400}{=} n \quad \rightarrow \quad 2 \times (2^{25})^{80} \stackrel{400}{=} n \quad \rightarrow$

$2 \times 32^{80} \stackrel{400}{=} n \quad \rightarrow \quad 2 \times 2^{400} \stackrel{400}{=} n \quad \rightarrow \quad 2 \times (2^{25})^{16} \stackrel{400}{=} n \quad \rightarrow \quad 2 \times 32^{16} \stackrel{400}{=} n \quad \rightarrow$

$2 \times 2^{80} \stackrel{400}{=} n \quad \rightarrow \quad 2^6 \times 2^{75} \stackrel{400}{=} n \quad \rightarrow \quad 2^6 \times (2^{25})^3 \stackrel{400}{=} n \quad \rightarrow \quad 2^6 \times 32^3 \stackrel{400}{=} n \quad \rightarrow$

$n \stackrel{400}{=} 352 \quad \rightarrow \quad 2002^{2001} \stackrel{\phi(1000)}{=} 352$

Now, if we use the fact that if $m \stackrel{\phi(k)}{=} n$ then $s^m \stackrel{k}{=} s^n$ then we get $2003^{2002^{2001}} \stackrel{1000}{=} 2003^{352}$ and hence (noting that $2003 \stackrel{1000}{=} 3$):

$$3^{2002^{2001}} \stackrel{1000}{=} 3^{352} = (3^{25})^{14} \times 3^2 \stackrel{1000}{=} 443^{14} \times 3^2 = (443^4)^3 \times 443^2 \times 3^2 \stackrel{1000}{=} 1^3 \times 443^2 \times 3^2 = 1766241$$

So, the last 3 digits of $2003^{2002^{2001}}$ are 241.

(**b**) Let $a = 63^{45}$. Noting that $\phi(400) = 160$ we have:

$63^{45} \stackrel{160}{=} a \quad \rightarrow \quad (63^4)^{11} \times 63 \stackrel{160}{=} a \quad \rightarrow \quad 1^{11} \times 63 \stackrel{160}{=} a \quad \rightarrow \quad 63 \stackrel{160}{=} a \quad \rightarrow$

$63 \stackrel{\phi(400)}{=} a \quad \rightarrow \quad 37^{63} \stackrel{400}{=} 37^a = 37^{63^{45}}$

Now, let $b = 37^{63^{45}}$. Noting that $\phi(1000) = 400$ we have:

$37^{63} \stackrel{400}{=} 37^{63^{45}} \quad \rightarrow \quad 37^{63} \stackrel{400}{=} b \quad \rightarrow \quad (37^6)^{10} \times 37^3 \stackrel{400}{=} b \quad \rightarrow \quad 9^{10} \times 37^3 \stackrel{400}{=} b \quad \rightarrow$

$253 \stackrel{400}{=} b \quad \rightarrow \quad 253 \stackrel{\phi(1000)}{=} b \quad \rightarrow \quad 301^{253} \stackrel{1000}{=} 301^b = 301^{37^{63^{45}}}$

Hence:

$$301^{37^{63^{45}}} \stackrel{1000}{=} 301^{253} = (301^{10})^{25} \times 301^3 \stackrel{1000}{=} 1^{25} \times 301^3 = 27270901$$

So, the last 3 digits of $301^{37^{63^{45}}}$ are 901.

Note: in the following we re-solve part (b) using a simpler (but less general) method:
It is easy to verify that:

$$301^{n \stackrel{10}{=} 1,2,3,4,5,6,7,8,9,10} \stackrel{1000}{=} 301, 601, 901, 201, 501, 801, 101, 401, 701, 001$$

Also, it is relatively easy to verify that $37^{63^{45}} \stackrel{10}{=} 3$.[90] Hence, $301^{37^{63^{45}}} \stackrel{1000}{=} 301^3 \stackrel{1000}{=} 901$, i.e. the last 3 digits of $301^{37^{63^{45}}}$ are 901 (as before).

3. Find all $n \in \mathbb{N}$ such that:

(**a**) 197^n ends in 677. (**b**) 831^n ends in 7841. (**c**) 936^n ends in 68754.

---

[90] For example, $63^{45} - 3 \stackrel{4}{=} (-1)^{45} - 3 = -4 \stackrel{4}{=} 0$ and hence $63^{45} - 3 = 4k$ ($k \in \mathbb{N}$). Therefore:

$$37^{63^{45}} \stackrel{10}{=} (-3)^{63^{45}} = (-3)^{63^{45}-3}(-3)^3 = (-3)^{4k}(-3)^3 = \left[(-3)^4\right]^k (-3)^3 \stackrel{10}{=} 1^k(-3)^3 = -27 \stackrel{10}{=} 3$$

Solution:
(**a**) On inspecting the low values of n we find that the lowest n such that $197^n \overset{1000}{=} 677$ is $n = 73$, while the lowest n such that $197^n \overset{1000}{=} 1$ is $n = 100$.[91] Hence:

$$197^{73+100k} = 197^{73} \times 197^{100k} = 197^{73} \times \left(197^{100}\right)^k \overset{1000}{=} 197^{73} \times 1^k = 197^{73} \overset{1000}{=} 677$$

i.e. 197^n ends in 677 for all $n = 73 + 100k$ where $k \in \mathbb{N}^0$.
(**b**) On inspecting the low values of n we find that the lowest n such that $831^n \overset{10000}{=} 7841$ is $n = 8$, while the lowest n such that $831^n \overset{10000}{=} 1$ is $n = 250$.[92] Hence:

$$831^{8+250k} = 831^8 \times 831^{250k} = 831^8 \times \left(831^{250}\right)^k \overset{10000}{=} 831^8 \times 1^k = 831^8 \overset{10000}{=} 7841$$

i.e. 831^n ends in 7841 for all $n = 8 + 250k$ where $k \in \mathbb{N}^0$.
(**c**) 936^n cannot end in 68754 because all natural powers of integers ending in 6 end in 6 (see rule 17 of § 1.8 of V1).

4. Show that the last digit of n^m is the same as the last digit of d_0^m (where $n \in \mathbb{N}^0$, $m \in \mathbb{N}$ and d_0 is the last digit of n).
Solution: Let $n = d_k \ldots d_2 d_1 d_0$ (where $d_k, \ldots, d_2, d_1, d_0$ are digits). We have (see Eq. 14 in V1):

$$n^m = (d_k \ldots d_2 d_1 d_0)^m = \left(d_k \times 10^k + \ldots + d_2 \times 10^2 + d_1 \times 10^1 + d_0\right)^m \overset{10}{=} d_0^m$$

i.e. the last digit of n^m is the same as the last digit of d_0^m.

5. Show that the last digit of n^5 is the same as the last digit of n (where $n \in \mathbb{N}^0$).
Solution: Let $n = d_k \ldots d_2 d_1 d_0$ (where $d_k, \ldots, d_2, d_1, d_0$ are digits). We have:

$0^5 = 0$ $1^5 = 1$ $2^5 = 32$ $3^5 = 243$ $4^5 = 1024$

$5^5 = 3125$ $6^5 = 7776$ $7^5 = 16807$ $8^5 = 32768$ $9^5 = 59049$

i.e. for $n = 0, 1, \ldots, 9$ we have $n^5 \equiv d_0^5 \overset{10}{=} d_0$. Regarding $n > 9$ we have (see Eq. 14 in V1):[93]

$$n^5 = (d_k \ldots d_2 d_1 d_0)^5 = \left(d_k \times 10^k + \ldots + d_2 \times 10^2 + d_1 \times 10^1 + d_0\right)^5 \overset{10}{=} d_0^5 \overset{10}{=} d_0$$

i.e. the last digit of n^5 is the same as the last digit of n for all $n \in \mathbb{N}^0$.

6. Show that no perfect square ends in 2, 3, 7, 8.
Solution: This is a consequence of the result of Problem 4 noting that the squares of 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 are: 0, 1, 4, 9, 16, 25, 36, 49, 64, 81.

7. Find the last digit of the quadratic expression $5n^2 - 3n + 17$ for all $n \in \mathbb{Z}$.
Solution: Let $f(n) \equiv 5n^2 - 3n + 17$. Now, we have:

$$f\left(n \overset{5}{=} 1, 2, 3, 4, 5\right) \overset{10}{=} 9, 1, 3, 5, 7$$

i.e. the last digit of the given expression for $n = 1 + 5k, 2 + 5k, 3 + 5k, 4 + 5k, 5 + 5k$ (where $k \in \mathbb{Z}$) is $9, 1, 3, 5, 7$ (respectively).

8. Find the last two digits of the factorial expression $7n! + 237$ for all $n \in \mathbb{N}^0$.
Solution: By inspection, the last two digits of the expression for $n = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ is 44, 44, 51, 79, 05, 77, 77, 17, 77, 97.
Regarding $n \geq 10$, the number of trailing zeros in $n!$ (and hence in $7n!$) is not less than two (see Eq. 84 in V1) and hence the last two digits of the sum $7n! + 237$ is the same as the last two digits of 237 (i.e. 37). So, the last two digits of the given expression is 37 for all $n \geq 10$.

[91] This inspection can be done by writing a simple code using modular arithmetic where exponentiation is done by repetitive multiplication in which only the last few digits of the product are taken in each stage. The reader can use the LastDigit1.cpp code (which is in the "Codes" directory) for this inspection.
[92] Again, the reader can use the LastDigit1.cpp code for this inspection.
[93] In fact, we can use the result of Problem 4 directly. However, we prefer this for clarity and demonstration.

9. Find the last digit of the exponential expression $699999993^n + 1$ for all $n \in \mathbb{N}$.
Solution: We have:
$$699999993^n + 1 = (11111111^n \times 9^n \times 7^n) + 1$$
Now:
11111111^n always terminates in 1 and hence it has no cycle (i.e. its period is 1).
9^n has a cycle of 2, i.e. it terminates in 9 for odd n and in 1 for even n.
7^n has a cycle of 4, i.e. it terminates in $7, 9, 3, 1$ corresponding to $n = 1 + 4k, 2 + 4k, 3 + 4k, 4 + 4k$ (where $k \in \mathbb{N}^0$).
So, $699999993^n + 1$ has a cycle of 4, i.e. it terminates in $4, 0, 8, 2$ corresponding to $n = 1 + 4k, 2 + 4k, 3 + 4k, 4 + 4k$.
10. Find the last digit of the expression $\left\lfloor \frac{x+1}{2} \right\rfloor^2 + 3 \left\lceil \frac{x}{2} + 2 \right\rceil$ for all $x \in \mathbb{Z}$.
Solution: In Problem 5 of § 12 it was shown that this expression is always even and hence the last digit can only be $0, 2, 4, 6, 8$. Moreover, this expression is equal to:
$$k^2 + 3k + 6 \text{ when } x \text{ is even} \qquad \text{and} \qquad k^2 + 5k + 10 \text{ when } x \text{ is odd}$$
Now, if we try $k^2 + 3k + 6 \overset{10}{=} 0, 2, 4, 6, 8$ we find that this congruence has solutions only for $0, 4, 6$. Similarly, if we try $k^2 + 5k + 10 \overset{10}{=} 0, 2, 4, 6, 8$ we find that this congruence has solutions only for $0, 4, 6$. So, the last digit of this expression can only be $0, 4, 6$. Further inspection should reveal that the last digit of this expression is $0, 0, 6, 6, 4, 4, 4, 4, 6, 6$ corresponding to $x \overset{10}{=} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$.

Chapter 15
Divisibility

1. Find all natural numbers of the form $abab$ which are divisible by 9 (where a, b are digits).
   Solution: We have $abab = 101 \times ab$. Now, 101 is not divisible by 9 and hence if $abab$ is divisible by 9 then ab must be divisible by 9, i.e. $a + b$ must be divisible by 9. So, we have only the following eleven possibilities: $ab = 09$, 18, 27, 36, 45, 54, 63, 72, 81, 90, 99.
2. Show that for any $n \in \mathbb{Z}$, $7|(n-1)$ *iff* $343|(n^3 - 3n^2 - 46n + 48)$.
   Solution: We note first that $n^3 - 3n^2 - 46n + 48 = (n-8)(n-1)(n+6)$ and $343 = 7^3$. Moreover, $n - 8 \overset{7}{=} n - 1 \overset{7}{=} n + 6$. Now:
   • If $7|(n-1)$ then $7|(n-8)$ and $7|(n+6)$ (noting that $n - 8 \overset{7}{=} n - 1 \overset{7}{=} n + 6$) and hence 7^3 divides their product which is $(n^3 - 3n^2 - 46n + 48)$, i.e. $343|(n^3 - 3n^2 - 46n + 48)$.
   • If $343|(n^3 - 3n^2 - 46n + 48)$ then 7 must divide each one of its three factors and hence 7 must divide $(n-1)$, i.e. $7|(n-1)$.[94]
3. Show that for any $n \in \mathbb{Z}$, $5|(n^3 - 3n^2 + 2n)$ *iff* $5 \not| (n^2 - 7n + 12)$ and vice versa.
   Solution: We have:
   • $n^3 - 3n^2 + 2n = n(n-1)(n-2)$ and hence it is obvious that the solutions of $n^3 - 3n^2 + 2n \overset{5}{=} 0$ are $n \overset{5}{=} 0, 1, 2$.
   • $n^2 - 7n + 12 = (n-3)(n-4)$ and hence it is obvious that the solutions of $n^2 - 7n + 12 \overset{5}{=} 0$ are $n \overset{5}{=} 3, 4$.
   So, the residue classes (mod 5) are partitioned (as solutions) between $n^3 - 3n^2 + 2n \overset{5}{=} 0$ and $n^2 - 7n + 12 \overset{5}{=} 0$ and hence what solves one of these congruences does not solve the other congruence and vice versa, i.e. $5|(n^3 - 3n^2 + 2n)$ *iff* $5 \not| (n^2 - 7n + 12)$ and vice versa.
4. Show that for any $\mathbb{N} \ni n > 2$ there are $x, y, z \in \mathbb{N}$ (where $x \neq y \neq z$ and $n^2 < x, y, z < n^3$) such that $z|(x^2 - y^2)$.
   Solution: For example, $x = n^2 + 2$, $y = n^2 + 1$ and $z = 2n^2 + 3$ meet these conditions because:
   $$x^2 - y^2 = \left(n^2 + 2\right)^2 - \left(n^2 + 1\right)^2 = 2n^2 + 3 = z$$
   and hence $z|(x^2 - y^2)$.
5. Find all $x, y \in \mathbb{Z}$ such that:
   (**a**) $(x^2 + y^2)/(x + y)$ is an integer multiple of 31. (**b**) $(x^2 + y^2)/(x + y)$ is a divisor of 35.
   (**c**) $(x^2 + y^2)/(x - y)$ is a divisor of 21.
   Solution:
   (**a**) $x = y = 0$ is not a possibility (assuming $0/0$ is not defined) and hence in the following we assume at least one of $x, y \neq 0$. Moreover, $x + y \neq 0$ (to avoid singularity) and hence $y \neq -x$. Now, since $(x^2 + y^2)/(x + y)$ is an integer multiple of 31 we must have (where $k \in \mathbb{Z}$):
   $$\frac{x^2 + y^2}{x + y} = 31k \qquad \rightarrow \qquad \frac{x^2 + y^2}{31} = k(x + y)$$
   i.e. $31|(x^2 + y^2)$. This implies that $x^2 + y^2 \overset{31}{=} 0$ whose only solution is $(x, y) \overset{31}{=} (0, 0)$. Accordingly, the solutions of this Problem are: $(x, y) = (31s, 31t)$ where $s, t \in \mathbb{Z}$ and $s + t \neq 0$.

[94] To be more clear we may say: if $343|(n^3 - 3n^2 - 46n + 48)$ then 7 must divide one of the three factors of the polynomial (noting that $343 = 7^3$) and hence 7 must divide all the three factors of the polynomial (noting that $n - 8 \overset{7}{=} n - 1 \overset{7}{=} n + 6$), i.e. $7|(n-1)$.

(**b**) Again, $x+y \neq 0$. Let a symbolize a divisor of 35, i.e. $a = \pm 1, \pm 5, \pm 7, \pm 35$. Hence, we must have $\frac{x^2+y^2}{x+y} = a$, that is:

$x^2 - ax + y^2 - ay = 0 \quad \rightarrow \quad 4x^2 - 4ax + 4y^2 - 4ay = 0 \quad \rightarrow$

$4x^2 - 4ax + a^2 + 4y^2 - 4ay + a^2 = 2a^2 \quad \rightarrow \quad (2x-a)^2 + (2y-a)^2 = 2a^2 \quad \rightarrow$

$X^2 + Y^2 = 2a^2$

Now, we have four cases to consider:

• $a = \pm 1$ and hence $X^2 + Y^2 = 2$. Now, the only possibility for 2 to be the sum of two squares is $(X, Y) = (\pm 1, \pm 1)$ and hence the solutions (x, y) are (noting that $x = y = 0$ is not a possibility):

$(0,1) \quad (1,0) \quad (1,1) \quad (-1,-1) \quad (-1,0) \quad (0,-1)$

• $a = \pm 5$ and hence $X^2 + Y^2 = 50$. Now, the only possibilities for 50 to be the sum of two squares are $(X, Y) = (\pm 1, \pm 7)$, $(\pm 5, \pm 5)$, $(\pm 7, \pm 1)$ and hence the solutions (x, y) are (noting that $x = y = 0$ is not a possibility):

$(2,-1) \quad (2,6) \quad (3,-1) \quad (3,6) \quad (-3,-6) \quad (-3,1) \quad (-2,-6) \quad (-2,1)$

$(0,5) \quad (5,0) \quad (5,5) \quad (-5,-5) \quad (-5,0) \quad (0,-5)$

$(-1,2) \quad (6,2) \quad (-1,3) \quad (6,3) \quad (-6,-3) \quad (1,-3) \quad (-6,-2) \quad (1,-2)$

• $a = \pm 7$ and hence $X^2 + Y^2 = 98$. Now, the only possibility for 98 to be the sum of two squares is $(X, Y) = (\pm 7, \pm 7)$ and hence the solutions (x, y) are (noting that $x = y = 0$ is not a possibility):

$(0,7) \quad (7,0) \quad (7,7) \quad (-7,-7) \quad (-7,0) \quad (0,-7)$

• $a = \pm 35$ and hence $X^2 + Y^2 = 2450$. Now, the only possibilities for 2450 to be the sum of two squares are $(X, Y) = (\pm 7, \pm 49)$, $(\pm 35, \pm 35)$, $(\pm 49, \pm 7)$ and hence the solutions (x, y) are (noting that $x = y = 0$ is not a possibility):

$(14,-7) \quad (14,42) \quad (21,-7) \quad (21,42) \quad (-21,-42) \quad (-21,7) \quad (-14,-42) \quad (-14,7)$

$(0,35) \quad (35,0) \quad (35,35) \quad (-35,-35) \quad (-35,0) \quad (0,-35)$

$(-7,14) \quad (42,14) \quad (-7,21) \quad (42,21) \quad (-42,-21) \quad (7,-21) \quad (-42,-14) \quad (7,-14)$

So in brief, we have 56 solutions.

(**c**) As before, we assume $x - y \neq 0$. Now, the divisors of 21 are $a = \pm 1, \pm 3, \pm 7, \pm 21$ and hence if we follow a similar approach to that of part (b) then we get:

• $a = -21$ leads to the solutions: $(x, y) = (-21, 0)$, $(-21, 21)$, $(0, 21)$.
• $a = -7$ leads to the solutions: $(x, y) = (-7, 0)$, $(-7, 7)$, $(0, 7)$.
• $a = -3$ leads to the solutions: $(x, y) = (-3, 0)$, $(-3, 3)$, $(0, 3)$.
• $a = -1$ leads to the solutions: $(x, y) = (-1, 0)$, $(-1, 1)$, $(0, 1)$.
• $a = 1$ leads to the solutions: $(x, y) = (0, -1)$, $(1, -1)$, $(1, 0)$.
• $a = 3$ leads to the solutions: $(x, y) = (0, -3)$, $(3, -3)$, $(3, 0)$.
• $a = 7$ leads to the solutions: $(x, y) = (0, -7)$, $(7, -7)$, $(7, 0)$.
• $a = 21$ leads to the solutions: $(x, y) = (0, -21)$, $(21, -21)$, $(21, 0)$.

So, these 24 pairs are all the solutions of this problem.

6. Find all $x, y, z \in \mathbb{Z}$ such that:

(**a**) $xy|(x^2 + y^2)$. (**b**) $xyz|(x^2 + y^2)$.

Solution:

(**a**) It is obvious that $xy \neq 0$. If $xy|(x^2 + y^2)$ then we have:

$$\frac{x^2+y^2}{xy} = k \quad \rightarrow \quad \frac{x}{y} + \frac{y}{x} = k \qquad (k \in \mathbb{Z})$$

In Problem 4 of § 4.1.10 of V1 we proved that if $x, y, k \in \mathbb{Z}$ $(xy \neq 0)$ then $\frac{x}{y} + \frac{y}{x} = k$ has no solution except when $y = \pm x$ (and hence $k = \pm 2$). So, $xy|(x^2+y^2)$ when $(x, y) = (s, -s)$ and when $(x, y) = (s, s)$ where $\mathbb{Z} \ni s \neq 0$.

(**b**) We note that $xyz|(x^2+y^2)$ implies $z\Big|\Big(\frac{x^2+y^2}{xy}\Big)$. Now, from the answer of part (a) we have $\frac{x^2+y^2}{xy} = \pm 2$ and hence $z = \pm 1, \pm 2$. Therefore, the solutions are (where $\mathbb{Z} \ni s \neq 0$):

$(x, y, z) = (s, -s, \pm 1)$ $(x, y, z) = (s, -s, \pm 2)$ $(x, y, z) = (s, s, \pm 1)$ $(x, y, z) = (s, s, \pm 2)$

7. Show that $66|(n^{21} - n)$ for all $n \in \mathbb{Z}$.

Solution: $n^{21} - n$ is always even and hence $2|(n^{21} - n)$. Also, by Fermat's little theorem we have:

$$n^{21} - n = \left(n^3\right)^7 - n \overset{3}{=} n^7 - n = n\left(n^3\right)^2 - n \overset{3}{=} n\,n^2 - n = n^3 - n \overset{3}{=} n - n = 0$$

i.e. $3|(n^{21} - n)$. Finally, by Fermat's little theorem we have:

$$n^{21} - n = n^{-1}\left(n^{11}\right)^2 - n \overset{11}{=} n^{-1}\,n^2 - n = n - n = 0$$

i.e. $11|(n^{21} - n)$.

So, $(n^{21} - n)$ is divisible by 2, 3 and 11 for all $n \in \mathbb{Z}$ and hence it is divisible by their product (noting that they are pairwise coprime) for all $n \in \mathbb{Z}$, i.e. $66|(n^{21} - n)$ for all $n \in \mathbb{Z}$.

8. Find all $x, y, z \in \mathbb{N}$ such that:

(**a**) $xyz\big|\big[(x+1)(y+1)(z+1)\big]$. (**b**) $\big[(x-1)(y-1)(z-1)\big]\big|xyz$.

(**c**) $\big[(x-1)(y-1)(z-1)\big]\big|(xyz-1)$. (**d**) $\big[(x+1)(y+1)(z+1)\big]\big|(xyz-1)$.

Solution:

(**a**) Let:

$$A \equiv \frac{(x+1)(y+1)(z+1)}{xyz} = \frac{xyz+xy+xz+yz+x+y+z+1}{xyz} = 1+\frac{1}{z}+\frac{1}{y}+\frac{1}{x}+\frac{1}{yz}+\frac{1}{xz}+\frac{1}{xy}+\frac{1}{xyz}$$

It should be obvious that the maximum value of A is 8, i.e. when $x = y = z = 1$ and hence all the 8 terms are equal to 1 (because otherwise some of the terms will be less than 1). So, we need only to consider $A = 1, 2, \ldots, 8$. However, let first assume that $x \leq y \leq z$.

• $\boldsymbol{A = 1}$: this is impossible because the numerator of A is greater than its denominator for any $x, y, z \in \mathbb{N}$ (or alternatively the sum of the last seven terms of A cannot be zero).

• $\boldsymbol{A = 2}$: x must be 2 or 3 because if $x = 1$ then $A > 2$ while if $x \geq 4$ then $A < 2$.

If $x = 2$ then we must have $4 \leq y \leq 6$ because otherwise $A > 2$ or $A < 2$. Now, if $x = 2$ and $y = 4$ then we have only one possibility for z (i.e. $z = 15$), and if $x = 2$ and $y = 5$ then we have only one possibility for z (i.e. $z = 9$), while if $x = 2$ and $y = 6$ then we have only one possibility for z (i.e. $z = 7$).

If $x = 3$ then we must have $3 \leq y \leq 4$ because otherwise $A < 2$. Now, if $x = 3$ and $y = 3$ then we have only one possibility for z (i.e. $z = 8$), while if $x = 3$ and $y = 4$ then we have only one possibility for z (i.e. $z = 5$).

So, only $(x, y, z) = (2, 4, 15)$, $(2, 5, 9)$, $(2, 6, 7)$, $(3, 3, 8)$, $(3, 4, 5)$ make $A = 2$.

• $\boldsymbol{A = 3}$: x must be 1 or 2 because otherwise $A < 3$.

If $x = 1$ then we must have $3 \leq y \leq 4$ because otherwise $A > 3$ or $A < 3$. Now, if $x = 1$ and $y = 3$ then we have only one possibility for z (i.e. $z = 8$), while if $x = 1$ and $y = 4$ then we have only one possibility for z (i.e. $z = 5$).

If $x = 2$ then we must have $y = 2$ because otherwise $A < 3$. Hence, we have only one possibility for z (i.e. $z = 3$).

So, only $(x, y, z) = (1, 3, 8)$, $(1, 4, 5)$, $(2, 2, 3)$ make $A = 3$.

• $\boldsymbol{A = 4}$: x must be 1 because otherwise $A < 4$. Accordingly, y must be 2 because if $y = 1$ then $A > 4$ while if $y \geq 3$ then $A < 4$. Now, if $x = 1$ and $y = 2$ then we have only one possibility for z, i.e. $z = 3$. So, only $(x, y, z) = (1, 2, 3)$ makes $A = 4$.

• $\boldsymbol{A = 5}$: x must be 1 because otherwise $A < 5$. Similarly, y must be 1 because otherwise $A < 5$. Now,

if $x = y = 1$ then we have only one possibility for z, i.e. $z = 4$. So, only $(x, y, z) = (1, 1, 4)$ makes $A = 5$.
• $\boldsymbol{A = 6}$: x must be 1 because otherwise $A < 6$. Similarly, y must be 1 because otherwise $A < 6$. Now, if $x = y = 1$ then we have only one possibility for z, i.e. $z = 2$. So, only $(x, y, z) = (1, 1, 2)$ makes $A = 6$.
• $\boldsymbol{A = 7}$: as before, we must have $x = y = 1$ because otherwise $A < 7$. Now, if $x = y = 1$ then we must have:

$$A = \frac{(1+1)(1+1)(z+1)}{1 \times 1 \times z} = \frac{4(z+1)}{z} = 7 \qquad \rightarrow \qquad 3z = 4$$

which has no integer solution. So, we have no solution for $A = 7$.
• $\boldsymbol{A = 8}$: as before, we must have $x = y = 1$ because otherwise $A < 8$. Now, if $x = y = 1$ then we have only one possibility for z, i.e. $z = 1$. So, only $(x, y, z) = (1, 1, 1)$ makes $A = 8$.
So far we were assuming $x \leq y \leq z$. Now, if we lift this condition (noting the symmetry in x, y, z) by permuting x, y, z (and hence permuting the above 12 solutions) then we get in total 55 solutions to the given divisibility statement.
(**b**) To avoid singularity we must have $x \neq 1$, $y \neq 1$ and $z \neq 1$. So, in the following we assume $x, y, z > 1$. Now, if $X = x - 1$, $Y = y - 1$ and $Z = z - 1$ then we have:

$$XYZ \big| \big[(X+1)(Y+1)(Z+1)\big] \qquad\qquad (X, Y, Z \in \mathbb{N})$$

So, this problem is the same as the problem of part (a) with X, Y, Z replacing x, y, z. Accordingly, we must have the same solutions for X, Y, Z as the solutions for x, y, z in part (a). The final solutions (x, y, z) will be obtained by the transformation: $(x, y, z) = (X + 1, Y + 1, Z + 1)$. So in brief, the main 12 solutions are: $(x, y, z) = (2, 2, 2)$, $(2, 2, 3)$, $(2, 2, 5)$, $(2, 3, 4)$, $(2, 4, 9)$, $(2, 5, 6)$, $(3, 3, 4)$, $(3, 5, 16)$, $(3, 6, 10)$, $(3, 7, 8)$, $(4, 4, 9)$, $(4, 5, 6)$, while the final 55 solutions are obtained by permuting these 12 solutions.
(**c**) To avoid singularity we must have $x, y, z > 1$. So, let:

$$A \equiv \frac{xyz - 1}{(x-1)(y-1)(z-1)}$$

The maximum value of A is 7, i.e. when $x = y = z = 2$. Following a similar analysis to the analysis of part (a) we find that the only solutions are: $(x, y, z) = (2, 2, 2)$, $(2, 2, 4)$, $(2, 4, 8)$, $(3, 5, 15)$ and their permutations. So in total, we have 16 solutions.
(**d**) Let:

$$\begin{aligned} A &\equiv \frac{xyz - 1}{(x+1)(y+1)(z+1)} = \frac{xyz - 1}{xyz + xy + xz + yz + x + y + z + 1} \\ &= \frac{xyz - 1}{(xyz - 1) + (xy + xz + yz + x + y + z + 2)} \end{aligned}$$

It is obvious that $0 \leq A < 1$. So, the only integer value of A is 0 which occurs when $x = y = z = 1$. Therefore, the only solution is: $(x, y, z) = (1, 1, 1)$.

9. Show that $12|(2^{n+2} + 5^{n+3} - 9)$ for all $n \in \mathbb{N}^0$.
Solution: $12|(2^{n+2} + 5^{n+3} - 9)$ is equivalent to $2^{n+2} + 5^{n+3} \stackrel{12}{\equiv} 9$. Now, for even n we have $2^{n+2} \stackrel{12}{\equiv} 4$ and $5^{n+3} \stackrel{12}{\equiv} 5$, while for odd n we have $2^{n+2} \stackrel{12}{\equiv} 8$ and $5^{n+3} \stackrel{12}{\equiv} 1$. Hence, the congruence $2^{n+2} + 5^{n+3} \stackrel{12}{\equiv} 9$ is always true, i.e. $12|(2^{n+2} + 5^{n+3} - 9)$ for all $n \in \mathbb{N}^0$.
10. Show that if $m^3|n^2$ then $m|n$ (where $m, n \in \mathbb{N}$).
Solution: If the (non-standard) prime factorization of m and n are $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and $n = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ then we have:

$$\frac{n^2}{m^3} = \frac{p_1^{2b_1} p_2^{2b_2} \dots p_k^{2b_k}}{p_1^{3a_1} p_2^{3a_2} \dots p_k^{3a_k}} = p_1^{2b_1 - 3a_1} p_2^{2b_2 - 3a_2} \dots p_k^{2b_k - 3a_k}$$

Now, since $m^3|n^2$ then we must have $p_i^{2b_i-3a_i} \geq 1$ for all $i = 1, 2, \ldots, k$. Hence:

$$p_i^{2b_i-3a_i} \geq 1 \quad \rightarrow \quad p_i^{2b_i} \geq p_i^{3a_i} \quad \rightarrow \quad 2b_i \geq 3a_i \quad \rightarrow$$

$$b_i \geq a_i \quad \rightarrow \quad \frac{n}{m} = \frac{p_1^{b_1}p_2^{b_2}\ldots p_k^{b_k}}{p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}} \quad \rightarrow \quad \frac{n}{m} = p_1^{b_1-a_1}p_2^{b_2-a_2}\ldots p_k^{b_k-a_k}$$

where $p_i^{b_i-a_i} \geq 1$ for all $i = 1, 2, \ldots, k$ (because $b_i \geq a_i$). This means that n/m is an integer and hence $m|n$.

We may also argue (more simply) that if $m^3|n^2$ then (where $k \in \mathbb{N}$):

$$\frac{n^2}{m^3} = k \quad \rightarrow \quad \left(\frac{n}{m}\right)^2 = km \quad \rightarrow \quad \frac{n}{m} = \sqrt{km}$$

Now, if a square root of an integer (i.e. km) is rational (i.e n/m) then the integer (i.e. km) is a perfect square. This means that n/m is an integer and hence $m|n$.

11. Find all $n \in \mathbb{N}$ such that $\sum_{x=1}^{n}(2x^5 - 6x^4 - x^2 + 9)$ is divisible by 33.

Solution: We have (see the identities of § 1.10 in V1):

$$\begin{aligned}\sum_{x=1}^{n}(2x^5 - 6x^4 - x^2 + 9) &= 2\left(\sum_{x=1}^{n}x^5\right) - 6\left(\sum_{x=1}^{n}x^4\right) - \left(\sum_{x=1}^{n}x^2\right) + 9\left(\sum_{x=1}^{n}1\right) \\ &= 2\left(\frac{n^2(n+1)^2(2n^2+2n-1)}{12}\right) - 6\left(\frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}\right) - \\ &\quad \left(\frac{n(n+1)(2n+1)}{6}\right) + 9n \\ &= \frac{10n^6 - 6n^5 - 65n^4 - 70n^3 - 20n^2 + 271n}{30}\end{aligned}$$

So, if the given series is divisible by 33 then $(10n^6 - 6n^5 - 65n^4 - 70n^3 - 20n^2 + 271n)$ must be divisible by 99 (noting that 33 and 10 are coprime), i.e. $10n^6 - 6n^5 - 65n^4 - 70n^3 - 20n^2 + 271n \overset{99}{=} 0$. The solution to this congruence equation is $n \overset{99}{=} 0, 44, 88$ (see § 3.2.1 of V1 as well as § 8.2 of the present volume). So, the given series is divisible by 33 *iff* $n = 44 + 99m$ or $n = 88 + 99m$ or $n = 99(1 + m)$ where $m \in \mathbb{N}^0$.

12. Find the remainder when:

(**a**) $29783^{54896302}$ is divided by 101. (**b**) 3671^{8924} is divided by 663.

(**c**) 56389^{7823} is divided by 5931.

Solution:

(**a**) If r represents the remainder then we have $29783^{54896302} \overset{101}{=} r$ and hence:

$$\begin{aligned}r &\overset{101}{=} 29783^{54896302} \overset{101}{=} 89^{54896302} = \left(89^{100}\right)^{548963}89^2 = \left(89^{\phi(101)}\right)^{548963}89^2 \overset{101}{=} 1^{548963}89^2 \\ &= 89^2 \overset{101}{=} 43\end{aligned}$$

where we used Euler's theorem in the fifth step (noting that 29783 and 101 are coprime).

(**b**) We have $663 = 3 \times 13 \times 17$. Let r be the remainder when 3671^{8924} is divided by 663 and hence $3671^{8924} \overset{663}{=} r$. Now:

$$\begin{aligned}3671^{8924} &\overset{3}{=} 2^{8924} = \left(2^2\right)^{4462} \overset{3}{=} 1^{4462} = 1 \\ 3671^{8924} &\overset{13}{=} 5^{8924} = \left(5^4\right)^{2231} \overset{13}{=} 1^{2231} = 1 \\ 3671^{8924} &\overset{17}{=} (-1)^{8924} = 1\end{aligned}$$

Now, since $3671^{8924} \overset{663}{=} r$ then we must have $r \overset{3}{=} 1$, $r \overset{13}{=} 1$ and $r \overset{17}{=} 1$. On solving this system of congruence equations[95] (using for instance the Chinese remainder theorem) we get: $r \overset{663}{=} 1$, i.e. the

[95] More simply, we can use rule 14 of § 2.7 of V1.

remainder when 3671^{8924} is divided by 663 is 1.
We may also solve this part by using Euler's theorem (in part). We note first that 3671 and 663 are coprime and $\phi(663) = 384$. Hence:

$$\begin{aligned} 3671^{8924} &\overset{663}{=} 356^{8924} = \left(356^{384}\right)^{23} \times 356^{92} = \left(356^{\phi(663)}\right)^{23} \times 356^{92} \overset{663}{=} 1^{23} \times 356^{92} = 356^{92} \\ &= \left(356^4\right)^{23} \overset{663}{=} 1^{23} = 1 \end{aligned}$$

(**c**) We have $5931 = 9 \times 659$. Let r be the remainder when 56389^{7823} is divided by 5931 and hence $56389^{7823} \overset{5931}{=} r$. Now:

$$\begin{aligned} 56389^{7823} &\overset{9}{=} 4^{7823} = \left(4^3\right)^{2607} 4^2 \overset{9}{=} 1^{2607} 4^2 = 16 \overset{9}{=} 7 \\ 56389^{7823} &\overset{659}{=} 374^{7823} = \left(374^7\right)^{1117} 374^4 \overset{659}{=} 50^{1117}\, 374^4 = \left(50^{11}\right)^{101} \left(50^6\right) 374^4 \\ &\overset{659}{=} 43^{101} \left(50^6\right) 374^4 = \left(43^7\right)^{14} 43^3 \left(50^6\right) 374^4 \overset{659}{=} 24^{14} \left(43^3\right) \left(50^6\right) 374^4 \\ &= 24^{11} \left(24^3\right) \left(43^3\right) \left(50^6\right) 374^4 \overset{659}{=} 50 \left(24^3\right) \left(43^3\right) \left(50^6\right) 374^4 \\ &= \left(24^3\right) \left(43^3\right) \left(50^7\right) 374^4 \overset{659}{=} (644)(427)(645)546 \overset{659}{=} 74 \end{aligned}$$

Now, since $56389^{7823} \overset{5931}{=} r$ then we must have $r \overset{9}{=} 7$ and $r \overset{659}{=} 74$. On solving this system of congruence equations we get: $r \overset{5931}{=} 4687$, i.e. the remainder when 56389^{7823} is divided by 5931 is 4687.

13. Comment on Problem 12.
Solution: Problem 12 shows that there are several (and possibly many) methods for solving this type of problems. These methods vary in applicability and convenience depending mostly on the nature of the given problem. Hence, we should always inspect different potential methods of solution before we make our choice. In fact, sometimes more basic approaches are the best choice. For example, part (b) of Problem 12 can be solved more easily by the following basic approach (as can be seen in the last steps in the second method):

$$3671^{8924} = \left(3671^4\right)^{2231} \overset{663}{=} 1^{2231} = 1$$

However, our purpose in Problem 12 is to demonstrate these methods (which can be the best or the must in some other problems). In fact, we have met and will meet other methods and techniques for solving this type of problems (see for instance Problem 20).

14. Show that 13 divides $\sum_{k=0}^{m} 7^k$ *iff* $m = 12n - 1$ (where $n \in \mathbb{N}$).
Solution: Regarding the **if part**, by Fermat's little theorem (as well as the power rule for congruence) we have: $7^{12n} - 1 \overset{13}{=} 0$. On factorizing this we get:

$$(7-1)\left(\sum_{k=0}^{12n-1} 7^k\right) \overset{13}{=} 0 \qquad \text{i.e.} \qquad 13 \text{ divides } 6\left(\sum_{k=0}^{12n-1} 7^k\right)$$

Now, 13 does not divide 6 and hence it must divide the given series (with $m = 12n - 1$).
Regarding the **only if part**, if $0 \le m \le 10$ then $\sum_{k=0}^{m} 7^k$ is not divisible by 13 (as we can easily check by simple calculations). On the other hand, if $m > 11$ and $m \neq 12n - 1$ then $m = (12n - 1) + s$ where $1 \le s \le 11$, that is:

$$\sum_{k=0}^{m} 7^k = \sum_{k=0}^{12n-1} 7^k + \sum_{k=12n}^{12n+s-1} 7^k \overset{13}{=} \sum_{k=12n}^{12n+s-1} 7^k = \sum_{k=0}^{s-1} 7^{k+12n} = 7^{12n} \sum_{k=0}^{s-1} 7^k \overset{13}{=} \sum_{k=0}^{s-1} 7^k$$

where the second step is because of the result of the "if part" while the last step is because $7^{12n} \overset{13}{=} 1$ (by Fermat's little theorem and the power rule for congruences). Now, $\sum_{k=0}^{s-1} 7^k$ is not divisible by 13 (as we concluded earlier in the case of $0 \le m \le 10$), and hence the given series is not divisible by 13 for any $m \neq 12n - 1$, i.e. if 13 divides the given series then $m = 12n - 1$.

15. Find all $x, y, z \in \mathbb{Z}$ such that $x^2y^2z^2|(x^2+y^2+z^2)$.
Solution: $xyz \neq 0$. Now, we have:

$$\frac{x^2+y^2+z^2}{x^2y^2z^2} = \frac{1}{y^2z^2} + \frac{1}{x^2z^2} + \frac{1}{x^2y^2} \equiv A$$

It is obvious that A cannot be greater than 3 (i.e. when $y^2z^2 = x^2z^2 = x^2y^2 = 1$) and hence we have only 3 possibilities (see Problem 7 of § 4.1.10 of V1):
• $A = 3$ and hence $y^2z^2 = x^2z^2 = x^2y^2 = 1$, i.e. $(x, y, z) = (\pm 1, \pm 1, \pm 1)$ considering all the 8 possibilities for the combination of signs.
• $A = 2$ and hence $(y^2z^2,\ x^2z^2,\ x^2y^2) = (1, 2, 2), (2, 1, 2), (2, 2, 1)$. None of these leads to an integer solution to x, y, z.
• $A = 1$ and hence $(y^2z^2,\ x^2z^2,\ x^2y^2)$ = (2,3,6), (2,6,3), (3,2,6), (3,6,2), (6,2,3), (6,3,2), (2,4,4), (4,2,4), (4,4,2), (3,3,3). None of these leads to an integer solution to x, y, z.
So in brief, we have only 8 solutions, i.e. $(x, y, z) = (\pm 1, \pm 1, \pm 1)$.

16. Find all $n \in \mathbb{Z}$ such that:
(**a**) $101|(n^{101}+1)$. (**b**) $71|(n^{360}-7)$.
Solution: We use Fermat's little theorem.
(**a**) $101|(n^{101}+1)$ is equivalent to $n^{101}+1 \overset{101}{=} 0$. Hence:

$$n^{101}+1 \overset{101}{=} 0 \quad \rightarrow \quad n+1 \overset{101}{=} 0 \quad \rightarrow \quad n \overset{101}{=} -1$$

So, 101 divides $n^{101}+1$ for all $n = 101k-1$ where $k \in \mathbb{Z}$.
(**b**) $71|(n^{360}-7)$ is equivalent to $n^{360}-7 \overset{71}{=} 0$. Hence:

$$n^{360}-7 \overset{71}{=} 0 \quad \rightarrow \quad \left(n^{71}\right)^5 n^5 \overset{71}{=} 7 \quad \rightarrow \quad n^5\, n^5 \overset{71}{=} 7 \quad \rightarrow \quad n^{10} \overset{71}{=} 7$$

The last congruence has no solution and hence there is no $n \in \mathbb{Z}$ such that 71 divides $n^{360}-7$.

17. Let p be a given prime number and let U_n symbolize the n-digit repunit number (where $\mathbb{N} \ni n > 1$).[96] Show that if U_n is the smallest repunit number that is divisible by p then $n|(p-1)$.
Solution: The n-digit repunit number can be written as $U_n = \frac{10^n-1}{9}$. Now, if U_n is divisible by p then we have:

$$\frac{10^n-1}{9} \overset{p}{=} 0 \quad \rightarrow \quad 10^n - 1 \overset{p}{=} 0 \quad \rightarrow \quad 10^n \overset{p}{=} 1$$

So, if U_n is the smallest repunit number that is divisible by p then $O_p10 = n$ because otherwise we will have $m < n$ such that $10^m \overset{p}{=} 1$ and this means that U_n is not the smallest repunit number that is divisible by p since U_m (which is divisible by p) is smaller than U_n. Now, from Problem 3 of § 1.3 we get $O_p10|\phi(p)$, i.e. $n|(p-1)$.

18. Let U_n symbolize the n-digit repunit number and p be a prime ≤ 47. Identify all p that cannot be a divisor to any repunit number (i.e. $p \not| U_n$ for any n).
Solution: . For instance:

$3\|U_3$	$7\|U_6$	$11\|U_2$	$13\|U_6$	$17\|U_{16}$	$19\|U_{18}$	$23\|U_{22}$
$29\|U_{28}$	$31\|U_{15}$	$37\|U_6$	$41\|U_5$	$43\|U_{21}$	$47\|U_{46}$	

So, among $2 \leq p \leq 47$ only 2 and 5 cannot be a divisor of repunit numbers. This is because 2 is even while repunit numbers are odd. Also, the residue of a repunit number modulo 5 is always 1.

19. Find the remainder when:
(**a**) 600! is divided by 601. (**b**) 730! is divided by 731. (**c**) 445! is divided by 6454.
Solution:
(**a**) By Wilson's theorem (noting that 601 is prime) we have: $(601-1)!+1 \overset{601}{=} 0$, i.e. $600! \overset{601}{=} -1 \overset{601}{=} 600$. Hence, the remainder when 600! is divided by 601 is 600.
(**b**) We have $731 = 17 \times 43$ and hence 730! is divisible by 731, i.e. the remainder is 0.
(**c**) The prime factorization of 6454 is $6454 = 2 \times 7 \times 461$ and hence 445! is not divisible by 6454 because it is not divisible by 461. Now, let r symbolize the remainder and hence $445! \overset{6454}{=} r$, i.e. $445! = r + 6454k$

[96] "Repunit number" stands for "repeated unit number" such as 11, 111, 1111. For instance, $U_2 = 11$ and $U_5 = 11111$.

(for some $k \in \mathbb{N}$). Since 445! and 6454 are divisible by 14 then r should also be divisible by 14, i.e. $r = 14\rho$ (for some $\rho \in \mathbb{N}$). Thus:

$445! \overset{6454}{=} 14\rho \quad \rightarrow \quad \frac{445!}{14} \overset{461}{=} \rho \quad \rightarrow \quad 445! \overset{461}{=} 14\rho \quad \rightarrow \quad 445! \frac{460!}{445!} \overset{461}{=} \frac{460!}{445!} r \quad \rightarrow$

$460! \overset{461}{=} \frac{460!}{445!} r \quad \rightarrow \quad -1 \overset{461}{=} \frac{460!}{445!} r \quad \rightarrow \quad 396r \overset{461}{=} -1 \quad \rightarrow \quad r \overset{461}{=} 383$

where:
steps 1 and 2 are from rules 9 and 6 of § 2.7 of V1,
step 5 is from Wilson's theorem (noting that 461 is prime),
step 6 is because $\frac{460!}{445!} = 446 \times 447 \times \cdots \times 460 \overset{461}{=} 396$, and
step 7 is because $r \overset{461}{=} -1 \times 396^* = -78 \overset{461}{=} 383$.
So, we have $r \overset{14}{=} 0$ (because $r = 14\rho$) and $r \overset{461}{=} 383$. On solving this system of congruence equations (using for instance the Chinese remainder theorem) we get: $r \overset{6454}{=} 2688$, i.e. the remainder when 445! is divided by 6454 is 2688.

20. Find the remainder when:
(**a**) $7^{29}16^{18}$ is divided by 23. (**b**) 7926064705871^{22315} is divided by 18.

Solution: In this Problem we use a method based on the index of integer (see § 1.5). In the following r symbolizes the remainder.
(**a**) A primitive root of 23 is 5 and we have $\big[$noting that $\phi(23) = 22\big]$:

$r \overset{23}{=} 7^{29}16^{18} \quad \rightarrow \quad I_{23,5}(r) \overset{\phi(23)}{=} I_{23,5}\left(7^{29}16^{18}\right) \quad \rightarrow$

$I_{23,5}(r) \overset{22}{=} 29\, I_{23,5}(7) + 18\, I_{23,5}(16) \quad \rightarrow \quad I_{23,5}(r) \overset{22}{=} 29 \times 19 + 18 \times 8 \quad \rightarrow$

$I_{23,5}(r) \overset{22}{=} 695 \quad \rightarrow \quad I_{23,5}(r) \overset{22}{=} 13$

So, $I_{23,5}(r) \overset{22}{=} 13$ $\big[$i.e. $I_{23,5}(r) \overset{\phi(23)}{=} 13\big]$ which means $r \overset{23}{=} 5^{13} \overset{23}{=} 21$. Hence, the remainder is 21.
(**b**) A primitive root of 18 is 5 and we have $\big[$noting that $\phi(18) = 6$ and $7926064705871 \overset{18}{=} 17\big]$:

$r \overset{18}{=} 7926064705871^{22315} \quad \rightarrow \quad r \overset{18}{=} 17^{22315} \quad I_{18,5}(r) \overset{\phi(18)}{=} I_{18,5}\left(17^{22315}\right) \quad \rightarrow$

$I_{18,5}(r) \overset{6}{=} 22315\, I_{18,5}(17) \quad \rightarrow \quad I_{18,5}(r) \overset{6}{=} 22315 \times 3 \overset{6}{=} 3$

So, $I_{18,5}(r) \overset{6}{=} 3$ $\big[$i.e. $I_{18,5}(r) \overset{\phi(18)}{=} 3\big]$ which means $r \overset{18}{=} 5^3 \overset{18}{=} 17$. Hence, the remainder is 17.

21. Find all $m \in \mathbb{Z}$ such that $m|(6n^2 - 14n - 10)$ and $m|(2n^3 - 8n + 6)$ for all $n \in \mathbb{Z}$.
Solution: On factorizing the two expressions we get: $6n^2 - 14n - 10 = 2(3n^2 - 7n - 5)$ and $2n^3 - 8n + 6 = 2(n-1)(n^2 + n - 3)$. So, the common factor of these expressions is 2. Hence, $m|(6n^2 - 14n - 10)$ and $m|(2n^3 - 8n + 6)$ for all $n \in \mathbb{Z}$ if $m = \pm 1$ and $m = \pm 2$.

22. Find all $m \in \mathbb{Z}$ such that $m|(4n^2 + 4n + 7)$ and $m|(n^2 + 5)$ for some $n \in \mathbb{Z}$.
Solution: We have:
• $m|(4n^2 + 4n + 7)$ and $m|(n^2 + 5)$ and hence $m\big|\big[(4n^2 + 4n + 7) - 4(n^2 + 5)\big]$, i.e. $m|(4n - 13)$.
• $m|(4n - 13)$ and hence $m|(4n - 13)^2$, i.e. $m|(16n^2 - 104n + 169)$.
• $m|(16n^2 - 104n + 169)$ and $m|(4n^2 + 4n + 7)$ and hence $m\big|\big[(16n^2 - 104n + 169) - 4(4n^2 + 4n + 7)\big]$, i.e. $m|(141 - 120n)$.
• $m|(4n - 13)$ and $m|(141 - 120n)$ and hence $m\big|\big[30(4n - 13) + (141 - 120n)\big]$, i.e. $m|(-249)$.
The divisors of 249 are $\pm 1, \pm 3, \pm 83, \pm 249$ and hence $m = \pm 1, \pm 3, \pm 83, \pm 249$.
It is worth noting that:
• ± 1 divides $(4n^2 + 4n + 7)$ and $(n^2 + 5)$ for all $n \in \mathbb{Z}$. This is because ± 1 divides any integer.
• ± 3 divides $(4n^2 + 4n + 7)$ and $(n^2 + 5)$ for all $n \overset{3}{=} 1$. This is because the solution of $4n^2 + 4n + 7 \overset{3}{=} 0$ is $n \overset{3}{=} 1$ while the solution of $n^2 + 5 \overset{3}{=} 0$ is $n \overset{3}{=} 1, 2$ and hence the solution of this system of congruence equations is $n \overset{3}{=} 1$ (see § 9.2.1).
• ± 83 divides $(4n^2 + 4n + 7)$ and $(n^2 + 5)$ for all $n \overset{83}{=} 24$. This is because the solution of $4n^2 + 4n + 7 \overset{83}{=} 0$

is $n \overset{83}{=} 24, 58$ while the solution of $n^2 + 5 \overset{83}{=} 0$ is $n \overset{83}{=} 24, 59$ and hence the solution of this system of congruence equations is $n \overset{83}{=} 24$.

• ± 249 divides $(4n^2+4n+7)$ and (n^2+5) for all $n \overset{249}{=} 190$. This is because the solution of $4n^2+4n+7 \overset{249}{=} 0$ is $n \overset{249}{=} 58, 190$ while the solution of $n^2 + 5 \overset{249}{=} 0$ is $n \overset{249}{=} 59, 107, 142, 190$ and hence the solution of this system of congruence equations is $n \overset{249}{=} 190$.

23. Find all $n \in \mathbb{Z}$ such that $9|(n-7)$, $17|(n+1)$ and $29|(n+11)$.
Solution: These divisibility statements are equivalent to the following congruence equations:

$$n \overset{9}{=} 7 \qquad\qquad n \overset{17}{=} -1 \qquad\qquad n \overset{29}{=} -11$$

On solving this system of congruence equations (e.g. by using the Chinese remainder theorem) we get: $n = 3382 + 4437k$ (where $k \in \mathbb{Z}$).

24. Show that the divisibility of $3m + n$ by 11 is equivalent to the divisibility of $47m - 10n$ by 11 (where $m, n \in \mathbb{Z}$).
Solution: We have:

$$47m - 10n = 3m + n + 44m - 11n = 3m + n + 11(4m - n)$$

Now, $11(4m - n)$ is divisible by 11 and hence the divisibility of $3m + n$ by 11 is equivalent to the divisibility of $47m - 10n$ by 11.

25. Let q and p be odd primes ($q \neq p$), n is a positive even integer and $k \in \mathbb{N}$. Show that if $p|(q^n + 1)$ then $p = 4k + 1$.
Solution: We have (where $n = 2\nu$ and $\nu \in \mathbb{N}$):

$$p|(q^n + 1) \quad \rightarrow \quad q^n + 1 \overset{p}{=} 0 \quad \rightarrow \quad q^{2\nu} + 1 \overset{p}{=} 0 \quad \rightarrow \quad (q^\nu)^2 \overset{p}{=} -1$$

i.e. -1 is a quadratic residue of p and hence $\left(\frac{-1}{p}\right) = 1$. So, from Problem 9 of § 1.8 we conclude that $p = 4k + 1$.

26. Let $m, n, k \in \mathbb{Z}$. Show that if $m|k$ and $n|k$ and $g = \gcd(m, n)$ then $\left(\frac{mn}{g}\right) \Big| k$.
Solution: Since $m|k$ and $n|k$ then g must be a factor of k (as well as a factor of m and n). So, let $m = g\mu$ and $n = g\nu$ while $k = g\kappa$. Accordingly, $\mu|\kappa$ and $\nu|\kappa$ where μ and ν are coprime (see point 9 in the preamble of § 2.4 of V1). Therefore, by rule 20 of § 1.9 of V1 we have $(\mu\nu)|\kappa$ which means that $\frac{\kappa}{\mu\nu}$ is an integer (say $\frac{\kappa}{\mu\nu} = A$ where $A \in \mathbb{Z}$). Now, if we multiply A by 1 in the form of g^2/g^2 then we get:

$$A = 1 \times A = \frac{g^2}{g^2} \times A = \frac{g^2}{g^2} \times \frac{\kappa}{\mu\nu} = \frac{g(g\kappa)}{(g\mu)(g\nu)} = \frac{gk}{mn} = \frac{k}{(mn)/g}$$

which means $\left(\frac{mn}{g}\right) \Big| k$.
Note: in Problem 6 of § 2.5 of V1 we proved the identity $mn = \gcd(m, n) \times \text{lcm}(m, n)$ using a prime factorization approach. This identity can also be obtained (possibly more easily and directly) as a corollary of the formulation (or method or logic) of the present Problem because (noting that μ and ν are coprime):

$$\text{lcm}(\mu, \nu) = \mu\nu \quad \rightarrow \quad g^2 \,\text{lcm}(\mu, \nu) = g\mu g\nu \quad \rightarrow \quad g \,\text{lcm}(g\mu, g\nu) = g\mu g\nu \quad \rightarrow$$
$$g \,\text{lcm}(m, n) = mn \quad \rightarrow \quad \gcd(m, n) \times \text{lcm}(m, n) = mn$$

27. Show that no odd prime of the form $p = 4k - 1$ can divide $n^2 + 1$ (where $k \in \mathbb{N}$ and $n \in \mathbb{Z}$).
Solution: If p divides $n^2 + 1$ then $n^2 + 1 \overset{p}{=} 0$, i.e. $n^2 \overset{p}{=} -1$ and hence $n^4 \overset{p}{=} 1$. Now, from Problem 1 of § 1.3 we conclude that $O_p n|4$, i.e. $O_p n = 1$ or $O_p n = 2$ or $O_p n = 4$. Now:
• If $O_p n = 1$ then $n^1 \overset{p}{=} 1$ and hence $n^2 \overset{p}{=} 1$ which contradicts $n^2 \overset{p}{=} -1$ (noting that p is an odd prime).
• If $O_p n = 2$ then $n^2 \overset{p}{=} 1$ which (again) contradicts $n^2 \overset{p}{=} -1$ (noting that p is an odd prime).
So, we must have $O_p n = 4$. Now, from Problem 3 of § 1.3 (noting that p and n must be coprime since $n^2 + 1 \overset{p}{=} 0$) we must have $4|\phi(p)$, i.e. $4|(p-1)$ and hence p must be of the form $4k + 1$, i.e. p cannot be of the form $4k - 1$ (see Problem 16 of § 2.2 of V1).

28. Show that $\frac{p^2-1}{24}$ is an integer for all $p \geq 5$ (where $p \in \mathbb{P}$).

Solution: This is because for $p \geq 5$ we have $\frac{p^2-1}{24} \geq 1$. Moreover:
• One of $(p-1)$ and $(p+1)$ must be divisible by 3 because $(p-1), p, (p+1)$ are three consecutive integers and p is not divisible by 3 because $p \geq 5$. Now, $p^2-1 = (p-1)(p+1)$ and hence p^2-1 must be divisible by 3.
• $(p-1)$ and $(p+1)$ are consecutive even numbers and hence one of them must be divisible by 2 and the other is divisible by 4 (i.e. one of them is a multiple of 2 and the other is a multiple of 4). Therefore, their product (which is equal to p^2-1) must be divisible by 8.
Thus, p^2-1 is divisible by 3 and by 8 and hence it must be divisible by 24 (noting that 3 and 8 are coprime), i.e. $\frac{p^2-1}{24}$ is an integer for all $p \geq 5$.

29. Show the following:
(**a**) p divides the sum of its quadratic residues (where p is a prime ≥ 5).
(**b**) p divides the sum of the squares of its quadratic non-residues (where p is a prime ≥ 7).
Solution:
(**a**) According to Problem 2 of § 1.6, the $(p-1)/2$ quadratic residues of p are: $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$. Hence, their sum is (see Eq. 16 in V1):

$$\sum_{k=1}^{(p-1)/2} k^2 = \frac{\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)\left(2\times\frac{p-1}{2}+1\right)}{6} = \frac{p^3-p}{24} = p\left(\frac{p^2-1}{24}\right)$$

which is divisible by $p \geq 5$ (noting that $\frac{p^2-1}{24}$ is an integer for $p \geq 5$; see Problem 28).
It is worth noting that although this proof is specific to the integers $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ the given proposition should also apply to their residue classes (mod p) since the integers in any class differ from each other by integer multiples of p and hence the sum of quadratic residues (represented by any integer in their classes) should be the same as above plus an algebraic sum of integer multiples of p and hence the sum remains divisible by p.
(**b**) Let S symbolize the sum of the squares of the quadratic non-residues of p and let r be a primitive root of p (see point 5 in the preamble of § 1.4). Now, since the quadratic non-residues of p are the odd powers of r (see Problem 7 of § 1.6) then we have:

$$S = \sum_{k=1}^{(p-1)/2} \left(r^{2k-1}\right)^2 = \sum_{k=1}^{(p-1)/2} r^{4k-2} \qquad \rightarrow \qquad r^4 S = \sum_{k=1}^{(p-1)/2} r^{4k+2} = \sum_{k=2}^{(p+1)/2} r^{4k-2}$$

Now, if we subtract S from $r^4 S$ we get:

$$r^4 S - S = \left(\sum_{k=2}^{(p+1)/2} r^{4k-2}\right) - \left(\sum_{k=1}^{(p-1)/2} r^{4k-2}\right) = r^{2p} - r^2 = (r^p - r)(r^p + r) \qquad \rightarrow \qquad r^4 S - S \overset{p}{=} 0$$

where the last step is because $r^p - r \overset{p}{=} 0$ by Fermat's little theorem. Accordingly, $S(r^4-1) \overset{p}{=} 0$ which implies that $S \overset{p}{=} 0$ or $(r^4-1) \overset{p}{=} 0$. However, for $p \geq 7$ we have $r^4 - 1 \overset{p}{\neq} 0$ (i.e. $r^4 \overset{p}{\neq} 1$) because r is a primitive root of p and hence its order is $(p-1)$, i.e. $r^4 \overset{p}{\neq} 1$. So, we must have $S \overset{p}{=} 0$, i.e. p divides the sum of the squares of its quadratic non-residues.
Finally, we should add a note similar to the note in the end of part (a), i.e. r and its powers represent residue classes and hence the proof is general. We should also note that part (a) can also be proved in a similar way to the proof of part (b), but we preferred (for the sake of diversity) to use a different approach.

Chapter 16
Sequences and Series

1. Find all the integer terms of the following sequences (where $n = 1, 2, 3, \ldots$):

   (**a**) $a_n = \frac{3n^3-5n^2+11n+7}{2n^2+2n-3}$. (**b**) $a_n = \frac{n^4+2n^3-5n-3}{n^2+n+12}$. (**c**) $a_n = \frac{2n^5+3n^3+14n^2+21}{2n^2+3}$.

   (**d**) $a_n = \frac{13-7n^2}{2n-17}$. (**e**) $a_n = \sum_{k=1}^{n} \frac{k^2+2k-3}{5}$.

   Solution:

   (**a**) We have:

$$\frac{3n^3-5n^2+11n+7}{2n^2+2n-3} = \frac{1}{2}\left(3n-8+\frac{47n-10}{2n^2+2n-3}\right)$$

   Now, $|47n-10| \geq |2n^2+2n-3|$ only for $n = 1, 2, \ldots, 22$. On inspecting these 22 terms we find only a_1 is an integer. Hence, only a_1 of this sequence is an integer.

   (**b**) We have:

$$\frac{n^4+2n^3-5n-3}{n^2+n+12} = n^2+n-13+\frac{153-4n}{n^2+n+12}$$

   Now, $|153-4n| \geq |n^2+n+12|$ only for $n = 1, 2, \ldots, 9$. On inspecting these 9 terms we find none of these terms is an integer. Hence, this sequence has no integer term.

   (**c**) We have:

$$\frac{2n^5+3n^3+14n^2+21}{2n^2+3} = \frac{(2n^2+3)(n^3+7)}{2n^2+3} = n^3+7$$

   Hence, all the terms of this sequence are integers.

   (**d**) We have:

$$\frac{13-7n^2}{2n-17} = \frac{1}{4}\left(-14n-119-\frac{1971}{2n-17}\right)$$

   Now, if a_n should be an integer then (as a necessary but not sufficient condition) $2n-17$ must divide 1971, i.e. $2n-17$ must be equal to the divisors of 1971 which are $1, 3, 9, 27, 73, 219, 657, 1971$ and their negatives. Considering all these divisors we find that only the following values of $n \in \mathbb{N}$ make $2n-17$ a divisor of 1971 and a_n an integer: $n = 4, 7, 8, 9, 10, 13, 22, 45, 118, 337, 994$. So, only the terms of the sequence with these values of n are integers.

   (**e**) We have (see Eqs. 15 and 16 of V1):

$$\begin{aligned}\sum_{k=1}^{n}\frac{k^2+2k-3}{5} &= \frac{1}{5}\left[\left(\sum_{k=1}^{n}k^2\right)+\left(2\sum_{k=1}^{n}k\right)-\left(\sum_{k=1}^{n}3\right)\right]\\ &= \frac{1}{5}\left[\left(\frac{n(n+1)(2n+1)}{6}\right)+2\frac{n(n+1)}{2}-3n\right]\\ &= \frac{1}{5}\left[\frac{2n^3+9n^2-11n}{6}\right] = \frac{2n^3+9n^2-11n}{30}\end{aligned}$$

   Now, the solutions of $2n^3+9n^2-11n \overset{30}{=} 0$ are $n \overset{5}{=} 0, 1, 2$. Hence, the integer terms of this sequence are $a_{n\overset{5}{=}0,1,2}$ (i.e. $a_1, a_2, a_5, a_6, a_7, a_{10}, a_{11}, a_{12}, a_{15}, a_{16}, a_{17}, \ldots$).

2. Find all $s \in \mathbb{Z}$ that make the series $\sum_{k=1}^{23}(s+k)^3$ a natural power of 23.

   Solution: We have:

$$\sum_{k=1}^{23}(s+k)^3 = \sum_{k=1}^{23}\left(s^3+3s^2k+3sk^2+k^3\right) = \left(\sum_{k=1}^{23}s^3\right)+\left(\sum_{k=1}^{23}3s^2k\right)+\left(\sum_{k=1}^{23}3sk^2\right)+\left(\sum_{k=1}^{23}k^3\right)$$

$$\begin{aligned} &= s^3\left(\sum_{k=1}^{23}1\right)+3s^2\left(\sum_{k=1}^{23}k\right)+3s\left(\sum_{k=1}^{23}k^2\right)+\left(\sum_{k=1}^{23}k^3\right) \\ &= 23s^3+3s^2\left(\frac{23(23+1)}{2}\right)+3s\left(\frac{23(23+1)(2\times 23+1)}{6}\right)+\left(\frac{23^2(23+1)^2}{4}\right) \\ &= 23s^3+828s^2+12972s+76176 = 23(s^3+36s^2+564s+3312) \end{aligned}$$

Now, the series is supposed to be a natural power of 23 and hence:

$$23(s^3+36s^2+564s+3312)=23^m \qquad \rightarrow \qquad s^3+36s^2+564s+3312=23^{m-1} \qquad (m\in\mathbb{N})$$

Now, for $m=1$ we have $s^3+36s^2+564s+3312=1$ which has no (integer) solution.
For $m>1$, $(s^3+36s^2+564s+3312)=(s+12)(s^2+24s+276)=23^{m-1}$ and hence we have 3 cases:
• $s+12=\pm 1$ and $23|(s^2+24s+276)$. However, these conditions are incompatible because $s=-13$ and $s=-11$ do no make $(s^2+24s+276)$ divisible by 23.
• $s^2+24s+276=\pm 1$ and $23|(s+12)$. However, $s^2+24s+276=\pm 1$ has no (integer) solution.
• $23|(s+12)$ and $23|(s^2+24s+276)$. However, the solution of $s+12\overset{23}{=}0$ is $s\overset{23}{=}11$ while the solutions of $s^2+24s+276\overset{23}{=}0$ are $s\overset{23}{=}0,22$ which are incompatible.
So in brief, there is no $s\in\mathbb{Z}$ that makes the series $\sum_{k=1}^{23}(s+k)^3$ a natural power of 23.

3. Find all the integer terms of the following sequences (where $n=1,2,3,\ldots$):
(**a**) $a_n=\sqrt{64n^6+16n^3+1}$. (**b**) $a_n=\sqrt{4n^2-24n+41}$. (**c**) $a_{n+1}=a_n+\sqrt{2a_n-1}$ $(a_1=1)$.
Solution:
(**a**) We have:

$$\sqrt{64n^6+16n^3+1}=\sqrt{(2^3n^3)^2+2(2^3n^3)+1}=\sqrt{(8n^3+1)^2}=8n^3+1$$

So, all the terms of this sequence are integers.
(**b**) We have:

$$\sqrt{4n^2-24n+41}=\sqrt{4n^2-24n+36+5}=\sqrt{(2n-6)^2+5}=\sqrt{N^2+5}$$

Now, if $\sqrt{4n^2-24n+41}$ is to be an integer then N^2+5 must be a perfect square, i.e. $N^2+5=m^2$ (where $m\in\mathbb{Z}$), i.e.

$$m^2-N^2=5 \qquad \rightarrow \qquad (m-N)(m+N)=(-1)(-5)=(-5)(-1)=(1)(5)=(5)(1)$$

On solving these 4 systems of equations we get (respectively): $N=-2,2,2,-2$ and hence $n=2,4,4,2$. So, only a_2 and a_4 are integers.
(**c**) We note first that this sequence is strictly increasing (so its terms are pairwise distinct) and all its terms are positive. We have $a_1=1$ and hence $a_2=1+\sqrt{2(1)-1}=2$. So, the first two terms of this sequence are integers. Now, we show that it is impossible for the other terms of this sequence to be integers. For the $(n+1)^{st}$ term $(n\geq 2)$ to be an integer we must have $a_n\in\mathbb{N}$ and $2a_n-1=m^2$ (where $m\in\mathbb{N}$), i.e.

$$a_n=\frac{m^2+1}{2}=\frac{(2x+1)^2+1}{2} \qquad (x\in\mathbb{N}^0) \tag{39}$$

where the second equality is justified because m must be odd (since a_n is supposedly an integer). Now, the difference d between any two consecutive terms of the sequence according to Eq. 39 should be at least:

$$d=\frac{(2x+3)^2+1}{2}-\frac{(2x+1)^2+1}{2}=4x+4$$

However, according to the sequence form (combined with the condition of oddity) the actual difference between two consecutive terms of the sequence is:

$$a_{n+1}-a_n=\sqrt{2a_n-1}=\sqrt{2\frac{(2x+1)^2+1}{2}-1}=\sqrt{(2x+1)^2}=2x+1$$

This difference is much smaller than d and hence these conditions are incompatible which means that no term (other than a_1 and a_2) can be an integer. So, only a_1 and a_2 of this sequence are integers.

4. Find all $n \in \mathbb{N}$ such that:
(**a**) $\sum_{k=1}^{n}(k^3+1)$ is divisible by 47. (**b**) $\sum_{k=1}^{n}(2k-1)^3$ is divisible by 13.
(**c**) $\sum_{k=1}^{n}(11^k-1)$ is divisible by 6.
Solution:
(**a**) We have (see Eq. 17 of V1):

$$\sum_{k=1}^{n}(k^3+1) = \left(\sum_{k=1}^{n}k^3\right) + \left(\sum_{k=1}^{n}1\right) = \frac{n^2(n+1)^2}{4} + n = \frac{n^4+2n^3+n^2+4n}{4}$$

So, if the given series is divisible by 47 then $(n^4+2n^3+n^2+4n)$ must be divisible by 47 (noting that 4 and 47 are coprime), i.e. $n^4+2n^3+n^2+4n \overset{47}{=} 0$. The solution to this congruence equation is $n \overset{47}{=} 0$ (see § 8.2). So, the given series is divisible by 47 *iff* $n = 47m$ where $m \in \mathbb{N}$.
(**b**) From Eq. 20 of V1 we have $\sum_{k=1}^{n}(2k-1)^3 = n^2(2n^2-1)$. Now, if 13 divides this series then 13 must divide n^2 (and hence divide n) or 13 must divide $(2n^2-1)$. However, 13 does not divide $(2n^2-1)$ because $2n^2-1 \overset{13}{=} 0$ has no solution. Therefore, if 13 divides this series then 13 must divide n. So, this series is divisible by 13 for all $n = 13m$ where $m \in \mathbb{N}$.
(**c**) By Euler's theorem (with the power rule for congruence) we have $11^{2m}-1 \overset{6}{=} 0$ where $m \in \mathbb{N}$. This means that all even terms of the series are 0 (mod 6) and hence $\sum_{k=1}^{2m}(11^k-1) \overset{6}{=} \sum_{k=1}^{2m-1}(11^k-1)$, i.e the sum of the first $2m$ terms is the same (mod 6) as the sum of the first $2m-1$ terms. Accordingly:

$$\begin{aligned}
\sum_{k=1}^{2}(11^k-1) &\overset{6}{=} \sum_{k=1}^{1}(11^k-1) \overset{6}{=} 4\\
\sum_{k=1}^{4}(11^k-1) &\overset{6}{=} \sum_{k=1}^{3}(11^k-1) \overset{6}{=} 2\\
\sum_{k=1}^{6}(11^k-1) &\overset{6}{=} \sum_{k=1}^{5}(11^k-1) \overset{6}{=} 0
\end{aligned}$$

As the last entry is 0 (mod 6), this cycle repeats itself and hence the given series is divisible by 6 for all $n = 5+6s$ and $n = 6(1+s)$ where $s \in \mathbb{N}^0$.[97]

5. Show that the series $\sum_{k=1}^{m} n_k^4$ is divisible by 4 where n_k are odd natural numbers and m is a natural multiple of 4 (i.e. $m = 4, 8, 12, \ldots$).
Solution: We have (where $s \in \mathbb{N}^0$):

$$n_k^4 = (2s+1)^4 = 16s^4+32s^3+24s^2+8s+1 \overset{4}{=} 1$$

Hence:

$$\sum_{k=1}^{m} n_k^4 \overset{4}{=} \sum_{k=1}^{m} 1 = m$$

Now, since m is a natural multiple of 4, it is divisible by 4 and hence the series $\sum_{k=1}^{m} n_k^4$ is divisible by 4.

[97] We note that:

$$\sum_{k=1}^{7}(11^k-1) \overset{6}{=} 11^7-1 \overset{6}{=} 11-1 \overset{6}{=} 4$$

where step 1 is because $\sum_{k=1}^{6}(11^k-1)$ is 0 (mod 6), and step 2 is because $11^6 \overset{6}{=} 1$ according to Euler's theorem (with the power rule for congruence). So, this should fully explain our claim that this cycle repeats itself (i.e. every 6 consecutive integers).

6. Show that the following series cannot be an integer for any value of $n \in \mathbb{N}$:

$$\sum_{k=1}^{n}(-1)^{k+1}\frac{k}{k+1}$$

Solution: This series cannot be an integer because for any $n \in \mathbb{N}$ its magnitude is less than 1 and greater than 0.[98] This is because if we start from the last term in the series $\left[\text{i.e. } (-1)^{n+1}\frac{n}{n+1}\right]$ then it is obviously less than 1 and greater than 0 in magnitude. Now, when we add to the last term its previous term $\left[\text{i.e. } (-1)^{n}\frac{n-1}{n}\right]$ which is opposite in sign and smaller in magnitude, the magnitude of the sum becomes less than the magnitude of $(-1)^{n+1}\frac{n}{n+1}$ but greater than 0. Now, if we add the next term $\left[\text{i.e. } (-1)^{n-1}\frac{n-2}{n-1}\right]$ the magnitude will restore some of its lost value [which it lost when we added the term $(-1)^{n}\frac{n-1}{n}$] but it cannot compensate all the loss and restore its original value (let alone exceeding it) and hence it remains less than 1 and greater than 0. This applies all over the series as we move backwards by adding the previous terms successively until we reach the first term. So, the magnitude of this series keeps oscillating (along its terms) but it remains always less than 1 and greater than 0 and hence the series cannot be an integer for any $n \in \mathbb{N}$. The plot of Figure 5 should provide more clarification and illustration to this argument.

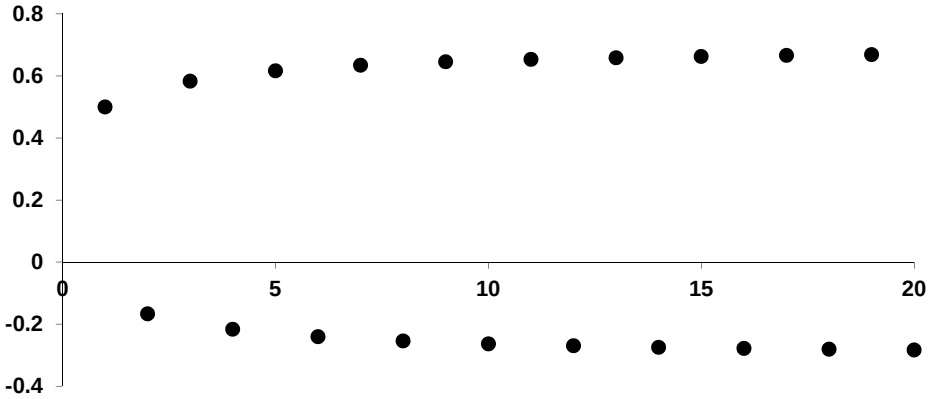


Figure 5: The plot of Problem 6 of § 16. The vertical axis represents the sum as a function of n (which is represented on the horizontal axis).

7. Give examples of natural numbers (greater than 1) which are coprime to all the terms of the following infinite sequences (where $n \in \mathbb{N}$):

(**a**) $a_n = 3^n + 5^n + 7^n$. (**b**) $b_n = 17^n - 11^n + 13^n - 1$. (**c**) $c_n = n^3 - 3n^2 + 1$.

Solution: The idea of this type of problems is simple, that is: we look for a prime number[99] which cannot divide any term of the given sequence, e.g. a prime p such that $3^n + 5^n + 7^n \overset{p}{\neq} 0$ for any $n \in \mathbb{N}$.

(**a**) The obvious example is $p = 2$ because all the terms of this sequence are odd and hence $a_n \overset{2}{\neq} 0$ for any $n \in \mathbb{N}$. Other examples are $p = 7$ and $p = 17$ because $a_n \overset{p}{\neq} 0$ for any one of these primes and for any $n \in \mathbb{N}$.[100]

(**b**) Two examples are $p = 11$ and $p = 13$ because $b_n \overset{p}{\neq} 0$ for any one of these primes and for any

[98] We note that for small n (e.g. $n = 1, 2, 3$) the proposition is obviously true. Hence, the focus in the following argument is on large n where the series consists of many terms.

[99] Choosing "prime number" is just to make the problem easier to solve and avoid unnecessary complications.

[100] For $p = 7$ we have $a_n \overset{7}{=} 1, 6, 5, 6, 1, 2$ corresponding to $n \overset{6}{=} 1, 2, 3, 4, 5, 6$ while for $p = 17$ we have $a_n \overset{17}{=} 15, 15, 2, 13, 13, 9, 16, 14, 2, 2, 15, 4, 4, 8, 1, 3$ corresponding to $n \overset{16}{=} 1, 2, \ldots, 16$.

$n \in \mathbb{N}$.[101]

(**c**) Some examples are $p = 2, 5, 7, 11, 13$ because $c_n \overset{p}{\neq} 0$ for any one of these primes and for any $n \in \mathbb{N}$.[102]

8. Give examples of natural numbers which are coprime to none of the terms of the following infinite sequences (where $n \in \mathbb{N}$):

(**a**) $a_n = n^3 + 5n + 6$. (**b**) $b_n = n^5 + 24n + 15$. (**c**) $c_n = n^9 - n$. (**d**) $d_n = 7^n - 4^n$.

Solution: The easiest way to solve this type of problems is to look for a small prime p that makes the congruence of the sequence identically zero (mod p), e.g. $a_n \overset{p}{=} 0$ for all $n \in \mathbb{N}$. Thus, any n which is a natural multiple of p will then be coprime to none of the terms of the sequence.

(**a**) $a_n \overset{3}{=} 0$ for all $n \in \mathbb{N}$ and hence any multiple of 3 is coprime to none of the terms of this sequence.

(**b**) $b_n \overset{5}{=} 0$ for all $n \in \mathbb{N}$ and hence any multiple of 5 is coprime to none of the terms of this sequence.

(**c**) $c_n \overset{2}{=} 0$, $c_n \overset{3}{=} 0$ and $c_n \overset{5}{=} 0$ for all $n \in \mathbb{N}$ and hence any multiple of 2 or 3 or 5 is coprime to none of the terms of this sequence.

(**d**) $d_n \overset{3}{=} 0$ for all $n \in \mathbb{N}$ (noting that $7^n - 4^n \overset{3}{=} 1^n - 1^n = 0$) and hence any multiple of 3 is coprime to none of the terms of this sequence.

9. Derive lower and upper bounds on the following series in terms of n:

(**a**) $\sum_{k=1}^{n} \frac{k}{k+1}$. (**b**) $\sum_{k=1}^{n} \sqrt{k}$.

Solution:

(**a**) $x/(x+1)$ is an increasing function and hence:

$$\begin{aligned}
\int_{k-1}^{k} \frac{x}{x+1}\,dx &< \frac{k}{k+1} < \int_{k}^{k+1} \frac{x}{x+1}\,dx \\
\Big[x - \ln(x+1)\Big]_{k-1}^{k} &< \frac{k}{k+1} < \Big[x - \ln(x+1)\Big]_{k}^{k+1}
\end{aligned}$$

Now, if we sum from $k = 1$ to $k = n$ we get:

$$\begin{aligned}
\left(\sum_{k=1}^{n} \Big[x - \ln(x+1)\Big]_{k-1}^{k}\right) &< \left(\sum_{k=1}^{n} \frac{k}{k+1}\right) < \left(\sum_{k=1}^{n} \Big[x - \ln(x+1)\Big]_{k}^{k+1}\right) \\
\Big[x - \ln(x+1)\Big]_{0}^{n} &< \left(\sum_{k=1}^{n} \frac{k}{k+1}\right) < \Big[x - \ln(x+1)\Big]_{1}^{n+1} \\
\Big[n - \ln(n+1)\Big] &< \left(\sum_{k=1}^{n} \frac{k}{k+1}\right) < \Big[n - \ln(n+2) + \ln(2)\Big]
\end{aligned}$$

(**b**) $\sqrt{x}$ is an increasing function and hence:

$$\begin{aligned}
\int_{k-1}^{k} \sqrt{k}\,dx &< \sqrt{k} < \int_{k}^{k+1} \sqrt{k}\,dx \\
\left[\frac{x^{3/2}}{3/2}\right]_{k-1}^{k} &< \sqrt{k} < \left[\frac{x^{3/2}}{3/2}\right]_{k}^{k+1}
\end{aligned}$$

Now, if we sum from $k = 1$ to $k = n$ we get:

$$\left(\sum_{k=1}^{n} \left[\frac{x^{3/2}}{3/2}\right]_{k-1}^{k}\right) < \left(\sum_{k=1}^{n} \sqrt{k}\right) < \left(\sum_{k=1}^{n} \left[\frac{x^{3/2}}{3/2}\right]_{k}^{k+1}\right)$$

[101] For $p = 11$ we have $b_n \overset{11}{=} 7, 6, 3, 2, 8, 2, 3, 6, 7, 1$ corresponding to $n \overset{10}{=} 1, 2, \ldots, 10$ while for $p = 13$ we have $b_n \overset{13}{=} 5, 11, 6, 5, 2, 1, 1, 6, 3, 11, 3, 12$ corresponding to $n \overset{12}{=} 1, 2, \ldots, 12$.

[102] The congruence equation $n^3 - 3n^2 + 1 \overset{p}{=} 0$ has no solution for $p = 2, 5, 7, 11, 13$ (see § 8.2).

$$\left[\frac{x^{3/2}}{3/2}\right]_0^n < \left(\sum_{k=1}^{n}\sqrt{k}\right) < \left[\frac{x^{3/2}}{3/2}\right]_1^{n+1}$$
$$\left[\frac{n^{3/2}}{3/2}\right] < \left(\sum_{k=1}^{n}\sqrt{k}\right) < \left[\frac{(n+1)^{3/2}-1}{3/2}\right]$$

10. Find the integer part of the following series as a function of n:
(**a**) $\sum_{k=0}^{n}\left(\frac{9}{10}\right)^k$. (**b**) $\sum_{k=0}^{n}\frac{1}{k!}$. (**c**) $\sum_{k=1}^{n}\frac{1}{k^2}$. (**d**) $\sum_{k=0}^{n}\frac{1}{m^k}$ $(\mathbb{N}\ni m>1)$.
Solution:
(**a**) This is a geometric series with $a=1$ and $r=9/10$ and hence it converges to $\left[1-(9/10)\right]^{-1}=10$ (see Eq. 22 in V1). So, all we need to do is to determine the values of n at which the series steps from one integer level to the next between 1 and 9. Now, we have (see Eq. 22 in V1):

$$\sum_{k=0}^{n}\left(\frac{9}{10}\right)^k=\frac{1-(9/10)^{n+1}}{1-(9/10)}=10\left[1-(9/10)^{n+1}\right]$$

On equating $10\left[1-(9/10)^{n+1}\right]$ to $1,2,\ldots,9$ and solving for n we find that the integer part is:[103]

1 ($n=0,1$) 2 ($n=2$) 3 ($n=3$) 4 ($n=4,5$) 5 ($n=6,7$)

6 ($n=8,9,10$) 7 ($n=11,\ldots,14$) 8 ($n=15,\ldots,20$) 9 ($n=21,\ldots$) 10 (at ∞)

(**b**) This series converges to e ($\simeq 2.718$) and hence its integer part can only be 1 or 2. Now, we have $\sum_{k=0}^{0}\frac{1}{k!}=1$ and $\sum_{k=0}^{1}\frac{1}{k!}=2$ and hence the integer part of this series is 1 for $n=0$ and 2 for $n=1,2,\ldots$ (to ∞).
(**c**) This series converges to $\pi^2/6$ ($\simeq 1.645$) and hence its integer part is always 1 (i.e. for $n=1,2,\ldots$).
(**d**) This series converges to $\frac{m}{m-1}$ and hence its integer part is always 1 (i.e. for $n=0,1,2,\ldots$).

11. Find the integer part of the following:
(**a**) $\sum_{n=0}^{10^4}\left(-\frac{1001}{1000}\right)^n$. (**b**) $\sum_{n=0}^{10^4}\frac{1}{\sqrt{n+1}+\sqrt{n}}$. (**c**) $\sum_{n=1}^{10^4}\sqrt[20]{n}$. (**d**) $\sum_{n=1}^{10^6}\frac{n}{n+1}$.
Solution:
(**a**) We have:

$$\sum_{n=0}^{10^4}\left(-\frac{1001}{1000}\right)^n=\sum_{n=0}^{5000}\left(-\frac{1001}{1000}\right)^{2n}+\sum_{n=0}^{4999}\left(-\frac{1001}{1000}\right)^{2n+1}=\sum_{n=0}^{5000}\left(\frac{1001}{1000}\right)^{2n}-\sum_{n=0}^{4999}\left(\frac{1001}{1000}\right)^{2n+1}\equiv A-B$$

Now, A is a geometric series with $a=1$ and $r=(1001/1000)^2$ while B is a geometric series with $a=(1001/1000)$ and $r=(1001/1000)^2$. Hence (see Eq. 22 in V1):

$$A=\frac{1-(1001/1000)^{10002}}{1-(1001/1000)^2}\simeq 10974281.17 \qquad B=\left(\frac{1001}{1000}\right)\frac{1-(1001/1000)^{10000}}{1-(1001/1000)^2}\simeq 10963316.85$$

So, $A-B\simeq 10964.32$ and hence the integer part of the given sum is 10964.
(**b**) We have:

$$\begin{aligned}\sum_{n=0}^{10^4}\frac{1}{\sqrt{n+1}+\sqrt{n}} &= \sum_{n=0}^{10^4}\frac{\sqrt{n+1}-\sqrt{n}}{n+1-n}=\sum_{n=0}^{10^4}(\sqrt{n+1}-\sqrt{n})\\ &= (\sqrt{1}-\sqrt{0})+(\sqrt{2}-\sqrt{1})+\cdots+(\sqrt{10000}-\sqrt{9999})+(\sqrt{10001}-\sqrt{10000})\end{aligned}$$

[103] For example: $10\left[1-(9/10)^{n+1}\right]=5$ leads to

$$n+1=\frac{\log(1/2)}{\log(9/10)}\simeq 6.58$$

and hence the series steps up from the 4 integer level to the 5 integer level at $n=6$.

$$= \quad -\sqrt{0} + \sqrt{10001} = \sqrt{10001} \simeq 100.005$$

Hence, the integer part of the given sum is 100.
(**c**) $\sqrt[20]{x}$ is an increasing function and hence:

$$\begin{aligned} \int_{n-1}^{n} \sqrt[20]{x}\,dx &< \sqrt[20]{n} < \int_{n}^{n+1} \sqrt[20]{x}\,dx \\ \left[\frac{x^{21/20}}{21/20}\right]_{n-1}^{n} &< \sqrt[20]{n} < \left[\frac{x^{21/20}}{21/20}\right]_{n}^{n+1} \end{aligned}$$

Now, if we sum from $n = 1$ to $n = 10^4$ we get:

$$\begin{aligned} \left(\sum_{n=1}^{10^4} \left[\frac{x^{21/20}}{21/20}\right]_{n-1}^{n}\right) &< \left(\sum_{n=1}^{10^4} \sqrt[20]{n}\right) < \left(\sum_{n=1}^{10^4} \left[\frac{x^{21/20}}{21/20}\right]_{n}^{n+1}\right) \\ \left[\frac{x^{21/20}}{21/20}\right]_{0}^{10000} &< \left(\sum_{n=1}^{10^4} \sqrt[20]{n}\right) < \left[\frac{x^{21/20}}{21/20}\right]_{1}^{10001} \\ 15094.22 &< \left(\sum_{n=1}^{10^4} \sqrt[20]{n}\right) < 15094.85 \end{aligned}$$

Hence, the integer part of the given sum is 15094.
(**d**) From part (a) of Problem 9 we have:

$$\begin{aligned} \Big[10^6 - \ln(10^6+1)\Big] &< \left(\sum_{n=1}^{10^6} \frac{n}{n+1}\right) < \Big[10^6 - \ln(10^6+2) + \ln(2)\Big] \\ 999986.18 &< \left(\sum_{n=1}^{10^6} \frac{n}{n+1}\right) < 999986.88 \end{aligned}$$

Hence, the integer part of the given sum is 999986.

12. Find the solutions of the following congruence series equations (where $x \in \mathbb{N}$ and $3 < p \in \mathbb{P}$):

(**a**) $\sum_{k=0}^{p-3} x^k \overset{p}{=} 0$. (**b**) $\sum_{k=0}^{p-3} x^k \overset{p}{=} -1$. (**c**) $\sum_{k=0}^{p-3} x^k \overset{p}{=} 1$.

Solution:
(**a**) If $x \overset{p}{=} 0$ then there is no solution (because $1 \overset{p}{\neq} 0$).
If $x \overset{p}{=} 1$ then there is no solution (because $p - 2 \overset{p}{\neq} 0$).
If $x \overset{p}{\neq} 0, 1$ then we have:

$\sum_{k=0}^{p-3} x^k \overset{p}{=} 0 \quad \rightarrow \quad \sum_{k=0}^{p-2} x^k \overset{p}{=} x^{p-2} \quad \rightarrow \quad \frac{x^{p-1}-1}{x-1} \overset{p}{=} x^{p-2} \quad \rightarrow$

$x^{p-1} - 1 \overset{p}{=} x^{p-2}(x-1) \quad \rightarrow \quad x^{p-2}(x-1) \overset{p}{=} 0$

where in step 1 we added x^{p-2} to both sides, in step 2 we used the geometric series formula, in step 3 we multiplied both side by $x - 1$, and in step 4 we used Fermat's little theorem. So, from the last congruence equation we must have: $x \overset{p}{=} 0$ or $x \overset{p}{=} 1$ which are not acceptable (because $x \overset{p}{\neq} 0, 1$).
Hence, there is no solution to the given congruence series equation.
(**b**) If $x \overset{p}{=} 0$ then there is no solution (because $1 \overset{p}{\neq} -1$).
If $x \overset{p}{=} 1$ then there is no solution (because $p - 2 \overset{p}{\neq} -1$).

If $x \overset{p}{\neq} 0, 1$ then we have:

$\sum_{k=0}^{p-3} x^k \overset{p}{=} -1 \quad \rightarrow \quad \sum_{k=0}^{p-2} x^k \overset{p}{=} x^{p-2} - 1 \quad \rightarrow \quad \frac{x^{p-1}-1}{x-1} \overset{p}{=} x^{p-2} - 1 \quad \rightarrow$

$x^{p-1} - 1 \overset{p}{=} (x-1)(x^{p-2} - 1) \quad \rightarrow \quad x^{p-1} - x^{p-2} - x + 1 \overset{p}{=} 0 \quad \rightarrow \quad x^{p-2} + x \overset{p}{=} 2$

where the steps are justified as in part (a). However, the only solution[104] to the last congruence equation is $x \overset{p}{=} 1$ which is not acceptable (because $x \overset{p}{\neq} 0, 1$).

Hence, there is no solution to the given congruence series equation.

(**c**) If $x \overset{p}{=} 0$ then we have a solution (because $1 \overset{p}{=} 1$).

If $x \overset{p}{=} 1$ then there is no solution (because $p - 2 \overset{p}{\neq} 1$).

If $x \overset{p}{\neq} 0, 1$ then we have:

$\sum_{k=0}^{p-3} x^k \overset{p}{=} 1 \quad \rightarrow \quad \sum_{k=0}^{p-2} x^k \overset{p}{=} x^{p-2} + 1 \quad \rightarrow \quad \frac{x^{p-1}-1}{x-1} \overset{p}{=} x^{p-2} + 1 \quad \rightarrow$

$x^{p-1} - 1 \overset{p}{=} (x-1)(x^{p-2} + 1) \quad \rightarrow \quad x^{p-1} - 1 \overset{p}{=} x^{p-1} + x - x^{p-2} - 1 \quad \rightarrow \quad x^{p-2} - x \overset{p}{=} 0 \quad \rightarrow$

$x(x^{p-3} - 1) \overset{p}{=} 0$

So, we must have $x \overset{p}{=} 0$ (which is not acceptable because $x \overset{p}{\neq} 0, 1$ although this solution was obtained already) or $x \overset{p}{=} 1$ (which is not acceptable because $x \overset{p}{\neq} 0, 1$) or $x \overset{p}{=} -1$, i.e. $x \overset{p}{=} p - 1$ (which is acceptable).

Hence, there are two solutions to the given congruence series equation: $x \overset{p}{=} 0$ and $x \overset{p}{=} p - 1$.

13. Find all $m, n, k \in \mathbb{N}$ such that $(2m-1)^2 + (2n-1)^2 = \sum_{s=1}^{k} (2s-1)$.

Solution: According to the formula of arithmetic series we have:

$$\sum_{s=1}^{k} (2s-1) = \frac{k\,(1+2k-1)}{2} = k^2$$

Now, if we remember that no perfect square can be the sum of two odd squares (see Problem 17 of § 4) then we can conclude that there are no $m, n, k \in \mathbb{N}$ that satisfy the given series equation.

---

[104] This is because:

$x^{p-2} + x \overset{p}{=} 2 \quad \rightarrow \quad x^{p-1} + x^2 \overset{p}{=} 2x \quad \rightarrow \quad 1 + x^2 \overset{p}{=} 2x \quad \rightarrow \quad x^2 - 2x + 1 \overset{p}{=} 0 \quad \rightarrow \quad (x-1)^2 \overset{p}{=} 0$

Chapter 17
Cryptography

1. In this introductory Problem of this chapter we briefly investigate one of the most common applications of number theory in real life which is in cryptography. The most famous and widely used method of cryptography is allegedly the RSA public key system and this is what we will investigate here. This method is based on modular arithmetic with the use of very large prime numbers which makes cracking the code (during the time in which the secrecy of the message is important) practically impossible (or supposedly so) due to the difficulty of factoring very large numbers. The basic idea of public key cryptography (and notably RSA) is rather simple although the technical details are rather messy. In brief, although the encoding method (i.e. the information and processes required to do the encryption) in this encryption method is public (and hence encoding can be done by anyone and notably the sender), the decoding method is secret because it depends on a piece of information available only to the receiver of the message (i.e. the one who is intended to be informed by the content of the message).
So, let us first define our symbols and explain the main concepts used in the RSA encryption system:
• p and q are very large prime numbers.
• n is the product of p and q, i.e. $n = pq$.[105]
• ϕ is the totient of n which is the product of $(p-1)$ and $(q-1)$, i.e. $\phi = (p-1)(q-1)$.
• r is the encryption exponent which is a natural number that is coprime to ϕ and $1 < r < \phi$.
• ρ is the decryption exponent which is the modular multiplicative inverse of r (modulo ϕ), i.e. $r\rho \overset{\phi}{=} 1$.
• m is the message text (represented numerically by integers) where m is coprime to p and q.
• c is the cipher text (represented numerically by integers).
• k is the public key (i.e. known to everyone or supposedly so)[106] which is used to encrypt the message text m. The public key is the pair (n, r), i.e. $k = (n, r)$.
• κ is the private key (i.e. known only to the receiver of the message) which is used to decrypt the cipher text c. The private key is the pair (n, ρ), i.e. $\kappa = (n, \rho)$.
• f is the encoding function which takes m and encrypt it (i.e. convert it to c) with the help of k. Accordingly, we have $c = f(m, k)$ where:

$$f(m, k) \overset{n}{=} m^r \tag{40}$$

• f^{-1} is the decoding function which takes c and decrypt it (i.e. convert it to m) with the help of κ. Accordingly, we have $m = f^{-1}(c, \kappa)$ where:

$$f^{-1}(c, \kappa) \overset{n}{=} c^{\rho} \tag{41}$$

• S is the sender of the message who uses the publicly available information (i.e. k and f) to encode m and convert it to c.
• R is the receiver of the message who uses the private information (i.e. p and q and hence κ) to decode c and hence retrieve m.
So, the idea is that any one (i.e. S) can use the publicly available information (i.e. k and f) to encode his message and send it to the receiver (i.e. R). However, the receiver is the only one who can (practically) decode the encrypted message (because he is the only one in possession of the private key). The security of this method of encryption originates from the fact that those who use this method to

[105] It is worth noting that the level of security of encryption increases with increasing the size of p and q (since this makes the factorization of n harder).
[106] In reality, the secrecy of the public key should increase the security of encryption and hence it adds another layer of security to the process of encryption.

communicate (i.e. the sender and receiver of encrypted messages) do not need to share any common secret since the required secret (i.e. the private key) is held by only one (i.e. the receiver).
Now, we need to substantiate our claim that the decoding function f^{-1} actually decodes the encrypted message (i.e. c) and hence it retrieves the original message (i.e. m). This is shown in the following (which essentially shows why the RSA encryption system should work):

$$f^{-1}(c,\kappa) \overset{n}{=} c^{\rho} = \big[f(m,k)\big]^{\rho} \overset{n}{=} \big[m^{r}\big]^{\rho} = m^{r\rho} \tag{42}$$

where we refer to Eqs. 40 and 41 (and the surrounding text) for justification. Now, from $r\rho \overset{\phi}{=} 1$ we have:

$$r\rho = 1 + a\phi = 1 + a(p-1)(q-1)$$

where $a \in \mathbb{Z}$. Moreover, $m^{p-1} \overset{p}{=} 1$ and $m^{q-1} \overset{q}{=} 1$ (from Fermat's little theorem). Hence:

$$\begin{aligned} m^{p-1} &\overset{p}{=} 1 \\ \big(m^{p-1}\big)^{a(q-1)} &\overset{p}{=} 1^{a(q-1)} \\ m \times \big(m^{p-1}\big)^{a(q-1)} &\overset{p}{=} m \times 1^{a(q-1)} \\ m^{1+a(p-1)(q-1)} &\overset{p}{=} m \\ m^{r\rho} &\overset{p}{=} m \end{aligned}$$

This similarly applies to q and hence we have: $m^{r\rho} \overset{q}{=} m$. Therefore, we have:[107] $m^{r\rho} \overset{pq}{=} m$ (i.e. $m^{r\rho} \overset{n}{=} m$) and hence we can add another step to Eq. 42, that is:

$$f^{-1}(c,\kappa) \overset{n}{=} c^{\rho} = \big[f(m,k)\big]^{\rho} \overset{n}{=} \big[m^{r}\big]^{\rho} = m^{r\rho} \overset{n}{=} m$$

This equation shows that by using f^{-1} we retrieved the original message text m from the cipher text c through this modular arithmetic manipulation (with the help of the publicly and privately available information). So, the secrecy of the encrypted message originates from the fact that the decryption of the coded message depends on the access to the private key which is known only to the receiver R. For any eavesdropper to decode the encrypted message he needs to know the private key κ which depends on knowing p and q (noting that κ depends on ρ which depends on $p-1$ and $q-1$ since ρ depends on ϕ which is the product of $p-1$ and $q-1$). However, knowing p and q by the eavesdropper requires factorization of n which is practically non-viable in the available time frame because p and q (and hence n) are very large.
Note: if we reverse the above argument we can make the public key encryption system a digital signature system. In brief, let a private key owner encode a message m using his private key (with the decoding function f^{-1}) and he makes his message public. Now, anyone in the public can decrypt the encoded message using the public key (with the encoding function f) through the following process:

$$f\big[f^{-1}(m,\kappa),k\big]$$

So, whoever receives the encrypted message will know that the message comes from the owner of the private key (i.e. it is a signed message). The justification is as follows:

$$f(c,k) \overset{n}{=} c^{r} = \big[f^{-1}(m,\kappa)\big]^{r} \overset{n}{=} \big[m^{\rho}\big]^{r} = m^{r\rho} \overset{n}{=} m$$

The rest should be similar to the above.

2. Give a simple numeric example for an RSA encryption system that can be used to communicate encrypted messages.
Solution: Let have the following:
• $p = 37$ and $q = 89$ (where we use small primes for simplicity).

[107] This can be justified, for instance, by rule 14 of § 2.7 of V1 or by the Chinese remainder theorem.

- $n = pq = 3293$.
- $\phi = (p-1)(q-1) = 36 \times 88 = 3168$.
- $r = 17$ (noting that 17 is coprime to 3168 and $1 < 17 < 3168$).
- $\rho = 17^*(\text{mod } 3168) = 2609$.
- $k = (3293, 17)$.
- $\kappa = (3293, 2609)$.
- $f(m,k)$ is the mapping: $m \rightarrow c \equiv m^{17}(\text{mod } 3293)$.
- $f^{-1}(c,\kappa)$ is the mapping: $c \rightarrow m \equiv c^{2609}(\text{mod } 3293)$.

So, if S encrypts the message $m = 13$ by using $f(m,k)$ then he gets: $c = 13^{17}(\text{mod } 3293) = 2607$. Accordingly, when R receives c then by using $f^{-1}(c,\kappa)$ he gets: $m = 2607^{2609}(\text{mod } 3293) = 13$ which is the original message.

3. Create and use an RSA encryption system to encode and decode the following message using ASCII code for conversion between text and numbers: "I WILL COME TO YOUR HOUSE TONIGHT.".
Solution: The numeric ASCII code for the message is (where each two digits represent a single character; please refer to the ASCII code table which is available on the Internet):

$$7332877376763267797769328479328979858232727985836932847978737172844 6 \quad (43)$$

We create the following RSA encryption system:
- $p = 97$ and $q = 101$.
- $n = pq = 9797$.
- $\phi = (p-1)(q-1) = 96 \times 100 = 9600$.
- $r = 23$ (noting that 23 is coprime to 9600 and $1 < 23 < 9600$).
- $\rho = 23^*(\text{mod } 9600) = 2087$.
- $k = (9797, 23)$.
- $\kappa = (9797, 2087)$.
- $f(m,k)$ is the mapping: $m \rightarrow c \equiv m^{23}(\text{mod } 9797)$.
- $f^{-1}(c,\kappa)$ is the mapping: $c \rightarrow m \equiv c^{2087}(\text{mod } 9797)$.

Now, let the sender S encode the numeric message of Eq. 43 as 4-digit blocks of integers (i.e. each 4-digit block represents two characters) where in the following list $c(m)$ represents $m^{23}(\text{mod } 9797)$, that is:

$c(7332) = 7940$ $c(8773) = 0185$ $c(7676) = 3434$ $c(3267) = 4437$ $c(7977) = 0351$

$c(6932) = 6271$ $c(8479) = 5155$ $c(3289) = 2080$ $c(7985) = 2741$ $c(8232) = 7333$

$c(7279) = 6087$ $c(8583) = 0452$ $c(6932) = 6271$ $c(8479) = 5155$ $c(7873) = 4650$

$c(7172) = 2829$ $c(8446) = 7743$

Accordingly, S will obtain and send the following numeric message:

$$7940018534344437035162715155208027417333608704526271515546502829 7743$$

The receiver R then decodes this numeric message as 4-digit blocks of integers where in the following list $m(c)$ represents $c^{2087}(\text{mod } 9797)$, that is:

$m(7940) = 7332$ $m(0185) = 8773$ $m(3434) = 7676$ $m(4437) = 3267$ $m(0351) = 7977$

$m(6271) = 6932$ $m(5155) = 8479$ $m(2080) = 3289$ $m(2741) = 7985$ $m(7333) = 8232$

$m(6087) = 7279$ $m(0452) = 8583$ $m(6271) = 6932$ $m(5155) = 8479$ $m(4650) = 7873$

$m(2829) = 7172$ $m(7743) = 8446$

So, R retrieves the original message in numeric format (i.e. what is in Eq. 43). He then uses ASCII code table to convert this numeric message to a text message and hence he obtains the original message text (i.e. I WILL COME TO YOUR HOUSE TONIGHT.).

4. Give a simple example of a digital signature system.
Solution: Let us use the encryption system of Problem 3 where R (after receiving the message "I WILL

COME . . .") wants to send a *signed* confirmation message so that anyone receives the confirmation message (notably S) will know for sure that the confirmation message comes from R not from an intruder or an impersonator. The confirmation message is: "I AM WAITING". Accordingly:

• The numeric ASCII code for the confirmation message is 733265773287657384737871.

• On applying the mapping $f^{-1}(m,\kappa)$ $\big[$i.e. $m \ \rightarrow \ c \equiv m^{2087}(\text{mod } 9797)$ where in the following list $c(m)$ represents $m^{2087}(\text{mod } 9797)\big]$ to the ASCII confirmation message (in blocks of 4 digits) R gets:

$c(7332) = 6319$ $\qquad$ $c(6577) = 6929$ $\qquad$ $c(3287) = 1411$

$c(6573) = 2194$ $\qquad$ $c(8473) = 7036$ $\qquad$ $c(7871) = 7509$

Hence, R will send the following encrypted message: 631969291411219470367509.

• When S receives this encrypted message he applies the mapping $f(c,k)$ $\big[$i.e. $c \ \rightarrow \ m \equiv c^{23}(\text{mod } 9797)$ where in the following list $m(c)$ represents $c^{23}(\text{mod } 9797)\big]$ to the encrypted message (in blocks of 4 digits) and hence S gets:

$m(6319) = 7332$ $\qquad$ $m(6929) = 6577$ $\qquad$ $m(1411) = 3287$

$m(2194) = 6573$ $\qquad$ $m(7036) = 8473$ $\qquad$ $m(7509) = 7871$

i.e. 733265773287657384737871 which is the original confirmation message in ASCII code (i.e. "I AM WAITING" in text). So, S knows for sure that this message comes from R, i.e. the confirmation message is a *signed* message (where the encryption represents the signature since R is the only one who holds the private key and hence R is the only one who can encrypt the message in this way).

Chapter 18
Number Theory and Computing

Computing is an essential tool in modern number theory. Many problems in number theory cannot be solved without employing computational tools and methods. In fact, in many cases computing is needed (or at least it is useful to use) even to tackle those number theory problems which are essentially of analytical type and hence they can be solved in a purely analytical way. Accordingly, developing basic computational knowledge and skills is a requirement for any modern number theorist.

Some number theorists may argue that we can use ready-made software packages and libraries to do our computational business and hence we do not need to learn computing or develop computational skills. However, this is not always true because there are always problems that cannot be tackled and solved by ready-made software packages and libraries (assuming they are available and user friendly and etc.).[108] Moreover, even if this is true, doing computing in number theory problems gives an insight that can be gained neither by analytical treatment and methodology nor by using ready-made software packages and libraries. So, practicing computing (in some shape and form) is beneficial (if not a necessity) in number theory even to enforce the analytical knowledge and skills (let alone its obvious benefit or necessity in certain aspects such as doing tests and checks). We should also emphasize on the special importance or necessity of computing in research.

It is useful to take note of the following remarks about this chapter and its content:

• The purpose of this chapter is to develop some very basic skills in dealing with number theory problems computationally. Most of the problems in this chapter that we tackle computationally are simple and hence they do not need more than simple algorithmic ideas and simple codes. We intend to build in the future volumes of this book on the simple ideas and techniques that we present in this chapter (and hence extending them in depth and breadth).

• This chapter is deliberately made very short because the idea of it is to give a small sample of number theory problems that can be tackled and solved computationally (alongside the computational codes and solutions of these problems). In fact, many other problems in this book can be tackled and solved computationally in a manner similar to the manner of the problems of this chapter. We encourage the reader (who is keen to learn how to use computing in number theory) to search for similar problems (in this book as well as outside this book) and tackle them computationally by simple algorithmic ideas and codes (similar or different to the ideas and codes that we present in this chapter).

• All the codes that we refer to in this chapter (and in this book) are in C++ and they are available on the Internet.[109]

• We intentionally kept the codes very basic to avoid distraction and additional computational cost (noting that the purpose of these codes is just to outline the way of implementing the basic ideas of the algorithms behind them).

• Artificial Intelligence (which we discussed briefly in the first volume of this book) is a specially important

[108] This is particularly true in the following cases:

• In bulk processing where we want to process a large number of data sets such as solving 1000 Diophantine equations or solving 200 linear congruence equations by the Chinese remainder theorem.

• In dealing with eccentric and exotic problems like dealing with large numbers or large exponentials or high-order polynomials of many variables.

As part of my regular work and activities (e.g. in research and writing) I regularly use various types of ready-made computational tools for solving computational problems or checking their solutions. However, I always find problems that cannot be solved by these tools and hence I need to use my computational knowledge and skills (especially in coding) to solve or check certain problems which ready-made computational tools fail to solve. Moreover, I always find problems which ready-made computational tools "solve" in a wrong way and hence again I need my computational knowledge and skills to solve them correctly.

[109] They are available from my webpage on ResearchGate.

computational tool that can have an impact in the future not only on the number theory problems of computational nature but even on the analytical investigation of some number theory problems. In fact, we expect this tool to dominate the research in certain areas of number theory in the near future. Hence, it is important for the next generation of mathematicians to develop their knowledge and skills in this regard. However, due to its rather complicated nature and the requirement of considerable space we do not discuss artificial intelligence in this volume although we hope to do some investigation about it in the future volumes.

18.1 Simple Tools

1. Write a simple code for calculating the index of integer (see § 1.5).
   Solution: See IndexOfInt.cpp code.
2. Write a simple code for generating a sequence of random numbers.
   Solution: See Random.cpp code. Also see Problem 12 of § 8.1.
3. Write a simple code for calculating the residue of a (large) factorial in a given modulo.
   Solution: See CongLargeFactorial.cpp code.
4. Write a simple code for calculating the residue of a (large) exponential in a given modulo.
   Solution: See CongLargeExponential.cpp code.

18.2 The Chinese Remainder Theorem

1. Write a simple code that reads integer entries of a system of linear congruence equations (i.e. residues corresponding to moduli) from a file and finds (by a computational algorithm based on the rationale of the Chinese remainder theorem) its solution.
   Solution: See the CRTS folder which contains the code as well as examples of input data (and one example of output). The idea of the algorithm is very simple, that is: to find the solution of the given system we loop over $0 \leq x < Mp$ (where Mp is the product of the moduli) to find the x value that satisfies all the given congruence equations (where we use modular arithmetic to identify this value).
2. Write a simple code for mass processing of (many) systems of linear congruence equations.
   Solution: See the CRTM folder which contains the code as well as an example of input file (and the corresponding output file). This code simply loop over the given systems where it solves them one by one by using the algorithm of Problem 1.

18.3 Congruence Equations and Systems

1. Find all the moduli m that satisfy the following congruence equation: $2x^3 + 5x^2 + 13x + 9 \stackrel{m}{=} 0$ (where $1 < m < 100$).
   Solution: The solutions are: $m = 3$, 7, 9, 13, 17, 21, 27, 29, 31, 39, 43, 47, 49, 51, 53, 61, 63, 71, 79, 81, 83, 87, 91, 93, 97 (see the FindModPoly folder which contains the code as well as the output file).
2. Find all $\mathbb{P} \ni p < 1000$ such that the congruence equation $x^7 + y^{19} \stackrel{p}{=} 153$ has no solution.
   Solution: See the FindModPolyPrimes folder which contains the code as well as the input and output files. It is worth noting that this Problem was solved theoretically in Problem 1 of § 8.3, and hence the computational solution in the present Problem verifies that solution.
3. Solve the following systems of mixed polynomial-exponential congruence equations (where $x, y \in \mathbb{N}^0$):

   (**a**) $2x^3 + 5y^2 + 8y + 1 \stackrel{115}{=} 0$ $\qquad$ $5^x + 7^y \stackrel{123}{=} 12.$

   (**b**) $x^3 + y \stackrel{7}{=} 0$ $\qquad$ $3^x + 4^y \stackrel{11}{=} 2.$

   Solution:
   (**a**) Simple initial investigation should reveal that the period of the first equation (mod 115) is 115 (for both x and y), while the x-period of 5^x (mod 123) is 20 and the y-period of 7^y (mod 123) is 40.[110] So,

[110] The Eq1Cycle.cpp and Eq2Cycle.cpp codes in the Codes\CongSys1\Cycle folder should help in identifying these periods.

the period of the $x \overset{115}{=}$ and $x \overset{20}{=}$ combination is $x \overset{460}{=}$ while the period of the $y \overset{115}{=}$ and $y \overset{40}{=}$ combination is $y \overset{920}{=}$.

Now, we can propose two simple computational approaches to solve this system:

• In this approach we find the solutions of the individual equations first (where these solutions are found computationally by the Eq1Sol.cpp and Eq2Sol.cpp codes which are in the Codes\CongSys1\CongSys1CRT\Sol folder). We then use the Chinese remainder theorem (or rather a computational algorithm based on its rationale) to find the solutions of the system. In brief, for every combination of a pair of solutions of the individual equations we loop over $0 \leq x < 460$ and over $0 \leq y < 920$ to find the (x, y) pair whose x component is congruent (mod 115) to the x component of the first equation and is congruent (mod 20) to the x component of the second equation and whose y component is congruent (mod 115) to the y component of the first equation and is congruent (mod 40) to the y component of the second equation. This (x, y) pair should be the solution of the system corresponding to that combination of the pair of solutions of the individual equations. So, by looping over all the combinations of these pairs of solutions of the individual equations[111] we will find all the solutions of the system. This approach is implemented in CongSys1CRT.cpp code (which is in the Codes\CongSys1\CongSys1CRT folder).

• Instead of solving these congruence equations individually and using the Chinese remainder theorem (or an algorithm based on its rationale) to find the solutions of the system (as we did in the previous point), we simply treat these equations as a system from the beginning and hence we just loop over x and y to find the (x, y) pairs that satisfy the individual equations simultaneously (and hence these pairs represent the intersection of their individual solutions in a modular sense). So, we need to loop over $0 \leq x < 460$ (i.e. over the entire period of the $x \overset{115}{=}$ and $x \overset{20}{=}$ combination) and over $0 \leq y < 920$ (i.e. over the entire period of the $y \overset{115}{=}$ and $y \overset{40}{=}$ combination). This approach is implemented in the CongSys1Loop.cpp code (which is in the Codes\CongSys1\CongSys1Loop folder).

Both these approaches produce the same (23) solutions which can be found in the corresponding output files (see the CongSys1CRTOut.txt and CongSys1LoopOut.txt files in the aforementioned folders). As indicated already, the codes (and all the input and output files) of both approaches are in the Codes\CongSys1 folder.

(**b**) This system was solved theoretically (or analytically) in Problem 4 of § 9.3.2. If we follow the approaches of part (a) then we find the same solutions. The codes (and all the input and output files) of both approaches are in the Codes\CongSys2 folder.

[111] We have 115 solutions for the first equation and 10 solutions for the second equation and hence we have 1150 combinations.

Index