The L/R symmetry and the categorization of natural numbers

Emmanuil Manousos

APM Institute for the Advancement of Physics and Mathematics, 13 Pouliou str., 11 523 Athens, Greece

Abstract

“Every natural number, with the exception of 0 and 1, can be written in a unique way as a linear combination of consecutive powers of 2, with the coefficients of the linear combination being -1 or +1”. According to this theorem we define the L/R symmetry of the natural numbers. The L/R symmetry gives the factors which determine the internal structure of natural numbers. As a consequence of this structure, we have an algorithm for determining prime numbers and for factorization of natural numbers.

Keywords: Number theory, Distribution of primes, Factorization.

2010 Mathematics Subject Classifications: 11N05, 11A51.

1 Introduction

In this article, we start by proving the theorem: “Every natural number, with the exception of 0 and 1, can be written in a unique way as a linear combination of consecutive powers of 2, with the coefficients of the linear combination being -1 or +1”. As a consequence of this theorem we have two fundamental symmetries of natural numbers: the symmetry L and the symmetry R. There exists a transformation which confesses the symmetries L and R. In fact, we have a single L/R symmetry instead of having two different symmetries.

The L/R symmetry categorizes the natural numbers and reveals to us the factors which determine their internal structure. Every natural number belongs to one of the following categories: it has symmetry L or it has symmetry R or it is not symmetric. In the categorization of natural numbers according to L/R symmetry there exist three numbers each of them is a distinct category contained of exactly one number. These numbers are 0, 1 and 3.

The order of the number of operations required for the factorization of a composite odd number C=Cn, with n digits in the decimal system, is10^n . The large number of operations makes the factorizations of natural numbers impossible, if the number of digits is extremely high. From the properties of the L/R symmetry we can develop a factorization algorithm of the natural numbers which can work by skipping all the complicated operations mentioned above. L/R symmetry provides information for the factors of an odd number even when we know nothing about these factors.

2 Natural numbers as linear combination of consecutive powers of 2

We prove the following theorem:

Theorem 2.1. *Every natural number, with the exception of* 0, *and* 1, *can be uniquely written as a linear combination of consecutive powers of* 2, *with the coefficients of the linear combination being* -1 *or* +1.

Proof. Let the odd number Π as given from equation

$$\Pi = \Pi(\nu, \beta_i) = 2^{\nu+1} + 2^{\nu} \pm 2^{\nu-1} \pm 2^{\nu-2} \pm ....\pm 2^1 \pm 2^0 = 2^{\nu+1} + 2^{\nu} + \sum_{i=0}^{\nu-1} \beta_i 2^i$$
$$\beta_i = \pm 1, i = 0,1,2,........,\nu-1 \quad . \quad (2.1)$$
$$\nu \in \mathbb{N}$$

From equation (2.1) for $\nu = 0$ we obtain

$$\Pi = 2^1 + 2^0 = 2 + 1 = 3.$$

We now examine the case where $\nu \in \mathbb{N}^*$. The lowest value that the odd number Π of equation (2.1) can obtain is

$$\Pi_{\min} = \Pi(\nu) = 2^{\nu+1} + 2^{\nu} - 2^{\nu-1} - 2^{\nu-1} - ....2^1 - 1$$

$$\Pi_{\min} = \Pi(\nu) = 2^{\nu+1} + 1. \quad (2.2)$$

The largest value that the odd number Π of equation (2.1) can obtain is

$$\Pi_{\max} = \Pi(\nu) = 2^{\nu+1} + 2^{\nu} + 2^{\nu-1} + ...2^1 + 1$$

$$\Pi_{\max} = \Pi(\nu) = 2^{\nu+2} - 1. \quad (2.3)$$

Thus, for the odd numbers $\Pi = \Pi(\nu, \beta_i)$ of equation (2.1) the following inequality holds

$$\Pi_{\min} = 2^{\nu+1} + 1 \le \Pi(\nu, \beta_i) \le 2^{\nu+2} - 1 = \Pi_{\max} . \quad (2.4)$$

The number $N(\Pi(\nu, \beta_i))$ of odd numbers in the closed interval $[2^{\nu+1}+1, 2^{\nu+2}-1]$ is

$$N(\Pi(\nu, \beta_i)) = \frac{\Pi_{\max} - \Pi_{\min}}{2} + 1 = \frac{(2^{\nu+2} - 1) - (2^{\nu+1} + 1)}{2} + 1$$

$$N(\Pi(\nu, \beta_i)) = 2^{\nu} . \quad (2.5)$$

The integers $\beta_i, i = 0,1,2,........,\nu - 1$ in equation (2.1) can take only two values, $\beta_i = -1 \vee \beta_i = +1$, thus equation (2.1) gives exactly $2^{\nu} = N\left(\Pi\left(\nu, \beta_i\right)\right)$ odd numbers. Therefore, for every $\nu \in \mathbb{N}^*$ equation (2.1) gives all odd numbers in the interval $\left[2^{\nu+1} + 1, 2^{\nu+2} - 1\right]$.

We now prove the theorem for the even numbers. Every even number α which is a power of 2 can be uniquely written in the form of $\alpha = 2^{\nu}, \nu \in \mathbb{N}^*$. We now consider the case where the even number α is not a power of 2. In that case, the even number α is written in the form of

$$\alpha = 2^l \Pi, \Pi = \text{odd}, \Pi \neq 1, l \in \mathbb{N}^*. \tag{2.6}$$

We now prove that the even number α can be uniquely written in the form of equation (2.6). If we assume that the even number α can be written in the form of

$$\begin{aligned} &\alpha = 2^l \Pi = 2^{l'} \Pi' \\ &l \neq l' (l > l') \\ &\Pi \neq \Pi' \\ &l, l' \in \mathbb{N}^* \\ &\Pi, \Pi' = odd \end{aligned} \tag{2.7}$$

the we obtain

$$\begin{aligned} &2^l \Pi = 2^{l'} \Pi' \\ &2^{l-l'} \Pi = \Pi' \end{aligned}$$

which is impossible, since the first part of this equation is even and the second odd. Thus, it is $l = l'$ and we take that $\Pi = \Pi'$ from equation (2.7). Therefore, every even number α that is not a power of 2 can be uniquely written in the form of equation (2.6). The odd number Π of equation (2.6) can be uniquely written in the form of equation (2.1), thus from equation (2.6) it is derived that every even number α that is not a power of 2 can be uniquely written in the form of equation

$$\begin{aligned} &\alpha = \alpha\left(l, \nu, \beta_i\right) = 2^l \left(2^{\nu+1} + 2^{\nu} + \sum_{i=0}^{\nu-1} \beta_i 2^i\right) \\ &l \in \mathbb{N}^*, \nu \in \mathbb{N} \\ &\beta_i = \pm 1, i = 0,1,2,........,\nu - 1 \end{aligned} \tag{2.8}$$

and equivalently

$$\alpha = \alpha(l, \nu, \beta_i) = 2^{l+\nu+1} + 2^{l+\nu} + \sum_{i=0}^{\nu-1} \beta_i 2^{l+i}$$
$$l \in \mathbb{N}^*, \nu \in \mathbb{N} \quad . \qquad (2.9)$$
$$\beta_i = \pm 1, i = 0, 1, 2, ..., \nu - 1$$

For 1 we take

$$1 = 2^0$$

$$1 = 2^1 - 2^0$$

thus, it can be written in two ways in the form of equation (2.1). Both the odds of equation (2.1) and the evens of the equation (2.8) are positive. Thus, 0 cannot be written either in the form of equation (2.1) or in the form of equation (2.8). □

In order to write an odd number $\Pi \neq 1, 3$ in the form of equation (2.1) we initially define the $\nu \in \mathbb{N}^*$ from inequality (2.4). Then, we calculate the sum

$$2^{\nu+1} + 2^{\nu}.$$

If it holds that $2^{\nu+1} + 2^{\nu} < \Pi$ we add the $2^{\nu-1}$, whereas if it holds that $2^{\nu+1} + 2^{\nu} > \Pi$ then we subtract it. By repeating the process exactly ν times we write the odd number Π in the form of equation (2.1). The number of ν steps needed in order to write the odd number Π in the form of equation (2.1) is extremely low compared to the magnitude of the odd number Π, as derived from inequality (2.4).

Example 2.1. For the odd number $\Pi = 23$ we obtain from inequality (2.4)

$$2^{\nu+1} + 1 < 23 < 2^{\nu+2} - 1$$

$$2^{\nu+1} + 2 < 24 < 2^{\nu+2}$$

$$2^{\nu} < 12 < 2^{\nu+1}$$

thus $\nu = 3$. Then, we have

$2^{\nu+1} + 2^{\nu} = 2^4 + 2^3 = 24 > 23$ (thus 2^2 is subtracted)

$2^4 + 2^3 - 2^2 = 20 < 23$ (thus 2^1 is added)

$2^4 + 2^3 - 2^2 + 2^1 = 22 < 23$ (thus $2^0 = 1$ is added)

$$2^4 + 2^3 - 2^2 + 2^1 + 1 = 23.$$

Fermat numbers F_s can be written directly in the form of equation (2.1), since they are of the form $\Pi_{\min}$,

$$F_s = 2^{2^s} + 1 = \Pi_{\min}(2^s - 1) = 2^{2^s} + 2^{2^s - 1} - 2^{2^s - 2} - 2^{2^s - 3} - .... - 2^1 - 1 \quad . \qquad (2.10)$$
$$s \in \mathbb{N}$$

Mersenne numbers M_p can be written directly in the form of equation (2.1), since they are of the form $\Pi_{\max}$,

$$M_p = 2^p - 1 = \Pi_{\max}(p-2) = 2^{p-1} + 2^{p-2} + 2^{p-3} + \ldots\ldots.. + 2^1 + 1 . \qquad (2.11)$$
$$p = prime$$

In order to write an even number α that is not a power of 2 in the form of equation (2.1), initially it is consecutively divided by 2 and it takes of the form of equation (2.6). Then, we write the odd number Π in the form of equation (2.1).

Example 2.2. By consecutively dividing the even number $\alpha = 368$ by 2 we obtain

$$\alpha = 368 = 2^4 \cdot 23 .$$

Then, we write the odd number $\Pi = 23$ in the form of equation (2.1),

$$23 = 2^4 + 2^3 - 2^2 + 2^1 + 1,$$

and we get

$$368 = 2^4\left(2^4 + 2^3 - 2^2 + 2^1 + 1\right)$$

$$368 = 2^8 + 2^7 - 2^6 + 2^5 + 2^4 .$$

This equation gives the unique way in which the even number $\alpha = 368$ can be written in the form of equation (2.9).

From inequality (2.4) we obtain

$$2^{\nu+1} + 1 \le \Pi \le 2^{\nu+2} - 1$$

$$2^{\nu+1} < 2^{\nu+1} + 1 \le \Pi \le 2^{\nu+2} - 1 < 2^{\nu+2}$$

$$2^{\nu+1} < \Pi < 2^{\nu+2}$$

$$(\nu+1)\ln 2 < \ln \Pi < (\nu+2)\ln 2$$

from which we get

$$\frac{\ln \Pi}{\ln 2} - 1 < \nu + 1 < \frac{\ln \Pi}{\ln 2}$$

and finally

$$\nu + 1 = \left[\frac{\ln \Pi}{\ln 2}\right] \qquad (2.12)$$

Where $\left[\frac{\ln \Pi}{\ln 2}\right]$ the integer part of $\frac{\ln \Pi}{\ln 2} \in \mathbb{R}$.

We now give the following definition:

Definition 2.1. *We define as the conjugate of the odd*

$$\Pi = \Pi(\nu, \beta_i) = 2^{\nu+1} + 2^{\nu} + \sum_{i=0}^{\nu-1} \beta_i 2^i$$
$$\beta_i = \pm 1, i = 0,1,2,........,\nu - 1 \qquad (2.13)$$
$$\nu \in \mathbb{N}^*$$

the odd Π^* *,*

$$\Pi^* = \Pi^*(\nu, \gamma_j) = 2^{\nu+1} + 2^{\nu} + \sum_{j=0}^{\nu-1} \gamma_j 2^j$$
$$\gamma_i = \pm 1, j = 0,1,2,........,\nu - 1 \qquad (2.14)$$
$$\nu \in \mathbb{N}^*$$

for which it holds

$$\gamma_k = -\beta_k \forall k = 0,1,2,........,\nu - 1 . \qquad (2.15)$$

For conjugate odds, the following corollary holds:

Corollary 2.1. *For the conjugate odds* $\Pi = \Pi(\nu, \beta_i)$ *and* $\Pi^* = \Pi^*(\nu, \gamma_i)$ *the following hold:*

1. $(\Pi^*)^* = \Pi$. (2.16)

2. $\Pi^* = 3 \cdot 2^{\nu+1} - \Pi$. (2.17)

3. Π *is divisible by* 3 *if and only if* Π^* *is divisible by* 3 .

4. *Two conjugate odd numbers cannot have common factor greater than 3.*

Proof. 1. The 1 of the corollary is an immediate consequence of definition 4.1.

2. From equations (2.13), (2.14) and (2.15) we get

$$\Pi + \Pi^* = (2^{\nu+1} + 2^{\nu}) + (2^{\nu+1} + 2^{\nu})$$

and equivalently

$$\Pi + \Pi^* = 3 \cdot 2^{\nu+1} .$$

3. If the odd Π is divisible by 3 then it is written in the form $\Pi = 3x, x = odd$ and from equation (4.17) we get $3x + \Pi^* = 3 \cdot 2^{\nu+1}$ and equivalently $\Pi^* = 3(2^{\nu+1} - x)$. Similarly we can prove the inverse

4. If $\Pi = xy, \Pi^* = xz$, x, y, z odd numbers, from equation (2.17) we have $x(y+z) = 3 \cdot 2^{\nu+1}$ and consequently is $x = 3$. □

From corollary 2.1 we have that 3 the only odd number which is equal to its conjugate: $3^* = 3 \cdot 2^{0+1} - 3 = 3$.

3 The L/R symmetry

We now give the following definition:

Definition 3.1. *Define as "symmetry" every specific algorithm which determines the signs of* $\beta_i = \pm 1, i = 0,1,2,........,\nu-1$ *in equation* (2.1):

$$\Pi = \Pi(\nu, \beta_i) = 2^{\nu+1} + 2^{\nu} \pm 2^{\nu-1} \pm 2^{\nu-2} \pm .... \pm 2^1 \pm 2^0 = 2^{\nu+1} + 2^{\nu} + \sum_{i=0}^{\nu-1} \beta_i 2^i$$
$$\beta_i = \pm 1, i = 0,1,2,........,\nu-1 .$$
$$\nu \in \mathbb{N}$$

In this article we study the symmetries L and R, which are determined by the following definition:

Definition 3.2.1. *The odd number Π in the equation* (2.1) *has symmetry L when there exists an index L so that*

$$\beta_L = +1$$
$$\beta_{L-1} = \beta_{L-2} = ... = \beta_1 = \beta_0 = -1. \qquad (3.1)$$
$$L \in \{1,2,3,...,\nu-1\}$$

2. *The odd number Π in the equation* (2.1) *has symmetry R when there exists an index R so that*

$$\beta_R = -1$$
$$\beta_{R-1} = \beta_{R-2} = ... = \beta_1 = \beta_0 = +1. \qquad (3.2)$$
$$R \in \{1,2,3,...,\nu-1\}$$

3. We will call asymmetric t*he odd numbers which have neither symmetry L nor symmetry R.*

4. *For each even number α,*

$$\alpha = 2^l \Pi, \Pi = \text{odd}, \Pi \neq 1, l \in \mathbb{N}^*$$

we define as the symmetry of α the symmetry of the odd Π.

We will note the symmetry of an odd Π by L=L(Π)=LΠ, or by R=R(Π)=RΠ. At first the L/R symmetry categorizes the odd numbers, and then the even numbers by 4 of definition 3.2. The odd number Π=1 cannot uniquely be written in the form of equation (2.1). So 1 and the powers of 2 are asymmetric numbers.

The odd numbers of the form

$As = 2^{\nu} + 1, \nu \in \mathbb{N}^*$

have $\beta_i = -1 \forall i = 0,1,2,...,\nu - 1$ in the equation (2.1), and so these are the only asymmetric odd numbers. From its definition we have that the Fermat numbers are asymmetric numbers. However, although 3 is a Fermat number it is asymmetric because of a different reason: It is the unique natural number which comes from equation (2.1) for ν=0,

$3 = 2^1 + 2^0 = 2^1 + 1, (\nu = 0)$.

In the categorization of natural numbers according to L/R symmetry, 3 is a distinct category contained just one element, number 3. There are two other natural number with this property, 0 and 1.

The even numbers of the form

$\alpha = 2^l \cdot As$

$l \in \mathbb{N}^*$

where As is asymmetric number, as well as the powers of 2 are the asymmetric even numbers. The rest even numbers are symmetric (so the symmetric even numbers are more than the asymmetric ones).

The theoretical study of the symmetries L and R has not been completed, so some of the following corollaries are just conjectures.

Corollary 3.1. (Conjecture) A. 1. *There aren't two consecutive powers of an odd number with symmetry R.*

2. *There isn't an odd number with symmetry R to all of its powers (immediate result of the conjecture 1).*

3. *With the exception of 3 itself, in all other powers of 3 alternate consecutively the symmetries L and R.*

4. *The factors, prime numbers or composites of Fermat numbers have symmetry L.*

B. *For the symmetric prime numbers A and B with symmetry L or R we have the following:*

5. L(A)<L(B)=>L(AB)=L(A).

6. L(A)<R(B)=>L(AB)=L(A)

7. R(B)<L(A)=>L(AB)=R(B).

8. R(A)<R(B)=>L(AB)=R(A).

The symmetry of an odd number can be found by writing it in the form of the equation (2.1). According to 4 of corollary 3.1, the factors, prime numbers or composites of Fermat numbers have symmetry L. Next, we have two examples:

Example 3.1. The prime number Q= 45592577 is a factor of $F_{10} = 2^{1024} + 1$. From the equation (2.12) we have ν+1=25, and then (see example 2.1) from the equation 2.1 we have

$$Q = 2^{25} + 2^{24} - 2^{23} + 2^{22} - 2^{21} + 2^{20} + 2^{19} - 2^{18} + 2^{17} + 2^{16} + 2^{15} + 2^{14} - 2^{13} + 2^{12}$$
$$+2^{11} - 2^{10} - 2^{9} - 2^{8} - 2^{7} - 2^{6} - 2^{5} - 2^{4} - 2^{3} - 2^{2} - 2^{1} - 1.$$

So the factor 45592577 of F_{10} has symmetry L 45592577=11.

Example 3.2. The prime number Q=568630647535356955169033410940867804839360742060818433 is a factor of $F_{12} = 2^{4096} + 1$. From the equation (2.12) we have ν+1=178, and then from equation 2.1 we have

$$Q = 2^{178} + 2^{177} - 2^{176} + 2^{175} + 2^{174} + 2^{173} + 2^{172} - 2^{171} + 2^{170} + 2^{169} + 2^{168} + 2^{167} + 2^{166}$$
$$+2^{165} - 2^{164} + 2^{163} - 2^{162} - 2^{161} - 2^{160} - 2^{159} + 2^{158} + 2^{157} + 2^{156} - 2^{155} - 2^{154} - 2^{153} - 2^{152}$$
$$-2^{151} + 2^{150} - 2^{149} + 2^{148} - 2^{147} - 2^{146} + 2^{145} - 2^{144} + 2^{143} - 2^{142} - 2^{141} - 2^{140} + 2^{139} + 2^{138}$$
$$-2^{137} - 2^{136} + 2^{135} - 2^{134} - 2^{133} + 2^{132} - 2^{131} + 2^{130} - 2^{129} + 2^{128} - 2^{127} + 2^{126} - 2^{125} - 2^{124}$$
$$-2^{123} - 2^{122} - 2^{121} + 2^{120} - 2^{119} + 2^{118} - 2^{117} + 2^{116} - 2^{115} + 2^{114} - 2^{113} - 2^{112} - 2^{111} - 2^{110}$$
$$-2^{109} - 2^{108} + 2^{107} - 2^{106} + 2^{105} - 2^{104} + 2^{103} - 2^{102} + 2^{101} - 2^{100} + 2^{99} + 2^{98} - 2^{97} + 2^{96} - 2^{95}$$
$$-2^{94} + 2^{93} - 2^{92} + 2^{91} + 2^{90} - 2^{89} + 2^{88} - 2^{87} + 2^{86} + 2^{85} + 2^{84} - 2^{83} + 2^{82} - 2^{81} + 2^{80} + 2^{79}$$
$$-2^{78} - 2^{77} - 2^{76} - 2^{75} + 2^{74} + 2^{73} - 2^{72} - 2^{71} - 2^{70} + 2^{69} + 2^{68} + 2^{67} + 2^{66} + 2^{65} + 2^{64} - 2^{63}$$
$$-2^{62} + 2^{61} - 2^{60} - 2^{59} - 2^{58} - 2^{57} - 2^{56} + 2^{55} - 2^{54} - 2^{53} - 2^{52} - 2^{51} - 2^{50} - 2^{49} + 2^{48} + 2^{47}$$
$$-2^{46} + 2^{45} + 2^{44} + 2^{43} + 2^{42} - 2^{41} - 2^{40} + 2^{39} - 2^{38} - 2^{37} - 2^{36} + 2^{35} - 2^{34} - 2^{33} + 2^{32} + 2^{31}$$
$$-2^{30} + 2^{29} + 2^{28} + 2^{27} + 2^{26} + 2^{25} + 2^{24} - 2^{23} + 2^{22} + 2^{21} + 2^{20} - 2^{19} - 2^{18} - 2^{17} - 2^{16} + 2^{15}$$
$$+2^{14} - 2^{13} - 2^{12} - 2^{11} - 2^{10} - 2^{9} - 2^{8} - 2^{7} - 2^{6} - 2^{5} - 2^{4} - 2^{3} - 2^{2} - 2^{1} - 1$$

So the factor 568630647535356955169033410940867804839360742060818433 of F_{12} has symmetry L 568630647535356955169033410940867804839360742060818433=14.

We give two more examples for the part B of the corollary 3.1:

Example 3.3. L(641)=6<L(114689)=13 =>L(641×114689)=6.

Example 3.4. R(607)= 4<R(16633)=6 =>L(607×16633)=4.

Next corollaries play an important role in factorization of Fermat numbers.

Corollary 3.2. *If the prime numbers Q_1 and Q_2 have symmetries $L(Q_1)$ and $L(Q_2)$ and holds $L(Q_1) < L(Q_2)$, then, the product $Q_1 Q_2$ has symmetry $L(Q_1 Q_2) = L(Q_1)$ or it is equal to a Fermat number.*

Proof. The corollary comes from the 4 of the corollary 3.1, and additionally taking into account that Fermat numbers are asymmetric. □

Corollary 3.3. (Conjecture) *For the symmetry L of the factors of a Fermat number*

$$F_S = 2^{2^S} + 1, S \in \mathbb{N} \qquad (3.3)$$

holds

$$L \in \Phi_S = \left\{S+1, S+2, S+3, ...\right\}. \tag{3.4}$$

We have the following example.

Example 3.5. For the known factors, prime numbers and composites of $F_{12} = 2^{4096}+1$ we have:

S=12

L114689=13

L26017793=15

L63766529=15

L190274191361=13

L1256132134125569=13

L568630647535356955169033410940867804839360742060818433=14

L(C1133)=13

where C1133 is a composite, non-factorized factor of F_{12} with 1133 digits. From the equations (3.3) we have

$$Q_1 = 114689 = 3\cdot 2^{15} + 2^{14}\cdot 1 + 1$$
$$Q_2 = 26017793 = 3\cdot 2^{23} + 2^{16}\cdot 13 + 1$$
$$Q_3 = 63766529 = 3\cdot 2^{24} + 2^{16}\cdot 205 + 1$$
$$Q_4 = 190274191361 = 3\cdot 2^{36} - 2^{14}\cdot 969497 + 1$$
$$Q_5 = 1256132134125569 = 3\cdot 2^{49} - 2^{14}\cdot 26410994027 + 1$$
$$Q_6 = 568630647535356955169033410940867804839360742060818433$$
$$= 3\cdot 2^{177} - 2^{15}\cdot 18478943754124043931111829347223324638874599481 3+1$$

$$C1133 = 3\cdot 2^{3761} + 2^{14}\cdot \Pi + 1$$

where Π is a negative number with 1128 digits.

4 The basic study of the L/R symmetry

In this chapter we prove the basic theorems for the L/R symmetry.

Theorem 4.1.1. *Every odd number Q with symmetry L can be written in the form*

$$Q = 3\cdot 2^{\nu} + 2^{L+1}\cdot \sum_{i=1}^{\nu-L-1} \beta_{\nu-i}\cdot 2^{\nu-L-1-i} + 1 = 3\cdot 2^{\nu} + 2^{L+1}\cdot \Pi + 1$$
$$= 2^{L+1}\cdot\left(3\cdot 2^{\nu-L-1} + \Pi\right) + 1, \nu + 1 = \left[\frac{\ln Q}{\ln 2}\right]. \tag{4.1}$$

The odd number $\Pi \in \mathbb{Z}^*$,

$$\Pi = \sum_{i=1}^{\nu-L-1} \beta_{\nu-i} \cdot 2^{\nu-L-i} \tag{4.2}$$

has the same sign as $\beta_{\nu-1} = \pm 1$*, and satisfies the inequality*

$$-2^{\nu-L-1} + 1 \le \Pi \le 2^{\nu-L-1} - 1. \tag{4.3}$$

2. *Every odd number D with symmetry R can be written in the form*

$$\begin{aligned} D &= 3\cdot 2^{\nu} + 2^{R+1} \cdot \sum_{i=1}^{\nu-R-1} \beta_{\nu-i} \cdot 2^{\nu-R-1-i} - 1 = 3\cdot 2^{\nu} + 2^{R+1} \cdot \Pi - 1 \\ &= 2^{R+1} \cdot \left(3\cdot 2^{\nu-R-1} + \Pi\right) - 1, \nu + 1 = \left[\frac{\ln D}{\ln 2}\right] \end{aligned} \tag{4.4}$$

The odd number $\Pi \in \mathbb{Z}^*$,

$$\Pi = \sum_{i=1}^{\nu-R-1} \beta_{\nu-i} \cdot 2^{\nu-R-i} \tag{4.5}$$

has the same sign as $\beta_{\nu-1} = \pm 1$ *, and satisfies the inequality*

$$-2^{\nu-R-1} + 1 \le \Pi \le 2^{\nu-R-1} - 1. \tag{4.6}$$

Proof. We prove the part 1 of the corollary. The proof of the part 2 is similar. If Q has symmetry L, from equation (2.1) we have

$$Q = 2^{\nu+1} + 2^{\nu} + \sum_{i=\nu-1}^{L+1} \beta_i \cdot 2^i + 2^L - 2^{L-1} - 2^{L-2} - ..... - 2^1 - 1$$

$$Q = 3\cdot 2^{\nu} + \sum_{i=\nu-1}^{L+1} \beta_i \cdot 2^i + 2^L - \left(2^{L-1} + 2^{L-2} + ... + 2^1 + 1\right)$$

$$Q = 3\cdot 2^{\nu} + \sum_{i=\nu-1}^{L+1} \beta_i \cdot 2^i + 2^L - \left(2^L - 1\right)$$

$$Q = 3\cdot 2^{\nu} + \sum_{i=\nu-1}^{L+1} \beta_i \cdot 2^i + 1$$

and taking into account that the highest power of 2 in the sum $\sum_{i=\nu-1}^{L+1} \beta_i \cdot 2^i$ is 2^{L+1} we take the equation (4.1). From equation (4.1) we have for the odd number Π,

$$\Pi = \sum_{i=1}^{\nu-L-1} \beta_{\nu-i} \cdot 2^{\nu-L-i}$$

which is the sum of successive powers of 2 with highest power $\beta_{\nu-1} \cdot 2^{\nu-L-1}$. So the odd number Π has the same sign as $\beta_{\nu-1} = \pm 1$. Moreover, the minimum value of Π is

$$\Pi_{\min} = \sum_{i=1}^{\nu-L-1} -2^{\nu-L-1-i} = -2^{\nu-L-1} + 1$$

and the maximum

$$\Pi_{\max} = \sum_{i=1}^{\nu-L-1} 2^{\nu-L-1-i} = 2^{\nu-L-1} - 1. \ \square$$

The following theorem concerns the symmetry of conjugate odd numbers.

Theorem 4.2.1. *For the odd number Q, with symmetry L, holds*

$$\begin{array}{l} Q = 3\cdot 2^{\nu} + 2^{L+1}\cdot\Pi + 1 \Leftrightarrow Q^{*} = 3\cdot 2^{\nu} - 2^{R+1}\cdot\Pi - 1 \\ R = L \end{array}. \tag{4.7}$$

2. *For the odd number D, with symmetry R, holds*

$$\begin{array}{l} D = 3\cdot 2^{\nu} + 2^{R+1}\cdot\Pi - 1 \Leftrightarrow D^{*} = 3\cdot 2^{\nu} - 2^{L+1}\cdot\Pi + 1 \\ L = R \end{array}. \tag{4.8}$$

Proof. Theorem is an immediate consequence of definitions 3.2, 2.1 and transformation (2.17). □

From equations (4.7) and (4.8) we have

$$Q\cdot Q^{*} + \left(2^{L+1}\cdot\Pi + 1\right)^{2} = 9\cdot 2^{2\nu} \tag{4.9}$$

$$D\cdot D^{*} + \left(2^{R+1}\cdot\Pi + 1\right)^{2} = 9\cdot 2^{2\nu}. \tag{4.10}$$

These equations are independent from the transformation of the conjugation, which is the transformation (2.17).

Now, we prove the following theorem:

Theorem 4.3.1. *For the odd numbers Q with symmetry L the equation*

$$\Pi = \Pi_{L} = \frac{Q - 3\cdot 2^{\nu} - 1}{2^{L+1}} \tag{4.11}$$

Gives the value of L, and the equation

$$\Pi = \Pi_{R} = \frac{D - 3\cdot 2^{\nu} + 1}{2^{R+1}} \tag{4.12}$$

gives R=0, and

$$\Pi_{L} = \frac{\Pi_{R} - 1}{2^{L}}. \tag{4.13}$$

2. *For the odd numbers D with symmetry R the equation (4.12) gives the value of R, the equation (4.11) gives L=0, and*

$$\Pi_{R} = \frac{\Pi_{L} - 1}{2^{R}}. \tag{4.14}$$

Proof. We prove the part 1 of the theorem. The proof of part 2 is similar. Trying to calculate the value of R, in case of an odd number Q with symmetry L in the form of equation (4.4), we get $Q = 3\cdot 2^{\nu} + 2^{R+1}\cdot \Pi_R - 1$. Combining this equation with the equation (4.1) we have

$$Q = 3\cdot 2^{\nu} + 2^{L+1}\cdot \Pi_L + 1 = 3\cdot 2^{\nu} + 2^{R+1}\cdot \Pi_R - 1$$
$$2 = 2^{R+1}\cdot \Pi_R - 2^{L+1}\cdot \Pi_L$$
$$1 = 2^{R}\cdot \Pi_R - 2^{L}\cdot \Pi_L$$

and finally

$$\left(1 = 2^{R}\cdot\left(\Pi_R - 2^{L-R}\cdot \Pi_L\right)\right)\vee\left(1 = 2^{L}\cdot\left(2^{R-L}\cdot \Pi_R - \Pi_L\right)\right).$$

These equations hold if and only if R=0 or L=0. Number Q has symmetry L, so R=0. Moreover we have

$$1 = \Pi_R - 2^{L-R}\cdot \Pi$$

and because R=0 we take the equation (4.13).□

As an example, we calculate again the L and Π for the number Q of example 3.2 by using the equations (4.11) and (4.12):

Example 4.1. For the odd number A=56863064753535695516903341094086780483936074206081843 we have ν=177 from equation (2.5). Then, the equation (4.12) gives R=0. So number A has symmetry L. Then we observe that the equation (4.11) is verified for L=1, L=2, L=3, ..., L=14. For the maximum value of L=14 the equation (4.11) gives Π=184789 437541 240439 311118 293472 233246 388745 994813.

From theorem 4.2 we conclude that symmetries L and R commute from transformation (2.17). So we have L/R symmetry. Theorem 4.3 gives one of the pairs $(L \geq 1 \wedge R = 0)\vee(L = 0 \wedge R \geq 1)$ for every odd number, independently of its symmetry. So, it gives a pair for the Fermat numbers:

$$\begin{aligned} &F_S = 2^{2^S} + 1, S \in \mathbb{N} \\ &L(F_S) = 2^S - 1 \quad . \\ &R(F_S) = 0 \end{aligned} \tag{4.15}$$

Now we prove the following corollary:

Corollary 4.1.1. *For every odd number D with symmetry R the next odd number D+2=Q has symmetry L, and holds*

$$\nu(D+2) = \nu(D) \Rightarrow L(D+2) = R \wedge \Pi_L(D+2) = \Pi_R(D). \tag{4.16}$$

2. *For every odd number Q with symmetry L the previous odd number Q-2=D has symmetry R, and holds*

$$\nu(Q-2) = \nu(Q) \Rightarrow R(Q-2) = L \wedge \Pi_R(Q-2) = \Pi_L(Q). \tag{4.17}$$

Poof. This corollary is an immediate consequence of theorem 4.1:

$$D+2=\left(3\cdot 2^{\nu}+2^{R+1}\cdot\Pi_R-1\right)+2=3\cdot 2^{\nu}+2^{R+1}\cdot\Pi_R+1=3\cdot 2^{\nu}+2^{L+1}\cdot\Pi_L+1=Q,$$

$$Q-2=\left(3\cdot 2^{\nu}+2^{L+1}\cdot\Pi_L+1\right)-2=3\cdot 2^{\nu}+2^{L+1}\cdot\Pi_L-1=3\cdot 2^{\nu}+2^{R+1}\cdot\Pi_R-1=D.$$

Theorem 2.1 makes a partition to the set of natural numbers contained of intervals of the form $\left[2^{\nu+1}+1,2^{\nu+2}-1\right],\nu\in\mathbb{N}^*$. From corollary 4.1 we have that the L/R symmetry makes a partition of the odd numbers of these intervals in $2^{\nu-1},\nu\geq 1$ pairs. We prove the following corollary:

Corollary 4.2. 1. *There are 4 numbers in the interval*

$$\Omega(\nu)=\left[2^{\nu+1}+1,2^{\nu+2}-1\right]=\left[2^{\nu+1}+1,3\cdot 2^{\nu}-1\right)\cup\left(3\cdot 2^{\nu}+1,2^{\nu+2}-1\right] \qquad (4.18)$$
$$\nu\in\mathbb{N}^*$$

with symmetry L/R=ν-1:

1.

$$\Phi_1(\nu)=2^{\nu+1}+1$$
$$L\left(\Phi_1(\nu)\right)=L\left(2^{\nu+1}+1\right)=\nu-1 \qquad (4.19)$$

2.

$$\Phi_2(\nu)=3\cdot 2^{\nu}-1$$
$$R\left(\Phi_2(\nu)\right)=R\left(3\cdot 2^{\nu}-1\right)=\nu-1 \qquad (4.20)$$

3.

$$\Phi_3(\nu)=3\cdot 2^{\nu}+1$$
$$L\left(\Phi_3(\nu)\right)=L\left(3\cdot 2^{\nu}+1\right)=\nu-1 \qquad (4.21)$$

4.

$$\Phi_4(\nu)=3\cdot 2^{\nu+2}-1$$
$$R\left(\Phi_4(\nu)\right)=R\left(3\cdot 2^{\nu+2}-1\right)=\nu-1. \qquad (4.22)$$

Proof. Corollary 4.2 is an immediate consequence of equations (4.11), (4.12). □

We name the intervals $\left[2^{\nu+1}+1,3\cdot 2^{\nu}-1\right)$ and $\left(3\cdot 2^{\nu}+1,2^{\nu+2}-1\right]$ as "A and B sub-interval of Ω". We define as "central boundary" of Ω the pair of (successive) odd numbers $3\cdot 2^{\nu}-1,3\cdot 2^{\nu}+1$.

From corollary 4.2 we have that the value of symmetry of the odd numbers Φ increases as ν increases. So we have the question: are there any other odd numbers which can have symmetry with large values? The answer comes from the quantification of part 1 of corollary 3.1:

Corollary 4.3. (Conjecture) With the exception of the numbers $\Phi_1, \Phi_2, \Phi_3, \Phi_4$, *the only powers of the odd numbers which have large L/R symmetry values are the numbers of the form*

$$\begin{gathered}\Theta = \Theta(\Pi, S) = \Pi^{2^S} \\ S, \Pi \in \mathbb{N}, \Pi = odd\end{gathered}, \tag{4.23}$$

$$L\left(2^{2^S}\right) \sim S\,. \tag{4.24}$$

2. *There are no numbers of the form of*

$$\begin{gathered}\Theta(\Pi, S) = \Pi^{2^S} \\ \Pi, S \in \mathbb{N}, \Pi = odd\end{gathered} \tag{4.25}$$

with symmetry R.

Next, we list five examples.

Example 4.2. The powers of 3 with even exponent have symmetry L. For the powers of the form 3^{2^S} the following equation holds

$$\begin{gathered}L\left(3^{2^S}\right) = S \\ S \in \mathbb{N}\end{gathered}.$$

For the rest powers of 3 with even exponent, the value of the symmetry L increases very slowly as the even exponent increases.

The powers of 3 with odd exponent

$$3^{2l+1}, l \in \mathbb{N}^*$$

have symmetry R. For small values of $l \in \mathbb{N}^*$ the values of symmetry are R=1, 2, 3 while if this value becomes higher than a specific number then it becomes constant.

$$\begin{gathered}R\left(3^{2l+1}\right) = 2 \\ l \in \mathbb{N}^*\end{gathered}.$$

Example 4.3. The powers of 5 have symmetry L. For the powers of the form 5^{2^S} following equation holds

$$\begin{gathered}L\left(5^{2^S}\right) = S - 1 \\ S \in \mathbb{N}\end{gathered}.$$

The powers of 5 with odd exponent have constant symmetry L=1.

Example 4.4. For powers of 7 with exponent being a power of 2 the following equation holds

$$L\left(7^{2^S}\right)=S+2$$
$$S\in\mathbb{N}^*$$

The symmetry of odd powers of 7 takes small values.

Example 4.5. The powers of 61 have symmetry L. For powers of 61 with exponent being a power of 2 the following equation holds

$$L\left(61^{2^S}\right)=S$$
$$S\in\mathbb{N}$$

The odd powers of 61 have constant symmetry L=1.

Example 4.6. The powers of 1001 = 7×11×13 have symmetry L. For powers of 1001 with exponent being a power of 2 the following equation holds

$$L\left(1001^{2^S}\right)=S+2 .$$

The odd powers of 1001 have constant symmetry L=2.

Corollaries 4.1, 4.2 and 4.3 give the distribution of symmetry L/R in the set $\mathbb{N}$ of the natural numbers.

5 An algorithm for determining prime numbers and factorization of natural numbers

The order of the number of operations required for the factorization of an composite odd number C=Cn, with n digits in decimal system is 10^n. The extremely high number of operations makes impossible this factorization if the number of digits is appropriately large [1]. The factorization of natural numbers can be done by using symmetries which calculate the factors of Cn by skipping the execution of these operations. L/R symmetry implies such an algorithm, by making use of part B of corollary 3.1, corollaries 4.2, 4.1, theorem 4.3, and the following corollary:

Corollary 5.1 (Conjecture) *For every asymmetric number of the form*

$$\Theta(2,S)=2^{2^S}, S\in\mathbb{N} \tag{5.1}$$

exists an interval around this number, whose length is of order

$$\varepsilon=2^{S+l}, l\in\{0,1,2,...\} \tag{5.2}$$

and this interval does not contain any prime numbers. The variable l *takes small values in the set* $\{0,1,2,...\}$.

Because of the accumulation of small prime numbers close to 0 the part 1 of the corollary holds for these values of S which satisfy $S\geq 5$.

In equation (5.2) l takes small values in the set $\{0,1,2,...\}$. Consequently, we know the length (5.2). This allows us to determine the prime numbers by using the equations

$$\begin{aligned} &P = 2^{2^S} \mp 1 - 2x \\ &P = 2^{2^S} \mp 1 + 2x \\ &\varepsilon = 2^{S+l}, l \in \mathbb{R} \\ &S, x \in \mathbb{N}, S \geq 5 \end{aligned} \quad (5.3)$$

From equation (5.3) for S=5, 6, 7, 8, 9 we get the first 10 prime numbers:

$$S = 5$$

$$P = 2^{32} - 1 - 2\cdot 2 = 2^{32} + 1 - 2\cdot 3 = 4294\ 967291$$

$$P = 2^{32} - 1 + 2\cdot 8 = 2^{32} + 1 + 2\cdot 7 = 4294\ 967311$$

$$\varepsilon = 2\cdot 8 - (-2\cdot 2) = 20$$

$$S = 6$$

$$P = 2^{64} - 1 - 2\cdot 29 = 2^{64} + 1 - 2\cdot 30 = 18\ 446744\ 073709\ 551557$$

$$P = 2^{64} - 1 + 2\cdot 7 = 2^{64} + 1 + 2\cdot 6 = 18\ 446744\ 073709\ 551629$$

$$\varepsilon = 2\cdot 7 - (-2\cdot 29) = 72$$

$$S = 7$$

$$P = 2^{128} - 1 - 2\cdot 79 = 2^{128} - 1 - 2\cdot 79 = 2^{128} + 1 - 2\cdot 80$$

$$= 340\ 282366\ 920938\ 463463\ 374607\ 431768\ 211297$$

$$P = 2^{128} - 1 + 2\cdot 26 = 2^{128} + 1 + 2\cdot 25$$

$$= 340\ 282366\ 920938\ 463463\ 374607\ 431768\ 211507$$

$$\varepsilon = 2\cdot 26 - (-2\cdot 79) = 210$$

$$S = 8$$

$$P = 2^{256} - 1 - 2\cdot 217 = 2^{256} + 1 - 2\cdot 218$$

$$= 115792\ 089237\ 316195\ 423570\ 985008\ 687907$$

$$853269\ 984665\ 640564\ 039457\ 584007\ 913129\ 639501$$

$$P = 2^{256} - 1 + 2\cdot 149 = 2^{256} + 1 + 2\cdot 148$$

$$= 115792\ 089237\ 316195\ 423570\ 985008\ 687907$$

$$853269\ 984665\ 640564\ 039457\ 584007\ 913129\ 640233$$

$$\varepsilon = 2\cdot 149 - (-2\cdot 217) = 732$$

$S = 9$

$P = 2^{512} - 1 - 2\cdot 284 = 2^{512} + 1 - 2\cdot 285$

$= 13407\ 807929\ 942597\ 099574\ 024998\ 205846\ 127479\ 365820\ 592393\ 377723$
$561443\ 721764\ 030073\ 546976\ 801874\ 298166\ 903427\ 690031\ 858186\ 486050$
$853753\ 882811\ 946569\ 946433\ 649006\ 083527$

$P = 2^{512} - 1 + 2\cdot 38 = 2^{512} + 1 + 2\cdot 37$

$= 13407\ 807929\ 942597\ 099574\ 024998\ 205846\ 127479\ 365820\ 592393\ 377723$
$561443\ 721764\ 030073\ 546976\ 801874\ 298166\ 903427\ 690031\ 858186\ 486050$
$853753\ 882811\ 946569\ 946433\ 649006\ 084171$

$\varepsilon = 2\cdot 38 - (-2\cdot 285) = 646$

For $S \to +\infty$ we obtain large prime numbers.

From the inequalities (4.3) and (4.6) we get

$$\begin{aligned} \nu &\geq L+1 \\ \nu &\geq R+1 \end{aligned} \tag{5.4}$$

$$\begin{aligned} |\Pi_L| &\leq 2^{\nu-L-1} \\ |\Pi_R| &\leq 2^{\nu-R-1}. \end{aligned} \tag{5.5}$$

From equations (4.1), for odd numbers Q with symmetry L, we have

$$Q - \left(3\cdot 2^{\nu} + 1\right) = 2^{L+1}\cdot \Pi_L \tag{5.6}$$

and

$$D - \left(3\cdot 2^{\nu} - 1\right) = 2^{R+1}\cdot \Pi_R \tag{5.7}$$

for the odd numbers D with symmetry R. From these equations we imply that numbers $2^{L+1}\cdot \Pi_L$ and $2^{R+1}\cdot \Pi_R$ express the distance of Q and D respectively from the central boundary of the interval Ω.

From the known prime numbers factors of Fermat numbers we have the following conclusions: The factors, prime numbers and composite of Fermat numbers have symmetry L. As their value increases, the prime number factors of Fermat numbers are shifted from one sub-interval of Ω to the other, fact which is equivalent with the change of sign of the odd number Π_L in equation (5.6). As their value increases, their distance from the central boundary of the Ω and the difference ν-L increase too. Consequently, for the prime numbers factors of Fermat numbers we know the sign of the odd number Π_L in equation (5.6).

From part B of corollary 3.1 we can determine the L/R symmetry of at least of one composite odd number whose factors are unknown. Next, we list two examples.

Example 5.1. From equation (2.12), for the number C1133 which is composite factor of F_{12} with 1133 digits, we get $\nu(C1133) = 3761$. Then, from equations (4.11), (4.12) we get L(C1133)=13. The factors of Fermat numbers have symmetry L, so from part 5 of corollary 3.1 we have that at least one of the factors of C1133 has symmetry L=13.

Example 5.2. For RSA-232 =
1009881397871923546909564894309468582818233821955573955141120516205831021338528545374366109757154363664913380084917065169921701524733294389270280234380960909804976440540711201965410747553824948672771374075011577182305398340606162079, from equation (2.12) we get that $\nu(RSA-232) = 766$. Then, from equations (4.11), (4.12) we have R(RSA-232)=4. The only acceptable combination which is compatible with part B of Corollary 3.1 is the following: The one factor of RSA-232 has symmetry L and the other has symmetry R, and the value of the symmetry of one of the two factors is 4 (L=4 or R=4), exactly the same as the symmetry of RSA-232.

The factorization algorithm of the odd numbers is based on the determining of prime numbers by using primality test [2-6] with specific characteristics. These characteristics of prime number factors of a composite odd number are determined by the use of properties of L/R symmetry. We list the three basic steps of the factorization algorithm for a composite odd number C=Cn, with n digits in decimal system:

Step 1. From equation (2.12) we calculate ν(Cn), and from equations (4.11), (4.12) we calculate the symmetry L or the symmetry R of Cn. From part B of corollary 3.1 we calculate the symmetry of at least on factor Q or D of Cn.

Step 2. By using the inequalities (5.4) for Q or D, we can determine the intervals in which ν(Q) and ν(D) belong. In order to determine these intervals we may use the properties of Cn, if it belongs to a specific number sequence.

Step 3. For any possible value of ν=ν(Q) or ν=ν(D) we determine the set $\Omega = \Omega_\nu$. Corollary 4.2 gives the type of symmetry, L or R, of the first and the last number of sub-intervals A and B of Ω_ν. Corollary 4.1 gives the way that symmetry L/R changes in the sub-intervals A and B of Ω_ν. Therefore, we know the position of Q with symmetry L, and of D with symmetry R within the set Ω_ν. Next, we determine the odd numbers Q or D for which

$$\begin{aligned} &\Pi_L = \frac{Q - 3\cdot 2^\nu - 1}{2^{L+1}} \in \mathbb{Z} \\ &\nu = \nu(Q) \end{aligned} \tag{5.8}$$

$$\begin{aligned} &\Pi_R = \frac{D - 3\cdot 2^\nu + 1}{2^{R+1}} \in \mathbb{Z} \\ &\nu = \nu(D) \end{aligned} \tag{5.9}$$

By using the primality test we can find the prime numbers Q or D of equations (5.8), (5.9). Then we check if prime numbers Q, D are factors of Cn: mod(Cn, Q)=0, mod(Cn, D)=0.

For every Fermat number the sign of Π_L changes as Q increases. Consequently we know the region of Ω_ν in which we will look for prime numbers Q. The two factors of RSA-232 have equal or nearly equal number of digits, thus it is

$$\nu(Q) \sim \frac{766}{2} = 383 \text{ and } \nu(D) \sim \frac{766}{2} = 383.$$

According to theorem 4.3 the consecutive pairs of odd numbers within the set Ω_ν have equal symmetries L/R and $\Pi_L = \Pi_R$. Corollary 4.3 gives the numbers with large value of symmetry L within the set Ω_ν. Corollary 5.1 gives sub-intervals of the set $\mathbb{N}$ of natural numbers which do not contain any prime numbers.

Acknowledgments

I would like to express my greatest thanking to Dr. Spyridoula Theodorou, Msc. Kyriaki Manousou, Msc. Andreas Panteris, Kyriakos Kefalas, Prof. Ilias Kotsireas, Dr. Konstantinos Panteris, Dr. Alexandros Kiupakis and the public benefit foundation Alexander S. Onassis for their contribution to the publication of this article.

References

[1] Duta, Cristina-Loredana, Laura Gheorghe, and Nicolae Tapus. "Framework for evaluation and comparison of integer factorization algorithms." *2016 SAI Computing Conference (SAI)*. IEEE, 2016.

[2] Apostol, Tom M. *Introduction to analytic number theory*. Springer Science & Business Media, 2013.

[3] Crandall, Richard, and Carl B. Pomerance. *Prime numbers: a computational perspective*. Vol. 182. Springer Science & Business Media, 2006.

[4] Gurevich, Alexander, and Boris, Kunyavskiĭ. "Primality testing through algebraic groups." *Arch. der Math*. 93.6 (2009): 555.

[5] Rempe-Gillen, Lasse, and Rebecca, Waldecker. Primality testing for beginners. *Amer. Math. Soc.*, 2014.

[6] Schoof, René. Four primality testing algorithms. *Algorithmic Number Theory*: *lattices, number fields, curves and cryptography, pp.* 101–126, Math. Sci. Res. Inst. Publ., 44, *Cambridge Univ. Press, Cambridge,* 2008.