

On prime numbers

© 2019 г. Prof. em. André Maisseu^{1,*}, Dr. Benoît Maisseu²

¹ University of Paris 1-La Sorbonne

² Ecole Supérieure d'Electricité “Supélec”

*e-mail: a.maisseu@bluewin.ch

Received October 15, 2018; revised October 29, 2018; accepted November 6, 2018

Abstract—The article addresses the problem of the representation of prime numbers. It is known that primes $P > 3$ are represented by the equation $P = 6 \cdot N \pm 1$, where N is an integer. However, not for all integers N , P is a prime number. The article proposes a representation of primes in the form of a hypothesis using the representation of an integer N through rational and irrational numbers. Thus, the article provides a scheme for the representation of primes using formulas depending on the values of the parameter numbers included in the proposed formulas. Within the framework of the proposed scheme, the classification of primes into groups is given. Two times six main basic groups are identified, through which further groups of prime numbers are cyclically formed. The authors of the article hope that the representation of primes proposed in it can be proved strictly mathematically and will find application in solving problems of the theory of numbers.

Keywords: prime numbers, composite number, rational, irrational, classification, groups

DOI: 10.1134/S2304487X19010085

1. THE FUNDAMENTAL EQUATION

According to [1, 2] all prime numbers $P > 3$ can be written in the form: $P = 6 \cdot N \pm 1$, $P \equiv (\pm 1) \pmod{6}$.

However, not all numbers having this form are prime numbers. This family of numbers, $\mathcal{F}P$, hence comprises **all** prime numbers **and** composite numbers, semi-prime or not. According to the same references, the square of any number $P \in \mathcal{F}P$, prime or not, has the form: $P^2 = 24 \cdot A + 1$, $P^2 \equiv 1 \pmod{24}$.

According to Kraft's theorem (1801) cited by Leonard Eugene Dickson in [2] and taken up by Gérard Villemin, for any number having the form $P = 6 \cdot N \pm 1$, if it is possible to find i and j such that

$N = 6 \cdot i \cdot j \pm (i \pm j)$, P is a composite number; if not, it is prime [3].

This rule implicitly assumes that i and j are natural numbers. Or, if the rule is extended to all real numbers, the following simple rule applies:

for N , called subscript of the number P , defined by the equation $P = 6 \cdot N \pm 1$,

where $N = 6 \cdot |i| \cdot |j| \pm (i \pm j)$, i and j being the coefficients of subscript N of the number P :

when i and j are natural numbers, strictly rational, P is a composite number;

when i and j irrational, P is a prime number.

On the opposite of the usual acceptance which rules numbers theory, prime numbers are not particular case. Its are general case of elements of $\mathcal{F}P$ set with

$P = 6N \pm 1$. It is composite numbers which are particular case, with i and j as natural rational numbers.

Example:

$P = 143 = 6 \cdot 24 - 1$, hence $N = 24$; giving: $i = 2$, $j = -2$.

We have $N = 6 \cdot |i| \cdot |j| + i + j = 6 \cdot 2 \cdot 2 + 2 + (-2) = 24$,

$P = 11 \cdot 13 \rightarrow P$ is a composite number,

$P = 451 = 6 \cdot 75 + 1$, hence $N = 75$; giving: $i = -2$, $j = -7$.

We have $N = 6 \cdot |i| \cdot |j| + i + j = 6 \cdot 2 \cdot 7 + -(-2) + + (-7) = 75$,

$P = 11 \cdot 41 \rightarrow P$ is a composite number,

$P = 179 = 6 \cdot 30 - 1$, hence $N = 30$; giving: $i = \sqrt{5}$, $j = -\sqrt{5}$.

We have $N = 6 \cdot |i| \cdot |j| + i + j = 6 \cdot \sqrt{5} \cdot \sqrt{5} + \sqrt{5} - \sqrt{5} = 30$,

$P = [(6 \cdot \sqrt{5}) + 1] \cdot [(6 \cdot \sqrt{5}) + -1] = 179 \rightarrow P$ is a prime number.

2. DEUX SUB-SET MIXING PRIME NUMBERS AND COMPOSITE NUMBERS, GROUPED INTO TWO TIMES SEVEN GROUPS

The prime and composites numbers defined by the equation $P = 6 \cdot N \pm 1$, belong to the same set $\mathcal{F}P$. Whether prime or composite, they are broken down into two subfamilies, $\mathcal{F}V$ and $\mathcal{F}VII$, whether $P = 6 \cdot N - 1$ or $P = 6 \cdot N + 1$, or according to whether i and j have different signs or the same sign. Each of the two families can be broken down into subfamilies.

2.1. $\mathcal{FV}$: $P = 6 \cdot N - 1$; i and j have different signs

The six subfamilies of $\mathcal{FV}$ are:

2.1.1.

$P \in \mathcal{FV}[-1]$ where $P = (-1) + k \cdot 36$ or $P = (-1) \bmod 36$,

$\mathcal{FV}[-1] \equiv \{35[1, -1], 71[\sqrt{2}, -\sqrt{2}], 107[\sqrt{3}, -\sqrt{3}], 143[2, -2], 179[\sqrt{5}, -\sqrt{5}], 215[1, -7], 251[\sqrt{7}, -\sqrt{7}], 287[7, -1], 323[3, -3], \dots\}$

2.1.2.

$P \in \mathcal{FV}[5]$ where $P = (5) + k \cdot 36$ or $P = 5 \bmod 36$,

$\mathcal{FV}[5] \equiv \{5[1, 0], 41[(1 + \sqrt{5})/2, (1 - \sqrt{5})/2], 77[2, -1], 113[(1 + \sqrt{13})/2, (1 - \sqrt{13})/2], 149[(1 + \sqrt{17})/2, (1 - \sqrt{17})/2], 185[1, -6], 221[3, -2], 257[(1 + \sqrt{29})/2, (1 - \sqrt{29})/2], \dots\}$

2.1.3.

$P \in \mathcal{FV}[11]$ where $P = (11) + k \cdot 36$ or $P = 11 \bmod 36$,

$\mathcal{FV}[11] \equiv \{11[2, 0], 47[(1 + \sqrt{2}), (1 - \sqrt{2})], 83[(1 + \sqrt{3}), (1 - \sqrt{3})], 119[3, -1], 155[1, -5], 191[(1 + \sqrt{6}), (1 - \sqrt{6})], 227[(1 + \sqrt{7}), (1 - \sqrt{7})], 263[(1 + \sqrt{8}), (1 - \sqrt{8})], \dots\}$

2.1.4.

$P \in \mathcal{FV}[17]$ where $P = (17) + k \cdot 36$ or $P = 17 \bmod 36$,

$\mathcal{FV}[17] \equiv \{17[3, 0], 53[(3 + \sqrt{13})/2, (3 - \sqrt{13})/2], 89[(3 + \sqrt{17})/2, (3 - \sqrt{17})/2], 125[1, -4], 161[4, -1], 197[(3 + \sqrt{29})/2, (3 - \sqrt{29})/2], 233[(1 + \sqrt{33})/2, (1 - \sqrt{33})/2], 269[(3 + \sqrt{37})/2, (3 - \sqrt{37})/2], 305[1, -10], \dots\}$

2.1.5.

$P \in \mathcal{FV}[23]$ where $P = (23) + k \cdot 36$ or $P = 23 \bmod 36$,

$\mathcal{FV}[23] \equiv \{23[4, 0], 59[(2 + \sqrt{5}), (2 - \sqrt{5})], 95[1, -3], 131[(2 + \sqrt{7}), (2 - \sqrt{7})], 167[(2 + \sqrt{8}), (2 - \sqrt{8})], 203[5, -1], 239[(2 + \sqrt{10}), (2 - \sqrt{10})], 275[2, -4], \dots\}$

2.1.6.

$P \in \mathcal{FV}[29]$ where $P = (29) + k \cdot 36$ or $P = 29 \bmod 36$,

$\mathcal{FV}[29] \equiv \{29[5, 0], 65[1, -2], 101[(5 + \sqrt{33})/2, (5 - \sqrt{33})/2], 137[(5 + \sqrt{37})/2, (5 - \sqrt{37})/2], 173[(5 + \sqrt{41})/2, (5 - \sqrt{41})/2], 209[2, -3], 245[(6, -1), \dots\}$

2.1.7. p. m.:

$P \in \mathcal{FV}[35] \equiv \mathcal{FV}[-1]$

$P \in \mathcal{FV}[41] \equiv \mathcal{FV}[5]$

etc...

2.2. $\mathcal{FVII}$: $P = 6 \cdot N + 1$; i and j have the same sign

For i and j having the same sign, the product $(i \cdot j)$ is necessarily positive. The six subfamilies of $\mathcal{FVII}$ are:

2.2.1.

$P \in \mathcal{FVII}[1]$ where $P = 1 + k \cdot 36$ or $P = 1 \bmod 36$

$\mathcal{FVII}[1] \equiv \{1[0, 0], 37[6, 0], 73[3 + \sqrt{8}, 3 - \sqrt{8}], 109[3 + \sqrt{7}, 3 - \sqrt{7}], 145[-5, -1], 181[3 + \sqrt{5}, 3 - \sqrt{5}], 217[5, 1], 253[-4, -2], 289[-3, -3], 325[4, 2] \& [-11, -1], \dots\}$

2.2.2.

$P \in \mathcal{FVII}[7]$ where $P = (7) + k \cdot 36$ or $P = 7 \bmod 36$,

$\mathcal{FVII}[7] \equiv \{7[1, 0], 43[(-5 + \sqrt{17})/2, -5 - \sqrt{17}], 79[(-5 + \sqrt{13})/2, -5 - \sqrt{13})/2], 115[-1, -4], 151[(-5 + \sqrt{5})/2, -5 - \sqrt{5})/2], 187[-2, -3], 223[(-11 + \sqrt{89})/2, (-11 - \sqrt{89})/2], 259[1, 6], 295[-1, -10], 331[(-11 + \sqrt{77})/2, (-11 - \sqrt{77})/2], \dots\}$

2.2.3.

$P \in \mathcal{FVII}[13]$ where $P = (13) + k \cdot 36$ or $P = 13 \bmod 36$,

$\mathcal{FVII}[13] \equiv \{13[2, 0], 49[1, 1], 85[-3, -1], 121[-2, -2], 157[(-8 + \sqrt{52})/2, (-8 - \sqrt{52})/2], 193[(-8 + \sqrt{48})/2, (-8 - \sqrt{48})/2], 229[(-8 + \sqrt{44})/2, (-8 - \sqrt{44})/2], 265[-9, -1], 301[7, 1], \dots\}$

2.2.4.

$P \in \mathcal{FVII}[19]$ where $P = (19) + k \cdot 36$ or $P = 19 \bmod 36$,

$\mathcal{FVII}[19] \equiv \{19[3, 0], 55[-1, -2], 91[1, 2], 127[(-9 + \sqrt{73})/2, (-9 - \sqrt{73})/2], 163[(-9 + \sqrt{69})/2, (-9 - \sqrt{69})/2], 199[(-9 + \sqrt{65})/2, (-9 - \sqrt{65})/2], 235[-1, -8], 271[(-9 + \sqrt{57})/2, (-9 - \sqrt{57})/2], 307[(-9 + \sqrt{53})/2, (-9 - \sqrt{53})/2], \dots\}$

2.2.5.

$P \in \mathcal{FVII}[25]$ where $P = (25) + k \cdot 36$ or $P = 25 \bmod 36$,

$\mathcal{FVII}[25] \equiv \{25[4, 0], 61[(-8 + \sqrt{52})/2, (-8 - \sqrt{52})/2], 97[(-8 + \sqrt{48})/2, (-8 - \sqrt{48})/2], 133[3, 1], 169[2, 2], 205[-1, -7], 241[(-8 + \sqrt{32})/2, (-8 - \sqrt{32})/2], \dots\}$

2.2.6.

$P \in \mathcal{FVII}[31]$ where $P = (31) + k \cdot 36$ or $P = 31 \bmod 36$,

$\mathcal{FVII}[31] \equiv \{31[5, 0], 67[(-7 + \sqrt{37})/2, (-7 - \sqrt{37})/2], 103[(-7 + \sqrt{33})/2, (-7 - \sqrt{33})/2], 139[(-7 + \sqrt{29})/2, (-7 - \sqrt{29})/2], 175[-1, -6] \& [1, 4], 211[(-7 + \sqrt{21})/2, (-7 - \sqrt{21})/2], 247[2, 3], \dots\}$

2.2.7. p. m.:

$P \in \mathcal{FVII}[37] \equiv \mathcal{FVII}[1]$

$P \in \mathcal{FVII}[43] \equiv \mathcal{FVII}[7]$

etc...

3. SOME EQUATIONS

Note: The equations used below are the usual equations, but imply numbers that may be rational or irrational according to whether the number is composite or prime.

Uses of the equation between N and its two subscripts, i and j , and of the equation between P and its subscript N , help easily establish the following equations. In all these equations, i and j are:

- either irrational numbers, in which case P is an integer;
- or rational integers, in which case P is a composite number.

3.1. N is subscript of P

(Note that the calculation of the various coefficients usually carried out with strictly rational integers, is extended to irrational numbers. $C_{2,n} = n(n-1)/2$.)

3.1.1. For $P \in \mathcal{FV}$: $P = 6 \cdot N - 1$; i and j have different signs

For $i > 0; j < 0$:

$$N = [24 \cdot (C_{2,i+1} + 2 \cdot C_{2,i}) + 1]^{1/2} \cdot j + i = [24 \cdot (2 \cdot C_{2,j+1} + C_{2,j}) + 1]^{1/2} \cdot i + j.$$

We know that pentagonal numbers are given by the following two equations:

$$H_n = n \cdot (3 \cdot n - 1)/2 = (3 \cdot n^2 - n)/2 = n + 3 \cdot C_2, \\ n = C_{2,i+1} + 2 \cdot C_{2,i} \rightarrow \{1, 5, 12, 22, \dots\} \text{ when } n \text{ is rational,}$$

$$G_n = n \cdot (3n + 1)/2 = (3 \cdot n^2 + n)/2 = 2 \cdot n + 3 \cdot C_2, \\ n = 2 \cdot C_{2,j+1} + C_{2,j} \rightarrow \{2, 7, 15, 26, \dots\} \text{ when } n \text{ is rational. This gives:}$$

$$N = [24 \cdot Hi + 1]^{1/2} \cdot j + i = [24 \cdot Gj + 1]^{1/2} \cdot i + j.$$

3.1.2. For $P \in \mathcal{FVII}$: $P = 6 \cdot N + 1$; i and j have the same sign

For $i > 0; j > 0$:

$$N = [24 \cdot (2 \cdot C_{2,i+1} + C_{2,i}) + 1]^{1/2} \cdot j + i = [24 \cdot (2 \cdot C_{2,j+1} + C_{2,j}) + 1]^{1/2} \cdot i + j,$$

$$N = [24 \cdot G_i + 1]^{1/2} \cdot j + i = [24 \cdot G_j + 1]^{1/2} \cdot i + j.$$

For $i < 0; j < 0$:

$$N = [24 \cdot (C_{2,i+1} + 2 \cdot C_{2,i}) + 1]^{1/2} \cdot j + i = [24 \cdot (C_{2,j+1} + 2 \cdot C_{2,j}) + 1]^{1/2} \cdot i + j,$$

$$N = [24 \cdot H_i + 1]^{1/2} \cdot j + i = [24 \cdot H_j + 1]^{1/2} \cdot i + j.$$

3.2. Roots of a number X and Y

Application of the equations between P , N , i and j , serves readily to establish the following equations:

3.2.1. For $P \in \mathcal{FV}$: $P = 6 \cdot N - 1$; i and j have different signs

For $i > 0; j < 0$:

$$X = 6 \cdot i - 1 = [24 \cdot (C_{2,i+1} + 2 \cdot C_{2,i}) + 1]^{1/2} = [24 \cdot H_i + 1]^{1/2},$$

$$Y = 6 \cdot |j| + 1 = [24 \cdot (2 \cdot C_{2,j+1} + C_{2,j}) + 1]^{1/2} = [24 \cdot G_j + 1]^{1/2}.$$

3.2.2. For $P \in \mathcal{FVII}$: $P = 6 \cdot N + 1$; i and j have the same sign

For $i > 0; j > 0$:

$$X = 6 \cdot i + 1 = [24 \cdot (2 \cdot C_{2,i+1} + C_{2,i}) + 1]^{1/2} = [24 \cdot G_i + 1]^{1/2},$$

$$Y = 6 \cdot j + 1 = [24 \cdot (2 \cdot C_{2,j+1} + C_{2,j}) + 1]^{1/2} = [24 \cdot G_j + 1]^{1/2}.$$

For $i < 0; j < 0$:

$$X = 6 \cdot |i| - 1 = [24 \cdot (C_{2,i+1} + 2 \cdot C_{2,i}) + 1]^{1/2} = [24 \cdot H_i + 1]^{1/2},$$

$$Y = 6 \cdot |j| - 1 = [24 \cdot (C_{2,j+1} + 2 \cdot C_{2,j}) + 1]^{1/2} = [24 \cdot H_j + 1]^{1/2}.$$

3.3. P as a function of i and j

3.3.1. For $P \in \mathcal{FV}$: $P = 6 \cdot N - 1$; i and j have different signs

For $i > 0; j < 0$:

$$P = 6 \cdot [24 \cdot H_i + 1]^{1/2} \cdot j + 6 \cdot i - 1 = 6[24 \cdot G_j + 1]^{1/2} \cdot i + 6 \cdot j - 1$$

3.3.2. For $P \in \mathcal{FVII}$: $P = 6 \cdot N + 1$; i and j have the same sign

For $i > 0; j > 0$:

$$P = 6 \cdot [24 \cdot G_i + 1]^{1/2} \cdot j + 6 \cdot i + 1 = 6 \cdot [24 \cdot G_j + 1]^{1/2} \cdot i + 6 \cdot j + 1.$$

For $i < 0; j < 0$:

$$P = 6 \cdot [24 \cdot H_i + 1]^{1/2} \cdot j + 6 \cdot i + 1 = 6 \cdot [24 \cdot H_j + 1]^{1/2} \cdot i + 6 \cdot j + 1.$$

3.4. A is cardinal of the number P

It is recalled that $P^2 = 24 \cdot A + 1$.

3.4.1. For $P \in \mathcal{FV}$: $P = 6 \cdot N - 1$; i and j have different signs

$$A = (3 \cdot N^2 - N)/2 = C_{2,N+1} + 2 \cdot C_{2,N},$$

$$A = 24 \cdot H_i \cdot G_j + H_i + G_j.$$

3.4.2. For $P \in \mathcal{FVII}$: $P = 6 \cdot N + 1$; i and j have the same sign

$$A = (3 \cdot N^2 + N)/2 = 2 \cdot C_{2,N+1} + C_{2,N}.$$

For $i > 0; j > 0$, A is therefore written:

$$A = 24 \cdot G_i \cdot G_j + G_i + G_j.$$

For $i < 0; j < 0$, A is therefore written:

$$A = 24 \cdot H_i \cdot H_j + H_i + H_j.$$

REFERENCES

1. Gérard Villemin. Ordre arithmétique. <http://villemin.gerard.free.fr/Wwwgymm/Premier/sequenc6.htm>.
2. Leonard Eugene Dickson. History of the Theory of Numbers, Volume I: Divisibility and Primality, 2005.
3. André Maisseu, Confidential memo. Académie des Sciences, Paris, 1997.

О простых числах

Профессор Андрэ Мэйсё^{a, *}, Доктор Бенуа Мэйсё^b

^a Университет Парижа 1 – Сорбонна,

Почетный президент всемирной организации работников атомной отрасли (WONUC)

^b Высшая школа электричества "Supélec" (Париж)

*e-mail: a.maisseu@bluewin.ch

Аннотация. В статье рассматривается проблема представление простых чисел. Известно, что простые числа $P > 3$ представлены с помощью равенства $P = 6 \cdot N \pm 1$, где N есть целое число. Однако не для всех целых чисел N P является простым числом. В статье предлагается в виде гипотезы представление простых чисел с помощью представления целого числа N через рациональные и иррациональные числа. Таким образом, в статье дана схема представления простых чисел с помощью формул в зависимости от значений чисел-параметров, входящих в предложенные формулы. В рамках предложенной схемы дана классификация простых чисел по группам. Выделено семь основных базовых групп, через которые циклично формируются дальнейшие группы простых чисел. Авторы статьи надеются, что предложенное в ней представление простых чисел может быть доказано строго математически и найдет применение в решении задач теории чисел.

Ключевые слова: простые числа, составные числа, рациональные числа, иррациональные числа, классификация, группы

DOI: 10.1134/S2304487X19010085

СПИСОК ЛИТЕРАТУРЫ

1. Жерар Вильмин. Арифметический порядок. <http://villemmin.gerard.free.fr/Wwwgymm/Premier/se-quenc6.htm>.
2. Леонард Эйжен Диксон. История теории чисел, том 1: Делимость и простота чисел, 2005.
3. Андрэ Мэйсё. Конфиденциальная записка. Академия наук, Париж, 1997.