Prime Numbers Classification with Linear and Quadratic Forms

Valeryi Meshkoff

Evpatoria, Republic of Crimea, Russian Federation

Abstract  It is known, that any prime number has presentation in linear and quadratic forms. These properties may be used for finding class subsets of prime numbers. For that it is showed, that all prime numbers simple quadratic forms consist of \( a^2 + mb^2, m = 1, \pm 2, 3 \). On these grounds it is examination for variants of prime numbers classification. It is discovered eight non-intersecting subsets of prime numbers, in conformity with equivalence classes modulo 24. The proposed classification is used for analyses Mersenne and Fermat numbers and composite numbers.

Keywords  Classification, Number, Form, Theorem, Single Presentation

1. Introduction

The fundamental theorem of arithmetic states that any positive integer can be represented in exactly one way as a product of prime numbers. The difference between primes are come to light if investigate their linear and quadratic forms. For instance, there are two subsets of primes with linear form \( 41n + \) and with linear form \( 43n + \). It is practically simplest prime number classification with equivalence classes modulo 4. It is used for elementary analyzing and proving in Number Theory. But anybody can to see in literature the absence further researching on classification theme. This paper is tried to fill this gap with more detailed classification with hope to use it for more complicated problems.

The offered classification is based on the old researches, begun by Albert Girard (1595-1632) and Pierre de Fermat (1601-1665) and in detail analyzed in [1, §1.7]. It was found, that only the prime numbers of line series \( 4n + 1 \) and with linear form \( 4n + 3 \). It is practically simplest prime number classification with equivalence classes modulo 4. It is used for elementary analyzing and proving in Number Theory. But anybody can to see in literature the absence further researching on classification theme. This paper is tried to fill this gap with more detailed classification with hope to use it for more complicated problems.

Its properties are exceptional, as \( a^2 + 4b^2 \) is a sum of two squares, and numbers \( a^2 + 5b^2 \) are subordinated to other rules. Therefore it is natural to classify prime numbers with its representations as a sum \( a^2 + mb^2, m = 1, 2, 3 \) and all other prime numbers, having not such presentation.

2. Prime Numbers with Other Quadratic Form

These other, as it is easy to check, are members of line series \( 24k - 1, k = \) . As a function of Euler \( \varphi(24) = 8 \), so asymptotically the quotas of these prime numbers contain \( 1/6 \) of the set of all prime numbers.

It is not difficult also to set that prime numbers \( a^2 + 5b^2 \in 4n + 1 \), so for the prime numbers \( 24k - 1 \) simple similar positive quadratic form does not exist.

However \( p = 24k - 1 \in 8n - 1 \), and from the elementary theory of numbers it is known, that in this case exist quadratic residue \( x^2 \equiv 2 \mod p \). So there is presentation as a quadratic form \( p = \pm(a^2 - 2b^2) > 0 \). For example \( 23 = 5^2 - 2 \cdot 1^2 = -(3^2 - 2 \cdot 4^2) \). It reveals connection with Diophantine equations

\[
y^2 - 2x^2 = \pm \omega, \omega \in \mathbb{P} = 24k - 1 \quad (1)
\]

Such equations have some number of endless sequences of decisions [1, p.404], that in case of prime \( \omega \) is taken to two sequences. There is the least (initial) decision in two sequences, and all successive decisions are defined from initial its and the sequence of decisions for Pell equations \( y^2 - 2x^2 = 1 \).

Without ambiguity we will accept, that prime numbers \( p = 24k - 1 \in a^2 - 2b^2 > 0 \). The sequence of such quadratic forms is endless, but has determination by its initial decision.
**Theorem.** Any prime number \( p = 24k - 1 = a^2 - 2b^2 \), where \( y_1 = a, x_1 = b \) are initial decisions Diophantine equations \( y^2 - 2x^2 = p \).

**Proof.** Prime number \( p = 24k - 1 = 8n - 1 \), therefore has quadratic residue \( z^2 \equiv 2 \pmod{p} \). It is identically to Diophantine equation \( z^2 - 2 \cdot 1^2 = \lambda \cdot p \). The left part of this equation has form \( c^2 - 2d^2 \), and executed condition \( (z, p) = (z, \lambda) = 1 \), i.e. these numbers are mutually simple. As \( p \) is prime number, then \( p \) and \( \lambda \) are the divisors of the left part of equation. But it is known [1, chapter 2 and exercise 2.4.4] from the elementary theory, that these numbers then must have forms \( 2^2 \cdot 2, 2^2 \cdot 2 \). Therefore we must have decisions corresponding to Diophantine equations. Sequence of decisions from equation \( y^2 - 2x^2 = p \) has an initial decision. A theorem is well-proven.

### 3. Basis and Variants of Classification

The stated allows offering simple and evident classification of the prime numbers, separated on four partly intersecting sets of circular, elliptic (two sets) and hyperbolic prime numbers.

It should be noted that in this classification the linear form \( 8n - 1 \) has not an obvious presentation. It is so, because these prime numbers are disintegrated on two non-intersecting sets depending on the value of residue \( n \pmod{3} \). If \( n = 3k \), we have the set of hyperbolic prime numbers. If \( n = 3k + 1 \), it is the set of Elliptic 2 prime numbers. And if \( n = 3k + 2 \) we have a sequence of component numbers multiple 3.

It is also necessary to distinguish the intersecting or partly intersecting sets of prime numbers, and hereupon having a few possible quadratic forms, and cases, when non-intersecting sets of prime numbers have identical quadratic forms. For example, prime numbers \( 8n + 1 \) and prime numbers \( 24k - 1 \) have a quadratic form \( a^2 - 2b^2 \), however belong to the non-intersecting sets, as \( 8n + 1 \neq 24k - 1 \).

On the other hand, circular prime number 97 has all quadratic forms of presentation, as \( 97 = 9^2 + 4^2 = 5^2 + 2 \cdot 6^2 = 7^2 + 3 \cdot 4^2 = 13^2 - 2 \cdot 6^2 \), but intersects only with Elliptic 2 prime numbers.

Enumerations of sets of prime numbers offered before, for example [2, page 188], are not classification, as are not based on general properties. The offered classification in the basis has such properties, namely: any product of prime numbers, with the identical quadratic form from Table 1, has the same quadratic form. From here it is, that product of prime numbers belonging to one of sets of Table 1, has the basic quadratic form of this set.

Thus, the basis for classification of prime numbers is the known formula for the special cases of composition of quadratic forms [1, p. 396]

\[
(a^2 + mb^2)(c^2 + md^2) = (ab - mcd)^2 + m(ad + bc)^2
\]

(2)

Mentioned above enumeration in [2, p. 188], such property does not possess, as use quadratic forms \( 2a^2 + 3b^2 \) for prime numbers characterizing.

On our basis it maybe to perfect and simplify the classification presented in Table 1, using only the non-intersecting sets of prime numbers.

| Prime numbers | Quadratic form | Linear form | Partly intersecting with sets: | Other possible forms of representations |
|---------------|----------------|-------------|---------------------------------|-----------------------------------------|
| Circular      | \( a^2 + b^2 \) | \( 4n + 1 \) | Elliptic 2                       | \( a^2 + 2b^2 (n = 2k) \)               |
|               |                |             |                                 | \( a^2 - 2b^2 (n = 2k) \)               |
|               |                |             |                                 | \( a^2 + 3b^2 (n = 3k) \)               |
| Elliptic 1    | \( a^2 + 2b^2 \) | \( 8n + 3 \) | Elliptic 2                       | \( a^2 + 3b^2 (n = 3k + 2) \)          |
| Elliptic 2    | \( a^2 + 3b^2 \) | \( 6n + 1 \) | Circular                        | \( a^2 + 2b^2 (n = 2k) \)               |
|               |                |             | Elliptic 1                       | \( a^2 + 2b^2 (n = 4k, n = 4k + 3) \)  |
|               |                |             |                                 | \( a^2 - 2b^2 (n = 4k, n = 4k + 1) \)  |
| Hyperbolic    | \( a^2 - 2b^2 \) | \( 24k - 1 \) |                                |                                         |
Table 2. Variant Classification with the non-intersecting sets of prime numbers

| Prime numbers | Quadratic form | Linear form | Quotas in the set of all prime numbers | Other possible forms of representations |
|---------------|---------------|-------------|----------------------------------------|----------------------------------------|
| Circular      | \(a^2 + b^2\) | \(4n + 1\)  | \(\frac{1}{2}\)                        | \(a^2 \pm 2b^2 (n = 2k)\)              |
|               |               |             |                                        | \(a^2 + 3b^2 (n = 3k)\)               |
| Elliptic 1    | \(a^2 + 2b^2\) | \(8n + 3\)  | \(\frac{1}{4}\)                        | \(a^2 + 3b^2 (n = 3k + 2)\)           |
| Elliptic 2    | \(a^2 + 3b^2\) | \(24n + 7\) | \(\frac{1}{8}\)                        | \(a^2 - 2b^2\)                        |
| Hyperbolic    | \(a^2 - 2b^2\) | \(24k - 1\) | \(\frac{1}{8}\)                        |                                        |

From Table 2 we see the possession for more detailed classification, if for basis to take non-intersecting subsets corresponding to the non-intersecting residue classes modulo 24.

We will designate quadratic forms as \(R\) – Circular, \(E1, E2\) – Elliptic 1 and 2, \(G\) – Hyperbolic.

Table 3. Prime numbers classification \((p > 3, n \geq 0)\) with the non-intersecting classes of equivalence

| Prime numbers | Basis quadratic form | Linear form | Quotas in the set of all prime numbers | Other possible forms of representations |
|---------------|----------------------|-------------|----------------------------------------|----------------------------------------|
| Circular      | \(R\)                | \(24n + 1\) | \(\frac{1}{8}\)                        | \(E1, E2, G\)                          |
| Circular      | \(R\)                | \(24n + 5\) | \(\frac{1}{8}\)                        |                                        |
| Circular      | \(R\)                | \(24n + 13\)| \(\frac{1}{8}\)                       | \(E2\)                                |
| Circular      | \(R\)                | \(24n + 17\)| \(\frac{1}{8}\)                       | \(E1, G\)                             |
| Elliptic 1    | \(E1\)               | \(24n + 11\)| \(\frac{1}{8}\)                        |                                        |
| Elliptic 1    | \(E1\)               | \(24n + 19\)| \(\frac{1}{8}\)                        | \(E2\)                                |
| Elliptic 2    | \(E2\)               | \(24n + 7\) | \(\frac{1}{8}\)                        | \(G\)                                 |
| Hyperbolic    | \(G\)                | \(24n + 23\)| \(\frac{1}{8}\)                        |                                        |

Data of Tables we have from decisions of equations \(a^2 + mb^2 = 24n + k, i = 1...8, m = 1, \pm 2, 3\).

It is Diophantine equations modulo 24, and similar problems are easy solved with computer programs Mathematica. We use function Reduce, for solving equations over the integers modulo 24, and there is simplification, as sense has only alternative: is decision or not.

4. Applications

Just as above, we may use classification for researching any subsets of primes with other linear, quadratic and polynomial forms. For instance, consider primes with above mentioned quadratic form \(2a^2 + 3b^2\). Just as above, we examine equations \(2a^2 + 3b^2 = k_i (Mod 24), i = 1...8, m = 1, \pm 2, 3\). The results may be presented as

Theorem. The prime numbers \(2a^2 + 3b^2\) have only quadratic and linear forms \((R, 24n + 5)\) and \((E1, 24n + 11)\).

For elementary sense we have \(2 \cdot 1^2 + 3 \cdot 1^2 = 5 = 2^2 + 1^2, 2 \cdot 2^2 + 3 \cdot 1^2 = 11 = 3^2 + 2 \cdot 1^2\) and so on.

Analogous results we have not only for primes with positive quadratic forms. If primes \(p \in 2a^2 - 3b^2 > 0\), then it has forms \((R, 24n + 5)\) and \((G, 24n + 23)\). If primes \(p \in 3a^2 - 2b^2 > 0\), then it has forms \((R, 24n + 1)\) and \((E1, 24n + 19)\). We can generalize above results for any polynomial forms \(P(x, y)\). But it may be presented as some application on Diophantine equations theory.

Theorem. The Diophantine equations \(P(x, y) = p\) may be has decision, if \(P(x, y) - p \equiv 0 (Mod 24)\), and can not has decision, if that condition do not exist.

The proof is evident, as we use primes classification Table 3 with non-intersecting subsets.

The got classification we will apply for the analysis of some problems of Number Theory with composite numbers. In the beginning we will consider the set of prime numbers \(M_p = 2^p - 1, p > 2, p \in \text{primes}\) of Marin Mersenne (1588-1648). It is not difficult directly to check, that for odd numbers a possible linear form \(24n + 7\) belongs only to Elliptic 2. Thus all prime numbers \(M_p > 3\) belong to...
Elliptic 2 and have except E2 yet quadratic form of presentation G. We will notice that for odd number index any number $2^{2m+1} - 1$, $m \geq 2$, must have quadratic form $G$. If it is composite number, then his divisors may be only primes $24n + 7$, or primes $24n + 1$, or primes $24n + 17$, or primes $24n + 23$. Only they have Hyperbolic quadratic form, as it appears from classification of Table 3.

Final conclusion: the composite number $2^{2m+1} - 1$, $m \geq 2$, can have an odd number of prime divisors $24n + 7$, with any number of prime divisors $24n + 1$, or equal numbers of prime divisors $24n + 17$ and $24n + 23$. In general case for possible variants of divisors of composite it is condition $(7)^{\prime}(1)^{\prime}(17)^{\prime}(-1)^{\prime} = 7(\text{mod} 24)$, where $n = i + j + k + l$ is number of divisors.

Alike we will consider Fermat numbers $F_m = 2^{2^m} + 1$, $m \geq 2$. It is not difficult to see, they have quadratic forms $R, E1, G$. Simple analysis by means of Table 3 classification results in a conclusion: the prime numbers $F_m = 2^{2^m} + 1$, $m \geq 2$, belong to the class $24n + 17$. A composite number $F_m = 2^{2^m} + 1$, $m \geq 2$, can have an odd number of prime divisors $24n + 17$ and any number of prime divisors $24n + 1$.

In general case for arbitrary numbers classification can be produced by means of computers with the corresponding programs.

Author was use the program Mathematica, working with the tasks of Number Theory.

As an example we will consider a number $N = 2^{198} + 1$. In the beginning we determine, is that number prime or composite, and for this purpose there are standard programs of Mathematica.

If it is prime number, then further we calculate $a \equiv N(\text{mod} 24)$, and classify it in obedience to Table 3. But for $N = 2^{198} + 1$ we get, that number is composite.

As $N$ has the quadratic form $R$, so all its prime constituents have the same quadratic form. Although $a \equiv N \equiv 17(\text{mod} 24)$, the prime constituents $24n + 17$ are not present. It is possible to define constituents, producing factorization of number, i.e. finding $N = \prod p_i^{\alpha_i}$. Also for this purpose there are standard programs, and the result usually appears as $N = \left\{ \{p_i, \alpha_i\}, ..., \{p_i, \alpha_i\}, ... \right\}$.

For classification this vector we easily transform in a vector $\vec{N} = \left\{ \{p_i\}, ..., \{p_i\}, ... \right\}$ and apply to its components the function of calculation residue modulo 24. As a result we will get a vector $\vec{N}(\text{mod} 24) \equiv \left\{ \{a_i\}, ..., \{a_i\}, ..., \right\}$, giving classification of prime numbers, and we have for $N$

$N(\text{mod} 24) = \{[5], [13], [13], [13], [13], [13], [13], [13], [13], [1], [1], [1]\}$

I.e. this number is product of 12 prime circular numbers, from it one is $24n + 5$, four are $24n + 1$, seven are $24n + 13$. We may to control, that $(13)^7(1)^4(5)^1 = 5\cdot 13 = 17(\text{mod} 24)$.

For that composite number we will consider the task of search of subsets, having identical quadratic forms, and the task of determination all such quadratic forms.

For product of circular prime numbers it is equivalent to finding of all decisions of equation $x^2 + y^2 = N$, $N = 2^{198} + 1$. Such task can be decided by means of Mathematica program Ordered Sum of Squares Representations. However appeared (it was 2007), that for the decision of that task the computer works a few hours, and virtual storage is not enough for that. It was unexpected for the developer of program Stan Wagon, one of authors of guidance [3], and author of that article appealed to him.

Wagon reported through two weeks, that on the basis of the new improvements of algorithm of «HalfGCD» [4] Daniel Lichtblau perfected program, and now it decides the task for 0, 3 secs. However to this time an author was worked out private program, on Wagon proposal afterwards named QRM (Quadratic Representations Meshkoff). It makes use only of formulae (2) and standard functions of Mathematica 1) Factor Integer and 2) Quadratic Representation. For that task QRM on the Wagon computer has time 0, 32 secs. The decision another way we can to get with Mathematica program Reduce, but the calculation time is about 5 secs, so it is not advantageous for big numbers.

Further comparisons for different numbers showed, that on the Wagon computer QRM some yields on speed. However on the private computer of author for QRM time of decision was 0,15-0,16 secs, and program of DL (sending from Wagon) did not work, as it was based on internal codes of firm Mathematica. In addition, QRM decided a task for the even values of $N$, and also for cases, when $N$ is product of prime numbers and part of them is not circular. These numbers are eliminated from product, and the task was decided for product of remaining circular prime numbers.

In like manner it can be built programs for other three quadratic presentations. Then for the examined task in the beginning we find $2^{11} = 2048$ different presentations of number $N = 2^{198} + 1$ in quadratic form $a^2 + b^2$. Further we eliminate from $N$ a number 5, and for the number of $N/5$ we get $2^{10} = 1024$ quadratic presentations of form $a^2 + 3b^2$. Except it, we have $2^3=8$ quadratic presentations
$a^2 \pm 2b^2$ of four prime numbers $24n + 1$. It is all possibilities composite number $N = 2^{198} + 1$ in relation to his divisors, having general quadratic presentations.

5. Conclusions

It would be much more difficult to decide similar tasks, having not the classification offered higher. That classification is natural and scientific, so it is at the same time the result and the important instrument of science research. If before primes as some objects seems to be grey or black and white ($4n + 1$ and $4n + 3$), now it is as we see the objects of eight colors.

The classification for composite numbers of two primes consists of these colors eight objects and 56 objects of two colors.

Composite numbers of three and more primes so are significantly complicate in sense of many colors objects, and there is one of explanations why Number Theory problems complication fast grow up for big numbers.

Author has hope, if offered classification find application in theoretical researching on Number Theory, as above showed instances confirm it, as well as applications for optimizing calculations and computer programs in this field.

This work is pioneer on that theme, so references are scarce. All well-known material on Number Theory, used in this work without references from MathWorld – A Wolfram Web Resource, especially its article: Eric W. Weisstein «Prime Number».

This work is first published on English of author’s manuscript 2007 year, now revised and corrected.

REFERENCES

[1] H.M. Edwards. Fermat’s Last Theorem. A genetic introduction to algebraic Number Theory. Springer Verlag, New York Heidelberg Berlin, 1977. (Russian edition: Moskow, 1980).

[2] T. Nagell. Diophantine Equations of the Second Degree. Ch. 6 in Introduction to Number Theory. Wiley, New York, 1951, 188-226.

[3] D. Bressoud, S. Wagon. Prime Imaginaries and Imaginary Primes. Ch. 9 in A Course in Computational Number Theory. Key College Publishing, San Francisco, 2000.

[4] D. Lichtblau. HalfGCD and Fast Rational Recovery. ISSAC’05, July 24–27, 2005, Beijing, China.