Bull. Math. Soc. Sci. Math. Roumanie
Tome 53(101) No. 3, 2010, 251–259

Principal quadratic real fields in connection with some additive problems

by
Mihai Epure and Alexandru Gica

Dedicated to the memory of Laurenţiu Panaitopol (1940-2008)
on the occasion of his 70th anniversary

Abstract

We first analyse the set of positive integers $n > 5$ for which $n - a^2$ is four times a prime number for any positive odd integer a such that $a^2 \leq n$ and for which $n - a^2$ is a prime number for any positive even integer a such that $a^2 \leq n$. There are only three numbers with these properties: $n = 21, 77, 437$. The second aim is to show that there are only five prime numbers $p > 13$ such that $p - a^2$ is four times a prime number for any odd positive integer $a > 1, a^2 \leq p$; namely $p = 17, 37, 101, 197, 677$. The third purpose is to show that there are only four positive integers $n \equiv 2 \pmod 8$ such that $n - a^2$ is the double of a prime number for any nonnegative even integer a such that $a^2 \leq n$; namely $n = 10, 26, 62, 362$. The tools for proving these results belong to algebraic number theory. The key is to point out some connections between these additive problems and the class numbers for some quadratic real fields.

Key Words: Class number, sum of squares and primes, principal quadratic real fields.
2010 Mathematics Subject Classification: Primary 11R29; Secondary 11P99.

1 Introduction

There are only nine principal quadratic imaginary fields $\mathbb{Q}(\sqrt{d})$, namely for

$$-d = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

The statement goes back to Gauss; but this problem was posed in the language of the quadratic forms. Heegner (see [11]) succeeded to solve this problem but there was a gap in his proof. Complete proofs were given by Stark (see [14]) and Baker (see [2]). The similar problem of finding the principal quadratic real fields is still an open problem. However, in the last years several progresses arose. A. Biró (see [3] and [4]) proved in 2003 two important results: Yokoi's conjecture which asserts that $h(m^2+4) = 1$ only for six values of $m = 1, 3, 5, 7, 13, 17$ (in the above result, $m^2 + 4$ has to be a squarefree positive integer) and Chowla's conjecture which says that $h(4m^2 + 1) = 1$ only for six values of $m = 1, 2, 3, 5, 7, 13$ (in the above result, $4m^2 + 1$ has to be a squarefree positive integer). In the above formulas $h(d)$ is the class number for the quadratic field $\mathbb{Q}(\sqrt{d})$ (d is a squarefree integer). In 2007, Byeon, Kim and Lee proved (see [5]) Mollin's conjecture which says that $h(m^2 - 4) > 1$ whenever $m > 21$ (in the above result, $m^2 - 4$ has to be a squarefree positive integer).

We will use these results to solve some additive problems.

In [9] the second author proved the following.

Theorem 1.1. *Let $p > 3$ be a prime number such that $p - a^2$ is four times a prime number for any positive odd integer a such that $a^2 \le p$. Then:*

i) $p = x^2 + 4$, where x is a prime number.

ii) $\left(\frac{p}{q}\right) = -1$, for any prime number q such that $2 < q < x$.

iii) $p - a^2$ is a prime number for any even nonnegative integer $a \neq 2$ such that $a^2 < p$.

iv) The ring $\mathbb{Z}[\frac{1+\sqrt{p}}{2}]$ is principal.

v) $h(-4p) = x + 1$ if $x \equiv 1 \pmod 4$ and $h(-4p) = x - 1$ if $x \equiv 3 \pmod 4$, where $h(-4p)$ is the class number of the quadratic imaginary field $\mathbb{Q}(i\sqrt{p})$.

vi) There are only six prime numbers with the property asserted in the statement of the theorem; namely $5, 13, 29, 53, 173, 293$.

Remark: We have to mention that we considered in this theorem (as the ancient scholars did) 1 as a prime number. From now on in this paper we will not consider 1 as a prime number.

The key point of the proof of Theorem 1.1 was a result of Biró (see [3]).

In [7] and [8] the second author studied the following.

Problem: Which are the positive integers n such that $n - a^2$ is a prime number for any positive even integer a such that $a^2 \le n$ and that $n - a^2$ is four times a prime number for any positive odd integer a such that $a^2 \le n$.

We proved the following.

Theorem 1.2. *Let $n > 5$ be a positive integer such that $n - a^2$ is a prime number for any positive even integer a such that $a^2 \le n$ and four times a prime number for any positive odd integer a such that $a^2 \le n$. Then:*

i) $n = p(p + 4)$, where p and $p + 4$ are prime numbers, and

ii) $\left(\frac{n}{q}\right) = -1$ for any prime number q such that $2 < q < p$.

iii) $h(-4n) = p + 1$, where $h(-4n)$ is the class number of the quadratic imaginary field $\mathbb{Q}(i\sqrt{n})$.

2 $21, 77, 437$.

We prove in this section that there are only three numbers with the properties stated in Theorem 1.2.

Theorem 2.1. *Let $n > 5$ be a positive integer such that $n - a^2$ is a prime number for any positive even integer a such that $a^2 \leq n$ and four times a prime number for any positive odd integer a such that $a^2 \leq n$. Then $n = 21, 77$ or 437.*

Proof: Let us first prove that the ring $R = \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ is principal (that is, the class number for the field $\mathbb{Q}(\sqrt{n})$ is one). It is sufficient (see [1], Corolary 4.3.7., page 224) to show that any maximal ideal I of R with $N(I) < \frac{\sqrt{n}}{2}$ is principal ($\frac{\sqrt{n}}{2}$ is Minkowski's constant for the field $\mathbb{Q}(\sqrt{n})$). Since $n \equiv 5 \pmod 8$, $2R$ is a maximal ideal (see [1], Theorem 3.4.19., page 160). Let $q > 2$ be a prime number which is smaller than the Minkowski's constant $\frac{\sqrt{n}}{2}$. Then

$$2 < q < \frac{\sqrt{n}}{2} = \frac{\sqrt{p^2 + 4p}}{2} < \frac{p+2}{2} < p.$$

Taking into account the inequalities $2 < q < p$ and the second statement of Theorem 1.2, we get

$$\left(\frac{n}{q}\right) = -1.$$

But this means that qR is a maximal ideal (see [1], Theorem 3.4.18., page 158). We proved that any maximal ideal I of R with $N(I) < \frac{\sqrt{n}}{2}$ is principal, hence $R = \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ is principal. Byeon, Kim and Lee (see [5]) proved Mollin's conjecture which says that $h(m^2 - 4) > 1$ whenever $m > 21$ (in the above result, $m^2 - 4$ has to be a squarefree positive integer). This implies in our case (since $R = \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ is principal and $n = (p+2)^2 - 4)$ that $p + 2 \leq 21$ and $p \leq 19$. It is now straightforward to check that only $n = 21, 77, 437$ are solutions for our problem ($221 = 13 \cdot 17$ is not a solution for our problem because $221 = 1 + 4 \cdot 5 \cdot 11$).

□

3 $17, 37, 101, 197, 677$.

Theorem 3.1. *Let $p > 13$ be a prime number such that $p - a^2$ is four times a prime number for any positive odd integer $a > 1$ such that $a^2 \leq p$. Then:*

i) $p = 4x^2 + 1$, where x is a prime number.

ii) $\left(\frac{p}{q}\right) = -1$, for any prime number q such that $2 < q < x$.

iii) The ring $\mathbb{Z}[\frac{1+\sqrt{p}}{2}]$ is principal.

iv) There are only five prime numbers with the property asserted in the statement of the theorem: $17, 37, 101, 197, 677$.

Remark: Theorem 1.1 and Theorem 3.1 look similar but they are different. Let us remember that in Theorem 1.1 we consider 1 as a prime number which is not the case in Theorem 3.1 where we consider that 1 is not a prime number. There is also another difference. In Theorem 1.1 a is a positive odd integer whereas in Theorem 3.1 a is an odd integer, $a \geq 3$.

Proof: Let p be a prime number with the properties asserted in the theorem. Since $p-9=4r$ where r is a prime number, we get $p \equiv 1 \pmod 4$. If $p \equiv 1 \pmod 8$, then $4r = p-9 \equiv 0 \pmod 8$, hence $r=2, p=17$. We may now suppose that $p \equiv 5 \pmod 8$. According to Fermat, we find a positive integer x and an odd positive integer b such that $p = 4x^2+b^2$. If $b \neq 1$ then we arrive to a contradiction since $4x^2 = p - b^2$ should be four times a prime number. Therefore $p = 4x^2+1$, where x is an odd integer with $x > 1$. Let us suppose that x is not a prime number. Then $x = qa$, where q is a prime number and a is an odd positive integer with $a > 1$. We have $1 < 2q-1 < 2q < x$ and $(2q-1)^2 < x^2 < p$. Therefore, according to the hypothesis, $p-(2q-1)^2$ has to be four times a prime number. But $p-(2q-1)^2 \equiv p-1 \equiv 0 \pmod q$ and the only possibility is that $p-(2q-1)^2 = 4q$ and we obtain the contradiction

$$p = (2q-1)^2 + 4q = 4q^2+1 < 4x^2+1 = p.$$

Therefore x should be a prime number and we proved the first statement of the theorem. As for the second statement, let us suppose that there exists a prime number q such that $2 < q < x$ and $\left(\frac{p}{q}\right) = 1$. Therefore there exists an odd positive integer $c < q$ such that $p \equiv c^2 \pmod q$. We have $c^2 < q^2 < x^2 < 4x^2+1 = p$ and we deduce that $p = c^2+4q$ if $c \neq 1$. But in this case we get a contradiction since

$$p = c^2+4q < q^2+4q < x^2+4x < 4x^2+1 = p.$$

The only possibility left is $c=1$ and q divides $p-1 = 4x^2$. Because $q > 2$ and x is a prime number we get $q = x$. This is a contradiction since $q < x$.

Let us now prove that the ring $R = \mathbb{Z}[\frac{1+\sqrt{p}}{2}]$ is principal (that is, the class number for the field $\mathbb{Q}(\sqrt{p})$ is one). It is sufficient (see [1], Corolary 4.3.7., page 224) to show that any maximal ideal I of R with $N(I) < \frac{\sqrt{p}}{2}$ is principal ($\frac{\sqrt{p}}{2}$ is Minkowski's constant for the field $\mathbb{Q}(\sqrt{p})$). Since $p \equiv 5 \pmod 8$, we get that $2R$ is a maximal ideal (see [1], Theorem 3.4.19., page 160). Let $q > 2$ be a prime number which is smaller than the Minkowski's constant $\frac{\sqrt{p}}{2}$. Then

$$2 < q < \frac{\sqrt{p}}{2} = \frac{\sqrt{4x^2+1}}{2} < \frac{2x+1}{2} < x+1.$$

If $2 < q < x$ we take into account the second statement of the theorem and we see that

$$\left(\frac{p}{q}\right) = -1.$$

But this means that qR is a maximal ideal (see [1], Theorem 3.4.18., page 158). Next we analyse the case $q = x$. Since $\left(\frac{p}{q}\right) = 1$, we get that $qR = Q_1Q_2$, where Q_1, Q_2 are different maximal ideals with $N(Q_1) = N(Q_2) = q$ (see again [1], Theorem 3.4.18., page 158). The polynomial $f(z) = z^2 - z + \frac{1-p}{4}$ modulo q is $z^2 - z = z(z-1)$ and therefore

$$Q_1 = qR + \frac{1+\sqrt{p}}{2}R = \frac{2q+1+\sqrt{p}}{2}R.$$

The last equality follows since $\frac{2q+1+\sqrt{p}}{2} \in Q_1$ and $N(\frac{2q+1+\sqrt{p}}{2}) = N(Q_1) = q$. Therefore Q_1 and Q_2 are principal ideals.

We proved that any maximal ideal I of R with $N(I) < \frac{\sqrt{p}}{2}$ is principal, hence $R = \mathbb{Z}[\frac{1+\sqrt{p}}{2}]$ is principal. But Biró proved (see [4]) Chowla's conjecture which says that $h(4m^2+1) = 1$ only for six values of $m = 1, 2, 3, 5, 7, 13$ (in the above result, $4m^2+1$ has to be a squarefree positive integer). This implies in our case (since $R = \mathbb{Z}[\frac{1+\sqrt{p}}{2}]$ is principal and $p = 4x^2+1$) that $x = 2, 3, 5, 7, 13$. Therefore $p = 17, 37, 101, 197, 677$ are the only solutions for our problem. The solution $x = 1, p = 5$ does not fit the statement of the theorem.

□

Remark: We will now use the Gauss's formula (see the fifth section of the celebrated book *Disquisitiones Arithmeticae*):

$$r_3(p) = 12h(-4p),$$

where by $h(-4p)$ we denote the cardinal of the ideal class group for the field $\mathbb{Q}(i\sqrt{p})$ and by $r_3(p)$ the number of ordered sets (x, y, z) such that x, y, z are integers satisfying the equality $p = x^2 + y^2 + z^2$. In the above formula $p \equiv 1 \pmod 4$. If p has the properties stated in the theorem we can show (using the above formula) that $h(-4p) = 2x + 4$ when x is a prime number such that $x \equiv 1 \pmod 4$ and that $h(-4p) = 2x - 4$ when x is a prime number such that $x \equiv 3 \pmod 4$. Of course, Biró's result implies this statement but we want to notice that the Gauss's formula can also solve the problem of computing the above class numbers.

4 $10, 26, 122, 362$.

Theorem 4.1. *Let $n \equiv 2 \pmod 8$ be a positive integer such that $n - a^2$ is the double of a prime number for any even nonnegative integer a such that $a^2 \leq n$. Then:*

i) $n = x^2 + 1$, where x is a prime number.

ii) $\left(\frac{n}{q}\right) = -1$, for any prime number q such that $2 < q < x$.

iii) The ring $\mathbb{Z}[\sqrt{n}]$ has class number two.

iv) There are only four numbers with the property asserted in the statement of the theorem: $n = 10, 26, 122, 362$.

Proof: Let n be a number with the properties asserted in the theorem. Since $n - 0 = 2r$ where r is a prime number and $n \equiv 2 \pmod 8$, we get $r \equiv 1 \pmod 4$. According to Fermat there exist positive odd integers x, y such that $n = x^2 + y^2$. If $x \neq 1$ and $y \neq 1$, let p be an odd prime such that p divides y. Obviously, $p \leq y = \sqrt{n - x^2} \leq \sqrt{n - 9}$. We have $n \equiv x^2 \pmod p$ and therefore we can find an even nonnegative integer a such that $n \equiv a^2 \pmod p$ and $a < p < \sqrt{n}$. According to the properties of n, we have $n = a^2 + 2p$. But we obtained a contradiction since

$$n = a^2 + 2p \leq (p-1)^2 + 2p = p^2 + 1 \leq n - 8.$$

Therefore x or y should be equal to one. Let us suppose that $y = 1$.

Let us suppose that x is not a prime number. Then $x = pa$, where p is a prime number and a is an odd positive integer, $a > 1$. Obviously, $3p < \sqrt{n}$. We have $n \equiv 1 \pmod p$ and therefore we can find an even nonnegative integer a such that $n \equiv a^2 \pmod p$ and $a < p < \sqrt{n}$. According to the properties of n, we have $n = a^2 + 2p$. But we obtained a contradiction since

$$n = a^2 + 2p \leq (p-1)^2 + 2p = p^2 + 1 < \frac{n}{9} + 1 < n.$$

Therefore x should be a prime number and we proved the first statement of the theorem. As for the second statement, let us suppose that there exists a prime number q such that $2 < q < x$ and $\left(\frac{n}{q}\right) = 1$. Therefore there exists an even positive integer $c < q$ such that $n \equiv c^2 \pmod q$. We have $c^2 < q^2 < x^2 < x^2 + 1 = n$ and we deduce that $n = c^2 + 2q$. But in this case we also get a contradiction since

$$n = c^2 + 2q \leq (q-1)^2 + 2q = q^2 + 1 < x^2 + 1 = n.$$

Let us now prove that the ring $R = \mathbb{Z}[\sqrt{n}]$ has class number two (that is, the class number for the field $\mathbb{Q}(\sqrt{n})$ is two). It is sufficient (see [1], Corolary 4.3.7., page 224) to analyse any maximal ideal I of R with $N(I) < \sqrt{n}$ ($\sqrt{n}$ is Minkowski's constant for the field $\mathbb{Q}(\sqrt{n})$). Since $n \equiv 2 \pmod 4$ we get that $2R = Q^2$, where Q is a maximal ideal with $N(Q) = 2$. Let $q > 2$ be a prime number which is smaller than Minkowski's constant $\sqrt{n}$. If $2 < q < x$, taking into account the second statement of the theorem, we see that

$$\left(\frac{n}{q}\right) = -1.$$

But this means that qR is a maximal ideal (see [1], Theorem 3.4.18., page 158). Now we have to analyse the case $q = x$. Since $\left(\frac{n}{q}\right) = 1$, we have $qR = Q_1 Q_2$, where Q_1, Q_2 are different maximal ideals with $N(Q_1) = N(Q_2) = q$. The polynomial $f(z) = z^2 - (x^2+1)$ modulo q is $z^2 - 1 = (z+1)(z-1)$ and therefore

$$Q_1 = qR + (1 + \sqrt{1+q^2})R.$$

We have $QQ_1 = (q + 1 + \sqrt{1+q^2})R$. The last equality follows since $(q + 1 + \sqrt{1+q^2}) \in Q_1$ and $N(q + 1 + \sqrt{1+q^2}) = 2q$. To show that the ring $\mathbb{Z}[\sqrt{n}]$ has class number two it is enough to prove that Q is not a principal ideal. Let us suppose that Q is a principal ideal. Then $Q = (a + b\sqrt{x^2+1})R$, where a, b are integers such that

$$a^2 - nb^2 = \pm 2.$$

The last equality holds since $N(Q) = 2$. We know that $n = 2r$, where r is a prime number such that $r \equiv 1 \pmod 4$. Let us suppose that $r \equiv 1 \pmod 8$. We have $n = A^2 + 2B^2$, where A, B are integers (see [10], Theorem 1, page 127). Since n is even, we get that A is even and therefore $n - A^2 = 2B^2$ is the double of a prime number which is obviously not true. Hence $r \equiv 5 \pmod 8$. But we have seen above that

$$a^2 - nb^2 = \pm 2.$$

Because $n = 2r$, we have $a^2 \equiv \pm 2 \pmod r$. But this is not true since $r \equiv 5 \pmod 8$ and in this case $\left(\frac{\pm 2}{r}\right) = -1$. Therefore Q is not a principal ideal and we get that the ring $\mathbb{Z}[\sqrt{n}]$ has class number two.

Byeon and Lee proved (see [6]) that $h(x^2+1) = 2$ only for four values of $x = 3, 5, 11, 19$ (in the above result, x is an odd positive integer and x^2+1 has to be a squarefree positive integer). Previously this was proved by R. A. Mollin and H. C. Williams under the assumption of the generalized Riemann hypothesis (see [13]). This implies in our case (since $R = \mathbb{Z}[\sqrt{n}]$ has class number two and $n = x^2+1$) that $x = 3, 5, 11, 19$. Therefore $n = 10, 26, 122, 362$ are the only solutions for our problem.

□

Remark 1: We will use now the Gauss's formula (see the fifth section of the celebrated book *Disquisitiones Arithmeticae*)

$$r_3(n) = 12h(-4n),$$

where by $h(-4n)$ we denote the cardinal of the ideal class group for the field $\mathbb{Q}(i\sqrt{n})$ and by $r_3(n)$ the number of ordered sets (x, y, z) such that x, y, z are integers satisfying the equality $n = x^2 + y^2 + z^2$; in the above formula $n \equiv 2 \pmod 8$. If n has the properties stated in the theorem we can show (using the above formula) that $h(-4n) = x + 1$ when x is a prime number such that $x \equiv 1 \pmod 4$ and that $h(-4n) = x - 1$ when x is a prime number such that $x \equiv 3 \pmod 4$. Of course, Byeon's and Lee's result implies this statement but we want to notice that the Gauss's formula can also solve the problem of computing the above class numbers.

Remark 2: We can also consider the problem of finding the positive integers $n \equiv 6 \pmod 8$ such that $n - a^2$ is the double of a prime number for any even nonnegative integer a such that $a^2 \leq n$. Following the same path as above we can prove that $n = (4y)^2 - 2$, the ring $\mathbb{Z}[\sqrt{n}]$ is principal and $h(-4n) = 4y$, where $h(-4n)$ is the cardinal of the ideal class group for the field $\mathbb{Q}(i\sqrt{n})$. A result of Mollin and Williams (see [12]) ensures us that $n = 14, 62, 398$ with one possible exception, but the existence of this possible exception has not been settled yet. This remark and the above theorem is connected with the problem of finding all the positive integers N such that $N - 2n^2$ is a prime for any nonnegative integers n such that $2n^2 \leq N$. Examples of such numbers are:

$$5, 7, 13, 31, 61, 181, 199.$$

From what we saw above it follows that besides these numbers it could only exist one more number N with the afore-mentioned property.

Acknowledgment: The first author wrote this paper as a part of the CNCSIS grant ID-PCE code 304, No. 51/2007.

References

[1] T. Albu, I. D. Ion, *Capitole de teoria algebrică a numerelor.* Ed. Academiei, Bucureşti, 1984.

[2] A. Baker, *Linear forms in the logarithms of algebraic numbers.* Mathematika, **13**(1966), 204–216.

[3] A. Biró, *Yokoi's conjecture.* Acta Arith., **106**(2003), 85–104.

[4] A. Biró, *Chowla's conjecture.* Acta Arith., **107**(2003), 179–194.

[5] D. Byeon, M. Kim, J. Lee, *Mollin's conjecture.* Acta Arith., **126**(2007), 99–114.

[6] D. Byeon, J. Lee, *Class number 2 problem for certain real quadratic fields of Richaud-Degert type.* J. Number Theory, **128**(2008), 865–883.

[7] A. Gica, *An additive problem.* An. Univ. Bucureşti Mat., **53**(2004), 229–234.

[8] A. Gica, *Some class numbers.* Math. Reports, **7** (**57**), *2* (2005), 113–117.

[9] A. Gica, *Some strange primes.* Bull. Math. Soc. Sci. Math. Roumanie, **51** (**99**), No. 3 (2008), 213–217.

[10] A. Gica, L. Panaitopol, *O introducere în aritmetică şi teoria numerelor.* Ed. Univ. Bucureşti, 2001.

[11] K. Heegner, *Diophantische Analysis und Modulfunktionen.* Math. Z., **56**(1952), 227–253.

[12] R. A. Mollin, H. C. Williams, *Period four and real quadratic fields of class number one.* Proc. Japan Acad. Ser. A Math. Sci., **65**(1989), 89–93.

[13] R. A. Mollin, H. C. Williams, *On a solution of a class number two problem for a family of real quadratic fields.* in *Computational Number Theory*, de Gruyter, Berlin/New York, 1991, 95–101.

[14] H. M. Stark, *A complete determination of the complex quadratic fields of class number one.* Michigan Math. J., **14**(1967), 1–27.

Received:4.07.2009
Revised 20.03 2010.

Institute of Mathematics of the Romanian Academy
Str. Griviţei 21
RO-014700 Bucharest, Romania,
E-mail: `epuremihai@yahoo.com`

University of Bucharest
Faculty of Mathematics
Str. Academiei 14
RO-010014 Bucharest 1, Romania
E-mail: `alexgica@yahoo.com`