Bull. Math. Soc. Sci. Math. Roumanie
Tome 51(99) No. 3, 2008, 213–217

Some strange primes*

by
Alexandru Gica

Abstract

The aim of this paper is to analyze the set of prime numbers $p > 3$ for which $p - a^2$ is four times a prime for any positive odd integer a such that $a^2 < p$ (we consider that 1 is a prime number). We show that for such prime numbers p we have $p = x^2 + 4$, where x is a prime number. We compute also the class number $h(-4p)$ for the quadratic imaginary field $\mathbb{Q}(i\sqrt{p})$ using a famous formula of Gauss. There are only six prime numbers with the above property.

Key Words: Class number, sum of squares and primes.
2000 Mathematics Subject Classification: Primary 11R29, Secondary 11P99.

1 Introduction

Finding all the positive integers N such that $N - 2n^2$ is a prime for any nonnegative integers n such that $2n^2 \leq N$ is an open problem. Examples of such N's are the numbers

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

There is not known until now if there is an $N > 199$ with the above property (see [6], page 35, exercise 4). In [3] and [4] we studied the following.

Problem: Which are the positive integers n such that $n - a^2$ is a prime for any positive even integer a such that $a^2 \leq n$ and that $n - a^2$ is four times a prime for any positive odd integer a such that $a^2 \leq n$. Here and throughout this paper we consider (as the ancient scholars did) that 1 is a prime number.

We proved the following results.

Theorem 1.1. *Let n a positive integer such that $n - a^2$ is a prime for any positive even integer a such that $a^2 \leq n$ and that $n - a^2$ is four times a prime for any positive odd integer a such that $a^2 \leq n$. Then*

[*] This paper was realised inside the programme of the grant 2-CEx06-11-20/25.07.2006.

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

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

The main goal of this paper is to study the following.

Problem: Which are the primes $p > 3$ such that $p - a^2$ is four times a prime for any positive odd integer a such that $a^2 \leq p$. If we compare the two problems, we observe that in the second one we impose the stronger condition that p is a prime number and we ignore what happens with $p - a^2$ for even integers a. We will prove the following.

Theorem 1.2. *Let* $p > 3$ *a prime number such that* $p - a^2$ *is four times a prime for any positive odd integer* a *such that* $a^2 \leq p$. *Then*

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

ii) $\left(\frac{p}{q}\right) = -1$, *for any prime* 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: $5, 13, 29, 53, 173, 293$.

2 $p = x^2 + 4$ and x is prime.

We prove in this section the first three statements of the theorem.

Proof: Let us first prove that $p = 8k + 5$, where k is a nonnegative integer. If we apply the hypothesis for $a = 1$, we infer that $p = 4q + 1$, where q is a prime number. If q is even, then $q = 2$ and $p = 9$; this is impossible since p is prime. Then $q = 2k + 1$ and $p = 8k + 5$. We will show now that $p = x^2 + 4$, where x is an odd positive integer. Since p is a prime number, $p \equiv 1 \pmod 4$, we have $p = x^2 + y^2$, where x and y are nonnegative integers and x is odd. By hypothesis, we know that $y^2 = p - x^2$ is four times a prime. The only possibility is $y^2 = 4$ (we recall that we consider 1 as a prime number). Therefore, $p = x^2 + 4$, where x is an odd positive integer. We will show later that x is prime.

For proving the second statement of the theorem let us suppose that there exists a prime number q such that $2 < q < x$ and $\left(\frac{p}{q}\right) = 1$. We deduce the existence of an odd positive integer a such that $p \equiv a^2 \pmod q$ and $1 \leq a \leq q-2$. We have $a^2 < q^2 < x^2 < x^2 + 4 = p$ and q divides $p - a^2$. By these and the hypothesis we obtain the equality $p = a^2 + 4q$ which leads to a contradiction since

$$p = a^2 + 4q \leq (x-2)^2 + 4q < (x-2)^2 + 4x = x^2 + 4 = p.$$

We have now the tools for proving that x is a prime number. If not, then there is a prime $q < x$ which is a divisor of x (obviously, $q \neq 2$ since x is odd). But in this case $2 < q < x$, $p = x^2 + 4 \equiv 4 \pmod q$ and

$$\left(\frac{p}{q}\right) = \left(\frac{4}{q}\right) = 1,$$

which contradicts the second statement of the theorem proved above. In this moment, the first statement of the theorem is completely proved.

The third statement of the theorem is obvious for $a = 0$. Let us suppose that the statement is not true and there exist an even integer, $4 \leq a < \sqrt{p}$ such that the number $A = p - a^2$ is not prime. Since A is odd and not prime, there exists a prime $q \neq 2$ divisor of A such that $q \leq \sqrt{A}$. But

$$q \leq \sqrt{A} = \sqrt{p - a^2} < \sqrt{p - 4} = x$$

and the second statement of the theorem ensure us that $\left(\frac{p}{q}\right) = -1$. But this is not true since $p \equiv a^2 \pmod q$ and, therefore, $\left(\frac{p}{q}\right) = \left(\frac{a^2}{q}\right) = 1$.

□

3 Class numbers.

In this section we wil prove the statements iv) and v) of Theorem 1.2.

Proof: Let us first 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 the result is obvious for $p = 5$, we can suppose that $p > 5$, which implies that $x \geq 2$. Since $p \equiv 5 \pmod 8$ (see the previous section), then $2R$ is a maximal ideal (see [1], Theorem 3.4.19., page 160). Let $q > 2$ a prime number which is smaller than Minkowski's constant $\frac{\sqrt{p}}{2}$. Then (since $x \geq 2$)

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

Taking into account the inequalities $2 < q < x$ and the second statement of the theorem, 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). We proved that any maximal ideal I of R with $N(I) < \frac{\sqrt{p}}{2}$ is principal and this means that $R = \mathbb{Z}[\frac{1+\sqrt{p}}{2}]$ is principal.

For the last statement of the theorem we need a formula which goes back to Gauss (in the fifth section of the celebrated book *Disquisitiones Arithmeticae*). The formula says that for a squarefree integer $n > 4, n \equiv 1, 2, 5, 6 \pmod 8$ we have

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

where we denote by $h(-4n)$ the cardinal of the ideal class group for the field $\mathbb{Q}(i\sqrt{n})$ and by $r_3(n)$ the number of triplets (x, y, z) such that x, y, z are integers satisfying the equality $n = x^2 + y^2 + z^2$. There are two others equalities of the same type: $r_3(n) = 0$ if $n \equiv 7 \pmod 8$ and $r_3(n) = 24h(-n)$ if $n \equiv 3 \pmod 8$ (as above, $n > 4$ is a squarefree integer and by $h(-n)$ we denote the cardinal of the ideal class group for the field $\mathbb{Q}(i\sqrt{n})$). We need only the first formula.
We have to count the number of triplets (t, y, z) such that t, y, z are nonnegative integers with $p = t^2 + y^2 + z^2$, $t < y$, t and y are even and z is odd. For finding this number we take into account the third statement of the theorem: if $a \neq 2$ is a nonnegative even integer such that $a^2 < p$, then $p - a^2$ is a prime number (and obviously $p - a^2 \equiv 1 \pmod 4$). Therefore, in this case, we have only one writing $p - a^2 = b^2 + c^2$, where b, c are nonnegative integers, b being even and c being odd (see [5], Theorem 5.2.6., page 122 for this result). If $a = 2$, then $p - 4 = x^2$ and since x is prime we have two writings $p - 4 = b^2 + c^2$ (b, c are nonnegative integers, b being even and c being odd) if $x \equiv 1 \pmod 4$ and only one such writing if $x \equiv 3 \pmod 4$ (see again [5], the formula which ends Theorem 5.2.6., page 122). Therefore we have to split the proof in two cases.

The case $x \equiv 1 \pmod 4$**:** Taking into account the above facts we infer that there are $\frac{x+3}{4}$ triplets (t, y, z) such that t, y, z are nonnegative integers with $p = t^2 + y^2 + z^2$, $t < y$, t and y being even and z being odd. If we change the order and the sign of t, y, z we obtain 48 triplets if $t \neq 0$ and 24 triplets if $t = 0$. Puting together all these informations we obtain that

$$12h(-4p) = r_3(p) = 48 \cdot \frac{x-1}{4} + 24 = 12x + 12, h(-4p) = x + 1.$$

The case $x \equiv 3 \pmod 4$**:** Taking into account the above facts we infer that there are $\frac{x+1}{4}$ triplets (t, y, z) such that t, y, z are nonnegative integers with $p = t^2 + y^2 + z^2$, $t < y$, t and y being even and z being odd. If we change the order and the sign of t, y, z we obtain 48 triplets if $t \neq 0$ and 24 triplets if $t = 0$. Puting together all these informations we obtain that

$$12h(-4p) = r_3(p) = 48 \cdot \frac{x-3}{4} + 24 = 12x - 12, h(-4p) = x - 1.$$

□

4 5,13,29,53,173,293.

It is easy to check that if $p \leq 10.000$ has the property that $p - a^2$ is four times a prime for any positive odd integer a such that $a^2 \leq p$, then $p =$

$5, 13, 29, 53, 173, 293$. In fact, there are no other prime numbers with the above property. This is a consequence of Yokoi's conjecture proved by A. Biro (see [2]).

Theorem 4.1. *Let $n = m^2 + 4$, where m is an odd positive integer. The ring $\mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ is principal only for six values of m: $m = 1, 3, 5, 7, 13, 17$.*

Now it is easy to prove the last statement of Theorem 1.2.

Proof: We proved above (point i) of Therem 1.2) that $p = x^2 + 4$, where x is an odd prime and that the ring $\mathbb{Z}[\frac{1+\sqrt{p}}{2}]$ is principal (point iv) of Theorem 1.2). The above quoted result of A. Biro ends now the proof of the last statement of Theorem 1.2.

□

References

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

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

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

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

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

[6] M. B. Nathanson, *Elementary Methods in Number Theory*, Springer-Verlag, 2000.

Received: 22.05.2008.

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