



ON SOME DIOPHANTINE EQUATIONS (I)

Diana Savin

Abstract

In this paper we study the equation $m^4 - n^4 = py^2$, where p is a prime natural number, $p \geq 3$. Using the above result, we study the equations $x^4 + 6px^2y^2 + p^2y^4 = z^2$ and the equations $c_k(x^4 + 6px^2y^2 + p^2y^4) + 4pd_k(x^3y + px^2y^3) = z^2$, where the prime number $p \in \{3, 7, 11, 19\}$ and (c_k, d_k) is a solution of the Pell equation, either of the form $c^2 - pd^2 = 1$ or of the form $c^2 - pd^2 = -1$.

I. Preliminaries.

We recall some necessary results.

Proposition 1.1. ([3], p.74) *The integer solutions of the Diophantine equation*

$$x_1^2 + x_2^2 + \dots + x_k^2 = x_{k+1}^2$$

are the following ones

$$\left\{ \begin{array}{l} x_1 = \pm(m_1^2 + m_2^2 + \dots + m_{k-1}^2 - m_k^2) \\ x_2 = 2m_1m_k \\ \dots\dots\dots \\ \dots\dots\dots \\ x_k = 2m_{k-1}m_k \\ x_{k+1} = \pm(m_1^2 + m_2^2 + \dots + m_{k-1}^2 + m_k^2), \end{array} \right.$$

with m_1, \dots, m_k integer numbers.

From the geometrical point of view, the solutions $(x_1, x_2, \dots, x_k, x_{k+1})$ are the sizes x_1, x_2, \dots, x_k of a right hyper-parallelipiped in the space \mathbf{R}^k and x_{k+1} is the length of its diagonal.

Proposition 1.2. ([1], p.150) *The quadratic field $Q(\sqrt{d})$, where $d \in \mathbf{N}^*$, d is square free, has an Euclidean ring of integers A (with respect to the norm N), for $d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$.*

Proposition 1.3. ([1], p.141) *Let $K = \mathbf{Q}(\sqrt{d})$ be a quadratic field with A as its ring of integers and $a \in A$. Then $a \in \mathbf{U}(A)$ if and only if $N(a) = 1$.*

Proposition 1.4. (Lagrange, [2], p.168) *Let $D \geq 2$ be a rational square-free integer and k be the number of incomplete denominators which make up the period of the regular continued fraction of the number $\alpha = \sqrt{D}$. Then (x_n, y_n) , with $x_n = A_{nk-1}$, $y_n = B_{nk-1}$, where $n \in \mathbf{N}^*$ when k is an even number, and $n \in 2\mathbf{N}^*$ when k is an odd number, verifies the equation $x^2 - Dy^2 = 1$ and gives all the positive solutions of the Pell equation. Particularly, the fundamental solution is (A_{k-1}, B_{k-1}) for k an even number, and (A_{2k-1}, B_{2k-1}) for k an odd number.*

By using Proposition 1.4., we obtain all the elements of $U(\mathbf{Z}[\sqrt{p}])$. These are $\pm\mu_k$, $k \in \mathbf{Z}$, where $\mu_k = c_k + d_k\sqrt{p} = (c_0 + d_0\sqrt{p})^{k+1}$, $k \in \mathbf{Z}$, (c_0, d_0) being the fundamental solution of the Pell equation $x^2 - py^2 = 1$.

Proposition 1.5. ([5], p.134) *Let p and k be two rational integers, $p \geq 0$, $p \neq h^2$, $\forall h \in \mathbf{N}^*$ and let be given the equation $x^2 - py^2 = k$.*

(i) *If $(x_0, y_0) \in \mathbf{N}^* \times \mathbf{N}^*$ is the minimal solution of the equation $x^2 - py^2 = 1$, $\varepsilon = x_0 + y_0\sqrt{p}$ and (x_i, y_i) , $i = \overline{1, r}$, are different solutions of the equation $x^2 - py^2 = k$, with $|x_i| \leq \sqrt{|k|\varepsilon}$, $|y_i| \leq \sqrt{\frac{|k|\varepsilon}{p}}$, then there exists an infinity of solutions of the given equation and these solutions have the form: $\mu = \pm\mu_i \varepsilon^n$ or $\mu = \pm\overline{\mu}_i \varepsilon^n$, $n \in \mathbf{Z}$, where $\mu_i = x_i + y_i\sqrt{p}$, $i = \overline{1, r}$.*

(ii) *If the given equation does not have solutions satisfying the above conditions, then it does not have any solutions.*

Proposition 1.6. ([7], p.123-127). *Consider the system*

$$\begin{cases} x^2 + ky^2 = z^2 \\ x^2 - ky^2 = t^2, \end{cases}$$

where $k \in \mathbf{N}$, $k \geq 2$, k is square free. *If the system has one solution $x, y, z, t \in \mathbf{Z}^*$, then (X, Y, Z, T) , where $X = x^4 + k^2y^4$, $Y = 2xyzt$, $Z = x^4 + 2kx^2y^2 - k^2y^4$, $T = x^4 - 2kx^2y^2 - k^2y^4$ is also a solution of the system. Therefore if the system has one integer solution, it has an infinity of integer solutions.*

Proposition 1.7. ([7], p.128) *The system*

$$\begin{cases} x^2 + 3y^2 = z^2 \\ x^2 - 3y^2 = t^2 \end{cases}$$

does not have nontrivial integer solutions.

Proposition 1.8. ([3], p. 115) *For $p \in \{3, 7, 11, 19\}$, the equation $c^2 - pd^2 = -1$ does not have integer solutions.*

2. Diophantine equation $m^4 - n^4 = 3y^2$

We shall take a particular p , namely we shall consider p a prime natural number, $p \geq 3$.

The main result of this section, which will be applied in the paper, is given in the following theorem:

Theorem 2.1. *The equation $m^4 - n^4 = 3y^2$ does not have nontrivial integer solutions.*

Proof. Assume that $(m,n)=1$. Otherwise, if $(m,n)=d \neq 1$, then $d^4/3y^2$ and, after simplifying with d^4 , we obtain an equation of the same type, satisfying the condition $(m, n) = 1$.

There are two cases:

[Case 1.] If m is odd and n is even or conversely, then $3y^2$ is odd, and, we get that y is odd.

We transform the equation $m^4 - n^4 = 3y^2$ and we get $n^4 + 3y^2 = m^4$, more explicitly, we have $(n^2)^2 + y^2 + y^2 = (m^2)^2$, and by applying the Proposition 1.1., we obtain: $n^2 = |3a^2 - b^2|$, $y = 2ab$, $m^2 = 3a^2 + b^2$, $a, b \in \mathbf{Z}$ and y is an even number, in contradiction with the hypothesis on y . Therefore, the equation $m^4 - n^4 = 3y^2$ does not have nontrivial integer solutions.

[Case 2.] If m and n are odd numbers, then, by using the same reasoning as in the Case 1, we obtain $n^2 = |3a^2 - b^2|$, $y = 2ab$, $m^2 = 3a^2 + b^2$, $a, b \in \mathbf{Z}$.

If $3a^2 \geq b^2$, we obtain $n^2 = 3a^2 - b^2$, $y = 2ab$, $m^2 = 3a^2 + b^2$, $a, b \in \mathbf{Z}$. Moreover if a and b are one even and another odd, then the equation could have solutions.

If a is an odd number and b is an even number, the equation $m^2 = 3a^2 + b^2$ has, according to Proposition 1.1., only the solutions: $b = 3r^2 - s^2$, $a = 2rs$, $m = 3r^2 + s^2$, $r, s \in \mathbf{Z}$.

Then a is an even number, which is a contradiction.

If a is an even number and b is an odd number, from $n^2 = 3a^2 - b^2$, $m^2 = 3a^2 + b^2$, it results $m^2 - n^2 = 2b^2$ and y is an even number, which is not the case.

Therefore, the equation $m^4 - n^4 = 3y^2$ does not have nontrivial integer solutions.

If $3a^2 \leq b^2$, we obtain $n^2 = b^2 - 3a^2$, $y = 2ab$, $m^2 = 3a^2 + b^2$, $a, b \in \mathbf{Z}$.

The Proposition 1.7. implies that the system

$$\begin{cases} n^2 = b^2 - 3a^2 \\ m^2 = b^2 + 3a^2 \end{cases}$$

does not have nontrivial integer solutions and then the equation $m^4 - n^4 = 3y^2$ does not have also nontrivial integer solutions m, n, y .

As straightforward applications of the Theorem 2.1., we obtain the next two propositions.

Proposition 2.2. *The equations $x^4 + 18x^2 y^2 + 9y^4 = z^2$ and $|x^4 - 18x^2 y^2 + 9y^4| = z^2$ do not have also nontrivial integer solutions.*

Proof. From the Theorem 2.1., the equation $m^4 - n^4 = 3y^2$ does not have nontrivial integer solutions m, n, y . We transform this equation using the same method as in the previous proof.

The equation $m^4 - n^4 = 3y^2$ is equivalent to $n^2 = |3a^2 - b^2|$, $y = 2ab$, $m^2 = 3a^2 + b^2$, $a, b \in \mathbf{Z}$.

If $3a^2 \not\equiv b^2$, we obtain $n^2 = b^2 - 3a^2$, which is equivalent to $n^2 + 3a^2 = b^2$, and, by Proposition 1.1., we get $n = \pm(3u^2 - v^2)$, $a = 2uv$, $b = \pm(3u^2 + v^2)$, $u, v \in \mathbf{Z}$. Therefore $n^4 = (3u^2 - v^2)^4$, and $y = \pm 4uv(3u^2 + v^2)$, hence $3y^2 = 48u^2v^2(3u^2 + v^2)^2$, and $n^4 + 3y^2 = (3u^2 - v^2)^4 + 48u^2v^2(3u^2 + v^2)^2$, which is equivalent to $n^4 + 3y^2 = (v^4 + 3^2u^4 + 18u^2v^2)^2$.

Then the equation $m^4 = (v^4 + 3^2u^4 + 18u^2v^2)^2$ does not have nontrivial integer solutions, hence the equation $m^2 = v^4 + 9u^4 + 18u^2v^2$ does not have nontrivial integer solutions.

We just proved that the equation $x^4 + 18x^2 y^2 + 9y^4 = z^2$ does not have nontrivial integer solutions.

If $3a^2 \equiv b^2$, we obtain $n^2 = b^2 - 3a^2$, $y = 2ab$, $m^2 = 3a^2 + b^2$, $a, b \in \mathbf{Z}$. $m^2 = 3a^2 + b^2$. Using the Proposition 1.1., we get $b = \pm(3r^2 - s^2)$, $a = 2rs$, $m = \pm(3r^2 + s^2)$, $r, s \in \mathbf{Z}$. Then $m^4 = (3r^2 + s^2)^4$, $3y^2 = 48r^2s^2(3r^2 - s^2)^2$ and $m^4 - 3y^2 = (3r^2 + s^2)^4 + 48r^2s^2(3r^2 - s^2)^2$. Finally, we get that the equation $n^4 = (s^4 + 3^2r^4 - 18r^2s^2)^2$ does not have nontrivial integer solutions, therefore the equation $z^2 = |x^4 + 9y^4 - 18x^2y^2|$ does not have nontrivial integer solutions.

The proof is ready.

Proposition 2.3. *The equation $c(x^4 + 18x^2 y^2 + 9y^4) + 12d(x^3y + 3xy^3) = z^2$, where (c, d) is a solution of the Pell equation $u^2 - 3v^2 = 1$, does not have nontrivial integer solutions.*

Proof. We know (by Proposition 1.2.) that the ring of algebraic integers A of the quadratic fields $\mathbf{Q}(\sqrt{3})$ is Euclidean with respect to the norm N and $A = \mathbf{Z}[\sqrt{3}]$. Consider the equation $m^4 - n^4 = 3y^2$ under the form $m^4 - 3y^2 = n^4$ in the ring $\mathbf{Z}[\sqrt{3}]$, knowing all the time that it has not nontrivial integer solutions.

Then $n^4 = (m^2 - y\sqrt{3})(m^2 + y\sqrt{3})$ and we try to see if have a proper common divisor $\alpha = c + d\sqrt{3} \in \mathbf{Z}[\sqrt{3}]$ of the elements $m^2 - y\sqrt{3}$ and $m^2 + y\sqrt{3}$.

Such a divisor α will divide also $2m^2$ and $2y\sqrt{3}$, which implies that its norm $N(\alpha) = |c^2 - 3d^2|$ divides $4m^4$ and $12y^2$. As $(m, y) = 1$, it follows that $N(\alpha)$ divides 4, hence $N(\alpha) \in \{1, 2, 4\}$.

$N(\alpha) = 1$ implies $\alpha \in U(A)$ and it is not a proper divisor.

If $N(\alpha) = 2$, then $c^2 - 3d^2 = \pm 2$. The equation $c^2 - 3d^2 = 2$ does not have integer solutions, as we see by using the "game of even and odd".

The equation $c^2 - 3d^2 = -2$ could have integer solutions if c and d are odd numbers. We want to apply the Proposition 1.5. and we need the fundamental solution of the equation $c^2 - 3d^2 = 1$, obtained by using the continued fraction method (by developing $\sqrt{3}$ in the continued fraction). We have $\sqrt{3} = [1, \overline{1, 2}]$, hence $a_0 = a_1 = 1$, $a_2 = 2$, $A_1 = 2$ and $B_1 = 1$, therefore we get $\varepsilon = 2 + \sqrt{3}$ associated to the fundamental solution $(2, 1)$ with positive components. Then $|c| \leq \sqrt{2\varepsilon}$ and $|d| \leq \sqrt{\frac{2\varepsilon}{3}}$, by replacing in the last inequality the value of ε and by an easy computation, we find $|d| \leq 2$, hence $d \in \{1, -1\}$. We get the solutions $\alpha = 1 \pm \sqrt{3}$. We see easily that $1 + \sqrt{3}$ and $1 - \sqrt{3}$ cannot be simultaneously divisors neither for $m^2 - y\sqrt{3}$ nor for $m^2 + y\sqrt{3}$, since then m , y and n are even numbers, which is false.

If $\alpha = 1 + \sqrt{3}$ is the common divisor, then α divides n^4 . As $N(\alpha) = 2$ is a prime number in \mathbf{Z} , α is prime in $\mathbf{Z}[\sqrt{3}]$. Hence α divides n and $\alpha^4 = (1 + \sqrt{3})^4$ divides $n^4 = (m^2 - y\sqrt{3})(m^2 + y\sqrt{3})$. But $(1 + \sqrt{3})^2 = 2(2 + \sqrt{3})$ and it follows that 2 divides $m^2 - y\sqrt{3}$ or $m^2 + y\sqrt{3}$, implying that m and y are even numbers, which is false. The same happens for $\alpha = 1 - \sqrt{3}$. Then $m^2 - y\sqrt{3}$ and $m^2 + y\sqrt{3}$ do not have common divisor $\alpha \in \mathbf{Z}[\sqrt{3}]$ with $N(\alpha) = 2$.

Take $N(\alpha) = 4$, hence $c^2 - 3d^2 = \pm 4$.

By considering the possible cases for c and d (odd and even), we see that $c^2 - 3d^2 = \pm 4$ could have integer solutions with c and d even numbers, hence, by simplifying with 4, we get the equations $a^2 - 3b^2 = \pm 1$ and $\alpha = 2\alpha'$, $\alpha' = a + b\sqrt{3}$ or $\alpha' = a - b\sqrt{3}$. Then 2 is a common divisor for m , n , y , which is not possible.

We just proved that $m^2 + y\sqrt{3}$ and $m^2 - y\sqrt{3}$ are prime to each other in $\mathbf{Z}[\sqrt{3}]$. But $m^4 - n^4 = 3y^2$ is equivalent to $(m^2 - y\sqrt{3})(m^2 + y\sqrt{3}) = n^4$. Then there exists an element $f + g\sqrt{3} \in \mathbf{Z}[\sqrt{3}]$ and there exists $k \in \mathbf{Z}$ such that $m^2 + y\sqrt{3} = (f + g\sqrt{3})^4(2 + \sqrt{3})^k$ or $m^2 + y\sqrt{3} = -(f + g\sqrt{3})^4 \cdot (2 + \sqrt{3})^k$ since the units of the ring $\mathbf{Z}[\sqrt{3}]$ are $\pm(2 + \sqrt{3})^k$, $k \in \mathbf{Z}$.

From the algorithm for computing the solutions of Pell equations, we obtain that $c + d\sqrt{3} \in \{\pm(2 + \sqrt{3})^k, k \in \mathbf{Z}\}$. Then $m^2 + y\sqrt{3} = (f + g\sqrt{3})^4(c + d\sqrt{3})$ and we get the system:

$$\begin{cases} m^2 = cf^4 + 18cf^2g^2 + 9cg^4 + 12f^3gd + 36fg^3d \\ y = 4cf^3g + 12cf^2g^2 + dg^4 + 18df^2g^2 + 9dg^4 \end{cases} .$$

This is equivalent to the system:

$$\begin{cases} m^2 = c(f^4 + 18f^2g^2 + 9g^4) + 12d(f^3g + 3fg^3) \\ y = d(f^4 + 18f^2g^2 + 9g^4) + 4c(f^3g + 3fg^3). \end{cases} \quad (1)$$

As the equation $m^4 - n^4 = 3y^2$ does not have nontrivial integer solutions, the system (1) also does not have nontrivial integer solutions. Then the first equation of the system

$$m^2 = c(f^4 + 18f^2g^2 + 9g^4) + 12d(f^3g + 3fg^3)$$

does not have nontrivial integer solutions.

3. Remarks on some Diophantine equations

We have seen that, in the case $p = 3$, the equation $m^4 - n^4 = 3y^2$ does not have nontrivial integer solutions.

Remark 3.1. *On the other hand, the equation $m^4 - n^4 = 7y^2$ has at least two solutions:*

(i) $m = 4, n = 3, y = 5$ and (ii) $m = 463, n = 113, y = 80\,880$, which means that it has many solutions.

How many solutions could have a Diophantine equation of the form $m^4 - n^4 = py^2$, for a prime p greater than 3?

We answer by the next theorem:

Theorem 3.2. *Let p be a natural prime number greater than 3. If the equation $m^4 - n^4 = py^2$ has a solution*

$m, n, y \in \mathbf{Z}^$, then it has an infinity of integer solutions.*

Proof. As above, $(m, n) = 1$, otherwise the equation can be simplified by d^4 , where $d = (m, n) \neq 1$.

We can consider the equivalent form of the equation, $n^4 + py^2 = m^4$, and we apply to it

Proposition 1.1. Its solution is of the form: $n^2 = |pa^2 - b^2|$, $y = 2ab$, $m^2 = pa^2 + b^2$, with $a, b \in \mathbf{Z}^*$. We see that y has to be even, therefore m and n are odd numbers.

If $pa^2 \geq b^2$ we obtain $n^2 = pa^2 - b^2, y = 2ab, m^2 = pa^2 + b^2, a, b \in \mathbf{Z}^*$.

The last equation $m^2 = pa^2 + b^2$ has, according to Proposition 1.1., only the solutions: $b = pr^2 - s^2, a = 2rs, m = pr^2 + s^2, r, s \in \mathbf{Z}^*$. Then a is an even number and b is an odd number. From $n^2 = pa^2 - b^2$ and $m^2 = pa^2 + b^2$, it follows $m^2 - n^2 = 2b^2$.

But m and n are odd numbers, hence $m^2, n^2 \equiv 1 \pmod{4}$, therefore $m^2 - n^2 \equiv 0 \pmod{4}$.

Since b is odd, then $b^2 \equiv 1 \pmod{4} \Rightarrow 2b^2 \equiv 2 \pmod{4}$, hence the equation $m^2 - n^2 = 2b^2$ does not have nontrivial integer solutions.

If $pa^2 \not\equiv b^2$, the first equation is $n^2 = b^2 - pa^2$, $a, b \in \mathbf{Z}$ and, from the Proposition 1.6, if the system:

$$\begin{cases} n^2 = b^2 - pa^2 \\ m^2 = pa^2 + b^2, \end{cases} \quad a, b \in \mathbf{Z},$$

has one solution in the set of integer numbers, then it has one infinity of integer solutions. It's the same for the equation $m^4 - n^4 = py^2$, p prime, $p \geq 3$: if it has one solution in the set of integer numbers, then it has an infinity of integer solutions.

Proposition 3.3. *Let p be a prime natural number, $p \geq 3$. If the equation $x^4 + 6px^2y^2 + p^2y^4 = z^2$ has a nontrivial solution in \mathbf{Z} , then it has an infinity of integer solutions. Also, if the equation $|x^4 - 6px^2y^2 + p^2y^4| = z^2$ has a nontrivial solution in \mathbf{Z} , then it has an infinity of integer solutions.*

Proof. From the Theorem 3.2., if the equation $m^4 - n^4 = py^2$ has a solution $m, n, y \in \mathbf{Z}$, then it has infinitely many integer solutions.

The equation $m^4 - n^4 = py^2$ is equivalent to the system:

$$\begin{cases} n^2 = |pa^2 - b^2| \\ y = 2ab \\ m^2 = pa^2 + b^2, \end{cases} \quad a, b \in \mathbf{Z}^*.$$

If $pa^2 \not\equiv b^2$, we obtain $n^2 = b^2 - pa^2$, therefore $n^2 + pa^2 = b^2$.

By using the Proposition 1.1., we get the form of the solutions: $n = \pm(pu^2 - v^2)$, $a = 2uv$, $b = \pm(pu^2 + v^2)$, $u, v \in \mathbf{Z}^*$, which implies that $n^4 = (pu^2 - v^2)^4$. The second equation: $y = 2ab$ is equivalent to $y = \pm 4uv(pu^2 + v^2)$ and this implies that $py^2 = 16pu^2v^2(pu^2 + v^2)^2$.

By introducing n^4 and py^2 in the given equation, we obtain $m^4 = (v^4 + p^2u^4 + 6pu^2v^2)^2$, which is equivalent to $m^2 = v^4 + p^2u^4 + 6pu^2v^2$.

But, from Theorem 3.2., if the equation $m^2 = v^4 + p^2u^4 + 6pu^2v^2$ has one solution $m, u, v \in \mathbf{Z}^*$, then it has an infinity of integer solutions.

Hence, if the equation $x^4 + 6px^2y^2 + p^2y^4 = z^2$ has one solution $x, y, z \in \mathbf{Z}$, then it has an infinity of integer solutions.

If $pa^2 \equiv b^2$, we obtain: $n^2 = b^2 - pa^2$, $y = 2ab$, $m^2 = pa^2 + b^2$, with $a, b \in \mathbf{Z}^*$.

Take $m^2 = pa^2 + b^2$ and apply Proposition 1.1., for getting the equivalent system:

$$\begin{cases} b = \pm(pr^2 - s^2) \\ a = 2rs \\ m = \pm(pr^2 + s^2), \end{cases} \quad r, s \in \mathbf{Z}$$

and $m^4 = (pr^2 + s^2)^4$.

Replacing py^2 and m^4 in the given equation, we obtain $n^4 = (s^4 + p^2r^4 - 6pr^2s^2)^2$, therefore $n^2 = |s^4 + p^2r^4 - 6pr^2s^2|$.

By Theorem 3.2., we know that, if the equation $n^2 = |s^4 + p^2r^4 - 6pr^2s^2|$ has one solution $m, u, v \in \mathbf{Z}^*$, then it has an infinity of integer solutions.

Hence, if the equation $|x^4 - 6px^2y^2 + p^2y^4| = z^2$ has one solution $x, y, z \in \mathbf{Z}$, then it has an infinity of integer solutions.

Proposition 3.4. *If the equation $c(x^4 + 6px^2y^2 + p^2y^4) + 4pd(x^3y + pxy^3) = z^2$, where $p \in \{11, 19\}$ and (c, d) is a solution of the Pell equation $u^2 - pv^2 = 1$ has one solution $x, y, z \in \mathbf{Z}^*$, then it has an infinity of integer solutions.*

Proof. If $p \in \{11, 19\}$ then $p \equiv 3 \pmod{8}$ and $p \equiv 3 \pmod{4}$.

From Proposition 1.2., the ring of integers A of the quadratic field $\mathbf{Q}(\sqrt{p})$ is Euclidean with respect to the norm $N, A = \mathbf{Z}[\sqrt{p}]$.

We study the equation $m^4 - n^4 = py^2$, where p is 11 or 19, in the ring

$\mathbf{Z}[\sqrt{p}]$.

We take the same way as in the proof of the Theorem 3.2. We have the equivalent form of the given equation: $(m^2 - y\sqrt{p})(m^2 + y\sqrt{p}) = n^4$. Let $\alpha \in \mathbf{Z}[\sqrt{p}]$ be a common divisor of $(m^2 - y\sqrt{p})$ and $(m^2 + y\sqrt{p})$. Take $\alpha = c + d\sqrt{p}$, $c, d \in \mathbf{Z}$, $\alpha \notin U(\mathbf{Z}[\sqrt{p}])$.

As in the proof of the Theorem 3.2., we get $N(\alpha) \in \{1, 2, 4\}$ and, since $\alpha \notin U(\mathbf{Z}[\sqrt{p}])$, $N(\alpha) \in \{2, 4\}$.

But $N(\alpha) = 2$ gives the equations $|c^2 - pd^2| = 2$, which means $c^2 - pd^2 = \pm 2$.

The equation $c^2 - pd^2 = 2$ has not integers solutions, as we see by taking all the cases for c and d .

For $p = 11$, we consider the equation: $c^2 - 11d^2 = -2$. We use the equation $c^2 - 11d^2 = 1$, developing $\sqrt{11}$ in a continued fraction. We get: $a_0 = 3, a_1 = 3, a_2 = 6$, and repeated figures, hence $\sqrt{11} = [a_0, \overline{a_1, a_2}] = [3, \overline{3, 6}]$. We need $A_1 = 10$ and $B_1 = 3$, therefore the fundamental solution of the equation $c^2 - 11d^2 = 1$ is $(10, 3)$ and $\varepsilon = 10 + 3\sqrt{11}$.

If the equation $c^2 - 11d^2 = -2$ has integer solutions (c, d) , then $|c| \leq \sqrt{2\varepsilon}$ and $|d| \leq \sqrt{\frac{2\varepsilon}{11}}$, hence $|d| \leq \sqrt{\frac{20+6\sqrt{11}}{11}} = \sqrt{\frac{(3+\sqrt{11})^2}{11}} = \frac{3+\sqrt{11}}{\sqrt{11}} \leq 2$.

Since $d \in \mathbf{Z}$ is an odd number, we get $d \in \{-1, 1\}$ and $c \in \{-3, 3\}$. Hence the solutions of the equation $c^2 - 11d^2 = -2$ are $\mu = \pm\varepsilon^k(3 \pm \sqrt{11})$, $k \in \mathbf{Z}$, i.e. $\mu = \pm(10 + 3\sqrt{11})^k(3 \pm \sqrt{11})$, $k \in \mathbf{Z}$.

Then a common divisor α , with $N(\alpha) = 2$ (in $\mathbf{Z}[\sqrt{11}]$) of $m^2 - \sqrt{11}y$ and $m^2 + \sqrt{11}y$ could be $\alpha = \pm(10 + 3\sqrt{11})^k(3 \pm \sqrt{11})$, $k \in \mathbf{Z}$.

As $3 + \sqrt{11}$ and $3 - \sqrt{11}$ are prime elements in $\mathbf{Z}[\sqrt{11}]$, because of their norm, if $(3 + \sqrt{11})(3 - \sqrt{11}) / (m^2 + y\sqrt{11})$, then $2 / (m^2 + y\sqrt{11})$, and therefore $2 / m$ and $2 / y$, which is not true.

We get that $m^2 + y\sqrt{11}$ can have (in $\mathbf{Z}[\sqrt{11}]$) only divisors of the type $\pm(10 + 3\sqrt{11})^t(3 + \sqrt{11})$, $t \in \mathbf{Z}$ or of the type $\pm(10 + 3\sqrt{11})^t(3 - \sqrt{11})$, $t \in \mathbf{Z}$, but not of both types simultaneously.

Analogously for $m^2 - y\sqrt{11}$.

If $(3 \pm \sqrt{11})^k / (m^2 + y\sqrt{11})$, with $k \in \mathbf{N}$, $k \geq 2$ (in $\mathbf{Z}[\sqrt{11}]$), then again m and n are even numbers, which is not the case.

Analogously, $m^2 - y\sqrt{11}$ cannot be divided by $(3 \pm \sqrt{11})^2$.

Hence $(3 + \sqrt{11})^2$ or $(3 - \sqrt{11})^2$ is the biggest power dividing n^4 .

But if $3 + \sqrt{11}$ divides $m^2 + y\sqrt{11}$ and $m^2 - y\sqrt{11}$, then $(3 + \sqrt{11})^2 / (m^2 + y\sqrt{11})(m^2 - y\sqrt{11})$. From $(3 + \sqrt{11}) / n^4$, we get that $(3 + \sqrt{11})^4 / n^4$, contradicting the assumption that $(3 + \sqrt{11})^2$ is the biggest power of $3 + \sqrt{11}$ which divides n^4 .

The same for $3 - \sqrt{11}$, it cannot divide n^4 .

We have proved that $m^2 + y\sqrt{11}$ and $m^2 - y\sqrt{11}$ cannot have common divisors in $\mathbf{Z}[\sqrt{11}]$, with the norm 2.

We have the same argument in the case $p = 19$ and the equation: $c^2 - 19d^2 = -2$.

Developing $\alpha = \sqrt{19}$ in a continued fraction, we get: $a_0 = 4$, $a_1 = 2$, $a_2 = 1$, $a_3 = 3$, $a_4 = 1$, $a_5 = 2$, $a_6 = 8$ and repeated figures, hence $\sqrt{19} = [a_0, \overline{a_1, a_2, a_3, a_4, a_5, a_6}] = [4, \overline{2, 1, 3, 1, 2, 8}]$. We have $(c_0, d_0) = (A_5, B_5)$, and $A_5 = 170$, hence $c_0 = 170$, $B_5 = 39$, hence $d_0 = 39$. Therefore $\varepsilon = 170 + 39\sqrt{19}$.

If the equation $c^2 - 19d^2 = -2$ has integer solutions (c, d) , then $|c| \leq \sqrt{2\varepsilon}$ and $|d| \leq \sqrt{\frac{2\varepsilon}{19}} = \sqrt{\frac{340 + 78\sqrt{19}}{19}} \leq 37$. Since d is an odd number, we have $d \in \{\pm 1, \pm 3, \dots, \pm 35\}$.

We come back to the equation $c^2 - 19d^2 = -2$.

If $d \in \{\pm 1, \pm 11, \pm 21, \pm 31, \pm 9, \pm 19, \pm 29\}$, this implies that the last figure of d^2 is 1, the last figure of $19d^2$ is 9, hence the last figure of c^2 is 7 and $c \notin \mathbf{Z}$.

If $d \in \{\pm 5, \pm 15, \pm 25, \pm 35\}$, this implies that the last figure of d^2 is 5, the last figure of $19d^2$ is 5, hence the last figure of c^2 is 3 and $c \notin \mathbf{Z}$.

The cases which remain to be studied are

$$d \in \{\pm 3, \pm 7, \pm 13, \pm 17, \pm 23, \pm 27, \pm 33\}.$$

If $d \in \{\pm 3\}$, then $c \in \{\pm 13\}$, hence $(13, 3)$, $(13, -3)$, $(-13, 3)$, $(-13, -3)$ are solutions of the equation $c^2 - 19d^2 = -2$.

For $d \in \{\pm 7, \pm 13, \pm 17, \pm 23, \pm 27, \pm 33\}$, we cannot find a solution $(c, d) \in \mathbf{Z}^2$.

Therefore the integer solutions of the equation $c^2 - 19d^2 = -2$ are of the form $\pm (170 + 39\sqrt{19})^t (13 \pm 3\sqrt{19})$, $t \in \mathbf{Z}$.

A divisor α , with $N(\alpha) = 2$ (in $\mathbf{Z}[\sqrt{19}]$) of $m^2 - y\sqrt{19}$ and $m^2 + y\sqrt{19}$ could be $\pm (170 + 39\sqrt{19})^t (13 \pm 3\sqrt{19})$, $t \in \mathbf{Z}$.

As in the Theorem 3.2., we show that, if $13 + 3\sqrt{19}$ divides $m^2 + y\sqrt{19}$, then $13 - 3\sqrt{19}$ cannot divide $m^2 - y\sqrt{19}$ and conversely. Then we show that, if $(13 + 3\sqrt{19})^t$, $t \in \mathbf{N}^*$, divides one of elements $m^2 \pm y\sqrt{19}$, then $t = 1$. Hence the common divisor α of $m^2 \pm y\sqrt{19}$ can be either $13 + 3\sqrt{19}$ or $13 - 3\sqrt{19}$. If $\alpha = 13 + 3\sqrt{19}$ (or $13 - 3\sqrt{19}$), then α^2 divides n^4 . Since α is prime in $\mathbf{Z}[\sqrt{19}]$, α divides n and therefore α^4 divides $n^4 = (m^2 + y\sqrt{19})(m^2 - y\sqrt{19})$, in contradiction with the assumption that α^2 is the greatest power of α dividing n^4 .

We get that, for $p \in \{11, 19\}$, $N(\alpha) \neq 2$.

If $N(\alpha) = 4$, then we get the equations $c^2 - pd^2 = \pm 4$, $p \in \{11, 19\}$.

We use the same argument as above, obtaining the impossibility of getting solutions for these equations.

We have just proved that, for $p \in \{11, 19\}$, $m^2 + y\sqrt{p}$ and $m^2 - y\sqrt{p}$ are relatively prime in $\mathbf{Z}[\sqrt{p}]$, which means that $m^2 + y\sqrt{p} = (c + d\sqrt{p})(f + g\sqrt{p})^4$, with $f, g \in \mathbf{Z}$ and (c, d) being a solution of the Pell equation $u^2 - pv^2 = 1$. Of course, then $m^2 - y\sqrt{p} = (c - d\sqrt{p})(f - g\sqrt{p})$.

By identifying the elements in the two members of the two equalities, we get the system:

$$\begin{cases} m^2 = c(f^4 + 6pf^2g^2 + p^2g^4) + 4pd(f^3g + pfg^3) \\ y = d(f^4 + 6pf^2g^2 + p^2g^4) + 4c(f^3g + pfg^3) \end{cases}.$$

It is obvious that, if the first equation of the above system has solutions in \mathbf{Z}^* , then, from the second equation, we get $y \in \mathbf{Z}$.

Hence as the equation $m^4 - n^4 = py^2$ has either none nontrivial integer solutions or an infinity of nontrivial integer solutions, the same will happen with the first equation of the above system:

Either the equation $m^2 = c(f^4 + 6pf^2g^2 + p^2g^4) + 4pd(f^3g + pfg^3)$ has no nontrivial integer solutions (m, f, g) or it has an infinity of nontrivial integer solutions, where (c, d) is a solution of the Pell equation $u^2 - dv^2 = 1$.

Proposition 3.5. *The equation of the form $c(x^4 + 42x^2y^2 + 49y^4) + 28d(x^3y + 7xy^3) = z^2$, where (c, d) is a solution of the Pell equation $u^2 - 7v^2 = 1$ has an infinity of integer solutions.*

Proof. From Proposition 1.2., if $p = 7$, the ring of integers A of the quadratic field $\mathbf{Q}(\sqrt{p})$ is Euclidean with respect to the norm N . Since $7 \equiv 3 \pmod{4}$, $A = \mathbf{Z}[\sqrt{7}]$.

We study the equation $m^4 - n^4 = 7y^2$ in the ring $\mathbf{Z}[\sqrt{7}]$.

This equation has at least a solution: $m = 463$, $n = 113$, $y = 80880$. But then it has an infinity of integer solutions.

Now, consider $m^4 - n^4 = 7y^2$ written as $(m^2 - y\sqrt{7})(m^2 + y\sqrt{7}) = n^4$. Let $\alpha \in \mathbf{Z}[\sqrt{7}]$ be a common divisor of $(m^2 - y\sqrt{7})$ and $(m^2 + y\sqrt{7})$, then $\alpha = c + d\sqrt{7}$, $c, d \in \mathbf{Z}$.

As $\alpha/(m^2 + y\sqrt{7})$ and $\alpha/(m^2 - y\sqrt{7})$, we have $\alpha/2m^2$ and $\alpha/2y\sqrt{7}$, so $N(\alpha)/4m^4$ (in \mathbf{Z}) and $N(\alpha)/28y^2$ (in \mathbf{Z}), hence $N(\alpha)/(4m^4, 28y^2)$. But $(m, n) = 1$ implies $(m, y) = 1$ (if $(m, y) = d > 1$ then d/n , which is false). Analogously by $(m, p) = 1$, we get $(m^4, py^2) = 1$, $(4m^4, 28y^2) = 4$, hence $N(\alpha) \in \{1, 2, 4\}$.

If $N(\alpha) = 2$, then $|c^2 - 7d^2| = 2$, this is $c^2 - 7d^2 = \pm 2$.

Firstly we solve the equation $c^2 - 7d^2 = 2$. We see that the equation $c^2 - 7d^2 = 2$ could have integer solutions (c, d) , with c, d odd numbers.

We consider the equation $c^2 - 7d^2 = 1$. We develop $\alpha = \sqrt{7}$ in a continued fraction and we get: $a_0 = [\sqrt{7}] = 2$, $\alpha_1 = \frac{\sqrt{7}+2}{3}$, $a_1 = 1$, $\alpha_2 = \frac{\sqrt{7}+1}{2}$, $a_2 = 1$, $\alpha_3 = \frac{\sqrt{7}+1}{3}$, $a_3 = 1$, $\alpha_4 = \sqrt{7} + 2$, $a_4 = 4$, $\alpha_5 = \frac{\sqrt{7}+2}{3} = \alpha_1$.

We get that $\sqrt{7} = [a_0, \overline{a_1, a_2, a_3, a_4}]$, hence $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$, and the number of the incomplete denominators is $k = 4$. Using Lagrange theorem, we find the fundamental solution of the equation $c^2 - 7d^2 = 1$ namely: $(8; 3)$. We have $\varepsilon = 8 + 3\sqrt{7}$. Then $c^2 - 7d^2 = 2$ has integer solutions (c, d) , if $|c| \leq \sqrt{2\varepsilon}$

and $|d| \leq \sqrt{\frac{2\varepsilon}{7}}$, and this implies $|d| \leq \sqrt{\frac{2(8+3\sqrt{7})}{7}} \leq \frac{8}{3}$.

But $d \in \mathbf{Z}$, d is an odd number, hence $d \in \{-1, 1\}$.

We go back to the equation $c^2 - 7d^2 = 2$ and we get $c \in \{-3, 3\}$, hence $(3, 1), (3, -1), (-3, 1), (-3, -1)$ are solutions for the equation $c^2 - 7d^2 = 2$.

All integer solutions of the equation $c^2 - 7d^2 = 2$ are $\mu = \pm \varepsilon^t(3 \pm \sqrt{7})$, $t \in \mathbf{Z}$.

We prove that $m^2 + y\sqrt{7}$ and $m^2 - y\sqrt{7}$ do not have common divisors of the type $\pm(8 + 3\sqrt{7})^t(3 \pm \sqrt{7})$, $t \in \mathbf{Z}$.

If $(3 + \sqrt{7}) / (m^2 + y\sqrt{7})$ and $(3 - \sqrt{7}) / (m^2 + y\sqrt{7})$ (in $\mathbf{Z}[\sqrt{7}]$), as $3 + \sqrt{7}$ and $3 - \sqrt{7}$ are prime elements in $\mathbf{Z}[\sqrt{7}]$ (their norm is 2, a prime element in \mathbf{N}), we get $(3 + \sqrt{7})(3 - \sqrt{7}) / (m^2 + y\sqrt{7})$, hence $2 / (m^2 + y\sqrt{7})$. Then

there exists $(a + b\sqrt{7}) \in \mathbf{Z}[\sqrt{7}]$ such that $m^2 + y\sqrt{7} = 2(a + b\sqrt{7})$, hence $m^2 = 2a$, $y = 2b$ implying $2 / m$ and $2 / y$. But $m^4 - n^4 = 7y^2$, and then $2/n$, a contradiction with the fact that $(m, n) = 1$. We get that $m^2 + y\sqrt{7}$ can have (in $\mathbf{Z}[\sqrt{7}]$) only divisors of the type $\pm(8 + 3\sqrt{7})^t(3 + \sqrt{7})$, $t \in \mathbf{Z}$ or the type $\pm(8 + 3\sqrt{7})^t(3 - \sqrt{7})$, $t \in \mathbf{Z}$, but not of both types simultaneously.

Analogously for $m^2 - y\sqrt{7}$.

If $(3 + \sqrt{7})^2 / (m^2 + y\sqrt{7})$ (in $\mathbf{Z}[\sqrt{7}]$), hence $(16 + 6\sqrt{7}) / (m^2 + y\sqrt{7})$,

implying $2/(m^2 + y\sqrt{7})$, hence $2/m$ and $2/y$ (in \mathbf{Z}), hence $2/n$, a contradiction with the fact that $(m, n) = 1$.

We get that $(3 + \sqrt{7})^k \nmid (m^2 + y\sqrt{7})$, for $k \in \mathbf{N}$, $k \geq 2$. Analogously for $m^2 - y\sqrt{7}$.

If $(3 + \sqrt{7}) \mid (m^2 + y\sqrt{7})$ and $(3 + \sqrt{7}) \mid (m^2 - y\sqrt{7})$ (in $\mathbf{Z}[\sqrt{7}]$), then $(3 + \sqrt{7})^2 \mid (m^2 + y\sqrt{7})(m^2 - y\sqrt{7})$, equivalently to $(3 + \sqrt{7})^2 \mid (m^4 - 7y^2)$, hence $(3 + \sqrt{7})^2 \mid n^4$ ($(3 + \sqrt{7})^2$ is the biggest power of $3 + \sqrt{7}$ which divides n^4).

But $3 + \sqrt{7}$ is a prime element in $\mathbf{Z}[\sqrt{7}]$ (since $N(3 + \sqrt{7}) = 2$ is a prime element in \mathbf{N}) hence $(3 + \sqrt{7}) \mid n$ and $(3 + \sqrt{7})^4 \mid n^4$, contradiction with the fact that 2 is the biggest power of $(3 + \sqrt{7})$ which divides n^4 .

From the previously proved, we get that $m^2 + y\sqrt{7}$ and $m^2 - y\sqrt{7}$ can't have common divisors of the type $\pm(8 + 3\sqrt{7})^t(3 + \sqrt{7})$, $t \in \mathbf{Z}$, in $\mathbf{Z}[\sqrt{7}]$.

Analogously, we prove that $m^2 + y\sqrt{7}$ and $m^2 - y\sqrt{7}$ can't have common divisors of the type $\pm(8 + 3\sqrt{7})^t(3 - \sqrt{7})$, $t \in \mathbf{Z}$, in $\mathbf{Z}[\sqrt{7}]$.

Now, we solve the equation $c^2 - 7d^2 = -2$. Taking all the cases for c and d , we get that $c^2 - 7d^2 \neq -2$.

As before, $m^2 + y\sqrt{7}$ and $m^2 - y\sqrt{7}$ can't have common divisors $\alpha \in \mathbf{Z}[\sqrt{7}]$, if $N(\alpha) = 2$.

If $N(\alpha) = 4$, then $c^2 - 7d^2 = \pm 4$.

Studying the equation $c^2 - 7d^2 = 4$, we see that c and d have to be even.

We denote $c = 2c'$, $d = 2d'$, $c', d' \in \mathbf{Z}$. Then $c^2 - 7d^2 = 4$ is equivalent to $(c')^2 - 7(d')^2 = 1$. Denote $\alpha' = c' + d'\sqrt{7}$, with $N(\alpha') = 1$, implying $\alpha' \in \mathbf{U}(\mathbf{Z}[\sqrt{7}])$, and $\alpha = 2\alpha'$. But $\alpha \mid (m^2 + y\sqrt{7})$ implies $2 \mid (m^2 + y\sqrt{7})$ (in $\mathbf{Z}[\sqrt{7}]$), hence there exists $(a + b\sqrt{7}) \in \mathbf{Z}[\sqrt{7}]$ such that $m^2 + y\sqrt{7} = 2(a + b\sqrt{7})$, hence $m^2 = 2a$ and $y = 2b$, implying $2 \mid m$ and $2 \mid y$ (in \mathbf{Z}). But $m^4 - n^4 = 7y^2$ implies $2 \mid n$, a contradiction with the fact that $(m, n) = 1$.

The case $c^2 - 7d^2 = -4$ is similar, hence $N(\alpha) \neq 4$.

We obtained that $N(\alpha) = 1$. As $m^2 + y\sqrt{7}$ and $m^2 - y\sqrt{7}$ are prime to each other in $\mathbf{Z}[\sqrt{7}]$ and $(m^2 + y\sqrt{7})(m^2 - y\sqrt{7}) = n^4$, there exists $(f + g\sqrt{7}) \in \mathbf{Z}[\sqrt{7}]$ and there exists $k \in \mathbf{Z}$ such that $m^2 + y\sqrt{7} = (c + d\sqrt{7})(f + g\sqrt{7})^4$, where $c + d\sqrt{7} \in \{\pm(8 + 3\sqrt{7})^k, k \in \mathbf{Z}\}$, $(8; 3)$ being the fundamental solution of the Pell equation $u^2 - 7v^2 = 1$.

We obtain: $m^2 + y\sqrt{7} = (c + d\sqrt{7})(f^4 + 4f^3g\sqrt{7} + 42f^2g^2 + 28fg^3\sqrt{7} + 49g^4)$.

We get the system:

$$\begin{cases} m^2 = cf^4 + 42cf^2g^2 + 49cg^4 + 28f^3gd + 196fg^3d \\ y = 4cf^3g + 28cfdg^3 + df^4 + 42df^2g^2 + 49dg^4 \end{cases},$$

which is equivalent to the system:

$$\begin{cases} m^2 = c(f^4 + 42f^2g^2 + 49g^4) + 28d(f^3g + 7fg^3) \\ y = d(f^4 + 42f^2g^2 + 49g^4) + 4c(f^3g + 7fg^3) \end{cases}.$$

We have already proved that the equation $m^4 - n^4 = 7y^2$ has an infinity of integer solutions.

Hence, the system

$$\begin{cases} m^2 = c(f^4 + 42f^2g^2 + 49g^4) + 28d(f^3g + 7fg^3) \\ y = d(f^4 + 42f^2g^2 + 49g^4) + 4c(f^3g + 7fg^3) \end{cases}$$

has an infinity of integer solutions. Moreover, the equation

$$m^2 = c(f^4 + 42f^2g^2 + 49g^4) + 28d(f^3g + 7fg^3)$$

has an infinity of integer solutions.

Remark 3.6. *We have got some solutions:*

(i) $f = 36, g = -13, m = 463$, for $k = 4, c = 32\ 257$ and $d = 12\ 192$,

(ii) $f = 561, g = -212, m = 463$, for $k = 8, c = 2\ 081\ 028\ 097$ and $d = 859\ 672\ 304$.

This has been done by considering the corresponding solutions for the equation

$$m^4 - n^4 = 7y^2, \text{ where } m = 463, y = 80\ 880 \text{ and } n = 113.$$

References

- [1] T. Albu, I.D.Ion, *Chapters of the algebraic theory of numbers (in Romanian)*, Ed. Academiei, București, 1984.
- [2] V. Alexandru, N.M. Goșoniu, *The elements of the theory of numbers (in Romanian)*, Ed. Universității București, 1999.
- [3] T. Andreescu, D. Andrica, *An Introduction in the Study of Diophantine Equations (in Romanian)*, Ed. Gil, Zalău, 2002.
- [4] L.J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.
- [5] L. Panaitopol, A. Gica, *An introduction in arithmetic and the theory of numbers (in Romanian)*, Ed. Universității București, 2001.
- [6] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1992.
- [7] W. Sierpinski, *What we know and what we do not know about prime numbers (in Romanian)*, (transl. from Polish edition, 1964), București.
- [8] C. Vraciu, M. Vraciu, *Basics of Arithmetic (in Romanian)*, Ed. All, București, 1998.
- [9] *Octagon, Mathematical Magazine*, vol. 10, nr. 2, October 2002.

”Ovidius” University of Constanta,
 Department of Mathematics and Informatics,
 8700 Constanta,
 Romania
 e-mail: dianet72@yahoo.com

