On some exponential Diophantine equations

Yann Bugeaud (Strasbourg)

Abstract. *We apply a new, deep result of Bilu, Hanrot & Voutier to solve completely some exponential Diophantine equations of the type* $D_1x^2 + D_2 = \lambda^2 y^p$*, where* D_1*,* D_2 *are given coprime positive integers,* $\lambda \in \{1, 2\}$*, and* x*,* y*,* $p \geq 3$ *are unknown.*

1. Introduction

Let D_1 and D_2 be coprime positive integers and let $\lambda = 1$ or 2. Diophantine equations of the type

$$D_1x^2 + D_2 = \lambda^2 y^p, \qquad (1)$$

in positive integers x, y and $p \geq 3$, with p prime, have been considered by several authors. The purpose of the present work is to improve previous results, thanks to a new, deep, theorem of Bilu, Hanrot & Voutier [2]. In [3], we have already applied the main result of [2] in a similar context, in order to obtain sharp upper bounds for the number of solutions of equations of type (1) when y is a fixed positive integer. Here, we use the same idea to solve completely some exponential Diophantine equations investigated previously, and to extend some of the results of [3].

Our aim is to point out that the definitive result obtained in [2] has many interesting applications in the field of Diophantine equations.

2. Statement of the results

Theorem 1 below solves a problem investigated by Le [7, 10] and by Mignotte [12], while Theorem 2 improves a result of Le [7]. We refer to [7] and to [10] for exhaustive references concerning previous works on these Diophantine equations, mainly by Nagell, Ljunggren and Blass.

1991 *Mathematics Subject Classification :* 11D61.

Theorem 1. *Let D_1 and D_2 be coprime positive integers. The only solutions of the Diophantine equation*

$$D_1x^2 + D_2^m = 4y^n, \qquad \text{in positive integers } x,\ y,\ m \text{ odd and } n \geq 5 \text{ prime},$$

with $\gcd(D_1x, D_2y) = 1$ *and n coprime with the class number of the quadratic field* $\mathbf{Q}(\sqrt{-D_1D_2})$, *are given by*

$$(y,n) \in \{(2,7),(2,13),(3,7),(4,7),(5,7)\}$$

and by $(y,n) = (F_i, 5)$ or $(L_i, 5)$, for $i \geq 2$, where F_i (resp. L_i) is the i-th term of the Fibonacci sequence (resp. the Lucas sequence) defined by $F_0 = 1$, $F_1 = 1$ and $F_k = F_{k-1} + F_{k-2}$ for $k \geq 2$ (resp. by $L_0 = 2$, $L_1 = 1$ and $L_k = L_{k-1} + L_{k-2}$ for $k \geq 2$).

Theorem 2. *Let D_1 and D_2 be coprime square-free positive integers and denote by h the class number of the quadratic field $\mathbf{Q}(\sqrt{-D_1D_2})$. Let $m \geq 0$ and $n \geq 5$ be integers with n prime and $\gcd(n, 2h) = 1$. The Diophantine equation*

$$D_1x^2 + 2^{2m}D_2 = y^n, \qquad \text{in coprime integers } x > 0 \text{ and } y > 1 \text{ odd},$$

has only the solutions $x^2 + 19 = 55^5$ and $x^2 + 341 = 377^5$.

The same method allows us also to improve the first statement of the Theorem of Le [9], where a result is proved only for sufficiently large D. We refer to [9] for further references concerning equation (3) below.

Theorem 3. *Let D be an odd positive integer. Then the Diophantine equation*

$$x^2 + D^m = 2^{n+2}, \qquad \text{in positive integers } x,\ m \text{ and } n, \tag{3}$$

has at most one solution, except for $D = 7$ and $D = 15$, in which cases (3) has, respectively, exactly 6 solutions, namely

$$(x,m,n) \in \{(1,1,1),(3,1,2),(5,1,3),(11,1,5),(13,3,7),(181,1,13)\},$$

and exactly 2 solutions, given by $(x,m,n) \in \{(1,1,2),(7,1,4)\}$.

Remark : We point out that our Theorem 3 considerably improves the first statement of the Theorem of [9], since here we assume $m \geq 1$, whereas Le put the stronger hypothesis $m > 1$.

Finally, we get the following improvement of the theorem of Le [6], who proved Theorem 4 below for (very) large values of D.

Theorem 4. *Let $D > 2$ be an integer and let p be an odd prime which does not divide D. If there exists a positive integer a with $D = 3a^2 + 1$ and $p = 4a^2 + 1$, then the Diophantine equation*

$$x^2 + D^m = p^n, \qquad \text{in positive integers } x,\ m \text{ and } n,$$

has at most three solutions (x, m, n), namely

$$(a, 1, 1),\ \ (8a^3 + 3a, 1, 3),\ \ (x_3, m_3, n_3),$$

with m_3 (if the third solution exists) even. Otherwise, the Diophantine equation

$$x^2 + D^m = p^n, \qquad \text{in positive integers } x,\ m \text{ and } n,$$

has at most two solutions. If these are (x_1, m_1, n_1) and (x_2, m_2, n_2), then $m_1 \not\equiv m_2$ mod 2.

Remark : In the statement of Theorem 4, we have excluded the case $D = 2$, since the Diophantine equation $x^2 + 2^m = y^n$, in positive integers x, m, y odd and $n > 2$, has been recently solved by Le [11]. Further, we observe that Le [6] assumed D to be non-power. The hypothesis is used in the proof, however the conclusion remains clearly true if D is a power, since both Diophantine equations $x^2 + 1 = y^n$ and $3x^2 + 1 = y^n$ have no solution with $y > 1$ and $n > 1$.

Remark : In [3, Corollary 5], improving upon previous results by Aigner [1] and Le [8], we have completely solved the equation

$$x^2 + 4D = y^p \quad \text{in coprime integers} \quad x, y \geq 1,$$

where D is a square-free positive integer and p is an odd prime not dividing the class number of the quadratic field $\mathbf{Q}(\sqrt{-D})$. We would like to point out that this equation could also be treated using the same arguments as in the proofs of Theorems 1 and 2.

3. On primitive divisors of Lucas and Lehmer sequences

Definition 1. *A Lucas pair (resp. a Lehmer pair) is a pair (α, β) of algebraic integers such that $\alpha + \beta$ and $\alpha\beta$ (resp. $(\alpha + \beta)^2$ and $\alpha\beta$ are non-zero coprime rational integers and α/β is not a root of unity. For a given Lucas pair (α, β), one defines the corresponding sequence of Lucas numbers by*

$$u_n = u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad (n = 0, 1, 2, \ldots).$$

For a given Lehmer pair (α, β), one defines the corresponding sequence of Lehmer numbers by

$$\tilde{u}_n = \tilde{u}_n(\alpha, \beta) = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n \text{ is odd,} \\[2mm] \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{if } n \text{ is even.} \end{cases}$$

We observe that every Lucas pair (α,β) is also a Lehmer pair, and

$$u_n = \begin{cases} \tilde{u}_n & \text{if } n \text{ is odd,} \\ (\alpha+\beta)\tilde{u}_n & \text{if } n \text{ is even.} \end{cases}$$

Definition 2. *Let (α,β) be a Lucas (resp. Lehmer) pair. The prime number p is a primitive divisor of the Lucas (resp. Lehmer) number $u_n(\alpha,\beta)$ (resp. $\tilde{u}_n(\alpha,\beta)$) if p divides u_n but does not divide $(\alpha-\beta)^2u_1\cdots u_{n-1}$ (resp. if p divides $\tilde{u}_n$ but does not divide $(\alpha^2-\beta^2)^2\tilde{u}_1\cdots\tilde{u}_{n-1}$).*

The following lemma is classical.

Lemma 1. *Let (α,β) be a Lucas (resp. Lehmer) pair. If the prime number p is a primitive divisor of the Lucas (resp. Lehmer) number $u_n(\alpha,\beta)$ (resp. $\tilde{u}_n(\alpha,\beta)$), then $n \equiv \pm 1 \bmod p$.*

Proof : This follows from Remark 1.1, (i) of Proposition 2.1 and Corollary 2.2 of [2]. $\square$

The key argument for our proof is the definitive result obtained by Bilu, Hanrot & Voutier [2].

Theorem BHV. *For any integer $n > 30$, every n-th term of any Lucas or Lehmer sequence has a primitive divisor. Further, for any positive integer $n \leq 30$, all Lucas sequences and all Lehmer sequences whose n-th term has no primitive divisor are explicitely determined.*

We do not state here the complete list of n-th term of Lucas and Lehmer sequences without primitive divisor: we refer the reader to [2]. However, in the course of our proof, we utilize the corresponding results of [2]. We should add that for most integers $n \leq 30$ Voutier [13] has given previously the complete list of Lucas sequences and Lehmer sequences whose n-th term has no primitive divisor. Further, one of the main tools of the proof of Theorem BHV is the theory of linear forms in logarithms.

4. Proofs

The proofs of Theorems 1 to 3 follow the same lines: we analyze the decomposition of both members of the equation into ideals in a suitable quadratic number field and, since the hypothesis on the class number of the field ensures that these ideals are principal, we get an equation satisfied by algebraic quadratic numbers. This method is described with many details e.g. in two papers by Ljunggren [4], [5].

As it is stated in [10], under the hypothesis of Theorem 1, there exist positive integers X_1 and Y_1 such that, setting

$$\varepsilon = \frac{X_1\sqrt{D_1}+Y_1\sqrt{-D_2}}{2} \quad \text{and} \quad \overline{\varepsilon} = \frac{X_1\sqrt{D_1}-Y_1\sqrt{-D_2}}{2}, \tag{4}$$

we have

$$D_1X_1^2 + D_2Y_1^2 = 4y = 4|\varepsilon|^2,$$

$$\gcd(D_1X_1, D_2Y_1) = 1 \tag{5}$$

and

$$\frac{\varepsilon^n - \overline{\varepsilon}^n}{\varepsilon - \overline{\varepsilon}} = \begin{cases} \pm n & \text{if } m > 1 \text{ and } n | D_2, \\ \pm 1 & \text{otherwise.} \end{cases} \tag{6}$$

The problem consists in handling with (6). In the previous papers, the authors apply the theory of linear forms in logarithms to obtain an upper bound for n. However, we infer from (4) and (5) that

$$\varepsilon\overline{\varepsilon} \quad \text{and} \quad (\varepsilon + \overline{\varepsilon})^2$$

are relatively prime integers. Hence, the left-hand side of equality (6) is the n-th term of a Lucas or Lehmer sequence, depending as $D_1 = 1$ or $D_1 > 1$. However, Lemma 1 shows that this term has no primitive divisor. Thanks to Theorem BHV, we have the complete list of all Lucas and Lehmer sequences without primitive divisor, and we can determine the different possible values for ε. We check that we obtain exactly the pairs (y, n) given in the statement of Theorem 1.

The proof of Theorem 2 follows the same lines. Indeed, as shown by Le [7], there exists an odd integer X_1 such that

$$D_1X_1^2 + 2^{2m}D_2 = y$$

and

$$\frac{\varepsilon^n - \overline{\varepsilon}^n}{\varepsilon - \overline{\varepsilon}} = \pm 1,$$

where

$$\varepsilon = X_1\sqrt{D_1} + 2^m\sqrt{-D_2} \quad \text{and} \quad \overline{\varepsilon} = X_1\sqrt{D_1} - 2^m\sqrt{-D_2}.$$

As for the proof of Theorem 3, we first observe that, since D is odd, we deduce that m is odd by arguing modulo 4. Then, setting

$$\varepsilon = \frac{x + D^{(m-1)/2}\sqrt{-D}}{2} \quad \text{and} \quad \overline{\varepsilon} = \frac{x - D^{(m-1)/2}\sqrt{-D}}{2},$$

Le [9] shows that if (3) has two different solutions, then there exists an odd integer $k > 1$ such that

$$\left| \frac{\varepsilon^k - \overline{\varepsilon}^k}{\varepsilon - \overline{\varepsilon}} \right| \quad \text{divides} \quad k.$$

By Lemma 1, this means that the k-th term of the Lucas sequence defined by ε and $\overline{\varepsilon}$ has no primitive divisor, and we conclude thanks to Theorem BHV.

The proof of Theorem 4 is similar and we omit it. We only wish to mention that the exceptional family of pairs $(D, p) = (3a^2 + 1, 4a^2 + 1)$ is a subset of the set $\mathcal{H}$ occurring in [3]. □

References

[1] A. Aigner, Die diophantische Gleichung $x^2 + 4D = y^p$ im Zusammenhang mit Klassenzahlen, Monatsh. Math 72 (1968), 1–5.

[2] Y. Bilu, G. Hanrot and P. Voutier (with an appendix by M. Mignotte), Existence of primitive divisors of Lucas and Lehmer numbers. Submitted.

[3] Y. Bugeaud and T. N. Shorey, On the number of solutions of the generalized Ramanujan–Nagell equation. Submitted.

[4] W. Ljunggren, On the Diophantine equation $Cx^2 + D = y^n$, Pacific J. Math. 14 (1964), 585–596.

[5] W. Ljunggren, On the Diophantine equation $Cx^2 + D = 2y^n$, Math. Scand. 18 (1966), 69–86.

[6] Le Maohua, The Diophantine Equation $x^2 + D^m = p^n$, Acta Arith. 52 (1989), 255–265.

[7] Le Maohua, On the Diophantine equations $d_1\, x^2 + 2^{2m}\, d_2 = y^n$ and $d_1\, x^2 + d_2 = 4\, y^n$, Proc. Amer. Math. Soc. 118 (1993), 67–70.

[8] Le Maohua, A Note on the Diophantine Equation $x^2 + 4D = y^p$, Monatsh. Math. 116 (1993), 283–285.

[9] Le Maohua, The Diophantine Equation $x^2 + D^m = 2^{n+2}$, Comm. Math. Univ. S. Pauli 43 (1994), 127–133.

[10] Le Maohua, On the Diophantine equations $D_1\, x^2 + D_2^m = 4y^n$, Monatsh. Math. 120 (1995), 121–125.

[11] Le Maohua, The Diophantine equation $x^2 + 2^m = y^n$, Chinese Sci. Bull. 42 (1997), 1515–1517.

[12] M. Mignotte, On the Diophantine equations $D_1\, x^2 + D_2^m = 4y^n$, Portugaliae Math. 54 (1997), 457–460.

[13] P. M. Voutier, Primitive divisors of Lucas and Lehmer sequences, Math. Comp. 64 (1995), 869–888.

Yann Bugeaud
Université Louis Pasteur
U. F. R. de mathématiques
7, rue René Descartes
67084 STRASBOURG