On the number of solutions of the generalized Ramanujan–Nagell equation

Yann Bugeaud *and* T. N. Shorey

Dedicated to Professor Alan Baker on his 60th birthday

Abstract. Let D_1 and D_2 be coprime positive integers and let k be an odd positive integer coprime with $D_1 D_2$. We consider the Diophantine equation $D_1 x^2 + D_2 = k^n$ in the unknowns $x \geq 1$, $n \geq 1$. We give a necessary and sufficient condition on D_1, D_2 and k under which this equation has at most $2^{\omega(k)-1}$ solutions where $\omega(k)$ denotes the number of distinct prime divisors of k. Thus, under a necessary and sufficient condition, the equation has at most one solution whenever k is a prime. We also consider some related equations and we prove that the Diophantine equation $x^2 + 7 = 4\,y^n$ has no solution in integers $x \geq 1$, $y > 2$ and $n > 1$.

1. Introduction

Let D_1 and D_2 be coprime positive integers, $D = D_1 D_2$ and let $k \geq 2$ be an integer coprime with D. Let $\lambda \in \{1, 2^{1/2}, 2\}$ be such that $\lambda = 2$ if k is even and we consider the equation

$$D_1 x^2 + D_2 = \lambda^2\, k^n \qquad \text{in integers } x \geq 1,\ n \geq 1. \tag{1}$$

We observe that D_1 is odd whenever $\lambda \in \{2^{1/2}, 2\}$. Further, there is no loss of generality in assuming that D_2 is odd if $\lambda \in \{2^{1/2}, 2\}$.

We observe that equation (1) includes the equation

$$D_1 x^2 + D_2 = \lambda'^2 k^n \quad \text{in integers } x \geq 1, n \geq 1 \tag{2}$$

where

$$\lambda' = \begin{cases} 1 & \text{if } k \text{ is odd,} \\ 2 & \text{if 2 divides } k \end{cases}$$

and equations

$$D_1 x^2 + D_2 = 4\, k^n \qquad \text{in integers } x \geq 1,\ n \geq 1 \tag{3}$$

and, for odd k,

$$D_1 x^2 + D_2 = 2\, k^n \qquad \text{in integers } x \geq 1,\ n \geq 1. \tag{4}$$

We denote by $\mathcal{N}(\lambda, D_1, D_2, k)$ the number of solutions (x, n) of equation (1).

1991 *Mathematics Subject Classification :* 11D61.

These notations will be kept throughout the paper. For $D_1 = 1$, $D_2 = 7$ and $k = 2$, equation (2) is the Ramanujan–Nagell equation, which is well-known. Nagell [25] confirmed a conjecture of Ramanujan by proving that $(x, n) = (1, 1), (3, 2), (5, 3), (11, 5)$ and $(181, 13)$ are the only solutions of the Ramanujan–Nagell equation. For $D_1 = 1$, equation (2) is usually called the generalized Ramanujan–Nagell equation.

Since the work of Mahler [24], we know that (1) has only finitely many solutions and there have been many attempts to provide sharp upper bounds for $\mathcal{N}(\lambda, D_1, D_2, p)$, where the letter p denotes a positive prime number, as always in the present paper. The first general result is due to Apéry [2, 3], who proved that for all $D_2 \geq 1$ and $p \geq 2$ except for $(D_2, p) = (7, 2)$, we have $\mathcal{N}(2, 1, D_2, 2) \leq 2$ and $\mathcal{N}(1, 1, D_2, p) \leq 2$ for $p > 2$. Further, Nagell [26] showed that $\mathcal{N}(2, 1, 7, 2) = 5$. The particular case $(D_1, p) = (1, 2)$ was completed by Beukers [7] who obtained that $\mathcal{N}(2, 1, 2^{r+2} - 1, 2) = 2$ for $r > 1$ while otherwise $\mathcal{N}(2, 1, D_2, 2) \leq 1$ when $D_2 \neq 7$. In his thesis, Beukers [6] also considered the case $\mathcal{N}(1, 1, D_2, p)$ where p is an odd prime and he gave some congruence conditions on D_2 under which (2) has at most one solution.

In a series of papers, Le [16, 17, 18, 20, 21] has obtained many new results on equation (1) including the following uniform upper bound [20, 21].

Theorem L. *Except for* $\mathcal{N}(2, 1, 7, 2) = 5$ *and* $\mathcal{N}(2, 3, 5, 2) = \mathcal{N}(2, 1, 11, 3) = \mathcal{N}(2, 1, 19, 5) = 3$, *we have* $\mathcal{N}(\lambda, D_1, D_2, p) \leq 2$.

Observe that Theorem L is sharp since there are infinite families of (D_1, D_2, k) with $\mathcal{N}(1, D_1, D_2, k) = 2$. However, results by Bender & Herzberg [4] and Le [18] assert that if p is sufficiently large compared with D or if $\max\{D_1, D_2, p\}$ is large enough, then $\mathcal{N}(1, D_1, D_2, p) \leq 1$ unless (D_1, D_2, p) belongs to one of these families. Further, Heuberger & Le [13] have proved that for any positive integer D_2, we have $\mathcal{N}(1, 1, D_2, 3) = \mathcal{N}(1, 1, D_2, 23) = 1$ except for $\mathcal{N}(1, 1, 2, 3) = 2$.

The main purpose of the present work is to considerably sharpen Theorem L by means of the exact determination of all triples (D_1, D_2, p) for which equation (1) has more than one solution. We also display in a separate section several important corollaries of our main result, which include the complete resolution of some Diophantine equations.

Acknowledgement : We would like to thank Maurice Mignotte for his numerous remarks and, especially, for the idea of the proof of Lemma 3. We are also indebted to Guillaume Hanrot who kindly solved some elliptic equations on our request, and to Kristin Lauter who pointed out the third equation of Lemma 2, which was forgotten in an earlier version of that work. Finally, we wish to thank the referee who pointed out an inaccuracy in a previous statement of Corollary 6.

2. Statement of the main result

As mentioned above, Theorem L is sharp in the sense that there are infinitely many triples (D_1, D_2, k) with $\mathcal{N}(\lambda, D_1, D_2, k) = 2$. Indeed, we define as follows four infinite families of triples (D_1, D_2, k). First, denote by (F_k) the Fibonacci sequence defined by $F_0 = 0$, $F_1 = 1$ and satisfying $F_k = F_{k-1} + F_{k-2}$ for all $k \geq 2$. Denote by (L_k) the Lucas sequence defined by $L_0 = 2$, $L_1 = 1$ and satisfying $L_k = L_{k-1} + L_{k-2}$ for all $k \geq 2$. Then set

$$\mathcal{F} := \{(F_{k-2\varepsilon}, L_{k+\varepsilon}, F_k) \mid k \geq 2, \varepsilon \in \{\pm 1\}\},$$

$$\mathcal{G} := \{(1, 4\,k^r - 1, k) \mid k \geq 2, r \geq 1\},$$

$$\begin{aligned}\mathcal{H} := \{(D_1, D_2, k) \mid \quad & \text{there exist positive integers } r \text{ and } s \\ & \text{such that } D_1 s^2 + D_2 = \lambda^2 k^r \text{ and } 3D_1 s^2 - D_2 = \pm\lambda^2\}.\end{aligned}$$

and

$$\mathcal{I} := \{(D_1, 1, u^2 - 1) \mid \quad u \geq 2 \text{ is even and there exists an integer } v \text{ such that } u^2 - D_1\, v^2 = 2\}.$$

To see that $\mathcal{H}$ is an infinite family, it suffices to observe that, for s and λ fixed, one can find infinitely many coprime integers D_1 and D_2 satisfying $3D_1 s^2 - D_2 = \pm\lambda^2$; then, one defines k by $D_1 s^2 + D_2 = \lambda^2 k^r$ with $r \geq 1$. We remark that if $(F_{k-2\varepsilon}, L_{k+\varepsilon}, F_k) \in \mathcal{F}$, then the equation

$$F_{k-2\varepsilon} x^2 + L_{k+\varepsilon} = 4F_k^n$$

has two solutions given by $n = 1$ and $n = 5$ (see Lemma 3 below). Further, it is an equation of type (1) since $\gcd(F_{k-2\varepsilon}, L_{k+\varepsilon})$ divides 4. We also observe that if $(1, 4\,k^r - 1, k) \in \mathcal{G}$ $\big($*resp.* $(D_1, D_2, k) \in \mathcal{H}\big)$, then $(x, n) = (1, r)$ and $(2\,k^r - 1, 2r)$ (*resp.* $(x, n) = (s, r)$ and $(8\,D_1 s^3/\lambda^2 \pm 3s, 3r)\big)$ are solutions of (1) with $\lambda = 2$ (*resp.* of (1)). Finally, we remark that for $(D_1, 1, u^2 - 1) \in \mathcal{H}$, the equation $D_1\,x^2 + 1 = (u^2 - 1)^n$ has the two solutions $(v, 1)$ and $(uv, 2)$. By an equation corresponding to $(D_1, D_2, k) \in \mathcal{G}$ or $(D_1, D_2, k) \in \mathcal{I}$, we understand equation (1) with $\lambda = 2$ or $\lambda = 1$, respectively.

We are now able to state our sharpening of Theorem L. It considerably improves the main results of [16, 17].

Theorem 1. *Let p be a prime number. Then, we have $\mathcal{N}(\lambda, D_1, D_2, p) \leq 1$ except for $\mathcal{N}(2, 13, 3, 2) = \mathcal{N}(\sqrt{2}, 7, 11, 3) = \mathcal{N}(1, 2, 1, 3) = \mathcal{N}(2, 7, 1, 2) = \mathcal{N}(\sqrt{2}, 1, 1, 5) = \mathcal{N}(\sqrt{2}, 1, 1, 13) = \mathcal{N}(2, 1, 3, 7) = 2$, and when (D_1, D_2, p) belongs to one of the infinite families $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$. In the latter case, we always have $\mathcal{N}(\lambda, D_1, D_2, p) = 2$, except for $\mathcal{N}(2, 1, 7, 2) = 5$ and $\mathcal{N}(2, 3, 5, 2) = \mathcal{N}(2, 1, 11, 3) = \mathcal{N}(2, 1, 19, 5) = 3$.*

Theorem 1 contains the result of Heuberger & Le [13] quoted in the Introduction. We would like to point out that their proof ultimately depends on hypergeometric methods, while ours rests on the theory of linear forms in logarithms. As proved by Bender & Herzberg and by Le, if equation (1) has solutions, then these can be put into $2^{\omega(k)-1}$ classes, where $\omega(k)$ denotes the number of distinct prime factors of k. A more detailed statement is given in Lemma 1 and the remark following Lemma 1. Theorem 1 is an immediate corollary of Theorem 2 below; for the definition of $\mathrm{h}(-4D)$, see Proposition 1.

Theorem 2. *Except for*

$$x^2 + 7 = 4 \times 2^n,$$

$$x^2 + 11 = 4 \times 3^n,$$

$$x^2 + 19 = 4 \times 5^n$$

and

$$3x^2 + 5 = 4 \times 2^n,$$

an equation corresponding to an element in infinite families $\mathcal{F}, \mathcal{G}$, and $\mathcal{H}$ has exactly two solutions in one class and has at most one solution in any other class. The solutions of the above equations are given by $n = 1, 2, 3, 5, 13$; $n = 1, 2, 5$; $n = 1, 2, 7$ and $n = 1, 3, 7$, respectively. Apart from the equations corresponding to elements in the infinite families $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ and to the equations quoted below, there is at most one solution of equation (1) in any class such that

$$n < \frac{4\sqrt{D}}{\pi}\,\log(2e\sqrt{D}).$$

These exceptional equations are

$$13x^2 + 3 = 4 \times 4^n,$$

$$7x^2 + 11 = 2 \times 9^n,$$

$$x^2 + 1 = 2 \times 5^n,$$

$$x^2 + 1 = 2 \times 13^n,$$

$$x^2 + 3 = 4 \times 7^n,$$

$$x^2 + 19 = 55^n,$$

$$x^2 + 341 = 377^n,$$

$$2x^2 + 1 = 3^n$$

and

$$7x^2 + 1 = 4 \times 2^n.$$

The solutions of the first two exceptions are given by $n = 1, 7$. The solutions of the third and the last but one exceptions are given by $n = 1, 2$. The solutions of the fourth and the last exceptions are given by $n = 1, 4$. The fifth exception has two solutions, given by $n = 1, 3$. Each of the remaining exceptions has precisely two solutions given by $n = 1, 5$.

The displayed equations corresponding to elements in the families $\mathcal{F}, \mathcal{G}$ and $\mathcal{H}$ in Theorem 2 will be referred as the first set of equations listed in Theorem 2. The remaining equations that are displayed in Theorem 2 will be referred as the second set of equations listed in Theorem 2.

Remarks : (i) We see from Theorem 2 that, except for

$$2x^2 + 1 = 3^n, \tag{5}$$

all the equations corresponding to elements in the family $\mathcal{I}$ have at most one solution in a class. Therefore, the two solutions exhibited of each equation $D_1\, x^2 + 1 = (u^2 - 1)^n$ other than (5) corresponding to family $\mathcal{I}$ lie in different classes. It is also interesting to note that, by Lemma 1 below, there are exactly two classes when $u - 1$ and $u + 1$ are primes or prime powers. In this case, we infer from Theorem 2 that (5) has only the two solutions given by $n = 1$ and $n = 2$.

(ii) We observe that the equation

$$65\, x^2 + 7 = 4 \times 18^n \tag{6}$$

does not appear among our list of exceptional equations, although this has the two solutions $(1, 1)$ and $(341, 5)$. Hence we deduce that these two solutions belong to distinct classes, that 5 divides $\mathrm{h}(-4 \times 65 \times 7)$ and that (6) has no other solution.

(iii) All the solutions of exceptional equations displayed in Theorem 2 have been completely determined. As explained in the course of our proof, some extra work is needed for $x^2 + 19 = 55^n$ and $x^2 + 341 = 377^n$, since 55 and 377 are not primes.

3. Corollaries of the main result

In this section, we display some important corollaries of Theorem 2, and we show how it can be used to solve some Diophantine equations (Corollaries 3, 4, 5 and 6) and to get new results on the divisibility of class numbers of imaginary quadratic fields. For a positive integer m, we write $d(m)$ for the number of positive integers dividing m.

Corollary 1. *Apart from the equations corresponding to elements in the infinite families $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ and the second set of equations listed in Theorem 2, equation (1) has at most $2^{\omega(k)-1}$ solutions.*

Corollary 2. *Apart from the equations corresponding to elements in infinite familites $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ and the second set of equations listed in Theorem 2, the number of solutions of equation (1) with n odd whenever $D_2 = 1$ and $\lambda \in \{1, 2\}$ is bounded by $d(\mathrm{h}(-4D))$ if $D_1 = 1$ or $D_2 = 1$ and by $d(\mathrm{h}(-4D))/2$ otherwise.*

Corollary 2 is good when $d(\mathrm{h}(-4D))$ is small. Suppose that equation (1) does not correspond to an element in $\mathcal{F}, \mathcal{G}$ and $\mathcal{H}$ and it is not among the second set of equations listed in Theorem 2. Then it is clear from the proof of Corollary 2 that it suffices to restrict to only those n which are divisors of $\mathrm{h}(-4D)$ (or $\mathrm{h}(-4D)/2$), according as $D_1 = 1$ or $D_2 = 1$ ($D_1 > 1$, $D_2 > 1$), respectively, and every such n contributes to at most one solution. In particular, equation (1) with $n = p \geq 3$ prime has at most one solution whenever the odd part of $\mathrm{h}(-4D)$ is a power of a prime. Further, we see that $\mathrm{h}(-4D) \geq 5$ whenever $n > 3$ and $D_1 = 1$. Moreover, equation (1) with $D_1 = \lambda = 1$ and $n = 3$ is a well–known equation which has been solved for several values of D_2. Hence we see that Corollary 2 may be applied to find all the solutions of equation (1) for several values of D_1 and D_2 in integers $x \geq 1$, $y > 1$ and $n > 1$. For example, we solve the following generalised Ramanujan–Nagell equation.

Corollary 3. *The only solutions of the equation*

$$x^2 + 7 = 4\,y^n \quad \text{in integers} \quad x \geq 1, y \geq 2, n > 1 \tag{7}$$

are $(x, y, n) \in \{(3, 2, 2), (5, 2, 3), (11, 2, 5), (181, 2, 13)\}$.

In fact, the proof of Corollary 3 applies to find all the solutions of several equations.

Corollary 4. *Let* D_1 *and* D_2 *be positive, coprime, square–free integer such that* $\mathrm{h}(-4D) = 1$ *or is a power of 2. If there is a solution in integers* $x \geq 1$, $y \geq 2$ *and* $p \geq 3$ *prime of the equation*

$$D_1\,x^2 + D_2 = 4\,y^p, \tag{8}$$

then, either

$$(D_1, D_2, p) \in \big\{(1, 7, 3), (1, 7, 5), (1, 7, 13), (1, 11, 5), (1, 19, 5), (1, 19, 7), (1, 341, 5), (3, 5, 3), (3, 5, 7), (13, 3, 7)\big\}$$

or $(D_1, D_2, p) \in \mathcal{F}$ *and* $p = 5$ *or* $(D_1, D_2, P) \in \mathcal{H}$ *and* $p = 3$. *Assume further that* $D_1\,D_2 \not\equiv 7 \pmod 8$. *Then the equation*

$$D_1\,x^2 + D_2 = y^p \tag{9}$$

has no solution in integers $x \geq 1$, $y \geq 2$ *and* $p \geq 3$ *prime, except for* $(D_1, D_2, p) \in \big\{(1, 19, 5), (1, 341, 5)\big\}$ *or* $(D_1, D_2, p) \in \mathcal{F}$ *and* $p = 5$, *or for* $(D_1, D_2, p) \in \mathcal{H}$ *and* $p = 3$.

We observe that the equations covered by Corollary 4 include equations (8) and (9) with

$$(D_1, D_2) \in \big\{(2, 3), (2, 5), (2, 11), (2, 29), (3, 2), (5, 2), (11, 2), (29, 2)\big\}.$$

Further, using Pari, we see that there are 749 positive, square-free integers D less than 10000, such that $\mathrm{h}(-4\,D) = 1$ or is a power of 2. For instance, we are now able to solve easily equation (9) for $D_1 = 1$ and

$$\begin{aligned} D_2 \in \{&2, 5, 6, 10, 13, 14, 17, 21, 22, 30, 33, 34,\\ &37, 41, 42, 46, 57, 58, 62, 65, 66, 69, 70, 73, 77, 78, 82, 85, 93, 94, 97\}, \end{aligned}$$

and we recover some of the results obtained by Cohn [12] (see also the references given there).

Remark : In a subsequent work [10], we will extend a previous work by Cohn [12] and solve many equations $x^2 + D = y^p$, for small positive values of D. When the prime p divides the class number of the quadratic field $\mathbf{Q}(\sqrt{-D})$, we recall that such equation gives rise to Thue equations.

Let Δ be a square–free positive integer and let p be an odd prime not dividing the class number of the quadratic field $\mathbf{Q}(\sqrt{-\Delta})$. Aigner [1] proved that if $p = 3$ or $p > 3$ and $\Delta < 47$, then the equation

$$x^2 + 4\,\Delta = y^p \quad \text{in coprime integers} \quad x, y \geq 1 \tag{10}$$

has no solution other than the ones given by

$$7^2 + 76 = 5^3, \quad 1015^2 + 76 = 101^3, \quad 155^2 + 364 = 29^3 \text{ and } 10681^2 + 364 = 485^3. \tag{11}$$

Further, Le [15] showed that equation (10) has no solution whenever either $p \in \{5, 7\}$ or $p > 3 \times 10^6$. Thanks to Theorem 2, we are now able to solve completely (10).

Corollary 5. *Let Δ be a square–free positive integer and let p be an odd prime not dividing the class number of the quadratic field $\mathbf{Q}(\sqrt{-\Delta})$. Then equation (10) has no solution other than the ones given by (11).*

Remark : A similar argument allows us to recover the result of Lesage [22] on the equation $x^2 + 2^{2n} = y^5$.

Next, we apply Theorem 2 to the following particular case of the equation of Goormaghtigh

$$\frac{x^3-1}{x-1} = \frac{y^n-1}{y-1} \quad \text{in integers } x > 1, y > 1, n > 3. \tag{12}$$

For a survey of results on the equation of Goormaghtigh, we refer to [31, section 3]. We observe that $(x, y, n) = (5, 2, 5)$ and $(90, 2, 13)$ are solutions of (12). Nesterenko and Shorey [27] proved that equation (12) with $x > y$ and odd $n < 25$ has no solution other than $(x, y, n) = (5, 2, 5)$ and $(90, 2, 13)$. The equation (12) also appears in [30]. It has been observed in [29] as an immediate consequence of the result of Nagell on the Ramanujan-Nagell equation that these are the only solutions of (12) with $y = 2$. Further, Le [21] derived from his Theorem L that $(x, y, n) = (5, 2, 5)$ and $(90, 2, 13)$ are the only solutions of (12) with $\omega(y) = 1$. We apply Theorem 2 to obtain the following extension of the preceding result.

Corollary 6. *For an integer $y > 2$, the number of pairs (x, n) satisfying (12) does not exceed $2^{\omega(y)-1} - 1$.*

In the third chapter of [25], Mollin describes some relationships between Diophantine equations and class number of quadratic fields. For example, as a corollary of a more general result, he proves (Theorem 3.1.1) that if $\Delta = b^2 - 4\,m^t < 0$, with $b > 0$, $m > 0$ and t an odd prime, is congruent to 1 modulo 4 and is the discriminant of $\mathbf{Q}(\sqrt{\Delta})$, then, under the hypothesis

$$b \text{ is not the greatest integer equal or less to } 2\,m^{t/2}, \tag{H}$$

the prime t divides the class number of $\mathbf{Q}(\sqrt{\Delta})$. As an application of Theorem 2, we are able to remove the condition (H) in the latter statement, at least when $t \geq 5$. A precise statement is as follows.

Corollary 7. *Let $D \equiv 1 \pmod 4$ be a positive square-free integer such that there exist integers $x \geq 1$, $y \geq 2$ and an odd prime p with $D = y^p - x^2$. Then, either p divides the class number of $\mathbf{Q}(\sqrt{-D})$, or we have*

$$(D, y, p) = (341, 377, 5).$$

Let $D \equiv 7 \pmod 8$ be a positive square-free integer such that there exist integers $x \geq 1$, $y \geq 2$ and an odd prime p with $D = 4\,y^p - x^2$. Then, either p divides the class number of $\mathbf{Q}(\sqrt{-D})$, or we have

$$(D, y, p) \in \{(7, 2, 3), (7, 2, 5), (7, 2, 13)\}.$$

Let $D \equiv 3 \pmod 8$ be a positive square-free integer such that there exist integers $x \geq 1$, $y \geq 2$ and an odd prime $p \geq 5$ with $D = 4\,y^p - x^2$. Then, either p divides the class number of $\mathbf{Q}(\sqrt{-D})$, or we have

$$(D, y, p) \in \{(11, 3, 5), (19, 5, 7)\}.$$

Here, we restrict our attention to the class number of imaginary quadratic fields, but Theorem 2 yields informations on imaginary quadratic orders, as well.

4. Auxiliary results

The classical approach for dealing with our problem rests on the explicit determination of the solutions of the equations

$$D_1\,X^2 + D_2\,Y^2 = k^Z, \quad X, Y, Z \in \mathbf{Z}, \ \gcd(X, Y) = 1, \quad Z > 0. \tag{13}$$

This question is connected with the theory of binary quadratic forms and it was considered by Bender & Herzberg [4]. By definition, for a, b, $c \in \mathbf{Z}$, the discriminant of the form $aX^2+2\,b\,XY+cY^2$ is $4D=4b^2-4ac$, thus $-4D$ is the discriminant of $D_1\,X^2+D_2\,Y^2$. The set of positive binary quadratic forms of discriminant $-4D$ is partitioned into a finite number of equivalence classes which we denote by $\mathrm{h}(-4D)$.

We recall from [25, chapter 1.5] some facts about the theory of quadratic orders. Let D_0 be a square–free integer and set $\sigma_0=1$ if $D_0 \not\equiv 1 \pmod 4$ and $\sigma_0=2$ otherwise. Then, $\Delta := 4\,D_0/\sigma_0^2$ is the discriminant of the quadratic field $\mathbf{Q}(\sqrt{D_0})$. We observe that the ring of integers $\mathbf{Z}_{D_0}$ in $\mathbf{Q}(\sqrt{D_0})$ is generated over $\mathbf{Z}$ by $w_{\Delta_0} := (\sigma_0-1+\sqrt{D})/\sigma_0$. Let f_Δ be a positive integer, and set $\Delta = f_\Delta^2\,\Delta_0$. Then Δ is the discriminant of the quadratic order O_Δ in $\mathbf{Q}(\sqrt{D_0})$ generated over $\mathbf{Z}$ by $w_\Delta := f_\Delta\,w_{\Delta_0}$. Since f_Δ is the index of O_Δ in $\mathbf{Z}_{D_0}$, we observe that there is a one–to–one correspondence between non–square integers congruent to 0 or 1 modulo 4 and orders in quadratic fields. Further, the set $I(\Delta)$ of proper fractional ideals in the order O_Δ is a group under multiplication. We denote by $P(\Delta)$ its sub–group composed by the principal ideals. The class number h_Δ of O_Δ is by definition the order of the quotient group $I(\Delta)/P(\Delta)$.

Proposition 1 below sums up basic statements of the theory of binary quadratic forms.

Proposition 1. *Let D be a positive integer. We have*

$$\mathrm{h}(-4D) < \frac{4\sqrt{D}}{\pi}\,\log(2e\sqrt{D}).$$

Further, $\mathrm{h}(-4D)$ is equal to the class number of the unique quadratic order of discriminant $-4D$.

Proof : The upper bound for $\mathrm{h}(-4D)$ follows from Theorems 11.4.3, 12.10.1 and 12.14.3 of Hua [14], while the last assertion is contained in Definition 5.2.7 of [11]. □

We consider a more general equation than (13) in the next result and we suppose that it has a solution.

Lemma 1. *(a) Let $D_1D_2 \notin \{1,3\}$. The solutions of equation*

$$D_1\,X^2+D_2\,Y^2=\lambda^2\,k^Z,\quad X,Y,Z\in\mathbf{Z},\ \gcd(X,Y)=1,\quad Z>0 \tag{14}$$

can be put into at most $2^{\omega(k)-1}$ classes. Further, in each such class $\mathcal{S}$, there is a unique solution (X_1,Y_1,Z_1) such that $X_1>0$, $Y_1>0$ and Z_1 is minimal among the solutions of $\mathcal{S}$. This minimal solution satisfies Z_1 divides $\mathrm{h}(-4D)$ if $D_1=1$ or $D_2=1$ and $2\,Z_1$ divides $\mathrm{h}(-4D)$ otherwise. Moreover, every solution (X,Y,Z) of (14) belonging to $\mathcal{S}$ can be expressed as

$$Z=Z_1\,t,\quad \left(\frac{X\sqrt{D_1}+Y\sqrt{-D_2}}{\lambda}\right)=\lambda_1\left(\frac{X_1\sqrt{D_1}+\lambda_2\,Y_1\sqrt{-D_2}}{\lambda}\right)^t \tag{15}$$

where $t\ge 1$ is an integer, $\lambda_1\in\{-1,1,-i,i\}$ and $\lambda_2\in\{-1,1\}$. If $\lambda=2^{1/2}$, then t is odd. Further $\lambda_1\in\{-1,1\}$ if $D_2\neq 1$ or t is odd and $\lambda_1\in\{-i,i\}$ if $D_2=1$ and t is even.
(b) Let $D_1D_2\in\{1,3\}$. Then the solutions of (14) can be put into at most $2^{\omega(k)-1}$ classes. Further, in each such class $\mathcal{S}$, there is a unique solution $(X_1,Y_1,1)$ with $X_1>0$, $Y_1>0$ such that every solution (X,Y,Z) of (14) belonging to $\mathcal{S}$ satisfies (15) with $Z_1=1$, $\lambda_1\in\{-1,1,-i,i,1+i,1-i\}$ if $D_1D_2=1$, $\lambda_1\in\left\{-1,1,-i,i,\frac{1+i\sqrt{3}}{2},\frac{1-i\sqrt{3}}{2},\frac{-1+i\sqrt{3}}{2},\frac{-1-i\sqrt{3}}{2}\right\}$ if $D_1D_2=3$ and $\lambda_2\in\{-1,1\}$.

Remark : Since a solution of (1) is also a solution of (14), we see that the solutions of (1) can be put into $2^{\omega(k)-1}$ classes as remarked in section 1.

Proof of Lemma 1 : If $\lambda=\lambda'$, this is a particular case of Theorems 2 and 3 of Le [19]. For other values of λ, the proof is similar. We need to make some changes only in the proofs of Lemmas 2 and 5 of Le [19]. We should change the definition of λ' of its Lemma 2 as $\lambda'=1$ if (our) $\lambda=1$, $\lambda'=1$ if $\lambda=2^{1/2}$ and $\lambda'=2$ if $\lambda=2$. For the proofs of these lemmas for the remaining values of λ, we should observe that D is odd whenever $\lambda\neq 1$ (see Theorems 1, 2 and 4 of [4] and Lemma 8 of Le [21]). Let $\lambda=2^{1/2}$. We show that t is odd. Assume the contrary, hence that t is even. If $\lambda\in\{-1,1\}$, we compare the real parts on both the sides of the second relation in (13) to derive that $D_1 = 2$ which is a contradiction. If $\lambda \in \{-i, i\}$, we compare the imaginary parts on both the sides of (15) to observe that D_2 is twice of a square and this is a contradiction. $\square$

The next lemma proves the assertion of Theorem 2 whenever $D_1D_2 \in \{1, 3\}$.

Lemma 2. *Let $D_1D_2 \in \{1, 3\}$. Apart from the equations*

$$x^2 + 1 = 2 \times 5^n,$$

$$x^2 + 1 = 2 \times 13^n$$

and

$$x^2 + 3 = 4 \times 7^n,$$

there is at most one solution of equation (1) in any class. The solutions of the exceptional equations are given by $n = 1, 2$, $n = 1, 4$ and $n = 1, 3$ respectively.

Proof : We have to consider the nine cases given by $(D_1, D_2) \in \{(1, 1), (1, 3), (3, 1)\}$ and $\lambda \in \{1, \sqrt{2}, 2\}$. Rather than (1), we prefer to deal with equations $D_1x^2 + D_2 = \lambda^2 y^n$ in integer variables $x \geq 1$, $y > 1$ and $n \geq 2$ such that $\lambda = 2$ if y is even. In fact, we will prove a stronger result than Lemma 2. Moreover, in some cases, we encounter equations of the shape $f(x) = ay^2$, with a an integer and f a polynomial of degree 3 or 4. All of these have been kindly solved by Guillaume Hanrot, using the programm of John Cremona (the curves defined below by (E_2), (E_3) and by the equation $3x^2 + 1 = 4y^3$ are all of genus zero), the computer package PARI, and the algorithm of Bilu & Hanrot described in [8].

Regarding $x^2 + 1 = 4y^n$, $x^2 + 3 = 2y^n$ and $3x^2 + 1 = 2y^n$ modulo 4, we conclude that these equations have no solutions, since in the last two ones, y is assumed to be odd.

Equations $x^2 + 1 = y^n$ and $x^2 + 3 = y^n$ with $n \geq 3$ have no solution. The result on the first equation dates back to V. A. Lebesgue (see [28], page 78) and on the second one is due to Cohn [12]. Further, it is easy to see that the systems of equations $x^2 + 1 = y$, $z^2 + 1 = y^2$ and $x^2 + 3 = y$, $z^2 + 3 = y^2$ have no solution.

Setting $x = 2z + 1$, the equation $x^2 + 3 = 4y^n$ is equivalent to $z^2 + z + 1 = y^n$, which, by results of Ljunggren and Nagell (see [28], page 117) has only one solution with $n \geq 3$, namely $18^2 + 18 + 1 = 7^3$. Further, the equation $x^2 + 3 = 4y^2 = (2y)^2$ has only the solution $(x, y) = (1, 1)$. Hence, we see that for a given $y > 1$, the equation $x^2 + 3 = 4y^n$ has at most one solution with $n \geq 1$, except $x^2 + 3 = 4 \times 7^n$, which has two solutions given by $n = 1, 3$.

Störmer (see [28], page 90) proved that $x^2 + 1 = 2y^n$ has no solution with $n > 1$ odd and $y > 1$. Further, Ljunggren (see [28], page 141) showed that $x^2 + 1 = 2y^4$ has only one solution with $y > 1$, namely $y = 13$, and we conclude that $x^2 + 1 = 2 \times 13^n$ has only two solutions given by $n = 1, 4$. Thus, it remains us to consider the system of equations $x^2 + 1 = 2y$, $z^2 + 1 = 2y^2$, which leads to the elliptic equation (E_1) $2z^2 = x^4 + 2x^2 - 1$. The latter has only the two solutions $(z, x) = (1, 1)$ and $(7, 3)$, hence the above system has a solution only for $y = 1$ and $y = 5$.

Ljunggren ([23] for odd $n > 1$) and Bennett & Walsh ([5, Theorem 1.2] for $n = 4$) proved that $3x^2 + 1 = 4y^n$ has no solution with $y > 1$ and $n \geq 3$. However, we may outline an alternative proof of Ljunggren's result when $n \geq 5$ is prime. In this case, we can rewrite our equation under the form $\left(\frac{1-ix\sqrt{3}}{2}\right)\left(\frac{1+ix\sqrt{3}}{2}\right) = y^n$. Since $\frac{1-ix\sqrt{3}}{2}$ and $\frac{1-ix\sqrt{3}}{2}$ are coprime, we deduce that there exist in $\mathbf{Q}(\sqrt{-3})$ a root of unity μ and an algebraic integer ε' such that $\frac{1-ix\sqrt{3}}{2} = \mu\varepsilon'^n$. Since the order of μ and n are coprime, there exists an algebraic integer $\varepsilon \in \mathbf{Q}(\sqrt{-3})$ such that $\mu\varepsilon'^n = \varepsilon^n$. Hence we have $\varepsilon^n + \overline{\varepsilon}^n = 1$, and we conclude by applying Theorem BHV below, exactly as in the last part of the proof of Theorem 2. We solve the equation (E_2) $Z^2 = 3X^4 + 2X^2 - 1$ to conclude that the system of equations $3x^2 + 1 = 4y$, $3z^2 + 1 = 4y^2$ has no solution with $y > 1$. Finally, we solve our equation with $n = 3$.

It remains us to consider $3x^2 + 1 = y^n$. Let n be divisible by an odd prime $q \geq 5$ and write $Y^q = y^n$. Then $3x^2 = (Y - 1) \times \frac{Y^q - 1}{Y - 1}$ and we conclude that $\frac{Y^q-1}{Y-1}$ is a square. This is excluded by the results of Nagell and Ljunggren (see [28], page 111). Further, the elliptic equation (E_3) $3x^2 + 1 = y^3$ has no solution, and, writing $3x^2+1=y^4$ under the form $(y^2-1)(y^2+1)=3x^2$, we observe that the latter equation has no solution. Thus either $n=1$ or $n=2$, and it remains only to consider the case of the system $3x^2+1=y$, $3z^2+1=y^2$. Eliminating y between the two equations, we get $z^2=x^2(3x^2+2)$, which is not possible since 2 is not a quadratic residue modulo 3.

By Lemma 1 (b), we see that there is only one class for each of the equations listed in Lemma 2. Therefore these equations have no solution other than the ones determined above. $\square$

Lemma 3. *Let (F_k) and (L_k) be the Fibonacci and the Lucas sequences defined in Section 2. For any integer $k \geq 2$ and any $\varepsilon \in \{\pm 1\}$, we have*

$$4F_k - F_{k+2\varepsilon} = L_{k-\varepsilon} \tag{16}$$

and

$$4L_k - L_{k+2\varepsilon} = 5F_{k-\varepsilon}. \tag{17}$$

Further, for any integer $k \geq 4$, we have

$$F_{k+2}\left(\frac{9F_{2k-1} - F_{2k-7} + (-1)^{k-1}\cdot 6}{10}\right)^2 + L_{k-1} = 4\,F_k^5 \tag{18}$$

and

$$F_{k-2}\left(\frac{9F_{2k+1} - F_{2k-5} + (-1)^{k}\cdot 6}{10}\right)^2 + L_{k+1} = 4\,F_k^5. \tag{19}$$

Proof : Fix $\varepsilon \in \{\pm 1\}$. Both the sides of (16) (*resp.* (17)) are binary linear recurring sequences with roots $\theta := (1+\sqrt{5})/2$ and $\overline{\theta} := (1-\sqrt{5})/2$. We check that they are equal for three consecutive values of k, whence we conclude that (16) (*resp.* (17)) is true for all integers k.

The same argument applies for (18) and (19). Indeed, we have here recurring sequences of order 6, with roots θ, $\overline{\theta}$, θ^3, $\overline{\theta}^3$, θ^5 and $\overline{\theta}^5$, and we easily check that (18) and (19) are true for $k \in \{1, \ldots 7\}$. $\square$

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

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

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

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

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

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

Let (α, β) be a Lucas (respectively Lehmer) pair. We recall that a prime number p is a *primitive divisor* of the Lucas number $u_n(\alpha, \beta)$ if p divides u_n but does not divide $(\alpha-\beta)^2 u_1 \cdots u_{n-1}$. Similarly, a prime number p is a *primitive divisor* of the Lehmer number $\tilde{u}_n(\alpha, \beta)$ if p divides $\tilde{u}_n$ but does not divide $(\alpha^2-\beta^2)^2 \tilde{u}_1 \cdots \tilde{u}_{n-1}$. We say that a Lucas sequence (respectively Lehmer sequence) is an $n-$defective Lucas sequence (respectively Lehmer sequence) if $u_n(\alpha, \beta)$ (respectively $\tilde{u}_n(\alpha, \beta)$) has no primitive divisor.

The key argument for our proof is the definitive result obtained by Bilu, Hanrot & Voutier [9].

Theorem BHV. *For any integer $n > 30$, every Lucas sequence and every Lehmer sequence is non n-defective. Further, for any positive integer $n \leq 30$, all n-defective Lucas sequence and all n-defective Lehmer sequence are explicitely determined.*

We do not state the precise classification of all n-defective Lucas and Lehmer sequences, we refer the reader to [9]. In the course of our proof, we will quote the corresponding results form [9]. We should add that for most integers $n \leq 30$ Voutier [32] has given previously a complete list of n-defective Lucas sequences and Lehmer sequences.

5. Proofs

Proof of Theorem 2 : Let (D_1, D_2, k) be given. There is no loss of generality in assuming that D_1 is square-free. By Lemma 2, we may suppose that $D_1D_2 \notin \{1, 3\}$. Assume that a class of solutions of (1) is non-empty and denote by (x_1, n_1) the solution with n_1 least. Then, let (x, n) be a solution in the same class such that there is no solution (r, s) with $n_1 < s < n$ and let also (X_1, Y_1, Z_1) be the least solution in the corresponding class of (14).

First, we consider the case that $D_2 > 1$. Then we see from Lemma 1 that

$$n_1 = Z_1 t', \quad \frac{x_1\sqrt{D_1} + \sqrt{-D_2}}{\lambda} = \lambda_1 \left(\frac{X_1\sqrt{D_1} + \lambda_2 Y_1\sqrt{-D_2}}{\lambda} \right)^{t'}$$

where t' is a positive integer and $\lambda_1, \lambda_2 \in \{-1, 1\}$. Let $t' = 2t_1$. We write

$$\frac{X_{t_1}\sqrt{D_1} + Y_{t_1}\sqrt{-D_2}}{\lambda} = \left(\frac{X_1\sqrt{D_1} + \lambda_2 Y_1\sqrt{-D_2}}{\lambda} \right)^{t_1}$$

and we obtain

$$\frac{x_1\sqrt{D_1} + \sqrt{-D_2}}{\lambda} = \lambda_1 \left(\frac{X_{t_1}^2 D_1 - Y_{t_1}^2 D_2 + 2X_{t_1}Y_{t_1}\sqrt{-D_1D_2}}{\lambda^2} \right).$$

Equating the coefficients of $\sqrt{-D_2}$ on both the sides, we get $\lambda = \pm 2X_{t_1}Y_{t_1}\sqrt{D_1}$, which implies that $D_1 = 1$, $\lambda = 2$ and $D_2 = 4k^r - 1$ for an integer $r \geq 1$. Hence $(D_1, D_2, k) = (1, 4k^r - 1, k)$ and $(X_1, Y_1, Z_1) = (1, 1, k^r)$. If t' is odd, we argue as in Le [20, p. 102] to observe that $Y_1 = 1$, and we see from Lemma 1 that $(X_1, Y_1, Z_1) = (x_1, 1, n_1)$. We apply again Lemma 1 to derive that

$$n = n_1 t, \quad \frac{x\sqrt{D_1} + \sqrt{-D_2}}{\lambda} = \lambda_1 \left(\frac{x_1\sqrt{D_1} + \lambda_2\sqrt{-D_2}}{\lambda} \right)^{t} \tag{20}$$

where $t > 1$ is an integer and $\lambda_1, \lambda_2 \in \{-1, 1\}$. If t is even, we argue as above to see that $t = 2$ and $(D_1, D_2, k) \in \mathcal{G}$. Now we suppose that t is odd. Let $t = t_2t_3$ where $t_2 > 1$ and $t_3 > 1$ are odd integers. Then we write

$$\frac{x\sqrt{D_1} + \sqrt{-D_2}}{\lambda} = \lambda_1 \left(\frac{X_2\sqrt{D_1} + Y_2\sqrt{-D_2}}{\lambda} \right)^{t_3}$$

where

$$\frac{X_2\sqrt{D_1} + Y_2\sqrt{-D_2}}{\lambda} = \left(\frac{x_1\sqrt{D_1} + \lambda_2\sqrt{-D_2}}{\lambda} \right)^{t_2}.$$

Then $|Y_2| = 1$ and $(|X_2|, n_1t_2)$ is a solution of (1). This is not possible since $n_1 < n_1t_2 < n$. Hence we conclude that t is prime.

We put

$$\varepsilon = \frac{x_1\sqrt{D_1} + \lambda_2\sqrt{-D_2}}{\lambda}, \; \overline{\varepsilon} = \frac{x_1\sqrt{D_1} - \lambda_2\sqrt{-D_2}}{\lambda}.$$

Then we see from (20) that

$$\left|\frac{\varepsilon^t - \overline{\varepsilon}^t}{\varepsilon - \overline{\varepsilon}}\right| = 1. \tag{21}$$

The numbers

$$u_t := \frac{\varepsilon^t - \overline{\varepsilon}^t}{\varepsilon - \overline{\varepsilon}}$$

are terms of a Lucas sequence if $D_1 = 1$ and of a Lehmer sequence otherwise. Further, with the terminology of Section 4, we observe that (21) implies that u_t is t-defective. By Theorem BHV, we know that the pair $(\varepsilon, \overline{\varepsilon})$ belong to a completely determined set and it remains to treat each element of this set. More precisely, Tables 1 and 3 of [9] list the integers n and the pairs (a, b) such that the Lucas number $v_n\left((a-\sqrt{b})/2, (a+\sqrt{b})/2\right)$ has no primitive divisor, which is a necessary condition for (21) to be satisfied. Say differently, if (21) is satisfied, it implies that for such a pair (a, b) with $b < 0$, we have $\varepsilon = (a - \sqrt{b})/2$. Since $\varepsilon\overline{\varepsilon} = (a^2 - b)/4$, the corresponding equation is $X^2 - b = 4\left((a^2-b)/4\right)^Z$ and it has at least two solutions given by $Z = 1$ and $Z = t$. Thus, we have to check all such pairs.

Similarly, Tables 2 and 4 of [9] list the integers n and the pairs (a, b) such that the Lehmer number $v_n\left((\sqrt{a}-\sqrt{b})/2, (\sqrt{a}+\sqrt{b})/2\right)$ has no primitive divisor. Recalling that we are only concerned with $a > 0$ and $b < 0$, this gives rise to the equation $a\,X^2 - b = 4\left((a-b)/4\right)^Z$ which has at least two solutions given by $Z = 1$ and $Z = t$. Further, the corresponding Lehmer sequence is given by induction by $v_0 = 0$, $v_1 = 1$, $v_k = \sqrt{a}v_{k-1} - (a-b)v_k/4$ if $k \geq 2$ is odd, and $v_k = \left(\sqrt{a}v_{k-1} - (a-b)v_k/4\right)/\sqrt{a}$ if $k \geq 2$ is even.

If $t = 3$, we equate the coefficients of $\sqrt{-D_2}$ on both the sides of (20) to obtain $3D_1x_1^2 - D_2 = \pm\lambda^2$ and $(D_1, D_2, k) \in \mathcal{H}$.

If $t = 5$, then we have to apply Theorem BHV, and we deduce another infinite family given by Table 4. However, if we restrict ourselves to the case $D_1 = 1$, then we have to quote their Table 1. Hence, we have only four equations with more than one solution (recall that D_2 is assumed to be odd when $\lambda = 2$):

$$x^2 + 7 = 4 \times 2^n,$$

$$x^2 + 11 = 4 \times 3^n,$$

$$x^2 + 19 = 55^n,$$

and

$$x^2 + 341 = 377^n.$$

We continue with Table 1. We see that there are no more equations with strictly more than one solution other than

$$x^2 + 19 = 4 \times 5^n.$$

Next, we turn to the case $D_1 > 1$. In view of what is already done, it remains to consider only the cases

$$t \in \{5, 7\}.$$

By Table 2 of [9], we see that for $t = 7$, we have only three equations with more than one solution, namely

$$3x^2 + 5 = 4 \times 2^n,$$

$$13x^2 + 3 = 4 \times 4^n$$

and

$$7x^2 + 11 = 2 \times 9^n.$$

Now, we deal with the case $t = 5$. Recall that we have denoted by (F_k) (*resp.* by (L_k)) the Fibonacci (*resp.* the Lucas) sequence defined by $F_0 = 0$, $F_1 = 1$ 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 $k \geq 2$). According to our discussion above, to Table 4 of [9] and to (14) and (15), the equation

$$D_1 x^2 + D_2 = 4\left(\frac{D_1 + D_2}{4}\right)^n$$

has solutions with $n = 1$ and $n = 5$ only if $(D_1, D_2) = (F_{k-2\varepsilon}, L_{k+\varepsilon})$ for $\varepsilon \in \{\pm 1\}$ and $k \geq 3$, or if $(D_1, D_2) = (L_{k-2\varepsilon}, 5F_{k+\varepsilon})$ for $\varepsilon \in \{\pm 1\}$ and $k \geq 2$ or $k = 0$. In the latter case, we observe that 5 divides D_2, hence, we see that 5 divides the corresponding quotient $(\varepsilon^5 - \overline{\varepsilon}^5)/(\varepsilon - \overline{\varepsilon})$, thus equation (21) cannot be satisfied.

As for the first case, which corresponds to elements of our family $\mathcal{H}$, we infer from Lemma 3 that, for $k \geq 3$, the equation

$$F_{k+2}\, x^2 + L_{k-1} = 4\, F_k^n \qquad \text{in integers } x \geq 1,\ n \geq 1 \tag{22}$$

has two solutions, given by $(x, n) = (1, 1)$ and $(x, n) = \big((9F_{2k-1} - F_{2k-7} + (-1)^{k-1} \cdot 6)/10, 5\big)$. Likewise, for $k \geq 3$, the equation

$$F_{k-2}\, x^2 + L_{k+1} = 4\, F_k^n \qquad \text{in integers } x \geq 1,\ n \geq 1 \tag{23}$$

has two solutions, given by $(x, n) = (1, 1)$ and $(x, n) = \big((9F_{2k+1} - F_{2k-5} + (-1)^k \cdot 6)/10, 5\big)$. Further, in case of equation (22), for $k \equiv 1 \pmod 6$, we see that $\gcd(F_{k+2}, L_{k-1}) = 2$, while, for $k \equiv 4 \pmod 6$, we observe that $\gcd(F_{k+2}, L_{k-1}) = 4$ since F_k is odd whenever $k \equiv 1, 4 \pmod 6$. Hence, $k \not\equiv 1, 4 \pmod 6$ leads to an equation of type (3) and $k \equiv 1 \pmod 6$ (*resp.* $k \equiv 4 \pmod 6$) yields an equation of type (4) (*resp.* (2)). Likewise, in case of equation (23), $k \not\equiv 2, 5 \pmod 6$ leads to an equation of type (3) and $k \equiv 5 \pmod 6$ (*resp.* $k \equiv 2 \pmod 6$) yields an equation of type (4) (*resp.* (2)).

The assertion for the first set of equations listed in Theorem 2 follows from Theorem L. This is also the case for the second set of equations listed in Theorem 2 other than the third and the fourth ones. For each of these equations, there are two classes of solutions. Further, we have proved that each of these two equations has a class where the solutions are given by $n = 1, 5$. Finally, using Pari, we get that $\mathrm{h}(-4 \times 55) = 4$ and $\mathrm{h}(-4 \times 377) = 16$, hence, by a similar argument as in the proof of Corollary 4, there is no solution in the other class. Thus we may suppose that equation (1) is different from the equations displayed in the statement of Theorem 2. It is clear from our proof that equation (1) has at most one solution in every class if it does not correspond to an element in one of the infinite families $\mathcal{F}, \mathcal{G}$ and $\mathcal{H}$. Now it remains to show that each of the equations corresponding to the families $\mathcal{F}, \mathcal{G}$ and $\mathcal{H}$ has at most 2 solutions in one class and has at most one solution in any other class. Suppose that $(D_1, D_2, k) \in \mathcal{F} \cup \mathcal{G} \cup \mathcal{H}$ with at least three distinct solutions in a class with (X_1, Y_1, Z_1) as the minimal solution of (12). Then we argue as in Le [18, Lemma 4] to conclude that it has two distinct solutions (r_1, s_1) and (r_2, s_2) such that

$$s_1 = Z_1 t_4\ ,\ \ s_2 = Z_1 t_5$$

where either t_4, t_5 are distinct odd primes and

$$\left| \frac{\varepsilon^{t_i} - \overline{\varepsilon}^{t_i}}{\varepsilon - \overline{\varepsilon}} \right| = 1 \ \text{ for } i = 4, 5 \tag{24}$$

or $(D_1, D_2, k) \in \mathcal{G}, s_1 = 2, s_2 = 4$. The latter possibility is excluded plainly and we apply again Theorem BHV as earlier to each of the relations (24) to arrive at a contradiction. It is also clear from our application of Theorem BHV that there is only one class given in section 2 where equation (1) has two solutions and it has at most one solution in all other classes. This completes the proof of Theorem 2 with $D_2 > 1$.

Now, we turn to the case $D_2 = 1$ and $D_1 > 1$. We derive from Lemma 1 that ther exist positive integers t_6, t_6' with $t_6 > t_6'$,

$$n = Z_1 t_6, \quad n_1 = Z_1 t_6'$$

and

$$\frac{x\sqrt{D_1} + \sqrt{-1}}{\lambda} = \lambda_1 \left(\frac{X_1\sqrt{D_1} + \lambda_2 Y_1 \sqrt{-1}}{\lambda} \right)^{t_6}, \tag{25}$$

$$\frac{x_1\sqrt{D_1}+\sqrt{-1}}{\lambda}=\lambda_1'\left(\frac{X_1\sqrt{D_1}+\lambda_2'Y_1\sqrt{-1}}{\lambda}\right)^{t_6'}, \tag{26}$$

where $\lambda_1,\lambda_1'\in\{-1,1,-i,i\}$ and $\lambda_2,\lambda_2'\in\{-1,1\}$. If both $\lambda_1,\lambda_1'\in\{-1,1\}$, we proceed as in the case $D_2>1$ to conclude the assertion of Theorem 1. Suppose that exactly one of λ_1 and λ_1' is an element of $\{-1,1\}$. Then we derive that $Y_1=1$ and $(x_1,n_1)=(X_1,Z_1)$. Therefore $\lambda_1'\in\{-1,1\}$ and $\lambda_1\in\{-i,i\}$. Now we see from Lemma 1 that t_6 is even and $\lambda\neq 2^{1/2}$. By putting

$$\varepsilon_1=\frac{x_1\sqrt{D_1}+\lambda_2\sqrt{-1}}{\lambda},\quad \overline{\varepsilon}_1=\frac{x_1\sqrt{D_1}-\lambda_2\sqrt{-1}}{\lambda},$$

we see from (25) that

$$\mid\varepsilon_1^{t_6}+\overline{\varepsilon}_1^{t_6}\mid=\frac{2}{\lambda}. \tag{27}$$

Now we see from (27) that $t_6=2$ implies that $\lambda=1$ and $(D_1,D_2,k)=(2,1,3)$ and we derive from Theorem L that the corresponding equation (1) has precisely two solutions given by $n=1,2$. Therefore, we may suppose that $t_6>2$. Further, we observe that

$$\frac{\varepsilon_1^{2t_6}-\overline{\varepsilon}_1^{2t_6}}{\varepsilon_1^2-\overline{\varepsilon}_1^2}=(\varepsilon_1^{t_6}+\overline{\varepsilon}_1^{t_6})\left(\frac{\varepsilon_1^{t_6}-\overline{\varepsilon}_1^{t_6}}{\varepsilon_1^2-\overline{\varepsilon}_1^2}\right)$$

has no primitive divisor. Indeed, $(\varepsilon_1^{2t_6}-\overline{\varepsilon}_1^{2t_6})/(\varepsilon_1^2-\overline{\varepsilon}_1^2)$ and $(\varepsilon_1^{t_6}-\overline{\varepsilon}_1^{t_6})/(\varepsilon_1^2-\overline{\varepsilon}_1^2)$ belong to the same Lehmer sequence, and, in view of (24), the only possible primitive divisor of $(\varepsilon_1^{2t_6}-\overline{\varepsilon}_1^{2t_6})/(\varepsilon_1^2-\overline{\varepsilon}_1^2)$ is 2 and this can occur only when $\lambda=1$. But in that case, we see that 2 divides $\varepsilon_1^2+\overline{\varepsilon}_1^2$, which is also an element of the same Lehmer sequence. Now we apply [9] to conclude $t_6\in\{4,6,12\}$. The case $t_6=4$ implies that $\lambda=2$ and $(D_1,D_2,k)=(7,1,2)$ and we see from Theorem L that the corresponding equation (1) has precisely two solutions given by $n=1,4$. Further, $t_6=6$ and $t_6=12$ are not possible by (27). Finally, we consider the case that (25) and (26) are valid with $\lambda_1,\lambda_1'\in\{-i,i\}$. Then we see from Lemma 1 that t_6 and t_6' are even positive integers satisfying

$$\mid\varepsilon_2^{t_6}+\overline{\varepsilon}_2^{t_6}\mid=\frac{2}{\lambda} \tag{28}$$

and

$$\mid\varepsilon_2^{t_6'}+\overline{\varepsilon}_2^{t_6'}\mid=\frac{2}{\lambda} \tag{29}$$

where

$$\varepsilon_2=\frac{X_1\sqrt{D_1}+\lambda_2Y_1\sqrt{-1}}{\lambda},\quad \overline{\varepsilon}_2=\frac{X_1\sqrt{D_1}-\lambda_2Y_1\sqrt{-1}}{\lambda}.$$

As earlier,we see that $\lambda\neq 2^{1/2}$. Now we apply [9] as in the preceding argument to derive that $t_6\in\{4,6,12\}$ and $t_6'\in\{2,4,6\}$. The possibilities $t_6=6,12$ are excluded by (28). Thus it remains to consider only $(t_6',t_6)=(2,4)$, which is excluded again by (28) and (29). □

Proof of Corollary 2 : Consider all the classes with the least solution (X,Y,Z) with $Z=Z_0$. Arrange them as

$$(X_1,Y_1,Z_0),(X_2,Y_2,Z_0),\ldots \text{with } Y_1\leq Y_2\leq\ldots. \tag{30}$$

Observe that $Y_1<Y_2<Y_3<\ldots$. Let us consider the class with the least solution (X_2,Y_2,Z_0). Suppose that the equation has a solution (X,Z) in this class. Then (15) is valid with $Z_1=Z_0, Y=1, X_1=X_2$ and $Y_1=Y_2$. Further, we see from Lemma 1 that (15) holds with $\lambda_1\in\{-1,1\}$ since n is odd if $D_2=1$ and $\lambda\in\{1,2\}$. Then we conclude, as in the proof of Theorem 2, that t is odd and $Y_2=1$. This is a contradiction. Therefore this class has no solution. This is also the case with the classes (X_3,Y_3,Z_0), $(X_4,Y_4,Z_0),\ldots$ Thus among all the classes with the least solutions as (30), the equation has at most one solution which lie in the class with the least solution (X_1,Y_1,Z_0). The number of possibilities for Z_0 is $d(\mathrm{h}(-4D))$ if $D_1=1$ or $D_2=1$ and $d(\mathrm{h}(-4D))/2$ otherwise. Hence the equation has at most $d(\mathrm{h}(-4D))$ solutions if $D_1=1$ or $D_2=1$ and $d(\mathrm{h}(-4D))/2$ otherwise. □

Proof of Corollary 3 : If $y = 2$, the assertion follows from the theorem of Nagell stated in section 1 on Ramanujan–Nagell equation . Thus we may suppose that $y \geq 3$. It suffices to show that (7) has no solution in integers $x \geq 1$ and $n > 1$. Let $x \geq 1$ and $n > 1$ be integers satisfying (7). Let (X_0, Y_0, Z_0) be the minimal solution of the class containing $(x, 1, n)$. Then we argue as in the proof of Corollary 2 to derive from Lemma 1 that $Y_0 = 1$. Since $\mathrm{h}(-28) = 1$ (see [14], page 316, or [11], Appendix B.1), we again apply Lemma 1 to see that $Z_0 = 1$. Finally we see from Corollary 2 and $\mathrm{h}(-28) = 1$ that $x = X_0$ and $n = Z_0 = 1$. This is a contradiction. $\square$

Proof of Corollary 4 : For a positive integer $D \not\equiv 7 \pmod 8$ with $\mathrm{h}(-4D)$ equals to 1 or to a power of 2, we work modulo 8 to see that $D_1 x^2 + D_2 = y^p$ has no solution when p is an odd prime and y is even. Further, with the notation of Corollary 3 and by the argument used in its proof, we claim that Z_0 is either 1 or a power of 2. Finally, we apply Theorem 2 to conclude the proof of Corollary 4. $\square$

Proof of Corollary 5 : Let Δ and p be as in the statement of Corollary 5. Recalling the results of Aigner and Le given just before the statement of Corollary 5,we may assume that $p \geq 11$. Form the remark (1.5.9) of [25, page 25], we claim that $\mathrm{h}(-16\,\Delta)$ is equal to 2 or 6 times the class number of $\mathbf{Q}(\sqrt{-\Delta})$, thus p does not divide $\mathrm{h}(-16\,\Delta)$. Assume that x and y are positive integers satisfying (10). Then we observe that $y > 1$ and we consider equation

$$X^2 + 4\,\Delta = y^n,$$

in integers $x \geq 1$ and $n \geq 1$. We consider a class of solutions of this equation containing (x, p). By Theorem 2, this class has no other solution. Therefore, we see from Lemma 1 that p divides $\mathrm{h}(-16\,\Delta)$. This is a contradiction and the corollary is proved. $\square$

Proof of Corollary 6 : Suppose that $x > 1, y > 2$ and $n > 3$ are integers satisfying (12). We re-write (12) as

$$(y-1)(2x+1)^2 + (3y+1) = 4y^n. \tag{31}$$

We divide both the sides of (31) by $\delta = 4$ or $\delta = 2$ according as $y \equiv 1 \pmod 4$ or $y \equiv 3 \pmod 4$, respectively. Further we put $\delta = 1$ if y is even. We observe that the triple $(D_1, D_2, k) = (\frac{y-1}{\delta}, \frac{3y+1}{\delta}, y)$ belongs to $\mathcal{H}$. Now we apply Theorem 2 to conclude that (31) has at most $2^{\omega(y)-1} + 1$ solutions in integers $x \geq 0$ and $n \geq 1$. On the other hand, we observe that $(x, n) = (0, 1)$ and $(x, n) = (y, 3)$ are solutions of (31), but not of (12) since n is assumed > 3 in that equation. The corollary is thus proved. $\square$

Proof of Corollary 7 : Let $D \equiv 1 \pmod 4$ be a square–free positive integer. Under the hypothesis of the theorem, there exists an odd integer $y \geq 2$ such that the equation

$$X^2 + D = y^n \tag{32}$$

has a solution (X, n) with $n = p$. We consider the class containing this solution. If this is the minimal solution of the class, we infer from Lemma 1 that p divides $\mathrm{h}(-4D)$, which, by Proposition 1, is equal to the class number of the quadratic field $\mathbf{Q}(\sqrt{-D})$, since this is the unique quadratic order of discriminant $-4D$. Thus we may suppose that this is not the minimal solution of the class. Then we see from Lemma 1 that the class has at least two distinct solutions of (32). It is clear that $(1, D, y)$ is not an element of $\mathcal{F}$ as well as $\mathcal{G}$. It is also not an element of $\mathcal{H}$, since $y^p \pm 1 \neq (2x)^2$ by the theorems of Lebesgue and Chao Ko (see Ribenboim [28], pages 78 and 92). Now we conclude the assertion by applying Theorem 1, which lists the values of D and y such that (28) has a class with strictly more than one solution.

As for the case $D \equiv 3 \pmod 4$, we proceed exactly as above, and we use Remark 1.5.9 of [25, page 25] to claim that the class number of the unique quadratic order of discriminant $-4D$ is equal to (*resp.* to 3 times) the class number of the quadratic field $\mathbf{Q}(\sqrt{-D})$ when $D \equiv 7 \pmod 8$ or $D = 3$ (*resp.* when $D \equiv 3 \pmod 8$). $\square$

References

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

[2] R. Apéry, Sur une équation diophantienne, C. R. Acad. Sci. Paris Sér. A 251 (1960), 1263–1264.

[3] R. Apéry, Sur une équation diophantienne, C. R. Acad. Sci. Paris Sér. A 251 (1960), 1451–1452.

[4] E. Bender and N. Herzberg, Some diophantine equations related to the quadratic form $ax^2 + by^2$, in "Studies in Algebra and Number Theory" (G.-C. Rota Ed.), pp. 219–272. Advances in Mathematics Supplementary Studies, Vol. 6, Academic Press, San Diego, 1979.

[5] M. A. Bennett and P. G. Walsh, The Diophantine equation $b^2X^4 - dY^2 = 1$, Proc. Amer. Math. Soc. 127 (1999), 3481–3491.

[6] F. Beukers, The generalised Ramanujan–Nagell Equation, Dissertation, 1979, R. U. Leiden.

[7] F. Beukers, On the generalized Ramanujan–Nagell equation, I, Acta Arith. 38 (1980/1981), 389–410.

[8] Y. Bilu and G. Hanrot, Solving superelliptic Diophantine equations with Baker's method, Compositio Math. 112 (1998), 273–312.

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

[10] Y. Bugeaud and G. Hanrot, On the generalized Ramanujan–Nagell equation. In preparation.

[11] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics 138, Springer Verlag, Berlin, Heidelberg, 1993.

[12] J. H. E. Cohn, The diophantine equation $x^2 + C = y^n$, Acta Arith. 65 (1993), 367–381.

[13] C. Heuberger and Le Maohua, On the generalized Ramanujan–Nagell equation $x^2 + D = p^z$, J. Number Th. 78 (1999), 312–331.

[14] L. K. Hua, Introduction to Number Theory, Springer Verlag, Berlin, 1982.

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

[16] Le Maohua, On the number of solutions of the diophantine equation $x^2 + D = p^n$, C. R. Acad. Sci. Paris Sér. A 317 (1993), 135–138.

[17] Le Maohua, On the Diophantine equation $D_1x^2 + D_2 = 2^{n+2}$, Acta Arith. 64 (1993), 29–41.

[18] Le Maohua, A note on the Generalized Ramanujan–Nagell Equation, J. Number Th. 50 (1995), 193–201.

[19] Le Maohua, Some Exponential Diophantine Equations. I. The Equation $D_1x^2 - D_2y^2 = \lambda k^z$, J. Number Th. 55 (1995), 209–221.

[20] Le Maohua, A Note on the Number of Solutions of the Generalized Ramanujan–Nagell Equation $D_1x^2 + D_2 = 4p^n$, J. Number Th. 62 (1997), 100–106.

[21] Le Maohua, On the Diophantine equation $(x^3 - 1)/(x - 1) = (y^n - 1)/(y - 1)$, Trans. Amer. Math. Soc. 351 (1999), 1063–1074.

[22] J.-L. Lesage, Localisation des solutions entières de l'équation $x^5 = y^2 + 2^{2n}\,d$, C. R. Acad. Sci. Paris Sér. A 323 (1996), 985–988.

[23] W. Ljunggren, Ueber die Gleischungen $1 + Dx^2 = 2y^n$ and $1 + Dx^2 = 4y^n$, Norske Vid. Selsk. Forhdl. 15 (1943), 115–118.

[24] K. Mahler, On the greatest prime factor of $ax^m + by^n$, Nieuw Archief voor Wisk. 3 (1953), 113–132.

[25] R. A. Mollin, Quadratics, CRC Press, New York, 1996.

[26] T. Nagell, The diophantine equation $x^2 + 7 = 2^n$, Ark. Math. 4 (1960), 185–187.

[27] Yu. V. Nesterenko and T.N.Shorey, On an equation of Goormaghtigh, Acta Arith. 83 (1998), 381-389.

[28] P. Ribenboim, Catalan's Conjecture, Academic Press, New York, 1994.

[29] T. N. Shorey, Some exponential diophantine equations (II), in Number Theory and Related Topics, ed. by S. Raghavan, Tata Institute of Fundamental Research, Bombay (1988).

[30] T. N. Shorey, Integers with identical digits, Acta Arith. 53 (1989), 187-205.

[31] T. N. Shorey, Exponential diophantine equations involving products of consecutive integers and related equations. To appear.

[32] 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
FRANCE

e-mail : bugeaud@math.u-strasbg.fr

T.N. Shorey
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
MUMBAI 400 005
INDIA
e-mail: shorey@math.tifr.res.in