ON THE DIOPHANTINE EQUATION $x^2 + C = 4y^n$

FLORIAN LUCA, SZABOLCS TENGELY, AND ALAIN TOGBÉ

Abstract. In this paper, we study the Diophantine equation $x^2 + C = 4y^n$ in nonnegative integers $x, y, n \geq 3$ with x and y coprime for various shapes of the positive integer C.

1. Introduction

The Diophantine equation

$$x^2 + C = y^n, \quad x \geq 1, \quad y \geq 1, \quad n \geq 3 \tag{1.1}$$

in integers $x,\ y,\ n$ once C is given has a rich history. In 1850, Lebesgue [24] proved that the above equation has no solutions when $C = 1$. In 1965, Chao Ko [21] proved that the only solution of the above equation with $C = -1$ is $x = 3,\ y = 2$. J.H.E. Cohn [19] solved the above equation for several values of the parameter C in the range $1 \leq C \leq 100$. A couple of the remaining values of C in the above range were covered by Mignotte and De Weger in [29], and the remaining ones in the recent paper [17]. In [34], all solutions of the similar looking equation $x^2+C = 2y^n$, where $n \geq 2$, x and y are coprime, and $C = B^2$ with $B \in \{3, 4, \ldots, 501\}$ were found.

Recently, several authors become interested in the case when only the prime factors of C are specified. For example, the case when $C = p^k$ with a fixed prime number p was dealt with in [13] and [23] for $p = 2$, in [11], [12] and [25] for $p = 3$, and in [10] for $p = 5$ and k odd. Partial results for a general prime p appear in [8] and [22]. All the solutions when $C = 2^a 3^b$ were found in [26], and when $C = p^a q^b$ where $\{p, q\} \subset \{2, 5, 13\}$, were found in the sequence of papers [3], [27] and [28]. For an analysis of the case $C = 2^\alpha\, 3^\beta\, 5^\gamma\, 7^\delta$, see [32]. The same Diophantine equation with $C = 2^\alpha\, 5^\beta\, 13^\gamma$ was dealt with in [20]. The Diophantine equation $x^2 + C = 2y^n$ was studied in the recent paper [2] for the families of parameters $C \in \{17^a,\ 5^{a_1} 13^{a_2},\ 3^{a_1} 11^{a_2}\}$. See also [9], [33], as well as the recent survey [4] for further results on equations of this type.

In this paper, we consider the Diophantine equation

$$x^2 + C = 4y^n, \quad x \geq 1, \quad y \geq 1, \quad \gcd(x, y) = 1, \quad n \geq 3, \quad C \geq 1. \tag{1.2}$$

We have the following results.

Theorem 1.1. *The only integer solutions (C, n, x, y) of the Diophantine equation* (1.3)

$$x^2 + C = 4y^n, \quad x, y \geq 1, \quad \gcd(x, y) = 1, \quad n \geq 3, \quad C \equiv 3 \mod 4, \quad 1 \leq C \leq 100$$

are given in the following table:

Date: August 3, 2009.

2000 *Mathematics Subject Classification.* 11D61, 11Y50.

Key words and phrases. Exponential equations, Diophantine equation.

$(3,n,1,1)$	$(3,3,37,7)$	$(7,3,5,2)$	$(7,5,11,2)$
$(7,13,181,2)$	$(11,5,31,3)$	$(15,4,7,2)$	$(19,7,559,5)$
$(23,3,3,2)$	$(23,3,29,6)$	$(23,3,45,8)$	$(23,3,83,12)$
$(23,3,7251,236)$	$(23,9,45,2)$	$(31,3,1,2)$	$(31,3,15,4)$
$(31,3,63,10)$	$(31,3,3313,140)$	$(31,6,15,2)$	$(35,4,17,3)$
$(39,4,5,2)$	$(47,5,9,2)$	$(55,4,3,2)$	$(59,3,7,3)$
$(59,3,21,5)$	$(59,3,525,41)$	$(59,3,28735,591)$	$(63,4,1,2)$
$(63,4,31,4)$	$(63,8,31,2)$	$(71,3,235,24)$	$(71,7,21,2)$
$(79,3,265,26)$	$(79,5,7,2)$	$(83,3,5,3)$	$(83,3,3785,153)$
$(87,3,13,4)$	$(87,3,1651,88)$	$(87,6,13,2)$	$(99,4,49,5)$

TABLE 1. Solutions for $1 \le C \le 100$.

Theorem 1.2. • *The only integer solutions of the Diophantine equation*

$$x^2 + 7^a \cdot 11^b = 4y^n, \quad x, y \ge 1, \quad \gcd(x,y) = 1, \quad n \ge 3, \quad a, b \ge 0 \tag{1.4}$$

are:

$5^2 + 7^1 \cdot 11^0 = 4 \cdot 2^3$, $11^2 + 7^1 \cdot 11^0 = 4 \cdot 2^5$, $31^2 + 7^0 \cdot 11^1 = 4 \cdot 3^5$,
$57^2 + 7^1 \cdot 11^2 = 4 \cdot 4^5$, $13^2 + 7^3 \cdot 11^0 = 4 \cdot 2^7$, $57^2 + 7^1 \cdot 11^2 = 4 \cdot 2^{10}$
$181^2 + 7^1 \cdot 11^0 = 4 \cdot 2^{13}$.

• *The only integer solutions of the Diophantine equation*

$$x^2 + 7^a \cdot 13^b = 4y^n, \quad x, y \ge 1, \quad \gcd(x,y) = 1, \quad n \ge 3, \quad a, b \ge 0 \tag{1.5}$$

are:

$5^2 + 7^1 \cdot 13^0 = 4 \cdot 2^3$, $5371655^2 + 7^3 \cdot 13^2 = 4 \cdot 19322^3$, $11^2 + 7^1 \cdot 13^0 = 4 \cdot 2^5$,
$13^2 + 7^3 \cdot 13^0 = 4 \cdot 2^7$, $87^2 + 7^3 \cdot 13^2 = 4 \cdot 4^7$, $181^2 + 7^1 \cdot 13^0 = 4 \cdot 2^{13}$,
$87^2 + 7^3 \cdot 13^2 = 4 \cdot 2^{14}$.

The plan of the paper is the following. In Section 2, we prove an important result using the theory of primitive divisors for Lucas sequences that will turn out to be very useful for the rest of the paper. We then find all the solutions of equation (1.2) for $1 \le C \le 100$ and $C \equiv 3 \mod 4$ in Section 3. In fact, using the results from Section 2, for each positive $C \le 100$ with $C \equiv 3 \mod 4$, we transform equation (1.2) into several elliptic curves that we solve using MAGMA except for the values $C = 47, 71, 79$ for which a class number issue appears. For these remaining cases, we transform equation (1.2) into Thue equations that we solve with PARI/GP. In the last section, we study equations (1.4) and (1.5). We note that reducing (1.4) modulo 4 we get that $a + b$ is odd and reducing (1.5) modulo 4 we have that a is odd. We will use these facts in the computations. For $n = 3,\ 4$, we turn these equations into elliptic curves on which we need to compute $\mathcal{S}$-integer points for some small finite sets $\mathcal{S}$ of places of $\mathbb{Q}$. These computations are done with MAGMA. For the remaining values of n, we use the theory of Section 2.

2. Auxiliary results

Clearly, if (x, y, C, n) is a solution of the Diophantine equation (1.2) and $d \ge 3$ is any divisor of n, then $(x, y^{n/d}, C, d)$ is also a solution of equation (1.2). Since $n \ge 3$, it follows that n either has an odd prime divisor d, or n is a multiple of

$d = 4$. We replace n by d and from now on we assume that n is either 4 or an odd prime.

Let α and β be distinct numbers such that $\alpha + \beta = r$ and $\alpha\beta = s$ are coprime nonzero integers. We assume that α/β is not a root of 1, which amounts to $(r, s) \neq (1, -1),\ (-1, -1)$. We write $\Delta = (\alpha - \beta)^2 = r^2 - 4s$. The *Lucas sequence of roots* $\alpha,\ \beta$ is the sequence of general term

$$u_m = \frac{\alpha^m - \beta^m}{\alpha - \beta} \qquad \text{for all } m \geq 0.$$

Given $m > 3$, a *primitive prime factor of* u_m is a prime p such that $p \mid u_m$ but $p \nmid \Delta \prod_{1\leq k\leq m-1} u_k$. Whenever it exists, it is odd and it has the property that $p \equiv \pm 1 \pmod{m}$. More precisely, $p \equiv \left(\frac{\Delta}{p}\right) \pmod{m}$, where, as usual, $\left(\frac{a}{p}\right)$ stands for the Legendre symbol of a with respect to p. The Primitive Divisor Theorem asserts that if $m \notin \{1, 2, 3, 4, 6\}$, then u_m always has a primitive divisor except for a finite list of triples (α, β, m), all of which are known (see [1] and [15]). One of our work-horses is the following result whose proof is based on the Primitive Divisor Theorem.

Lemma 2.1. *Let C be a positive integer satisfying $C \equiv 3 \mod 4$, which we write as $C = cd^2$, where c is square-free. Suppose that (x, y, C, n) is a solution to the equation (1.2), where $n \geq 5$ is prime. Let $\alpha = (x + i\sqrt{c}d)/2,\ \beta = (x - i\sqrt{c}d)/2$ and let $\mathbb{K} = \mathbb{Q}[\alpha]$. Then one of the following holds:*

(i) *n divides the class number of $\mathbb{K}$.*

(ii) *There exist complex conjugated algebraic integers u and v in $\mathbb{K}$ such that the nth term of the Lucas sequence with roots u and v has no primitive divisors.*

(iii) *There exists a prime $q \mid d$ not dividing c such that $q \equiv \left(\frac{c}{q}\right) \pmod{n}$.*

Proof. The proof is immediate. Write (1.2) as

$$\left(\frac{x + i\sqrt{c}d}{2}\right)\left(\frac{x - i\sqrt{c}d}{2}\right) = y^n.$$

Note that since $C \equiv 3 \pmod 4$, it follows that the two numbers α and β appearing in the left hand side of the above inequality are algebraic integers. Their sum is x and their product implies $x^2 + C = 4y^n$, and these two integers are coprime. Passing to the level of ideals in $\mathbb{K}$, we get that the product of the two coprime ideals $\langle\alpha\rangle$ and $\langle\beta\rangle$ is an nth power of an ideal in $\mathcal{O}_{\mathbb{K}}$. Here, for $\gamma \in \mathcal{O}_{\mathbb{K}}$ we write $\langle\gamma\rangle$ for the principal ideal $\gamma\mathcal{O}_{\mathbb{K}}$ generated by γ in $\mathcal{O}_{\mathbb{K}}$. By unique factorization at the level of ideals, we get that both $\langle\alpha\rangle$ and $\langle\beta\rangle$ are nth powers of some other ideals. Unless (i) happens, both $\langle\alpha\rangle$ and $\langle\beta\rangle$ are powers of some principal ideals. Write

$$\langle\alpha\rangle = \langle u\rangle^n = \langle u^n\rangle \qquad \text{for some } u \in \mathcal{O}_{\mathbb{K}}.$$

Passing to the levels of elements, we get that α and u^n are associated. Since $\mathbb{K}$ is a complex quadratic field, the group of units in $\mathcal{O}_{\mathbb{K}}$ is finite of orders 2, 4 or 6, all coprime to n. Thus, by replacing u with a suitable associate, we get that $\alpha = u^n$. Conjugating, we get $\beta = v^n$, where $v = \overline{u}$. Thus,

$$u^n - v^n = \alpha - \beta = i\sqrt{c}d.$$

Now clearly, $u - v = i\sqrt{c}d_1$ for some integer d_1. Thus,

$$\frac{u^n - v^n}{u - v} = \frac{d}{d_1} \mid d.$$

The left hand side is the nth term of a Lucas sequence. Unless (ii) happens for this sequence, the left hand side above has a primitive divisor as a Lucas sequence. This primitive divisor q does not divide cd_1 (since c is a divisor of $\Delta = (u-v)^2 = cd_1^2$). It clearly must divide d and it satisfies $q \equiv \left(\frac{c}{q}\right) \pmod n$, which is precisely (iii). □

3. Proof of Theorem 1.1

• First, we suppose that $n = 3$. Then for each positive integer $C \leq 100$ which is congruent to $3 \mod 4$, equation (1.2) becomes

$$Y^2 = X^3 + C_1, \tag{3.1}$$

where $X = 4y,\ Y = 4x,\ C_1 = -16C$. We use the MAGMA function `IntegralPoints` to find all the solutions in Table 1 with $n = 3$.

• Secondly, we suppose that $n = 4$. Then for each positive integer $C \leq 100$ which is congruent to $3 \mod 4$ we solve equation (1.2) using the MAGMA function `IntegralQuarticPoints` by transforming it first into

$$Y^2 = X^4 + C_1, \tag{3.2}$$

where $X = 2x,\ Y = 2y,\ C_1 = -4C$. In case (C, n, x, y) is a solution such that y is a power of an integer, i.e. $y = y_1^k$, then (C, nk, x, y_1) is also a solution. We can also deal with this in an elementary way by observing that $(Y - X^2)(Y + X^2) = C_1$, therefore both $Y - X^2$ and $Y + X^2$ are divisors of the number C_1.

• Thirdly, we consider the case when $n \geq 5$ is prime. For each positive integer $C \leq 100$ which is congruent to $3 \mod 4$, we write $C = cd^2$ and look at $\mathbb{K} = \mathbb{Q}[ic^{1/2}]$. The class numbers of the resulting fields are $h = 1, 2, 3, 4, 6, 8$ except for $C = 47, 79$ for which $h = 5$, and $C = 71$ for which $h = 7$, respectively. We will study later the equations

$$x^2 + 47 = 4y^5, \qquad x^2 + 79 = 4y^5, \qquad x^2 + 71 = 4y^7. \tag{3.3}$$

For the time being, we assume that item (i) of Lemma 2.1 is fulfilled. We next look at items (ii) and (iii) of Lemma 2.1. If (iii) holds, then we get some n^{th} member of a Lucas sequence whose prime factors are among the primes in d. But $100 > C = cd^2 \geq 3d^2$, so $d \leq 5$. Since also $n \geq 5$, it is impossible that this n^{th} member of the Lucas sequence has primitive divisors. So, item (iii) cannot happen. For item (ii) of Lemma 2.1, we checked in the tables in Bilu-Hanrot-Voutier [15] and Abouzaid [1], and we obtain the solutions in Table 1. It remains to study the three exceptional equations appearing in (3.3).

We will apply the following scheme to each of the equations in (3.3). Note that in each case we have $C = c$, so $d = 1$. Then we rewrite the equation $x^2 + C = 4y^p$, where in each case $p = h_{\mathbb{K}}$ is prime and is the order of the class group of $\mathbb{K}$, into the form $\alpha\bar{\alpha} = y^p$, where $\alpha = (x + i\sqrt{C})/2$. We conclude from this that $(\alpha) = \mathfrak{a}$ for some ideal $\mathfrak{a}$. Suppose that $\mathfrak{b}$ is a fixed representative of the class of $\mathfrak{a}^{-1}$ in the ideal class group of $\mathbb{K}$. Then $(\alpha) = \mathfrak{b}^p(\mathfrak{b}\mathfrak{a})^p$. The ideals (α) and $\mathfrak{b}\mathfrak{a}$ are principal; hence, so is $\mathfrak{b}^{-p}$. Writing $\mathfrak{b}\mathfrak{a} = (\gamma)$ and $\mathfrak{b}^{-p} = (\beta)$ for some algebraic integers β and γ in $\mathbb{K}$, we obtain (replacing, if necessary, β by $-\beta$, and using the fact that in all cases the only units in $\mathcal{O}_{\mathbb{K}}$ are ± 1) the relation $\alpha = \beta\gamma^p$. Similarly, $\bar{\alpha} = \bar{\beta}\bar{\gamma}^p$, and subtracting the above two relations we obtain the equation $\beta\gamma^p - \bar{\beta}\bar{\gamma}^p = i\sqrt{C}$. Substituting $\gamma = (u + vi\sqrt{C})/2$, we get a Thue equation in u and v of degree p. In this way, each of the three equations (3.3) yields $h_{\mathbb{K}}$ Thue equations, one for each ideal class. In the next subsections, we will use this scheme to write down the $h_{\mathbb{K}}$ Thue equations corresponding to each of the equations (3.3). However, in each of the three cases we will not consider the trivial ideal class as the corresponding case is solved by the Primitive Divisors Theorem. Thus, we will only deal with $p - 1$ ideal classes in each of the three cases. Furthermore, among the remaining $p - 1$ classes, only half will be considered because in each case the complex conjugation induces the automorphism $\mathfrak{a} \mapsto \mathfrak{a}^{-1}$ of the class group. Hence, it remains to obtain and solve two Thue equations for each of the first two equations from (3.3), and three Thue equations for the third one.

3.1. **The equation $x^2+47 = 4y^n$.** Let us start by creating the two Thue equations.

$$\langle 2\rangle = \mathfrak{b}_1\mathfrak{b}_2,$$

where $\theta = 1 + i\sqrt{47})/2$, $\mathfrak{b}_1 = \langle\theta, 2\rangle = \langle(1 + i\sqrt{47})/2, 2\rangle$, and $\mathfrak{b}_2 = \langle\theta - 1, 2\rangle = \langle(1 - i\sqrt{47})/2, 2\rangle$. A system of representatives for the nonzero elements of the class group of $\mathbb{K}$ is $\mathfrak{b}_1, \mathfrak{b}_1^2, \mathfrak{b}_2 = \mathfrak{b}_1^{-1}, \mathfrak{b}_2^2 = \mathfrak{b}_1^{-2}$. Let $\alpha = (x+i\sqrt{47})/2$ and $\beta = (9+i\sqrt{47})/2$.

With the previous notations, assume that the inverse of $\mathfrak{a}$ sits in the class of $\mathfrak{b}_2 = \mathfrak{b}_1^{-1}$. Then

$$\mathfrak{b}_2^5\langle\alpha\rangle = (\mathfrak{b}_2\mathfrak{a})^5 = \langle\gamma^5\rangle.$$

Since $\mathfrak{b}_2^5 = \langle\overline{\beta}\rangle$, we get that $\langle\alpha\overline{\beta}\rangle = \langle\gamma^5\rangle$. Writing $\gamma = (u + i\sqrt{47}v)/2$ with some integers u and v which are congruent modulo 2. Since

$$\alpha\overline{\beta} = \frac{9x + 47 + i(9 - x)i\sqrt{47}}{4},$$

it follows, by replacing γ with $-\gamma$ if necessary, identifying the real and imaginary parts from the equation $\alpha\overline{\beta}$, and then eliminating x from the two obtained equations we arrive at the Thue equation

$$1024 = u^5 + 45u^4v - 470u^3v^2 - 4230u^2v^3 + 11045uv^4 + 19881v^5. \tag{3.4}$$

The case of the conjugate equation (i.e., when the class of $\mathfrak{a}$ sits in the class of $\mathfrak{b}_2^5$) leads to the same Thue equation with v replaced by $-v$ and 1024 replaced by its negative. We use PARI/GP [30] to solve the above Thue equation (3.4) and the solutions found are $(u, v) = (\pm 4, 0)$. This gives us the solution $(x, y) = (9, 2)$.

Assume now that the inverse of $\mathfrak{a}$ sits in the class of $\mathfrak{b}_1^2 = \langle\beta^2\rangle$. Then, by a similar argument, we get that

$$\alpha\beta^2 = \gamma^5,$$

for some $\gamma = (u + i\sqrt{47}v)/2 \in \mathcal{O}_{\mathbb{K}}$. Note that

$$\alpha\beta^2 = \frac{17x - 423 + i(9x + 17)\sqrt{47}}{4}.$$

Identifying real and imaginary parts, we have

$$\begin{aligned}\frac{17x - 423}{4} &= \frac{1}{32}(u^5 - 470u^3v^2 + 11045uv^4);\\ \frac{9x + 17}{4} &= \frac{1}{32}(5u^4v - 470u^2v^3 + 2209v^5).\end{aligned}$$

Multiplying the first equation by 9, the second by 17, and subtracting the resulting equations, we get

$$-2^{15} = 9u^5 - 85u^4v - 4230u^3v^2 + 7990u^2v^3 + 99405uv^4 - 37553v^5.$$

With PARI/GP, we deduce that these Thue equations have no solutions.

3.2. **The equation $x^2 + 79 = 4y^n$.** The same argument works for 79. We will only sketch the proof without too many details. Here, $2^7 = 7^2 + 79$. We take

$$\alpha = (x + i\sqrt{79})/2 \text{ and } \beta = (7 + i\sqrt{79})/2.$$

So, we only need to distinguish two remaining cases:

Case 1. *$\alpha\beta$ is a fifth power in $\mathbb{K}$.*

We then get

$$\alpha\beta = \frac{7x - 79 + i(x+7)\sqrt{79}}{4} = \left(\frac{u + iv\sqrt{79}}{2}\right)^5.$$

Identifying real and imaginary parts, we have

$$\begin{aligned} \frac{7x-79}{4} &= \frac{1}{32}(u^5 - 790u^3v^2 + 31205uv^4); \\ \frac{x+7}{4} &= \frac{1}{32}(5u^4v - 790u^2v^3 + 6241v^5). \end{aligned}$$

Multiplying the second equation by 7 and subtracting it from the first one leads to

$$-1024 = u^5 - 35u^4v - 790u^3v^2 + 5530u^2v^3 + 31205uv^4 - 43687v^5. \tag{3.5}$$

When $\alpha\overline{\beta}$ is a fifth power in $\mathbb{K}$, one is lead to a similar equation as above but with the positive sign in the left hand side. We use PARI/GP to solve these Thue equations. The resulting solutions are $(u, v) = (\pm 4, 0)$. This gives us the solution $(x, y) = (7, 2)$.

Case 2. *$\alpha\beta^2$ is a fifth power in $\mathbb{K}$.*

We proceed as in Case 1 and we obtain

$$-32768 = 7u^5 + 75u^4v - 5530u^3v^2 - 1180u^2v^3 + 218435uv^4 + 93615v^5. \tag{3.6}$$

When $\alpha\overline{\beta}^2$ is a fifth power in $\mathbb{K}$, then the resulting Thue equation has the same right hand side but the sign on the left hand side is positive. These Thue equations have no solutions.

3.3. **The equation $x^2 + 71 = 4y^n$.** We use the same method. Here, $21^2 + 71 = 2^9$, so we take

$$\alpha = (x + i\sqrt{71})/2 \text{ and } \beta = (21 + i\sqrt{71})/2.$$

Assume that

$$\alpha\beta = \frac{21x - 71 + i(x+21)\sqrt{71}}{4} = \left(\frac{u + iv\sqrt{71}}{2}\right)^7.$$

Identifying real and imaginary parts, we have

$$\begin{aligned} \frac{21x-71}{4} &= \frac{1}{128}(u^7 - 1491u^5v^2 + 176435u^3v^4 - 2505377uv^6); \\ \frac{x+21}{4} &= \frac{1}{128}(7u^6v - 2485u^4v^3 + 105861u^2v^5 - 357911v^7). \end{aligned}$$

To eliminate x, we multiply the second equation by 21 and subtract the resulting equation from the first one. We get

$$\begin{aligned}\pm 16384 = u^7 - 147u^6v - 1491u^5v^2 + 52185u^4v^3 + 176435u^3v^4 \\ -2223081u^2v^5 - 2505377uv^6 + 7516131v^7.\end{aligned} \tag{3.7}$$

The sign + appears in the left hand side when $\alpha\overline{\beta} = \gamma^7$. We use PARI/GP to solve these Thue equations and obtain the solutions $(u, v) = (\pm 4, 0)$. We get the solution $(x, y) = (21, 2)$.

Next, we consider $\alpha\beta^2$ and we have

$$\begin{aligned}\pm 2097152 = 21u^7 - 1295u^6v - 31311u^5v^2 + 459725u^4v^3 \\ +3705135u^3v^4 - 19584285u^2v^5 - 52612917uv^6 + 66213535v^7.\end{aligned} \tag{3.8}$$

The sign + on the left hand side appears when $\alpha\overline{\beta}^2 = \gamma^7$. These Thue equations have no solutions.

Finally, we take $\alpha\beta^3$ to obtain

$$\begin{aligned}\pm 268435456 = 313u^7 - 8379u^6v - 466683u^5v^2 + 2974545u^4v^3 \\ +55224155u^3v^4 - 126715617u^2v^5 - 784183001uv^6 + 428419467v^7.\end{aligned} \tag{3.9}$$

Again the sign + in the left hand side appears when $\alpha\overline{\beta}^3 = \gamma^7$. We checked that these last Thue equations (3.9) are all impossible modulo 43.

This finishes the proof of Theorem 1.1.

4. Proof of Theorem 1.2

4.1. **The equation (1.4).** First we deal with the cases $n \in \{3, 4\}$.

- The case $n = 3$. We transform equation (1.4) as follows

$$X^2 = Y^3 - 4^2 \cdot 7^{a_1} \cdot 11^{b_1},$$

where $a_1, b_1 \in \{0, 1, 2, 3, 4, 5\}$. Now we need to determine all the $\{7, 11\}$-points on the above 36 elliptic curves. The coefficients are getting too large making the computations time consuming. Thus, we use a different approach instead. We give the details in case of equation (1.4). We have

$$\frac{x + 7^\alpha 11^\beta\sqrt{-7}}{2} = \left(\frac{u + v\sqrt{-7}}{2}\right)^3, \quad \text{or}$$
$$\frac{x + 7^\alpha 11^\beta\sqrt{-11}}{2} = \left(\frac{u + v\sqrt{-11}}{2}\right)^3.$$

After subtracting the conjugate equation we obtain

$$4 \cdot 7^\alpha 11^\beta = 3u^2v - 7v^3,$$
$$4 \cdot 7^\alpha 11^\beta = 3u^2v - 11v^3.$$

In the case of the first equation, one can easily see that $11 \mid v$, and in the latter case that $7 \mid v$. Therefore, we have $v \in \{\pm 11^\beta, \pm 4 \cdot 11^\beta, \pm 7^\alpha \cdot 11^\beta, \pm 4 \cdot 7^\alpha \cdot 11^\beta\}$, and $v \in \{\pm 7^\alpha, \pm 4 \cdot 7^\alpha, \pm 7^\alpha \cdot 11^\beta, \pm 4 \cdot 7^\alpha \cdot 11^\beta\}$, respectively.

If $v = \pm 11^{\beta}$, then we get that $\alpha \in \{0,1\}$, and it is sufficient to solve the following equations

$$\begin{aligned} 3u^2 &= 7V^4 \pm 4, \\ 3u^2 &= 7V^4 \pm 28, \\ 3u^2 &= 7 \cdot 11^2 V^4 \pm 4, \\ 3u^2 &= 7 \cdot 11^2 V^4 \pm 28, \end{aligned}$$

with $V = 11^k$. Here and in what follows, $k = \lfloor \beta/2 \rfloor$. We use the MAGMA [16] software and its function `SIntegralLjunggrenPoints` to determine all integral points on the above curves. We obtain $(u,v) = (\pm 1, \pm 1)$. Thus, $(x,y) = (5,2)$.

The other cases $v \in \{\pm 4 \cdot 11^{\beta}, \pm 7^{\alpha} \cdot 11^{\beta}, \pm 4 \cdot 7^{\alpha} \cdot 11^{\beta}, \pm 7^{\alpha}, \pm 4 \cdot 7^{\alpha}, \pm 7^{\alpha} \cdot 11^{\beta}, \pm 4 \cdot 7^{\alpha} \cdot 11^{\beta}\}$ can be handled in a similar way and do not yield any new solutions. The only solution of equation (1.4) with $n = 3$ is

$$5^2 + 7^1 \cdot 11^0 = 4 \cdot 2^3.$$

- The case $n = 4$. We can rewrite equation (1.4) as follows:

$$x^2 = 4y^4 - 7^{\alpha} 11^{\beta}, \qquad \text{where } \alpha, \beta \in \{0,1,2,3\}, \quad \mathcal{S} = \{7, 11\}.$$

The problem can now be solved by applying standard algorithms for computing $\mathcal{S}$-integral points on elliptic curves (see, for example, [31]). We use the MAGMA [16] function `SIntegralLjunggrenPoints` to determine all $\mathcal{S}$-integral points on the above curves. No solution of equation (1.4) was found.

- If $n \geq 5$ is a prime, then by Lemma 2.1, it follows easily that $n = 5$, or

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

It is easy to see that the class number of $\mathbb{K}$ is 1 when $\mathbb{K} = \mathbb{Q}[i\sqrt{d}]$ with $d \in \{7, 11\}$.

- The case $n = 5$. We describe the method in case of equation (1.4). We have

$$\begin{aligned} \frac{x + 7^{\alpha} 11^{\beta} \sqrt{-7}}{2} &= \left(\frac{u + v\sqrt{-7}}{2} \right)^5, \quad \text{or} \\ \frac{x + 7^{\alpha} 11^{\beta} \sqrt{-11}}{2} &= \left(\frac{u + v\sqrt{-11}}{2} \right)^5. \end{aligned}$$

After subtracting the conjugate equation we obtain

$$\begin{aligned} 16 \cdot 7^{\alpha} 11^{\beta} &= v(5u^4 - 70u^2v^2 + 49v^4), \quad \text{or} \\ 16 \cdot 7^{\alpha} 11^{\beta} &= v(5u^4 - 110u^2v^2 + 121v^4). \end{aligned}$$

Therefore v is composed by the primes $2, 7$ and 11. We rewrite the above equations as follows

$$\begin{aligned} Y^2 &= \pm 2^{a_1} 7^{a_2} 11^{a_3} (5X^4 - 70X^2 + 49), \quad \text{or} \\ Y^2 &= \pm 2^{a_1} 7^{a_2} 11^{a_3} (5X^4 - 110X^2 + 121), \end{aligned}$$

where $a_i \in \{0,1\}$. Many of these equations do not have solutions in $\mathbb{Q}_p$ for some prime p, where here by $\mathbb{Q}_p$ we mean the p-adic field. We use the MAGMA [16] function `SIntegralLjunggrenPoints` to determine all $\{2,7,11\}$-integral points on the remaining curves. We obtain the following solutions:

curve	$\{2, 7, 11\}$-integral points
$Y^2 = -11(5X^4 - 70X^2 + 49)$	$(\pm 3, \pm 44), (\pm \frac{3}{2}, \pm \frac{121}{4})$
$Y^2 = -(5X^4 - 70X^2 + 49)$	$(\pm 1, \pm 4)$
$Y^2 = 5X^4 - 70X^2 + 49$	$(0, 7)$
$Y^2 = 11(5X^4 - 70X^2 + 49)$	$(\pm 7, \pm 308)$
$Y^2 = 5X^4 - 110X^2 + 121$	$(0, \pm 11), (\pm 1, \pm 4)$

We use the above points on the elliptic curves to find the corresponding solutions of equation (1.4). For example, the solution $(X, Y) = (3, 44)$ of the first elliptic curve gives the solution $(n, a, b, x, y) = (5, 1, 2, 57, 4)$. The solution $(X, Y) = (1, 4)$ of the second elliptic curve yields the solution $(n, a, b, x, y) = (5, 1, 0, 11, 2)$. The solution $(n, a, b, x, y) = (5, 0, 1, 31, 3)$ is obtained from the solution $(X, Y) = (1, 4)$ of the last elliptic curve, while the solution $(n, a, b, x, y) = (10, 1, 2, 57, 2)$ is obtained easily from the solution $(n, a, b, x, y) = (5, 1, 2, 57, 4)$.

- The case $n > 5$. Here, by Lemma 2.1, we have

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

We provide the details of the computations in case of equation (1.4). It remains to find all integral points on the following elliptic curves

$$Y^2 = X^3 + 4 \cdot 7^{2\alpha} 11^{2\beta} y^n,$$

where $0 \leq \alpha, \beta \leq 2$ and $(y, n) \in \{(2, 7), (2, 13), (3, 7), (4, 7), (5, 7)\}$. Using MAGMA, we get the following solutions:

(α, β)	$(2, 7)$	$(2, 13)$	$(3, 7)$
$(0, 0)$	$X \in \{\pm 8, -7, 4, 184\}$	$X \in \{\pm 32, -28, 16, 736\}$	$X \in \{-18, 117\}$
$(0, 1)$	$X \in \{-28\}$	$X \in \{-112\}$	$X \in \{-99, -18, 22, 198\}$
$(0, 2)$	$\emptyset$	$\emptyset$	$\emptyset$
$(1, 0)$	$X \in \{-28, 8, 56, 497\}$	$X \in \{-112, -7, 32, 224, 1988\}$	$X \in \{198\}$
$(1, 1)$	$X \in \{-28, 56, 1736, 61037816\}$	$X \in \{-112, 224, 6944, 244151264\}$	$X \in \{198, 333, 15598\}$
$(1, 2)$	$\emptyset$	$\emptyset$	$\emptyset$
$(2, 0)$	$X \in \{392\}$	$X \in \{1568\}$	$X \in \{-234\}$
$(2, 1)$	$X \in \{-503, -392, 49, 2744\}$	$X \in \{-2012, -1568, 196, 5537, 10976\}$	$X \in \{198, 37566\}$
$(2, 2)$	$\emptyset$	$\emptyset$	$\emptyset$

(α, β)	$(4, 7)$	$(5, 7)$
$(0, 0)$	$X \in \{0\}$	$\emptyset$
$(0, 1)$	$X \in \{0\}$	$X \in \{-275\}$
$(0, 2)$	$X \in \{0\}$	$\emptyset$
$(1, 0)$	$X \in \{-112, 0, 128, 420, 896\}$	$\emptyset$
$(1, 1)$	$X \in \{0\}$	$\emptyset$
$(1, 2)$	$X \in \{0, 21669648\}$	$\emptyset$
$(2, 0)$	$X \in \{0, 25872\}$	$\emptyset$
$(2, 1)$	$X \in \{-1536, 0, 1617\}$	$\emptyset$
$(2, 2)$	$X \in \{0\}$	$\emptyset$

One can check, for example, that $(y, n, \alpha, \beta, X) = (2, 7, 0, 0, -7)$ yields the solution $13^2 + 7^3 \cdot 11^0 = 4 \cdot 2^7$, while the solution $181^2 + 7^1 \cdot 11^0 = 4 \cdot 2^{13}$ is obtained from $(y, n, \alpha, \beta, X) = (2, 13, 1, 0, -7)$.

4.2. **The equation** (1.5)**.** We use a similar method as for equation (1.4).

- The case $n = 3$. We transform equation (1.5) as follows

$$X^2 = Y^3 - 4^2 \cdot 7^{a_1} \cdot 13^{b_1},$$

where $a_1 \in \{1, 3, 5\}, b_1 \in \{0, 1, 2, 3, 4, 5\}$. Now we need to determine all the $\{7, 13\}$-points on the above 18 elliptic curves. Among the 18 curves, there are only 6 curves having rank greater than 0. MAGMA determined the appropriate Mordell-Weil groups except in case $(a_1, b_1) = (5, 4)$. We deal with this case separately. By computations similar to those done for equation (1.4) when $n = 5$, one can see the $\{7, 13\}$-points on the 5 curves lead to the solutions

$$(x, y, a, b) = (5, 2, 1, 0), (5371655, 19322, 3, 2).$$

If $(a_1, b_1) = (5, 4)$, then we obtain

$$4 \cdot 7^{3\alpha_1+2} 13^{3\beta_1+2} = v(3u^2 - 7v^2).$$

One can easily see that $13 \mid v$ and $7 \nmid u$. So, we have $v \in \{\pm 7^{3\alpha_1+2} \cdot 13^{3\beta_1+2}, \pm 4 \cdot 7^{3\alpha_1+2} \cdot 13^{3\beta_1+2}\}$. If $v = \pm 7^{3\alpha_1+2} \cdot 13^{3\beta_1+2}$, then the equations we need to solve are

$$\begin{aligned} 3u^2 &= 7V^4 \pm 4, \\ 3u^2 &= 7^3 V^4 \pm 4, \\ 3u^2 &= 7 \cdot 13^2 V^4 \pm 4, \\ 3u^2 &= 7^3 \cdot 13^2 V^4 \pm 4. \end{aligned}$$

We do not get any new solutions. If $v = \pm 4 \cdot 7^{3\alpha_1+2} \cdot 13^{3\beta_1+2}$, then by similar computations we do not get any new solutions.

- The case $n = 4$. We can rewrite equation (1.5) as follows:

$$x^2 = 4y^4 - 7^\alpha 13^\beta, \quad \text{where } \alpha, \beta \in \{0, 1, 2, 3\}, \quad \mathcal{S} = \{7, 13\}.$$

As previously, we use the MAGMA [16] function `SIntegralLjunggrenPoints` to determine all the $\mathcal{S}$-integral points on the above curves. We find no solution of equation (1.5) with $n = 4$.

- If $n \geq 5$ is a prime, then by Lemma 2.1, we have that $n = 5$ or $(y, n) \in \{(2, 7), (2, 13), (3, 7), (4, 7), (5, 7)\}$. A short calculation assures that the class number of $\mathbb{K}$ is 1 or 2 when $\mathbb{K} = \mathbb{Q}[i\sqrt{d}]$ with $d \in \{7, 91\}$.

- The case $n = 5$. Here, we have

$$\begin{aligned} 16 \cdot 7^\alpha 13^\beta &= v(5u^4 - 70u^2v^2 + 49v^4), \quad \text{or} \\ 16 \cdot 7^\alpha 13^\beta &= v(5u^4 - 910u^2v^2 + 8281v^4). \end{aligned}$$

Therefore v is composed by the primes $2, 7$ and 13. We rewrite the above equations as follows

$$\begin{aligned} Y^2 &= \pm 2^{a_1} 7^{a_2} 13^{a_3} (5X^4 - 70X^2 + 49), \quad \text{or} \\ Y^2 &= \pm 2^{a_1} 7^{a_2} 13^{a_3} (5X^4 - 910X^2 + 8281), \end{aligned}$$

where $a_i \in \{0, 1\}$. Many of these equations do not have solutions in $\mathbb{Q}_p$ for some prime p. We use the MAGMA [16] function `SIntegralLjunggrenPoints` to determine all $\{2, 7, 13\}$-integral points on the remaining curves. We obtain the following solutions $(0, \pm 7)$, $(\pm 1, \pm 4)$, $(0, \pm 91)$, $(\pm 13, \pm 52)$.

- The case $n > 5$. By Lemma 2.1, we have

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

We find all integral points on the following elliptic curves

$$Y^2 = X^3 + 4 \cdot 7^{2\alpha} 13^{2\beta} y^n,$$

where $0 \leq \alpha, \beta \leq 2$ and $(y, n) \in \{(2, 7), (2, 13), (3, 7), (4, 7), (5, 7)\}$. Using a similar method to that of the case $n > 5$ of equation (1.4), we obtain the desired solutions.

Acknowledgments The authors express their gratitude to the anonymous referee for constructive suggestions which improved the quality of the paper. Research of the first author was supported in part by grants SEP-CONACyT 79685 and PAPIIT 100508. The second author was supported by OTKA PD75264 and János Bolyai Research Scholarship of the Hungarian Academy of Sciences. The third author thanks Purdue University North Central for the support.

References

[1] M. Abouzaid, *Les nombres de Lucas et Lehmer sans diviseur primitif*, J. Th. Nombres Bordeaux **18** (2006), 299–313.

[2] F. S. Abu Muriefah, F. Luca, S. Siksek and Sz. Tengely, *On the Diophantine equation* $x^2 + C = 2y^n$, Preprint, 2007.

[3] F. S. Abu Muriefah, F. Luca and A. Togbé, *On the equation* $x^2 + 5^a \cdot 13^b = y^n$, Glasgow J. Math. **50** (2008), 175–181.

[4] F. S. Abu Muriefah and Y. Bugeaud, *The Diophantine equation* $x^2 + c = y^n$*: a brief overview*, Rev. Colombiana Mat. **40** (2006), 31–37.

[5] F. S. Abu Muriefah, *On the diophantine equation* $x^2 + 5^{2k} = y^n$, Demonstratio Mathematica **319** (2006), 285–289.

[6] S. A. Arif and A. Al-Ali, *On the Diophantine equation* $x^2 + q^{2k+1} = 4y^n$, Internat. J. Math. Math. Sci. **31** (2002), 695–699.

[7] S. A. Arif and A. Al-Ali, *On the Diophantine equation* $ax^2 + q^m = 4y^n$, Acta Arith. **103** (2002), 343–346.

[8] S. A. Arif and F. S. Abu Muriefah, *On the Diophantine equation* $x^2 + q^{2k+1} = y^n$, J. Number Theory **95** (2002), 95–100.

[9] S. A. Arif and F. S. Abu Muriefah, *The Diophantine equation* $x^2 + q^{2k} = y^n$, Arab. J. Sci. Eng. Sect. A Sci. **26** (2001), 53–62.

[10] F. S. Abu Muriefah and S. A. Arif, *The Diophantine equation* $x^2 + 5^{2k+1} = y^n$, Indian J. Pure Appl. Math. **30** (1999), 229–231.

[11] S. A. Arif and F. S. Abu Muriefah, *The Diophantine equation* $x^2 + 3^m = y^n$, Internat. J. Math. Math. Sci. **21** (1998), 619–620.

[12] S. A. Arief and F. S. Abu Muriefah, *On a Diophantine equation*, Bull. Austral. Math. Soc. **57** (1998), 189–198.

[13] S. A. Arif and F. S. Abu Muriefah, *On the Diophantine equation* $x^2 + 2^k = y^n$, Internat. J. Math. Math. Sci. **20** (1997), 299–304.

[14] Yu. Bilu, *On Le's and Bugeaud's papers about the equation* $ax^2 + b^{2m-1} = 4c^p$, Monatsh. Math. **137** (2002), 1–3.

[15] Yu. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte*, J. reine angew. Math. **539** (2001), 75–122.

[16] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[17] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation*, Compos. Math. **142** (2006), 31–62.

[18] Y. Bugeaud, *On some exponential Diophantine equations*, Monatsh. Math. **132** (2001), 193–197.

[19] J. H. E. Cohn, *The Diophantine equation* $x^2 + c = y^n$, Acta Arith. **65** (1993), 367–381.

[20] E. Goins, F. Luca and A. Togbé, *The Diophantine equation* $x^2 + 2^\alpha 5^\beta 13^\gamma = y^n$, Algorithmic Number Theory, 8th International Symposium ANTS VIII, LNCS 5011, Springer Berlin/Heidelberg, 430–442.

[21] C. Ko, *On the Diophantine equation* $x^2 = y^n + 1$, $xy \neq 0$, Sci. Sinica **14** (1965), 457–460.

[22] M. Le, *An exponential Diophantine equation*, Bull. Austral. Math. Soc. **64** (2001), 99–105.

[23] M. Le, *On Cohn's conjecture concerning the Diophantine equation* $x^2 + 2^m = y^n$, Arch. Math. (Basel) **78** (2002), 26–35.

[24] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation* $x^m = y^2 + 1$, Nouv. Annal. des Math. **9** (1850), 178–181.

[25] F. Luca, *On a Diophantine Equation*, Bull. Austral. Math. Soc. Vol. **61** (2000), 241–246.

[26] F. Luca, *On the equation* $x^2 + 2^a \cdot 3^b = y^n$, Int. J. Math. Math. Sci. **29** (2002), 239–244.

[27] F. Luca and A. Togbé, *On the equation* $x^2 + 2^a \cdot 5^b = y^n$, Int. J. Number Theory, **4 (6)** (2008), 973–979.

[28] F. Luca and A. Togbé, *On the equation* $x^2 + 2^a \cdot 13^b = y^n$, Colloquium Mathematicum, to appear.
[29] M. Mignotte and B. M. M. de Weger, *On the Diophantine equations* $x^2 + 74 = y^5$ *and* $x^2 + 86 = y^5$, Glasgow Math. J. **38** (1996), 77–85.
[30] PARI/GP, version `2.1.7`, Bordeaux, 2005, http://pari.math.u-bordeaux.fr/.
[31] A. Pethő, H. G. Zimmer, J. Gebel and E. Herrmann, *Computing all S-integral points on elliptic curves*, Math. Proc. Cambridge Philos. Soc. **127** (1999), 383–402.
[32] I. Pink, *On the diophantine equation* $x^2 + 2^\alpha \cdot 3^\beta \cdot 5^\gamma \cdot 7^\delta = y^n$, Publ. Math. Debrecen **70** (2006), 149–166.
[33] Sz. Tengely, *On the Diophantine equation* $x^2 + q^{2m} = 2y^p$, Acta Arith. **127** (2007), 71–86.
[34] Sz. Tengely, *On the Diophantine equation* $x^2 + a^2 = 2y^p$, Indag. Math. (N.S.) **15** (2004), 291–304.

Instituto de Matemáticas UNAM, Campus Morelia Ap. Postal 61-3 (Xangari), C.P. 58089, Morelia, Michoacán, Mexico
E-mail address: `fluca@matmor.unam.mx`

Mathematical Institute, University of Debrecen, P.O.Box 12, 4010 Debrecen, Hungary
E-mail address: `tengely@math.klte.hu`

Mathematics Department, Purdue University North Central, 1401 S, U.S. 421, Westville IN 46391 USA
E-mail address: `atogbe@pnc.edu`