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

F. S. ABU MURIEFAH, F. LUCA, S. SIKSEK, SZ. TENGELY

Abstract. In this paper, we study the Diophantine equation $x^2 + C = 2y^n$ in positive integers x, y with $\gcd(x, y) = 1$, where $n \geq 3$ and C is a positive integer. If $C \equiv 1 \pmod 4$ we give a very sharp bound for prime values of the exponent n; our main tool here is the result on existence of primitive divisors in Lehmer sequence due Bilu, Hanrot and Voutier. We illustrate our approach by solving completely the equations $x^2 + 17^{a_1} = 2y^n$, $x^2 + 5^{a_1}13^{a_2} = 2y^n$, and $x^2 + 3^{a_1}11^{a_2} = 2y^n$.

1. introduction

The Diophantine equation $x^2 + C = y^n$, in integer unknowns x, y and $n \geq 3$, has a long and distinguished history. The first case to have been solved appears to be $C = 1$: in 1850, Victor Lebesgue [24] showed, using an elementary factorization argument, that the only solution is $x = 0$, $y = 1$. Over the next 140 years many equations of the form $x^2 + C = y^n$ have been solved using Lebesgue's elementary trick. In 1993, John Cohn [17] published an exhaustive historical survey of this equation which completes the solution for all but 23 values of C in the range $1 \leq C \leq 100$. In a second paper, [19], Cohn shows that the tedious elementary argument can be eliminated by appealing to the remarkable recent theorem [8] on the existence of primitive divisors of Lucas sequences, due to Bilu, Hanrot and Voutier. The next major breakthrough came in 2006 when Bugeaud, Mignotte and Siksek [13] applied a combination of Baker's Theory and the modular approach to the equation $x^2 + C = y^n$ and completed its solution for $1 \leq C \leq 100$.

It has been noted recently (e.g. [1], [3], [4]) that the result of Bilu, Hanrot and Voutier can sometimes be applied to equations of the form $x^2 + C = y^n$ where instead of C being a fixed integer, C is the product of powers of fixed primes $p_1, \ldots, p_k$.

By comparison, the Diophantine equation $x^2 + C = 2y^n$, with the same restrictions, has received little attention. For $C = 1$, John Cohn [18], showed that the only solutions to this equation are $x = y = 1$ and $x = 239$, $y = 13$ and $n = 4$. The fourth-named author studied [29] the equation $x^2 + q^{2m} = 2y^p$ where m, p, q, x, y are integer unknowns with $m > 0$, and p, q are odd primes and $\gcd(x, y) = 1$. He proved that there are only finitely many solutions (m, p, q, x, y) for which y is not

Date: August 13, 2008.

2000 *Mathematics Subject Classification.* Primary 11D61; Secondary 11Y50.

Key words and phrases. exponential Diophantine equations, primitive divisors.

F. Luca is supported by grant CONACyT 46755. S. Siksek is supported by a grant from the UK Engineering and Physical Sciences Research Council, and by a Marie–Curie International Reintegration Grant (MIRG-CT-2006-044530). Sz. Tengely is supported in part by the Magyary Zoltán Higher Educational Public Foundation.

a sum of two consecutive squares. He also studied the equation for fixed q and resolved it when $q = 3$.

The purpose of this paper is to perform a deeper study of the equation $x^2 + C = 2y^n$, both in the case where C is a fixed integer, as well as in the case where C is the product of powers of fixed primes. Principally, we show that in some cases this equation can be solved by appealing to the theorem of Bilu, Hanrot and Voutier on primitive divisors of *Lehmer sequences*. In particular, we prove the following theorem.

Theorem 1. *Let C be a positive integer satisfying $C \equiv 1 \pmod 4$, and write $C = cd^2$, where c is square-free. Suppose that (x, y) is a solution to the equation*

$$x^2 + C = 2y^p, \qquad x,\ y \in \mathbb{Z}^+, \quad \gcd(x, y) = 1, \tag{1}$$

where $p \geq 5$ is a prime. Then either

(i) *$x = y = C = 1$, or*
(ii) *p divides the class number of the quadratic field $\mathbb{Q}(\sqrt{-c})$, or*
(iii) *$p = 5$ and $(C, x, y) = (9, 79, 5)$, $(125, 19, 3)$, $(125, 183, 7)$, $(2125, 21417, 47)$, or*
(iv) *$p \mid (q - (-c|q))$, where q is some odd prime such that $q \mid d$ and $q \nmid c$. Here $(c|q)$ denotes the Legendre symbol of the integer c with respect to the prime q.*

Theorem 2. *The only solutions to the equation $x^2 + C = 2y^n$ with x, y coprime integers, $n \geq 3$, and $C \equiv 1 \pmod 4$, $1 \leq C < 100$ are*

$$1^2 + 1 = 2 \cdot 1^n, \quad 79^2 + 9 = 2 \cdot 5^5, \quad 5^2 + 29 = 2 \cdot 3^3, \quad 117^2 + 29 = 2 \cdot 19^3,$$
$$993^2 + 29 = 2 \cdot 79^3, \quad 11^2 + 41 = 2 \cdot 3^4, \quad 69^2 + 41 = 2 \cdot 7^4, \quad 171^2 + 41 = 2 \cdot 11^4,$$
$$1^2 + 53 = 2 \cdot 3^3, \quad 25^2 + 61 = 2 \cdot 7^3, \quad 51^2 + 61 = 2 \cdot 11^3, \quad 37^2 + 89 = 2 \cdot 9^3.$$

Proof. Theorem 1 implies that either $(C, x, y) \in \{(1, 1, 1), (9, 79, 5)\}$ or $p \in \{2, 3\}$. It remains to solve the equations $x^2 + C = 2y^3$ and $x^2 + C = 2y^4$ for $C \equiv 1 \pmod 4$, $1 \leq C < 100$. Hence, we have reduced the problem to computing integral points on certain elliptic curves. Using the computer package MAGMA [10], we find the solutions listed in the theorem. □

Theorem 1 yields the following straightforward corollary.

Corollary 1.1. *Let $q_1, \ldots, q_k$ be distinct primes satisfying $q_i \equiv 1 \pmod 4$. Suppose that $(x, y, p, a_1, \ldots, a_k)$ is a solution to the equation*

$$x^2 + q_1^{a_1} \ldots q_k^{a_k} = 2y^p, \tag{2}$$

satisfying

$$x,\ y \in \mathbb{Z}^+, \qquad \gcd(x, y) = 1, \qquad a_i \geq 0, \qquad p \geq 5 \text{ prime}.$$

Then either

(i) *$x = y = 1$ and all the $a_i = 0$, or*
(ii) *p divides the class number of the quadratic field $\mathbb{Q}(\sqrt{-c})$ for some square-free c dividing $q_1 q_2 \ldots q_k$, or*
(iii) *$p = 5$ and $(\prod q_i^{a_i}, x, y) = (125, 19, 3)$, $(125, 183, 7)$, $(2125, 21417, 47)$, or*
(iv) *$p \mid (q_i^2 - 1)$ for some i.*

We illustrate by solving completely the equations

$$x^2 + 17^{a_1} = 2y^n,$$
$$x^2 + 5^{a_1}13^{a_2} = 2y^n,$$
$$x^2 + 3^{a_1}11^{a_2} = 2y^n,$$

under the restrictions $\gcd(x, y) = 1$, and $n \geq 3$.

Theorem 3. *The only solutions to the equation*

$$x^2 + 17^{a_1} = 2y^n, \qquad a_1 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

are

$$1^2 + 17^0 = 2 \cdot 1^n, \quad 239^2 + 17^0 = 2 \cdot 13^4, \quad 31^2 + 17^2 = 2 \cdot 5^4.$$

The only solutions to the equation

$$x^2 + 5^{a_1}13^{a_2} = 2y^n, \qquad a_1, a_2 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

are

$$\begin{gathered}
1^2 + 5^0 \cdot 13^0 = 2 \cdot 1^n, \quad 9^2 + 5^0 \cdot 13^2 = 2 \cdot 5^3, \quad 7^2 + 5^1 \cdot 13^0 = 2 \cdot 3^3, \\
99^2 + 5^2 \cdot 13^0 = 2 \cdot 17^3, \quad 19^2 + 5^2 \cdot 13^1 = 2 \cdot 7^3, \quad 79137^2 + 5^2 \cdot 13^3 = 2 \cdot 1463^3, \\
253^2 + 5^2 \cdot 13^4 = 2 \cdot 73^3, \quad 188000497^2 + 5^8 \cdot 13^4 = 2 \cdot 260473^3, \\
239^2 + 5^0 \cdot 13^0 = 2 \cdot 13^4.
\end{gathered}$$

The only solutions to the equation

$$x^2 + 3^{a_1}11^{a_2} = 2y^n, \qquad a_1, a_2 \geq 0, \quad \gcd(x, y) = 1, \quad n \geq 3,$$

are

$$\begin{gathered}
1^2 + 3^0 \cdot 11^0 = 2 \cdot 1^n, \quad 351^2 + 3^0 \cdot 11^4 = 2 \cdot 41^3, \quad 13^2 + 3^4 \cdot 11^0 = 2 \cdot 5^3, \\
5^2 + 3^4 \cdot 11^2 = 2 \cdot 17^3, \quad 27607^2 + 3^4 \cdot 11^2 = 2 \cdot 725^3, \quad 545^2 + 3^6 \cdot 11^0 = 2 \cdot 53^3, \\
679^2 + 3^6 \cdot 11^2 = 2 \cdot 65^3, \quad 1093^2 + 3^8 \cdot 11^4 = 2 \cdot 365^3, \\
410639^2 + 3^{10} \cdot 11^2 = 2 \cdot 4385^3, \quad 239^2 + 3^0 \cdot 11^0 = 2 \cdot 13^4, \quad 79^2 + 3^2 \cdot 11^0 = 2 \cdot 5^5.
\end{gathered}$$

2. Arithmetic of Some Biquadratic Fields

In this section, we let c be a square-free positive integer such that $c \equiv 1 \pmod 4$. We let $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{-c})$.

Lemma 2.1. *The field $\mathbb{K}$ has Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and precisely three quadratic subfields: $\mathbb{L}_1 = \mathbb{Q}(\sqrt{2})$, $\mathbb{L}_2 = \mathbb{Q}(\sqrt{-c})$ and $\mathbb{L}_3 = \mathbb{Q}(\sqrt{-2c})$. The ring of integers $\mathcal{O}_{\mathbb{K}}$ has $\mathbb{Z}$-basis*

$$\left\{1, \ \sqrt{2}, \ \sqrt{-c}, \ \frac{1 + \sqrt{-c}}{\sqrt{2}}\right\}.$$

The class number of h of $\mathbb{K}$ is $h = 2^{-i}h_2h_3$ where h_2, h_3 are respectively the class numbers of $\mathbb{L}_2$ and $\mathbb{L}_3$, and $0 \leq i \leq 2$.

Proof. The ring of integers can be read off from the tables in Kenneth Williams' seminal paper on integers of biquadratic fields [31].

For the relation between class numbers, see [9].

$\square$

3. Lehmer Sequences

We briefly define Lehmer sequences and state some relevant facts about them. 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), the corresponding *Lehmer sequence* $\{u_n\}$ is given by

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

Two Lehmer pairs (α_1, β_1) and (α_2, β_2) are said to be *equivalent* if $\alpha_1/\alpha_2 = \beta_1/\beta_2 \in \{\pm 1, \pm\sqrt{-1}\}$. One sees that general terms of Lehmer sequences corresponding to equivalent pairs are the same up to signs.

A prime q is called a *primitive divisor* of the term u_n if q divides u_n but q does not divide $(\alpha^2 - \beta^2)^2 u_1 \dots u_{n-1}$. We shall not state the full strength of the theorems of Bilu, Hanrot and Voutier [8] as this would take too long, but merely the following special cases:

(i) if $n > 30$, then u_n has a primitive divisor;
(ii) if $n = 11$, 17, 19, 23 or 29, then u_n has a primitive divisor;
(iii) u_7 and u_{13} have primitive divisors unless (α, β) is equivalent to

$$\left((\sqrt{a} - \sqrt{b})/2, (\sqrt{a} + \sqrt{b})/2\right), \tag{3}$$

where (a, b) is one of $(1, -7)$, $(1, -19)$, $(3, -5)$, $(5, -7)$, $(13, -3)$, $(14, -22)$.
(iv) u_5 has a primitive divisor unless (α, β) is equivalent to a Lehmer pair of the form (3) where
- $a = F_{k+2\epsilon}$, $b = F_{k+2\epsilon} - 4F_k$ for some $k \geq 3$, $\epsilon = \pm 1$, where F_n is the Fibonacci sequence given by $F_0 = F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$;
- $a = L_{k+2\epsilon}$, $b = L_{k+2\epsilon} - 4L_k$ for some $k \geq 0$, $k \neq 1$, $\epsilon = \pm 1$, where L_n is the Lucas sequence given by $L_0 = 2$, $L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$.

Lemma 3.1. *Let c be a positive square-free integer, $c \equiv 1 \pmod 4$. Let U, V be odd integers such that* $\gcd(U, cV) = 1$. *Suppose moreover that* $(c, U^2, V^2) \neq (1, 1, 1)$. *Write*

$$\alpha = \frac{U + V\sqrt{-c}}{\sqrt{2}}, \qquad \beta = \frac{U - V\sqrt{-c}}{\sqrt{2}}. \tag{4}$$

Then (α, β) is a Lehmer pair. Denote the corresponding Lehmer sequence by $\{u_n\}$. Then u_p has a primitive divisor for all prime $p \geq 7$. Moreover, u_5 has a primitive divisor provided that

$$(c, U^2, V^2) \neq (1, 1, 9),\ (5, 1, 1),\ (5, 9, 1),\ (85, 9, 1). \tag{5}$$

Proof. Throughout, we shall write $x = U/(V\sqrt{-c})$ and use the fact that

$$t = \frac{x+1}{x-1} \qquad \text{iff} \qquad x = \frac{t+1}{t-1}.$$

We shall also repeatedly use the easy fact that, for $\epsilon = \pm 1$ and $k \geq 0$, both $\gcd(F_{k+2\epsilon}, F_{k+2\epsilon} - 4F_k)$ and $\gcd(L_{k+2\epsilon}, L_{k+2\epsilon} - 4L_k)$ are either 1, 2 or 4.

Note that α, β are algebraic integers by Lemma 2.1. Moreover $(\alpha+\beta)^2 = 2U^2$, $\alpha\beta = (U^2+cV^2)/2$ are coprime rational integers. We next show that α/β is not a root of unity. But

$$\alpha/\beta = \frac{x+1}{x-1}$$

is in $\mathbb{Q}(\sqrt{-c})$ and so if it is a root of unity, it must be ± 1, $\pm\sqrt{-1}$, $(\pm 1 \pm \sqrt{-3})/2$. From our assumptions on c, U and V, we find that this is impossible. In particular, $\pm\sqrt{-1}$ leads to $(c, U^2, V^2) = (1,1,1)$, which we have excluded.

It remains to show that u_p has a primitive divisor. Suppose otherwise. Then

$$\frac{x+1}{x-1} = \pm\left(\frac{\sqrt{a}-\sqrt{b}}{\sqrt{a}+\sqrt{b}}\right) \qquad \text{or} \qquad \frac{x+1}{x-1} = \pm\sqrt{-1}\left(\frac{\sqrt{a}-\sqrt{b}}{\sqrt{a}+\sqrt{b}}\right),$$

where (a,b) is one of the pairs listed in (iii), (iv) above.

Let us first deal with the case $(x+1)/(x-1) = \pm\sqrt{-1}(\sqrt{a}-\sqrt{b})/(\sqrt{a}+\sqrt{b})$. Solving for x and squaring we obtain

$$\frac{U^2}{-cV^2} = \frac{a-b \mp 2\sqrt{-ab}}{b-a\mp 2\sqrt{-ab}},$$

which implies that $a=b$ or that $-ab$ is a square. This is not possible for the pairs listed in (iii), whilst for (iv) it leads to equations that can easily be solved with the help of Lemma 3.2 below.

Next we deal with the case $(x+1)/(x-1) = \pm(\sqrt{a}-\sqrt{b})/(\sqrt{a}+\sqrt{b})$. This leads to $x = -(\sqrt{a}/\sqrt{b})^{\pm 1}$. Squaring we obtain

$$\frac{U^2}{-cV^2} = \left(\frac{a}{b}\right)^{\pm 1} = \left(\frac{a'}{b'}\right)^{\pm 1}.$$

where $a' = a/\gcd(a,b)$ and $b' = b/\gcd(a,b)$. Since U and cV are coprime we have

$$\begin{cases} \pm U^2 = a', \\ \mp cV^2 = b', \end{cases} \qquad \text{or} \qquad \begin{cases} \pm U^2 = b', \\ \mp cV^2 = a'. \end{cases}$$

One quickly eliminates all the possibilities in (iii) mostly using the fact that $c \equiv 1 \pmod 4$. For the possibilities in (iv), we obtain equations of the form solved in Lemma 3.2 and these lead to one of the possibilities excluded in (5). This completes the proof of the lemma. $\square$

In the proof of Lemma 3.1, we needed the following results about Fibonacci and Lucas numbers.

Lemma 3.2. *Let $\{F_n\}_{n\geq 0}$ and $\{L_n\}_{n\geq 0}$ be the Fibonacci and Lucas sequences. The only solutions to the equation $F_n = u^2$ have $n = 0,\ 1,\ 2$ or 12. The only solutions to $F_n = 2u^2$ have $n = 3$ or 12. The only solutions to the equation $L_n = v^2$ have $n = 1$ or 3. The only solutions to the equation $L_n = 2v^2$ have $n = 0$ or 6.*

The only solutions to the equation

$$F_{k+2\epsilon} - 4F_k = \pm 2^r u^2, \qquad \epsilon = \pm 1, \quad k, r \geq 0, \quad u \in \mathbb{Z}, \tag{6}$$

have $(k,\epsilon) = (0,\pm 1),\ (1,1),\ (2,\pm 1),\ (4,1),\ (5,-1),\ (7,1)$. The only solutions to the equation

$$L_{k+2\epsilon} - 4L_k = \pm 2^r u^2, \qquad \epsilon = \pm 1, \quad k, r \geq 0, \quad u \in \mathbb{Z}, \tag{7}$$

have $(k,\epsilon) = (1,1),\ (4,-1),\ (6,1)$.

Proof. The results about Fibonacci and Lucas numbers of the form $2^r u^2$ are classical. See, for example, [15], [16].

It remains to deal with (6) and (7). Here, we may take $r = 0$, 1. We explain how to deal with (6) with $r = 0$:

$$F_{k+2\epsilon} - 4F_k = \pm u^2, \qquad \epsilon = \pm 1, \quad k \geq 0, \quad u \in \mathbb{Z};$$

the other cases are similar. We make use of Binet's formula for Fibonacci numbers:

$$F_n = \frac{\lambda^n - \mu^n}{\sqrt{5}}, \qquad \lambda = \frac{1+\sqrt{5}}{2}, \quad \mu = \frac{1-\sqrt{5}}{2}.$$

Our equation can thus be rewritten as

$$\gamma\lambda^k - \delta\mu^k = u^2\sqrt{5}, \qquad \gamma = \lambda^{2\epsilon} - 4, \quad \delta = \mu^{2\epsilon} - 4.$$

Let $v = \gamma\lambda^k + \delta\mu^k$. It is clear that $v \in \mathbb{Z}$. Moreover,

$$v^2 = (\gamma\lambda^k + \delta\mu^k)^2 = (\gamma\lambda^k - \delta\mu^k)^2 + 4\gamma\delta(\lambda\mu)^k = 5u^4 \pm 20.$$

Let $X = 5u^2$, and $Y = 5uv$. Then $Y^2 = X(X^2 \pm 100)$. Thus, we have reduced the problem to computing integral points on a pair of elliptic curves. Using the computer package `MAGMA` [10], we find that

$$(X, Y) = (0, 0), \ (5, \pm 25), \ (20, \pm 100), \ (\pm 100, 0).$$

The remaining equations similarly lead to integral points on elliptic curves which we found using `MAGMA`. Working backwards, we obtain the solutions given in the lemma. □

4. Proof of Theorem 1

We follow the notation from the statement of the theorem. We shall suppose that $(C, x, y) \neq (1, 1, 1)$ and p does not divide the class number of the $\mathbb{Q}(\sqrt{-c})$. We will show that either statement (iii) or (iv) of the theorem must hold.

Considering equation (1) modulo 4 reveals that x and y are odd. We work first in $\mathbb{Q}(\sqrt{-c})$. Since $c \equiv 1 \pmod 4$, this has ring of integers $\mathcal{O} = \mathbb{Z}[\sqrt{-c}]$. Moreover, $(2) = \mathfrak{q}^2$, where $\mathfrak{q}$ is a prime ideal of $\mathcal{O}$. It is clear that the principal ideals $(x + d\sqrt{-c})$ and $(x - d\sqrt{-c})$ have $\mathfrak{q}$ as their greatest common factor. From (1) we deduce that

$$(x + d\sqrt{-c})\mathcal{O} = \mathfrak{q} \cdot \mathfrak{a}^p,$$

where $\mathfrak{a}$ is some ideal of $\mathcal{O}$. Now multiply both sides by $2^{(p-1)/2}$. We obtain

$$2^{(p-1)/2}(x + d\sqrt{-c})\mathcal{O} = (\mathfrak{q}\mathfrak{a})^p.$$

Since the class number of $\mathbb{Q}(\sqrt{-c})$ is not divisible by p, we see that $\mathfrak{q}\mathfrak{a}$ is a principal ideal. Moreover, as c is positive, the units of $\mathbb{Z}[\sqrt{-c}]$ are ± 1. Hence

$$2^{(p-1)/2}(x + d\sqrt{-c}) = (U + V\sqrt{-c})^p \tag{8}$$

for some integers U, V. Since x, d, c are odd, we deduce that U and V are both odd. Moreover, $y = (U^2 + cV^2)/2$. From the coprimality of x and y we see that U, cV are coprime.

In conclusion,

$$\frac{x + d\sqrt{-c}}{\sqrt{2}} = \left(\frac{U + V\sqrt{-c}}{\sqrt{2}}\right)^p,$$

where U, V, c satisfy the conditions of Lemma 3.1.

Let α, β be as in (4). Let $\{u_n\}$ be the corresponding Lehmer sequence. We note that

$$\alpha^p - \beta^p = d\sqrt{-2c}, \qquad \alpha - \beta = V\sqrt{-2c}.$$

Thus, $V \mid d$ and $u_p \mid d/V$. By Lemma 3.1, u_p has a primitive divisor unless $p = 5$ and (c, U^2, V^2) is one of the possibilities listed in (5). These possibilities lead to cases given in item (iii) of the theorem. Thus, we may exclude these and so assume that u_p has a primitive divisor q. Our objective now is to show that (iv) holds. Clearly, $q \mid d$, but by the definition of the primitive divisor, $q \nmid (\alpha^2 - \beta^2)^2$ and so, in particular, $q \nmid c$. To complete the proof, let

$$\gamma = U + V\sqrt{-c}, \qquad \delta = U - V\sqrt{-c}.$$

Write $v_n = (\gamma^n - \delta^n)/(\gamma - \delta)$. We note that $q \mid v_p$ but, from the accumulated facts, $q \nmid (\gamma - \delta)\gamma\delta$. We claim that $q \mid v_{q-(-c|q)}$. Given our claim, it follows from [12, Lemma 5], that p divides $q - (-c|q)$. Now let us prove our claim. If $(-c|q) = 1$, then

$$\gamma^{q-1} \equiv \delta^{q-1} \equiv 1 \pmod{q},$$

and hence $q \mid v_{q-1}$. Suppose $(-c|q) = -1$. Then, by the properties of the Frobenius automorphism, we have

$$\gamma^q \equiv \delta \pmod{q}, \qquad \delta^q \equiv \gamma \pmod{q}.$$

Hence,

$$\gamma^{q+1} - \delta^{q+1} \equiv \gamma\delta - \gamma\delta \equiv 0 \pmod{q},$$

proving $q \mid v_{q+1}$ as required. This completes the proof of the theorem.

Remark. In the proof of Theorem 1, it would have been possible to factorize the left-hand side of (1) in $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{-c})$. Doing this, the hypothesis that would be needed is that p does not divide the class number of $\mathbb{K}$. By Lemma 2.1, the class number of $\mathbb{Q}(\sqrt{-c})$ divides the class number of $\mathbb{K}$, up to powers of 2. Thus, we obtained a stronger result by working in $\mathbb{Q}(\sqrt{-c})$ instead of $\mathbb{K}$.

5. Dealing with small exponents

Let $q_1, \ldots, q_k$ be distinct primes. In this section, we explain how to solve the equation

$$x^2 + q_1^{a_1} \ldots q_k^{a_k} = 2y^n, \tag{9}$$

for small values of n. The method can be applied more easily to the equation $x^2 + C = 2y^n$. This section is meant to complement Theorem 1 and Corollary 1.1.

For the cases $n = 3$ and $n = 4$, we show that (9) can be reduced to computing $\mathcal{S}$-integral points on a handful of elliptic curves. The problem can now be solved by applying standard algorithms for computing S-integral points on elliptic curves (see, for example, [26]). Fortunately these algorithms are available as an inbuilt functions in the computer package `MAGMA` [10].

Suppose $n = 4$. We are then dealing with an equation of the form $x^2 + C = 2y^4$. Now write $C = cz^4$, where c is fourth power free and made up only of the primes $q_1, \ldots, q_k$. There are clearly only 4^k possibilities for c. Write

$$Y = \frac{2xy}{z^3}, \qquad X = \frac{2y^2}{z^2}.$$

We immediately see that (X, Y) is an $\mathcal{S}$-integral point on the elliptic curve $Y^2 = X(X^2 - 2c)$, where $\mathcal{S} = \{q_1, \ldots, q_k\}$.

Similarly, if $n = 3$, we are dealing with an equation of the form $x^2 + C = 2y^3$. We then write $C = cz^6$ for some sixth power free integer c made up with the primes $q_1, \ldots, q_k$. There are only 6^k possibilities for c. For each such c, let

$$X = \frac{2y}{z^2}, \qquad Y = \frac{2x}{z^3}.$$

Observe that (X, Y) is an $\mathcal{S}$-integral point on the elliptic curve $Y^2 = X^3 - 4c$.

If $n \geq 5$, then we require $\mathcal{S}$-integral points on finitely many curves of genus ≥ 2. Here it is often—but not always—possible to compute all the rational points on the curves using some variant of the method of Chabauty [11], [21], [25], [30].

6. Proof of Theorem 3

In this section, we prove Theorem 3. We consider the three Diophantine equations mentioned in the theorem separately.

- The equation $x^2 + 17^{a_1} = 2y^n$. Corollary 1.1 implies that either $(a_1, x, y) = (0, 1, 1)$ or $p \in \{2, 3\}$, where p is a prime divisor of n. Therefore it remains to solve the equations $x^2 + 17^{a_1} = 2y^3$ and $x^2 + 17^{a_1} = 2y^4$. We apply the method described in Section 5 to determine all integral solutions. We obtain the following solutions

$$\begin{aligned} &1^2 + 17^0 = 2 \cdot 1^3, \quad 1^2 + 17^0 = 2 \cdot 1^4, \\ &239^2 + 17^0 = 2 \cdot 13^4, \quad 31^2 + 17^2 = 2 \cdot 5^4. \end{aligned}$$

- The equation $x^2 + 5^{a_1}13^{a_2} = 2y^n$. In this case, Corollary 1.1 yields that either

$$(a_1, a_2, x, y, n) \in \{(0, 0, 1, 1, n), (3, 0, 19, 3, 5), (3, 0, 183, 7, 5)\},$$

or $p \in \{2, 3, 7\}$, where p is a prime divisor of n. If $p = 2$ or 3, then the method of Section 5 provides all solutions of the corresponding equations. Now we deal with the case $p = 7$. We have that $5^{a_1}13^{a_2} \in \{1\square, 5\square, 13\square, 65\square\}$. Assume that $5^{a_1}13^{a_2} = \square$. Working in the imaginary quadratic field $\mathbb{Q}[i]$, we easily get

$$5^{b_1}13^{b_2} = (U - V)(U^6 + 8U^5V - 13U^4V^2 - 48U^3V^3 - 13U^2V^4 + 8UV^5 + V^6).$$

One can obtain all integral solutions of the Thue equations $U^6 + 8U^5V - 13U^4V^2 - 48U^3V^3 - 13U^2V^4 + 8UV^5 + V^6 = \pm1, \pm5, \pm13, \pm65$. The only solutions are $(U, V) \in \{(\pm1, 0), (0, \pm1)\}$. So we may assume that

$$\begin{aligned} &U - V = \pm 5^{c_1}13^{c_2}, \\ &U^6 + 8U^5V - 13U^4V^2 - 48U^3V^3 - 13U^2V^4 + 8UV^5 + V^6 = \pm 5^{b_1 - c_1}13^{b_2 - c_2}, \end{aligned}$$

with $b_1 - c_1, b_2 - c_2 \geq 2$. Considering the above system of equations modulo 5 and modulo 13 we get a contradiction. If $5^{a_1}13^{a_2} = 5d^2, 13d^2$ or $65d^2$, then equation (8) leads to

$$\begin{aligned} 5d^2 &: \quad 8d = V(7U^6 - 175U^4V^2 + 525U^2V^4 - 125V^6), \\ 13d^2 &: \quad 8d = V(7U^6 - 455U^4V^2 + 3549U^2V^4 - 2197V^6), \\ 65d^2 &: \quad 8d = V(7U^6 - 2275U^4V^2 + 88725U^2V^4 - 274625V^6), \end{aligned}$$

respectively. It follows that V is a divisor of $8d$, so the prime divisors of V belong to the set $\{2, 5, 13\}$. Therefore the above equations can be written as

$$\begin{aligned}\square &= X^3 \pm 175\omega_1 X^2 + 3675\omega_1^2 X \pm 6125\omega_1^3,\\ \square &= X^3 \pm 455\omega_2 X^2 + 24843\omega_2^2 X \pm 107653\omega_2^3,\\ \square &= X^3 \pm 2275\omega_3 X^2 + 621075\omega_3^2 X \pm 13456625\omega_3^3,\end{aligned}$$

where $\omega_1, \omega_2, \omega_3 \in \{2^{\alpha_1} 5^{\alpha_2} 13^{\alpha_3} : \alpha_i = 0, 1\}$. We use MAGMA [10] to determine all $\{2, 5, 13\}$-integral points on the above elliptic curves. Then we find (U, V) and the corresponding solutions (x, y, a_1, a_2).

- Equation $x^2 + 3^{a_1} 11^{a_2} = 2y^n$. Note that $x^2 + 3\square = 2y^p$ and $x^2 + 11\square = 2y^p$ can be excluded modulo 8. Hence it remains to deal with the equations $x^2 + \square = 2y^p$ and $x^2 + 33\square = 2y^p$. We apply Theorem 1 with $3^{2b_1} 11^{2b_2} = C \equiv 1 \pmod 4$ and $33 \cdot 3^{2c_1} 11^{2c_2} = C \equiv 1 \pmod 4$. In the former case we obtain that $(x, y, a_1, a_2, n) \in \{(1, 1, 0, 0, n), (79, 5, 2, 0, 5)\}$ or $p \in \{2, 3\}$. In the latter case we get that $p = 2$. If $p = 2$ or 3, then the method of Section 5 provides all solutions of the corresponding equations. The proof of Theorem 3 is completed.

References

[1] F. S. Abu Muriefah, *On the Diophantine equation* $x^2 + 5^{2k} = y^n$, Demonstratio Math. **39** (2006), no. 2, 285–289.

[2] F. S. Abu Muriefah and Y. Bugeaud, *The diophantine equation* $x^2 + c = y^n$*: a brief overview*, Rev. Colombiana Mat. **40** (2006), no. 1, 31–37.

[3] F. S. Abu Muriefah, F. Luca and A. Togbé, *On the Diophantine equation* $x^2 + 5^a 13^b = y^n$, to appear in Glasgow Math. J.

[4] S. A. Arif and F. S. Abu Muriefah, *On the Diophantine equation* $x^2 + q^{2k+1} = y^n$, J. Number Theory **95** (2002), no. 1, 95–100.

[5] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *User's guide to PARI-GP*, version 2.3.2. (See also `http://pari.math.u-bordeaux.fr/`)

[6] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), 23–54.

[7] Yu. Bilu, G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory **60** (1996), 373–392.

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

[9] W. Bosma and B. de Smit, *Class number relations from the computational point of view*, Journal of Symbolic Computation **11** (2001), 1–15.

[10] W. Bosma, J. Cannon and C. Playoust: *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://www.maths.usyd.edu.au/`)

[11] N. Bruin, *Chabauty methods using elliptic curves*, J. reine angew. Math. **562** (2003), 27–49.

[12] Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek, *Perfect powers from products of terms in Lucas sequences*, J. reine angew. Math., to appear.

[13] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell Equation*, Compositio Mathematica **142** (2006), 31–62.

[14] Y. Bugeaud, M. Mignotte and S. Siksek, *A multi-Frey approach to some multi-parameter families of Diophantine equations*, Can. J. Math., to appear.

[15] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. **39** (1964), 537–540.

[16] J. H. E. Cohn, *Lucas and Fibonacci numbers and some Diophantine equations*, Proc. Glasgow Math. Assoc. **7** (1965), 24–28.

[17] J. H. E. Cohn, *The Diophantine equation* $x^2 + C = y^n$, Acta Arith. **LXV.4** (1993), 367–381.

[18] J. H. E. Cohn, *Perfect Pell Powers*, Glasgow Math. J. **38** (1996), 19–20.

[19] J. H. E. Cohn, *The Diophantine equation* $x^2 + C = y^n$*, II*, Acta Arith. **109.2** (2003), 205–206.

[20] J. E. Cremona, *Elliptic curve data*, http://www.warwick.ac.uk/ masgaj/

[21] E. V. Flynn, *A flexible method for applying Chabauty's Theorem*, Compositio Math. **105** (1997), 79–94.

[22] G. Hanrot, *Solving Thue equations without the full unit group*, Math. Comp. **69** (2000), 395–405.

[23] W. Ivorra and A. Kraus, *Quelques résultats sur les équations* $ax^p + by^p = cz^2$, Canad. J. Math. **58** (2006), no. 1, 115–153.

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

[25] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, preprint, 19 September 2006.

[26] 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), no. 3, 383–402.

[27] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Tracts in Mathematics 87, Cambridge University Press, Cambridge, 1986.

[28] W. A. Stein, *Modular Forms: A Computational Approach*, American Mathematical Society, Graduate Studies in Mathematics 79, 2007.

[29] Sz. Tengely, *On the Diophantine equation* $x^2 + q^{2m} = 2y^p$, Acta Arith. **127** (2007), no. 1, 71–86.

[30] J. L. Wetherell, *Bounding the Number of Rational Points on Certain Curves of High Rank*, Ph.D. dissertation, University of California at Berkeley, 1997.

[31] K. S. Williams, *Integers of Biquadratic Fields*, Canad. Math. Bull. **13** (1970), no. 4, 519–526.

Fadwa S. Abu Muriefah, Riyadh University for girls, Science Section (Mathematics), P.O. Box 60561, Riyadh 11555, Saudi Arabia

E-mail address: abumuriefah@yahoo.com

Florian Luca, Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México

E-mail address: fluca@matmor.unam.mx

Samir Siksek, Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom

E-mail address: S.Siksek@warwick.ac.uk

Szabolcs Tengely, Mathematical Institute, University of Debrecen, and the Number Theory Research Group, of the Hungarian Academy of Sciences, P.O.Box 12, 4010 Debrecen, Hungary

E-mail address: tengely@math.klte.hu