

# 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. When  $C \not\equiv 1 \pmod{4}$  we explain how the equation can be solved using the multi-Frey variant of the modular approach. 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  $p_1, \dots, p_k$ .

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

---

*Date:* September 18, 2007.

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).

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*

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

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*

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

Theorem 1 yields the following straightforward corollary.

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

$$(2) \quad x^2 + q_1^{a_1} \dots q_k^{a_k} = 2y^p,$$

satisfying

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

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  $q_1 q_2 \dots q_k$ , 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  $x^2 + 17^{a_1} = 2y^n$  and  $x^2 + 5^{a_1} 13^{a_2} = 2y^n$ , under the restrictions  $\gcd(x, y) = 1$ , and  $n \geq 3$ .

In cases when  $C \not\equiv 1 \pmod{4}$  one may try to use the modular approach [6] to solve the equation. Experience suggests that this is unlikely to succeed for equations of the form (2) which involve several variable exponents, and that one should instead invoke the multi-Frey variant of the modular approach [14]. We illustrate this by solving the equation  $x^2 + 3^{\alpha_1} 11^{\alpha_2} = 2y^n$ .

**Theorem 3.** *The only solutions to the equation*

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

are ??? *The only solutions to the equation*

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

are ??? *The only solutions to the equation*

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

are ???

## 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  $h = 2^{-i} h_2 h_3$  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].

□

## 3. LEHMER SEQUENCES

We briefly define Lehmer sequences and state some relevant facts about them. A *Lehmer pair* is a pair  $(\alpha, \beta)$  of algebraic integers such that  $(\alpha + \beta)^2$  and  $\alpha\beta$  are non-zero coprime rational integers and  $\alpha/\beta$  is not a root of unity. For a Lehmer pair  $(\alpha, \beta)$ , 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  $(\alpha_1, \beta_1)$  and  $(\alpha_2, \beta_2)$  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  $(\alpha, \beta)$  is equivalent to

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

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  $(\alpha, \beta)$  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*

$$(4) \quad \alpha = \frac{U + V\sqrt{-c}}{\sqrt{2}}, \quad \beta = \frac{U - V\sqrt{-c}}{\sqrt{2}}.$$

*Then  $(\alpha, \beta)$  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*

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

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

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

We shall also repeated use of 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  $\alpha, \beta$  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  $\alpha/\beta$  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  $\pm 1, \pm\sqrt{-1}, (\pm 1 \pm \sqrt{-3})/2$ . 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

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

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

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

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*

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

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

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

*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  $r = 0$ :

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

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

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

Our equation can thus be rewritten as

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

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.  $\square$

#### 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  $\mathbb{Q}(\sqrt{-c})$  are  $\pm 1$ . Hence

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

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

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

Thus,  $V \mid d$  and  $u_p \mid d/V$ . By Lemma 3.1,  $u_p$  has a primitive divisor unless  $q = 5$  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 definition of primitive divisor,  $q \nmid (\alpha^2 - \beta^2)^2$  and so, in particular,  $q \nmid c$ . To complete the proof, let

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

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

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

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

$$(8) \quad x^2 + q_1^{a_1} \dots q_k^{a_k} = 2y^n,$$

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 (8) 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  $\mathcal{S}$ -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  $q_1, \dots, q_k$ . There are clearly only  $4^k$  possibilities for  $c$ . Write

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

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

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  $q_1, \dots, q_k$ . There are only  $6^k$  possibilities for  $c$ . For each such  $c$ , let

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

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  $\geq 2$ . 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. APPLYING THE MODULAR APPROACH

In this section, we apply the modular approach to equation (2). Ivorra and Kraus [23] give an exhaustive recipe for Frey curves and level-lowering for equations of the form  $Uu^n + Vv^n = Ww^2$  under the assumption that the three terms in the equation are coprime.

Let  $E$  be an elliptic curve over the rationals of conductor  $N$ . For a prime of good reduction  $l$  we write  $\#E(\mathbb{F}_l)$  for the number of points on  $E$  over the finite field  $\mathbb{F}_l$ , and let  $a_l(E) = l + 1 - \#E(\mathbb{F}_l)$ . Suppose that  $f = q + \sum_{i \geq 2} c_i q^i$  is a newform of weight 2 and level  $N$  with coefficients  $c_i$  generating the number field  $\mathbb{K}/\mathbb{Q}$ . We

shall say that the curve  $E$  arises modulo  $p$  from the newform  $f$  (and write  $E \sim_p f$ ) if there is some prime ideal  $\mathfrak{P} \mid p$  of  $\mathbb{K}$  such that for all but finitely many primes  $l$  we have  $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$ .

We consider equation (1) with  $C = 17^{\alpha_1}$  and  $C = 3^{\alpha_1} 11^{\alpha_2}$ . Rewrite equation (1) as follows

$$(9) \quad 2y^p + t_1^{\beta_1} t_2^{\beta_2} z^p = x^2,$$

where  $(t_1, t_2) \in \{(17, 1), (3, 11)\}$  and  $\beta_i < p$  for  $i = 1, 2$ . Suppose that we have a solution  $(x, y, z)$  of equation (9). Associate to this solution the following Frey curves

$$\begin{aligned} E_1 : \quad Y^2 &= X^3 + 2xX^2 + 2y^p X, \\ E_2 : \quad Y^2 &= X^3 + 2xX^2 + t_1^{\beta_1} t_2^{\beta_2} y^p X. \end{aligned}$$

Applying Proposition 3.3 from [23] we obtain that

$$N(E_1)_p = N(E_2)_p = 2^7 \prod_{l \mid t_1 t_2} l.$$

Ribet's Theorem tells us that there are newforms  $f_1, f_2$  of levels  $N(E_1)_p, N(E_2)_p$  such that  $E_1 \sim_p f_1$  and  $E_2 \sim_p f_2$ . We apply the so-called multi-Frey approach [14] to bound the exponent  $p$ . We follow [14, Section 4]. For  $\phi \in \mathbb{F}_l$  let

$$D'_l(E_\phi, f) = \begin{cases} \text{Norm}_{\mathbb{K}/\mathbb{Q}}(a_l(E_\phi) - c_l), & \text{if } E_\phi \text{ is non-singular,} \\ \text{Norm}_{\mathbb{K}/\mathbb{Q}}((l+1)^2 - c_l^2), & \text{if } E_\phi \text{ is nodal,} \end{cases}$$

and

$$D_l(E_\phi, f) = \begin{cases} D'_l(E_\phi, f), & \text{if } \mathbb{K} = \mathbb{Q}, \\ lD'_l(E_\phi, f), & \text{otherwise.} \end{cases}$$

If  $l$  is a prime of moderate reduction for  $E_1$  and  $E_2$ , we then let

$$B_{l,\phi} = \gcd\{D_l(E_{1,\phi}, f_1), D_l(E_{2,\phi}, f_2)\},$$

and

$$B_l = \text{lcm}\{B_{l,\phi} : \phi \in \mathbb{F}_l\}.$$

As in [14] Proposition 4.1, we have that  $p \mid B_l$ . Note that this argument allows us to bound  $p$  provided we find  $l$  such that  $B_l \neq 0$ . If the newforms are irrational, then  $c_l \notin \mathbb{Q}$  for infinitely many of the coefficients; hence,  $B_l \neq 0$ .

- The equation  $x^2 + 17^{\alpha_1} = 2y^p$ .  
In this case, we have that  $N(E_1)_p = N(E_2)_p = 2^7 \cdot 17$ . We can compute the newforms at this level using MAGMA. There are 16 such newforms, all of them are defined over some number field of degree at least two. The previously described method is therefore successful here and we obtain that  $p$  is 3 or 5.
- The equation  $x^2 + 3^{\alpha_1} 11^{\alpha_2} = 2y^p$ .  
We have that  $N(E_1)_p = N(E_2)_p = 2^7 \cdot 3 \cdot 11$ . There are 40 newforms at this level half of them being rational. By means of the argument we mentioned above we get that  $p \in \{3, 5, 7, 13\}$  except in case of the following



20 pairs of newforms

$$\begin{aligned} & (f_1, f_{10}), (f_2, f_{11}), (f_3, f_{16}), (f_4, f_{19}), (f_5, f_{20}), \\ & (f_6, f_7), (f_7, f_6), (f_8, f_9), (f_9, f_8), (f_{10}, f_1), \\ & (f_{11}, f_2), (f_{12}, f_{13}), (f_{13}, f_{12}), (f_{14}, f_{15}), (f_{15}, f_{14}), \\ & (f_{16}, f_3), (f_{17}, f_{18}), (f_{18}, f_{17}), (f_{19}, f_4), (f_{20}, f_5), \end{aligned}$$

where these newforms are such that

$f_1 \mapsto 4224A1$	$f_2 \mapsto 4224B1$	$f_3 \mapsto 4224C1$	$f_4 \mapsto 4224D1$
$f_5 \mapsto 4224E1$	$f_6 \mapsto 4224F1$	$f_7 \mapsto 4224G1$	$f_8 \mapsto 4224H1$
$f_9 \mapsto 4224I1$	$f_{10} \mapsto 4224J1$	$f_{11} \mapsto 4224K1$	$f_{12} \mapsto 4224L1$
$f_{13} \mapsto 4224M1$	$f_{14} \mapsto 4224N1$	$f_{15} \mapsto 4224O1$	$f_{16} \mapsto 4224P1$
$f_{17} \mapsto 4224Q1$	$f_{18} \mapsto 4224R1$	$f_{19} \mapsto 4224S1$	$f_{20} \mapsto 4224T1$

and the notation  $f_1 \mapsto 4224A1$  means that  $f_1$  corresponds to the elliptic curve 4224A1 in Cremona's tables [20].

To eliminate the remaining 20 pairs, we do the same computations as before using  $l = 5, 7$  and 19. This time we also collect information related to the exponents  $\alpha_1$  and  $\alpha_2$ . Consider the pair  $(f_1, f_{10})$ . In  $\mathbb{F}_5$ , the order of 3 is 4 and we obtain that in those cases when we do not get a bound for  $p$  we have

$$\alpha_1 \equiv 1 \text{ or } 3 \pmod{4}.$$

Similarly, using  $l = 7$ , we get that

$$\alpha_1 \equiv 0, 2 \text{ or } 4 \pmod{6},$$

a contradiction. In the following table, we summarize the computations which eliminate the remaining pairs.

pair	$\alpha_1 \pmod{4}$	$\alpha_1 \pmod{6}$	$\alpha_1 \pmod{18}$
$(f_2, f_{11})$	$\{1, 3\}$		$\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$
$(f_3, f_{16})$	$\{3\}$		$\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$
$(f_4, f_{19})$	$\{1, 3\}$	$\{0, 2, 4\}$	
$(f_5, f_{20})$	$\{1, 3\}$		$\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$
$(f_6, f_7)$	$\{3\}$		$\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$
$(f_8, f_9)$	$\{1, 3\}$	$\{0, 2, 4\}$	
$(f_{12}, f_{13})$	$\{1, 3\}$	$\{0, 2, 4\}$	
$(f_{14}, f_{15})$	$\{1, 3\}$		$\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$
$(f_{17}, f_{18})$	$\{1, 3\}$		$\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$

Note that among the 20 pairs there are 10 symmetric ones and it turns out that  $(f_i, f_j)$  can be eliminated using the same primes as in case of  $(f_j, f_i)$ . Therefore, we indicated only the pairs  $(f_i, f_j)$  with  $i < j$ .

#### 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 l'équation  $x^m = y^2 + 1$* , *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, GIRLS COLLEGE OF EDUCATION, SCIENCE SECTION (MATHEMATICS),  
 P.O. BOX 60561, RIYADH 11555, SAUDI ARABIA  
*E-mail address:* abumuriefa@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](mailto:S.Siksek@warwick.ac.uk)

SZABOLCS TENGELY, MATHEMATICAL INSTITUTE, UNIVERSITY OF DEBRECEN, DEBRECEN, HUN-  
GARY

*E-mail address:* [tengely@math.klte.hu](mailto:tengely@math.klte.hu)