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 $x^2 + 17 = 2y^n$, $x^2 + 5^2 \cdot 13 = 2y^n$, and $x^2 + 3^2 \cdot 11 = 2y^n$.

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 $x^2 + q^{2m} = 2y^n$ 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
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

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

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

$$1^2 + 1 = 2 \cdot 1^1, \quad 79^2 + 9 = 2 \cdot 5^5, \quad 5^2 + 29 = 2 \cdot 3^3, \quad 117^2 + 29 = 2 \cdot 19^3,$$

$$993^2 + 29 = 2 \cdot 79^3, \quad 11^2 + 41 = 2 \cdot 3^4, \quad 69^2 + 41 = 2 \cdot 7^4, \quad 171^2 + 41 = 2 \cdot 11^4,$$

$$1^2 + 53 = 2 \cdot 3^3, \quad 25^2 + 61 = 2 \cdot 7^3, \quad 51^2 + 61 = 2 \cdot 11^3, \quad 37^2 + 89 = 2 \cdot 9^3.$$

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 $x^2 + C = 2y^n$ 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.

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

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

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 $q_1 q_2 \cdots q_k$, 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 $i$. 

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 Blu, Hanrot and Voutier on primitive divisors of Lehmer sequences. In particular, we prove the following theorem.
Lemma 2.1. The field \( \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}) \) has Galois group \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) and precisely three quadratic subfields: \( \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-c}) \) and \( \mathbb{Q}(\sqrt{-2c}) \). The ring of integers \( \mathcal{O}_K \) has \( \mathbb{Z} \)-basis

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

The class number of \( K \) is \( h = 2^{-i}h_2h_3 \) where \( h_2, h_3 \) are respectively the class numbers of \( \mathbb{Q}(\sqrt{2}) \) and \( \mathbb{Q}(\sqrt{-2c}) \), 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 \((\alpha, \beta)\) of algebraic integers such that \((\alpha + \beta)^2 \text{ and } \alpha\beta\) 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 \((\alpha^2 - \beta^2)^2 u_1 \ldots u_{n-1}\). 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

\[
(\sqrt{\alpha} - \sqrt{\beta})/2, (\sqrt{\alpha} + \sqrt{\beta})/2,
\]

where \((\alpha, b)\) 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

\[
\bullet \ a = F_{k+2\epsilon}, \ b = F_{k+2\epsilon} - 4F_k \text{ for some } k \geq 3, \ \epsilon = \pm 1, \text{ where } F_n \text{ is the Fibonacci sequence given by } F_0 = F_1 = 1 \text{ and } F_{n+2} = F_{n+1} + F_n \text{ for all } n \geq 0;
\]

\[
\bullet \ a = L_{k+2\epsilon}, \ b = L_{k+2\epsilon} - 4L_k \text{ for some } k \geq 0, \ k \neq 1, \ \epsilon = \pm 1, \text{ where } L_n \text{ is the Lucas sequence given by } L_0 = 2, L_1 = 1 \text{ and } L_{n+2} = L_{n+1} + L_n \text{ for all } n \geq 0.
\]

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

\[
\alpha = \frac{U + V\sqrt{-c}}{\sqrt{2}}, \quad \beta = \frac{U - V\sqrt{-c}}{\sqrt{2}}.
\]

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

\[
(c, U^2, V^2) \neq (1, 1, 9), (5, 1, 1), (5, 9, 1), (85, 9, 1).
\]

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

\[
t = \frac{x + 1}{x - 1} \text{ iff } x = \frac{t + 1}{t - 1}.
\]

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 $\alpha, \beta$ 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 $c \equiv 1$ (mod 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.

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

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

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

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

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 $r = 0$:

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

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

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

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

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

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

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

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

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

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 \( p = 5 \) 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, \( q \mid (\alpha^2 - \beta^2)^2 \) and so, in particular, \( q \mid c \). 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, \( q \mid (\gamma - \delta)\gamma\delta \). We claim that \( q \mid v_{q(h-cq)} \). 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 \( K = \mathbb{Q}(\sqrt{2}, \sqrt{-c}) \). Doing this, the hypothesis that would be needed is that \( p \) does not divide the class number of \( K \). By Lemma 2.1, the class number of \( \mathbb{Q}(\sqrt{-c}) \) divides the class number of \( K \), up to powers of 2. Thus, we obtained a stronger result by working in \( \mathbb{Q}(\sqrt{-c}) \) instead of \( K \).

5. **Dealing with Small Exponents**

Let \( q_1, \ldots, q_k \) be distinct primes. In this section, we explain how to solve the equation
\[
(9) \quad x^2 + q_1^{a_1} \cdots q_k^{a_k} = 2y^n,
\]
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 (9) can be reduced to computing \( S \)-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
\[
Y = \frac{2xy}{z^2}, \quad X = \frac{2y^2}{z^2}.
\]
We immediately see that \( (X, Y) \) is an \( S \)-integral point on the elliptic curve \( Y^2 = X(X^2 - 2c) \), where \( S = \{q_1, \ldots, q_k\} \).
Similarly, if \( n = 3 \), we are dealing with an equation of the form \( x^2 + C = 2y^3 \). We then write \( C = c_2^6 \) 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

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

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

If \( n \geq 5 \), then we require \( S \)-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. Proof of Theorem 3

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

- The equation \( x^2 + 17a_1 = 2y^6 \). 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 is possible to solve the equations \( x^2 + 17a_1 = 2y^6 \) and \( x^2 + 17a_1 = 2y^9 \). We apply the method described in Section 5 to determine all integral solutions. We obtain the following solutions

\[
1^2 + 17^0 = 2 \cdot 1^3, \quad 1^2 + 17^0 = 2 \cdot 1^4,
\]

\[
239^2 + 17^0 = 2 \cdot 13^4, \quad 31^2 + 17^2 = 2 \cdot 5^4.
\]

- The equation \( x^2 + 5a_113a_2 = 2y^6 \). 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 \( 5^a13^b \in \{3, 5, 13, 65\} \). Assume that \( 5^a13^b = 13 \). Working in the imaginary quadratic field \( \mathbb{Q}[i] \), we easily get

\[
5^b13^a = (U - V)(U^6 + 8U^5V - 13U^4V^2 - 48U^3V^3 - 13U^2V^4 + 8UV^5 + V^6).
\]

One can obtain all integral solutions of the Thue equations \( U^6 + 8U^5V - 13U^4V^2 - 48U^3V^3 - 13U^2V^4 + 8UV^5 + V^6 = \pm 1, \pm 5, \pm 13, \pm 65 \). The only solutions are \((U, V) \in \{(\pm 1, 0), (0, \pm 1)\}\). So we may assume that

\[
U - V = \pm 5^b13^c, \quad U^6 + 8U^5V - 13U^4V^2 - 48U^3V^3 - 13U^2V^4 + 8UV^5 + V^6 = \pm 5^{b_1-c_1}13^{b_2-c_2},
\]

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 \( 5^a13^b = 5^d, 13^d \) or \( 65^d \), then equation (8) leads to

\[
5d^2 : \quad 8d = V(7U^6 - 175U^4V^2 + 525U^2V^4 - 125V^6),
\]

\[
13d^2 : \quad 8d = V(7U^6 - 455U^4V^2 + 3549U^2V^4 - 2197V^6),
\]

\[
65d^2 : \quad 8d = V(7U^6) - 2275U^4V^2 + 88725U^2V^4 - 274625V^6),
\]
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

\[
\square = X^3 + 175\omega_1^2 X^2 + 3675\omega_1^2 X \pm 6125\omega_1^2 + 539,
\]

\[
\square = X^3 + 455\omega_2^2 X^2 + 24843\omega_2^2 X \pm 107653\omega_2^2 + 539,
\]

\[
\square = X^3 + 2275\omega_3^2 X^2 + 621075\omega_3^2 X \pm 13456625\omega_3^2 + 539,
\]

where \( \omega_1, \omega_2, \omega_3 \in \{2^{10}, 5^{22}, 13^{11} : \alpha_i = 0, 1\} \). 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** \( x^2 + 3^i 11^a = 2y^2 \). 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 \( 3^{2k+1} 11^2 = C \equiv 1 \pmod{4} \) and \( 33 \cdot 3^{2k+1} 11^2 = C \equiv 1 \pmod{4} \). 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**


Fadwa S. Abu Muriefa, 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: flucamatem.unam.mx

Samar 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