ON THE DIOPHANTINE EQUATION $x^2 + 2^a \cdot 11^b = y^n$

ISMAIL NACI CANGUL*, MUSA DEMIRCI, FLORIAN LUCA, ÁKOS PINTÉR†, AND GÖKHAN SOYDAN

ABSTRACT. In this note, we resolve the Diophantine equation $x^2 + 2^a \cdot 11^b = y^n$ with coprime positive integers $x$, $y$ and positive integers $n \geq 3$.

1. Introduction

The history of the Diophantine equation

$$x^2 + C = y^n, \quad x \geq 1, \quad y \geq 1, \quad n \geq 3$$

(1)

goes back to the 1850’s. In 1850, Lebesque [24] proved that the Diophantine equation (1) has no solutions when $C = 1$. For a fixed value of $n$, the Diophantine equation (1) is actually a special case of the Diophantine equation $ax^2 + by^2 + c = dx^n$, where $a, b, c$ and $d$ are integers with $a \neq 0$, $b^2 - 4ac \neq 0$ and $d \neq 0$, which has only a finite number of solutions in integers $x$ and $y$ when $n \geq 3$ [22]. Cohn [17] solved the Diophantine equation (1) for most values of $C$ in the range $1 \leq C \leq 100$. In [29], Mignotte and de Weger found all the positive integer solutions $(x, y)$ of the two Diophantine equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$, respectively, thus covering some of the cases left over by Cohn. In [14], Bugeaud, Mignotte and Siksek covered the remaining cases.

Variations of the Diophantine equation (1) were also considered by various mathematicians. For theoretical upper bounds for the exponent $n$ we refer to [16] or [21], however, these estimates are based on Baker’s theory, so they are huge. In [32], all the positive integer solutions $(x, y, n)$ of the Diophantine equation $x^2 + B^2 = 2y^n$ with $B \in \{3, 4, \ldots, 501\}$ were found under the conditions that $n \geq 3$ and that gcd$(x, y) = 1$. The equation $x^2 + C = 2y^n$ with $C$ a fixed positive integer and under the similar restrictions $n \geq 3$ and gcd$(x, y) = 1$ was studied in [2].

Yet a different variant of this problem when $C$ is an arbitrary power of a fixed prime was studied by various authors. In [10], the positive integer solutions $(x, y, k, n)$ of the Diophantine equations $x^2 + 2^k = y^n$ satisfying certain conditions have been found. In [23], Le verified a conjecture of Cohn from [18] proving that all the solutions of the Diophantine equation $x^2 + 2^k = y^n$ in positive integers $x, y, k, n$ with $2 \nmid y$ and $n \geq 3$ are $(x, y, k, n) = (5, 3, 1, 3), (7, 3, 5, 4), (11, 5, 2, 3)$.

All the integer solutions $(x, y, m, n)$ of the Diophantine equation $x^2 + 3^m = y^n$ with $n \geq 3$ were found in [9] (for odd $m$) and in [26] (for even $m$). For various results on other particular cases of the Diophantine equation $x^2 + p^m = y^n$, where $p$ is a fixed prime, see [4, 6, 7, 8, 27].

*The author was supported by the research fund of Uludağ University Project no: F-2006/40 and F-2008/31.
†The author was supported by grants T67580 and K75566 from the HNFSR, and by János Bolyai Fellowship.

FEBRUARY 2010 39
The last variant of the Diophantine equation (1) that we mention is when \( C \) is a product of powers of a few fixed primes. For example, all the positive integer solutions of the Diophantine equation (1), again under the assumptions that \( n \geq 3 \) and \( x \) and \( y \) are coprime with \( C \) of the forms \( C = 2^a \cdot 3^b \cdot 5^c \cdot 13^d \), \( 2^a \cdot 5^b \cdot 13^c \), \( 2^a \cdot 5^b \cdot 13^d \) were found in \([3, 20, 25]\) and \([28]\), respectively. Pink \([30]\) has obtained some results on the case \( C = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \). Recently, Bérczes and Pink \([12]\) resolved (1) with \( C = p^{2k} \) where \( 2 \leq p < 100 \) prime, \( \gcd(x, y) = 1 \) and \( n \geq 3 \). A more exhaustive survey on this type of problem is \([5]\).

Here, we add to the existing literature on this last type of Diophantine equation by studying the Diophantine equation
\[
x^2 + 2^a \cdot 11^b = y^n, \quad x \geq 1, \quad y \geq 1, \quad \gcd(x, y) = 1, \quad n \geq 3, \quad a \geq 0, \quad b \geq 0,
\]
again under the assumptions that \( n \geq 3 \) and that \( x \) and \( y \) are coprime. Our result is the following.

**Theorem 1.** The only solutions of the Diophantine equation (2) are
\[
n = 3, \quad (x, y, a, b) \in \{(2, 5, 0, 2), (4, 3, 0, 1), (5, 3, 1, 0), (5, 9, 6, 1), \}
\[
(9, 5, 2, 1), (11, 5, 2, 0), (58, 15, 0, 1), (117, 25, 4, 2), (835, 89, 6, 2), \}
\[
(5497, 785, 8, 6), (5805, 323, 1, 2), (6179, 345, 18, 1), (9324, 443, 0, 3), \}
\[
(9959, 465, 10, 3), (404003, 5465, 12, 2)\};
\]
\[
n = 4, \quad (x, y, a, b) = (7, 3, 5, 0);
\]
\[
n = 5, \quad (x, y, a, b) = (1, 3, 1, 2), (241, 9, 3, 2);
\]
\[
n = 6, \quad (x, y, a, b) = (5, 3, 6, 1), (117, 5, 4, 2);
\]
\[
n = 10, \quad (x, y, a, b) = (241, 3, 3, 2).
\]

One can deduce from the above result the following corollary.

**Corollary 2.** The only integer solutions of the Diophantine equation
\[
x^2 + 11^c = y^n, \quad x \geq 1, \quad y \geq 1, \quad \gcd(x, y) = 1, \quad n \geq 3, \quad c > 0
\]
are \((x, y, c, n) = (2, 5, 2, 3), (4, 3, 1, 3), (58, 15, 1, 3), (9324, 443, 3, 3)\).

Several cases of the Diophantine equation (2) have been dealt with previously. For example, for \( a = 0 \) and odd \( b \), all solutions have been found in \([31]\) by using an elementary method, while for \( a = 0 \) and even \( b \) they appear in \([12]\). The fact that there are no solutions when \( a \geq 3 \) and \( n \geq 13 \) follows from Theorem 1.3 in \([11]\), where the method used was the modular approach à la Wiles’ proof of Fermat’s Last Theorem. The remaining cases seem to be new.

For the proof, we apply the method used in \([3]\). We first treat the cases \( n = 4 \) and \( n = 3 \). This is done by transforming equation (2) into several elliptic equations written in quartic models and cubic models, respectively, for which we need to determine all their \( \{2, 11\} \)-integer points. At this stage we note that in \([19]\) Gebel, Hermann, Pethő and Zimmer developed a practical method for computing all \( S \)-integral points on elliptic curves. Their method is implemented in MAGMA as a routine under the name \texttt{Integral Points}. In the last section, we study the remaining cases by using primitive divisors of Lucas sequences. All the computations are done with MAGMA \([15]\) and Cremona’s program \texttt{mwrank}.

Before starting, we note that since \( n \geq 3 \), it follows that \( n \) is either a multiple of 4 or a multiple of an odd prime \( p \). Furthermore, if \( d \mid n \) is such that \( d \in \{4, p\} \) with \( p \) an odd prime
and \((x, y, a, b, n)\) is a solution of our equation (2), then \((x, y^{n/d}, a, b, d)\) is also a solution of our equation satisfying the same restrictions. Thus, we may replace \(n\) by \(d\) and \(y\) by \(y^{n/d}\) and from now on assume that \(n \in \{4, p\}\). Furthermore, note that when \(b = 0\), then our equation reduces to the equation \(x^2 + 2^a = y^n\), all whose solutions are already known from [23]. Thus, we shall assume that \(b > 0\). Since \(11^b \equiv 3, 1 \pmod{8}\) according to whether \(b\) is odd or even, respectively, it follows by considerations modulo 8 that either \(a\) is even, for otherwise with \(a\) odd we would get that \(x^2 + 11^b \equiv 2, 4 \pmod{8}\), and this last even number cannot be a perfect power of exponent \(\geq 3\) of some integer.

2. The Case \(n = 4\)

Here we have the following result.

**Lemma 3.** The Diophantine equation (2) has no solution with \(n = 4\) and \(b > 0\).

**Proof.** Equation (2) can be written as

\[
\left(\frac{x^2}{z^2}\right)^2 + A = \left(\frac{y^4}{z^4}\right),
\]

where \(A\) is fourth-power free and defined implicitly by \(2^a \cdot 11^b = A \cdot z^4\). Clearly, \(A = 2^{a_1} \cdot 11^{b_1}\), where \(a_1, b_1 \in \{0, 1, 2, 3\}\). We recall here that if \(S\) is a finite set of prime numbers, then an \(S\)-integer is a rational number of the form \(r/s\) with coprime integers \(r\) and \(s > 0\) such that all the prime factors of \(s\) are in \(S\). Thus, the problem is reduced to determining all the \(\{2, 11\}\)-integer points \((U, V) = (y/z, x/z^2)\) on the 16 elliptic curves in quartic models

\[V^2 = U^4 - 2^{a_1} \cdot 11^{b_1},\]

with \(a_1, b_1 \in \{0, 1, 2, 3\}\). We use the subroutine \texttt{SIntegralJunggrenPoints} of MAGMA [15] to determine the \(\{2, 11\}\)-integral points on the above elliptic curves and we only find the following solutions

\[(U, V, a_1, b_1) = (\pm 1, 0, 0, 0), \ (\pm 3/2, \pm 7/4, 1, 0).
\]

They do not lead to solutions of our original equation with \(b > 0\). \(\square\)

3. The Case \(n = 3\)

**Lemma 4.** The only solutions \((x, y, a, b)\) to equation (2) with \(n = 3\) and \(b > 0\) are

\[(2, 5, 0, 2), (4, 3, 0, 1), (5, 9, 6, 1), (9, 5, 2, 1), (58, 15, 0, 1), (117, 25, 4, 2), (835, 89, 6, 2), (5497, 785, 8, 6), (5805, 323, 1, 2), (6179, 345, 18, 1), (9324, 443, 0, 3), (9959, 465, 10, 3), (404003, 5465, 12, 2).
\]

**Proof.** We proceed as in the previous section except that now we create cubic models of elliptic equations. Namely, we rewrite equation (2) as

\[
\left(\frac{x^3}{z^3}\right)^2 + A = \left(\frac{y^3}{z^3}\right)^3,
\]

where \(A\) is sixth-power free and defined implicitly by \(2^a \cdot 11^b = A \cdot z^6\). Certainly, \(A = 2^{a_1} \cdot 11^{b_1}\), where \(a_1, b_1 \in \{0, 1, 2, 3, 4, 5\}\). We thus get

\[V^2 = U^3 - 2^{a_1} \cdot 11^{b_1},\]

FEBRUARY 2010 41
and we need to determine all the \( \{2, 11\} \)-points \((U, V)\) on the above 36 elliptic curves. Using \texttt{SIntegralPoints} subroutine of MAGMA and checking the rank of elliptic curves using \texttt{mrank}, we find that \((U, V, a_1, b_1)\) must be one of the following quadruples:

- \((1, 0, 0, 0), (3, 4, 0, 1), (15, 58, 0, 1), (9/4, 5/8, 0, 1), (345/64, 6179/512, 0, 1), (5, 2, 0, 2), (89/4, 835/8, 0, 2), (5465/16, 404003/64, 0, 2), (11, 0, 0, 3), (443, 9324, 0, 3), (3, 5, 1, 0), (11, 33, 1, 2), (323, 5805, 1, 2), (33/4, 143/8, 1, 2), (2, 2, 2, 0), (5, 11, 2, 0), (785/484, 5497/10648, 2, 0), (5, 9, 2, 1), (82, 702, 2, 4), (2, 0, 3, 0), (33, 187, 3, 2), (22, 0, 3, 3), (25, 117, 4, 2), (33, 121, 4, 3), (465/4, 9959/8, 4, 3), (473, 10285, 5, 3), (2057, 93291, 5, 4).

Identifying the coprime positive integers \(x\) and \(y\) from the above list and checking the condition \(b > 0\), one obtains the solutions listed in the statement of the lemma (note that not all of them lead to coprime values for \(x\) and \(y\)).

From the above lemma, we can also read the solutions for which \(n > 3\) is a multiple of 3. Namely, they are obtained from the above list when \(y\) is a perfect power. A quick inspection of the list reveals that the only such cases is when \(n = 3\) and \(y = 9\) or 25 leading to the solutions \((x, y, a, b, n) = (5, 3, 6, 1, 6)\) or \((117, 5, 4, 2, 6)\), respectively.

4. The Case \(n > 3\) Is A Prime

\textbf{Lemma 5.} If \(n > 3\) is a prime, then all the solutions to equation (2) are \((x, y, a, b, n) = (1, 3, 1, 2, 5)\) and \((241, 9, 3, 2, 5)\).

\textit{Proof.} For the beginning of the argument, we only assume that \(n\) is not a power of 2. Rewrite equation (2) as

\[ x^2 + dz^2 = y^n, \]

where \(d = 1, 2, 11, 22\) according to the parities of the exponents \(a\) and \(b\). Here, \(z = 2^n \cdot 11^\beta\) for some nonnegative integers \(a\) and \(\beta\). Thus, our equation becomes

\[ (x + i\sqrt{d}z)(x - i\sqrt{d}z) = y^n. \tag{3} \]

Write \(K = \mathbb{Q}[i\sqrt{d}]\). Observe that since \(b > 0\) and either \(a > 0\) or \(x\) is even, it follows that \(y\) is always odd. Thus, the two ideals \((x + iz\sqrt{d})\mathcal{O}_K\) and \((x - iz\sqrt{d})\mathcal{O}_K\) are coprime in the ring of integers \(\mathcal{O}_K\). Indeed, if \(I\) is some ideal dividing both the above principal ideals, then \(I\) divides both \(2z = (x + i\sqrt{d}z) + (x - i\sqrt{d}z)\) and \(y\), which are two coprime integers, so \(I = \mathcal{O}_K\). Moreover, the class number of \(K\) is always 1 or 2 and \(n\) is coprime to both the class number of \(K\) and to the cardinality of the group of units of \(\mathcal{O}_K\), which is 4 or 2 according to whether \(d = 1\) or \(d > 1\), respectively, because \(n\) is an odd prime. Furthermore, \{1, \(i\sqrt{d}\}\) is always an integral basis for \(\mathcal{O}_K\) except when \(d = 11\) in which case an integral basis is \{1, (1 + i\sqrt{11})/2\}. It thus follows that equation (3) entails that there exist \(u\) and \(v\) such that

\[ x + i\sqrt{d}z = (u + iv\sqrt{d}v)^n. \tag{4} \]

Here, either both \(u\) and \(v\) are integers, or \(2u\) and \(2v\) are both odd integers, and this last case can occur only when \(d = 11\). Writing \(\lambda = u + iv\sqrt{d}\), conjugating the above relation and eliminating \(x\) from the resulting equations, we get that

\[ 2i\sqrt{d}z = \lambda^n - \overline{\lambda}^n, \]

\[ 42 \]
yields
\[ \frac{2^\alpha \cdot 11^\beta}{v} = \frac{\lambda^n - \overline{\lambda}^n}{\lambda - \overline{\lambda}} \]  
(5)

Let us now recall that if \( \lambda \) and \( \overline{\lambda} \) are roots of a quadratic equation of the form \( x^2 - rx - s = 0 \) with nonzero coprime integers \( r \) and \( s \) and such that \( \lambda/\overline{\lambda} \) is not a root of unity, then the sequence \( \{L_m\}_{m \geq 0} \) of general term

\[ L_m = \frac{\lambda^m - \overline{\lambda}^m}{\lambda - \overline{\lambda}} \quad \text{for all } m \geq 0 \]

is called a Lucas sequence. It can also be defined inductively as \( L_0 = 2, L_1 = 1 \) and \( L_{m+2} = L_{m+1} + L_m \). Let us verify that our pair of numbers \((\lambda, \overline{\lambda})\) satisfies the necessary conditions to insure that the right hand side of equation (5) is the \( n \)th term \( L_n \) of a Lucas sequence. Note that \( \lambda \) and \( \overline{\lambda} \) are the roots of

\[ x^2 - (\lambda + \overline{\lambda})x + |\lambda|^2 = x^2 - 2(2u)x + y, \]

and \( 2u \) and \( y \) are coprime integers. Indeed, for if not, since \( y \) is odd, it follows that there exists an odd prime \( q \) dividing both \( 2u \) and \( y = u^2 + dv^2 \). Thus, \( q \) divides \( 4y = (2u)^2 + d(2v)^2 \), and since \( q \) divides the integer \( 2u \), it follows that \( q \) divides either \( d \) or \( 2v \). In either case, we get that \( q \) divides both algebraic integers

\[ (2u \pm i\sqrt{d}(2v))^n = 2^n(x \pm i\sqrt{d}z), \]

In particular, \( q \) divides the sum of the above two algebraic numbers which is \( 2u^{n+1}x \), and since \( q \) is odd, we get that \( q \) divides \( x \). This contradicts the fact that \( x \) and \( y \) are coprime.

Next, we check that \( \lambda/\overline{\lambda} \) is not a root of unity. Assume otherwise. Since this number is also in \( \mathbb{K} \), it follows that the only possibilities are \( \lambda/\overline{\lambda} = \pm 1, \text{ or } \pm i \). The first possibilities give \( u = 0 \), or \( v = 0 \), leading to \( x = 0 \), or \( z = 0 \), respectively, which are impossible. The second possibility leads to \( u = \pm v \), therefore \( y = u^2 + v^2 = 2a^2, \text{ or } 2y = (2u)^2 \). This is again impossible since \( y \) is odd and \( 2u \) is an integer. Hence, indeed the right hand side of equation (5) is the \( n \)th term of a Lucas sequence. For any nonzero integer \( k \), let us define \( P(k) \) as the largest prime dividing \( k \) with convention that \( P(\pm 1) = 1 \). Equation (5) leads to the conclusion that

\[ P(L_n) = P\left(\frac{2^\alpha \cdot 11^\beta}{v}\right) \leq 11. \]  
(6)

Let us now recall that a prime factor \( q \) of \( L_m \) is called \textit{primitive} if \( q \nmid L_k \) for any \( 0 < k < m \) and \( q \nmid (\lambda - \overline{\lambda})^2 = -4dv^2 \). It is known that when \( q \) exists, then \( q \equiv \pm 1 \pmod{m} \), where the sign coincides with the Legendre symbol \( -d \mid q \). We now recall that a particular instance of the Primitive Divisor Theorem for Lucas sequences implies that, if \( n \geq 5 \) is prime, then \( L_n \) always has a prime factor except for finitely many \textit{exceptional triples} \((\lambda, \overline{\lambda}, n)\), and all of them appear in Table 1 [13] (see also [1]).

Let us first assume that we are dealing with a number \( L_n \) without a primitive divisor. Then a quick look at Table 1 in [13] reveals that this is impossible. Indeed, all exceptional triples have \( n = 5, 7 \) or \( 13 \); of these, there is one example with \( n = 5 \) such that \( \lambda \in \mathbb{Q}[\sqrt{-d}] \) with \( d \in \{1, 2, 11, 22\} \), which is \( \lambda = \pm(1 \pm i\sqrt{11})/2 \). With such a value for \( \lambda \), we get that \( y = |\lambda|^2 = 3, \text{ or } d = 11 \), therefore the equation is \( x^2 + C = 3^2 \), where \( C = 2^a \cdot 11^b \), with \( a \) even and \( b \) odd. Since \( 3^2 > 3^3 \), we get that \( b = 1 \), and next that \( a \in \{0, 2, 4\} \), but none of these possibilities yields an integer value for \( x \).
THE FIBONACCI QUARTERLY

Now let us analyze the possibility when the Lucas number \( L_n \) appearing in the right hand side of equation (5) has a primitive divisor. Since \( n \geq 5 \), it follows that \( P(L_n) > 5 \), and so \( P(L_n) = 11 \). Since \( n \) is prime and 2 cannot be a primitive divisor of \( L_n \), it follows that 11 is primitive for \( L_n \). Thus, \( 11 \equiv 1 (mod \ n) \). Since \( n \geq 5 \) is prime, the only possibility is \( n = 5 \) and since \( 11 \equiv 1 (mod \ 5) \), we get that \( (−d \mid 11) = 1 \). Since \( d \in \{1, 2, 11, 22\} \), the only possibility is \( d = 2 \). In particular, \( u \) and \( v \) are integers. Now since \( P(L_n) = 11 \) is coprime to \(-4dv^2\), we get that \( v = \pm 2^\alpha \) for some \( \alpha \leq \alpha \). Reducing equation (5) modulo 2, we get that

\[
±2^{v−\alpha}11^\beta = \frac{(u + i\sqrt{2}v)^5 - (u - i\sqrt{2}v)^5}{2i\sqrt{2}v} \equiv 5u^4 \pmod{2},
\]

and since \( y = u^2 + 2v^2 \) is odd, we get that \( u \) is odd; therefore \( \alpha_1 = \alpha \). With \( n = 5 \) and \( v = \pm 2^\alpha \), equation (4) becomes

\[
±11^\beta = 5u^4 - 20a^2v^2 + 4v^4.
\]

Note that both when \( \alpha = 0 \) (so, \( v = \pm 1 \)), and when \( \alpha \geq 0 \) (so, \( 4 \mid v^2 \)), since \( u \) is odd it follows that the right hand side of the above equation is congruent to 5 (mod 8). So, \( ±11^\beta \equiv 5 \pmod{8} \), showing that \( \beta \) is odd and the sign on the left hand side is negative. Writing \( \beta = 2\beta_0 + 1 \), we get that

\[
-11V^2 = 5U^4 - 20U^2 + 4,
\]

where \((U, V) = (u/v, 11^\beta/v^2)\) is a \( \{2\}\)-integer point on the above elliptic curve. With MAGMA, we get that the only such points on the above curve are \((U, V) = (±1, ±1)\) and \((±1/2, ±1/4)\) leading to \((u, v) = (±1, ±1)\) and \((±1, ±2)\), respectively. They lead to the desired solutions for \( n = 5 \), and to the unique solution for \( n = 10 \).

\[\square\]

5. Acknowledgement

We thank the referee and Professor Nikos Tzanakis for providing us with some references.

References

ON THE DIOPHANTINE EQUATION $x^2 + 2^a \cdot 11^b = y^n$


MSC2000: 11D41, 11D61

Department of Mathematics, Uludağ University, 16059 Bursa, TURKEY
E-mail address: cangul@uludag.edu.tr

Department of Mathematics, Uludağ University, 16059 Bursa, TURKEY
E-mail address: mdemirci@uludag.edu.tr

Mathematical Institute, Universidad Nacional Autónoma de México, CP 58089, Morelia, Michoacán, MEXICO
E-mail address: fluca@matmor.unam.mx

Institute of Mathematics, Number Theory Research Group of the Hungarian Academy of Sciences, University of Debrecen, 4010 Debrecen, HUNGARY
E-mail address: pinterak@freemail.hu

Department of Mathematics, Uludağ University, 16059 Bursa, TURKEY
E-mail address: gsoydan@uludag.edu.tr