On the diophantine equation $x^2 + 5^k 17^l = y^n$

István Pink, Zsolt Rábai

Abstract. Consider the equation in the title in unknown integers $(x, y, k, l, n)$ with $x \geq 1$, $y > 1$, $n \geq 3$, $k \geq 0$, $l \geq 0$ and $\gcd(x, y) = 1$. Under the above conditions we give all solutions of the title equation (see Theorem 1).

1 Introduction

There are many results concerning the generalized Ramanujan-Nagell equation

$$x^2 + D = y^n,$$

where $D > 0$ is a given integer and $x, y, n$ are positive integer unknowns with $n \geq 3$. Results obtained for general superelliptic equations clearly provide effective finiteness results for this equation, too (see for example [9], [45], [47], and the references given there).

The first result concerning the above equation was due to V. A. Lebesque [28] who proved that there are no solutions for $D = 1$. Ljunggren [29] solved (1) for $D = 2$, and Nagell [39], [40] solved it for $D = 3, 4$ and $5$. In his elegant paper [21], Cohn gave a fine summary of the earlier results on equation (1). Further, he developed a method by which he found all solutions of the above equation for 77 positive values of $D \leq 100$. For $D = 74$ and $D = 86$, equation (1) was solved by Mignotte and de Weger [35]. By using the theory of Galois representations and modular forms Bennett and Skinner [8] solved (1) for $D = 55$ and $D = 95$. On combining the theory of linear forms in logarithms with Bennett and Skinner’s method and with several additional ideas, Bugeaud, Mignotte and Siksek [13] gave all the solutions of (1) for the remaining 19 values of $D \leq 100$.

Let $S = \{p_1, \ldots, p_s\}$ denote a set of distinct primes and $\mathcal{S}$ the set of non-zero integers composed only of primes from $S$. Put $P := \max\{p_1, \ldots, p_s\}$ and denote by $Q$ the product of the primes of $S$. In recent years, equation (1) has been considered also in the more general case when $D$ is no longer fixed but $D \in \mathcal{S}$ with $D > 0$. It follows from Theorem 2 of [46] that in (1) $n$ can be bounded from above by an

\textit{2010 MSC:} 11D41, 11D61

\textit{Key words:} exponential diophantine equations, primitive divisors
effectively computable constant depending only on \( P \) and \( s \). In [25] an effective upper bound was derived for \( n \) which depends only on \( Q \). Cohn [20] showed that if \( D = 2^{2k+1} \) then equation (1) has solutions only when \( n = 3 \) and in this case there are three families of solutions. The case \( D = 2^{2k} \) were considered by Arif and Abu Muriefah [2]. They conjectured that the only solutions are given by \((x, y) = (2^k, 2^{2k+1})\) and \((x, y) = (11 \cdot 2^{k-1}, 5 \cdot 2^{(k-1)/3})\), with the latter solution existing only when \((k, n) = (3M + 1, 3)\) for some integer \( M \geq 0 \). Partial results towards this conjecture were obtained in [2] and [19] and it was finally proved by Arif and Abu Muriefah [5]. Arif and Abu Muriefah [3] proved that if \( D = 3^{2k+1} \) then (1) has exactly one infinite family of solutions. The case \( D = 3^{2k} \) has been solved by Luca [31] under the additional hypothesis that \( x \) and \( y \) are coprime. In fact in [32] Luca solved completely equation (1) if \( D = 2^a 3^b \) and \( \gcd(x, y) = 1 \). Abu Muriefah [1] established that equation (1) with \( D = 5^{2k} \) may have a solution only if 5 divides \( x \) and \( p \) does not divide \( k \) for any odd prime \( p \) dividing \( n \). The case \( D = 2^a 3^b 5^c 7^d \) with \( \gcd(x, y) = 1 \), where \( a, b, c, d \) are non-negative integers was studied by Pink [41].

2 Results

Consider the following equation

\[ x^2 + 5^k 17^l = y^n \]  

(2)

in integer unknowns \( x, y, k, l, n \) satisfying

\[ x \geq 1, \ y > 1, \ n \geq 3, \ k \geq 0, \ l \geq 0 \ \text{and} \ \gcd(x, y) = 1. \]  

(3)

**Theorem 1.** Consider equation (2) satisfying (3). Then all solutions of equation (2) are:

\[(x, y, k, l, n) \in \{(94, 21, 2, 1, 3), (2034, 161, 3, 2, 3), (8, 3, 0, 1, 4)\}.

**Remark 1.** We may assume without loss of generality that in (2) \( n \geq 5 \) prime or \( n \in \{3, 4\} \). The proof of our Theorem 1 is organized as follows. If \( n \geq 5 \) prime we
use some properties of Lucas sequences, to derive a sharp upper bound for \( n \) (see also Pink [41], Theorem 2). Then we apply the result of Bilu, Hanrot and Voutier [11] concerning the existence of primitive prime divisors in Lucas sequences.

If \( n \in \{3, 4\} \) there is a general method for giving all solutions of equations of the form \( x^2 + p^k q^l = y^n \). Namely the problem is reduced to finding \( S \)-integral points on several elliptic curves, where \( S = \{p, q\} \). This works well, but in some cases the computation of the rank and the Mordell-Weil group becomes very time consuming so we need another approach. By using the parametrization provided by Lemma 1 we get several equations of the form

\[
X \pm Y = 3u^2,
\]

where \( X, Y \) are \( S \)-units and \( S = \{p, q\} \). These equations are considered locally to get a contradiction or are transformed to Ljunggren-type equations. In fact, we have to give all \( S \)-integral points on the resulting Ljunggren-type curves. Then, using MAGMA we solve completely the equations under consideration.

3 Auxiliary results

Let \( S = \{p_1, \ldots, p_s\} \) be a set of distinct primes and denote by \( S \) the set of non-zero integers composed only of primes from \( S \). Equation (2) is a special case of an equation of the type

\[
X^2 + D = Y^n,
\]

where

\[
gcd(X, Y) = 1
\]

and

\[
D \in S, \quad D > 0, \quad X \geq 1, \quad Y > 1, \quad n \geq 3.
\]

The next lemma provides a parametrization for the solutions of equation (4).

**Lemma 1.** Suppose that equation (4) has a solution under the assumptions (5) and (6) with \( n \geq 3 \) prime. Denote by \( d > 0 \) the square-free part of \( D = dc^2 \) and let \( h \) be the class number of the field \( \mathbb{Q}(\sqrt{-d}) \). Then equation (5) has a solution with \( d \not\equiv 7 \pmod{8} \) in one of the following cases:

(a) there exist \( u, v \in \mathbb{Z} \) such that \( x + c\sqrt{-d} = (u + v\sqrt{-d})^n \) and \( y = u^2 + dv^2 \).

(b) \( d \equiv 3 \pmod{8} \) and there exist \( U, V \in \mathbb{Z} \) with \( U \equiv V \equiv 1 \pmod{2} \) such that \( x + c\sqrt{-d} = \left( \frac{U+V\sqrt{-d}}{2} \right)^3 \) and \( y = \frac{U^2 + dV^2}{4} \).

(c) \( n = 3 \) if \( D = 3u^2 \pm 8 \) or if \( D = 3u^2 \pm 1 \) for some \( u \in \mathbb{Z} \).

(d) \( n = 5 \) if \( D \in \{19, 341\} \).

(e) \( p \mid h \).

**Proof.** This is a theorem of Cohn [22].
Recall that a Lucas pair is a pair \((\alpha, \beta)\) of algebraic integers such that \(\alpha + \beta\) and \(\alpha\beta\) are non-zero coprime rational integers and \(\alpha/\beta\) is not a root of unity. Given a Lucas pair \((\alpha, \beta)\) one defines the corresponding sequence of Lucas numbers by
\[
L_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad (n = 0, 1, 2, \ldots).
\]

A prime number \(p\) is called a primitive divisor of \(L_n\) if \(p\) divides \(L_n\) but does not divide \((\alpha - \beta)^2L_1 \cdots L_{n-1}\).

The next lemma gives a necessary condition for an odd prime \(p\) to be a primitive prime divisor of the \(n\)-th term of a Lucas sequence if \(n\) is an odd prime. Namely we have the following.

**Lemma 2.** Let \(L_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}\) be a Lucas sequence and suppose that \(n\) is an odd prime. Further, let \(A = (\alpha - \beta)^2\). If \(p\) is a primitive prime divisor of \(L_n\) then \(n \mid p - (\frac{A}{p})\), where \((\frac{\cdot}{p})\) denotes the Legendre symbol with respect to the prime \(p\).

**Proof.** See Carmichael [18].

The next lemma is a deep result of Bilu, Hanrot and Voutier [11] concerning the existence of primitive prime divisors in a Lucas sequence.

**Lemma 3.** Let \(L_n = L_n(\alpha, \beta)\) be a Lucas sequence. If \(n \geq 5\) is a prime then \(L_n\) has a primitive prime divisor except for finitely many pairs \((\alpha, \beta)\) which are explicitly determined in Table 1 of [11].

**Proof.** This follows from Theorem 1.4 of [11] and Theorem 1 of [49].

The following lemma of Holzer gives a criterium for the existence of solutions of ternary quadratic equations.

**Lemma 4.** Let \(a, b, c\) be coprime integers, and consider the equation
\[
ax^2 + by^2 + cz^2 = 0 \quad (7)
\]
where \(x, y, z\) are unknown integers. If there is a non-trivial solution for (7), then there is one satisfying
\[
|x| \leq \sqrt{|bc|}, \quad |y| \leq \sqrt{|ac|}, \quad |z| \leq \sqrt{|ab|}.
\]

**Proof.** See [37].

## 4 Proof of the Theorem

We introduce some notations which will be used in the course of the proof of our Theorem. Consider equation (2) satisfying the assumptions (3). Denote by \(d > 0\) the square-free part of \(5^k17^l\) that is \(5^k17^l = d(5^a17^b)^2\) where \(d \in \{1, 5, 17, 85\}\) and \(a, b \in \mathbb{Z}_{\geq 0}\). Further, let \(K\) be the imaginary quadratic field \(K = \mathbb{Q}(\sqrt{-d})\) and denote by \(h\) the class number of \(K\). As was mentioned in Remark 1, we have to distinguish essentially three cases without loss of generality. Namely, we may assume that in equation (2) \(n \geq 5\) prime or \(n \in \{3, 4\}\).
Case 1: \( n \geq 5 \) prime. Suppose first that (2) holds satisfying (3) with \( n \geq 5 \) prime. If in (2) \( y > 1 \) is even we obviously have that \( x \) is odd. Since for any odd integer \( t \) we have \( t^2 \equiv 1 \pmod{8} \) we get that \( 1 + d \equiv 0 \pmod{8} \) by reducing (2) modulo 8. This leads to \( d \equiv 7 \pmod{8} \) for \( d \in \{1,5,17,85\} \) which is clearly a contradiction. Hence in what follows we may assume that in (2) \( y > 1 \) is odd (and hence \( x \geq 1 \) is even). Since for \( d \in \{1,5,17,85\} \) the class number of the field \( K = \mathbb{Q}(\sqrt{-d}) \) is 1 or \( 2^m \), \( (m \geq 1) \) we get by Lemma 1 that equation (2) can have a solution under assumption (3) with \( n \geq 5 \) prime only in the cases (a) and (d). Since \( k \geq 1 \) and \( l \geq 1 \) we see that in (2) \( D = 19 \) cannot occur. Further, if \( D = 341 = 11 \cdot 31 \) then since \( D = 5^k \cdot 17^l \) this choice for \( D \) is impossible, too. Hence equation (2) can have a solution only in case (a) of Lemma 1. Namely, using the parametrization provided by Lemma 1 and taking complex conjugation, we get

\[
(x + 5^a 17^b \sqrt{-d})^n = (u + v \sqrt{-d})^n \quad \text{and} \quad (x - 5^a 17^b \sqrt{-d})^n = (u - v \sqrt{-d})^n
\]

(8)

for some \( u, v \in \mathbb{Z} \). Further, we also have \( y = v^2 + dv^2 \). By (9) we see that \( u \mid x \) and since \( y > 1 \) is odd and \( \gcd(x,y) = 1 \) we get that \( \gcd(2u,y) = 1 \). Let \( \alpha = u + v \sqrt{-d} \) and \( \beta = u - v \sqrt{-d} \). Then \( \gcd(\alpha \beta, \alpha + \beta) = \gcd(y,2u) = 1 \). If \( \alpha/\beta \) is a root of unity then since \( n \geq 5 \) is prime we have \( \alpha/\beta \in \{\pm 1, \pm i\} \) if \( d = 1 \). This leads to \( u = 0 \) or \( u = \pm v \). Now \( u = 0 \) yields \( x = 0 \) which is a contradiction by (4). If \( u = \pm v \) then 2 | \( y = u^2 + v^2 \) which contradicts the fact that \( y \) is odd. If \( d \in \{5,17,85\} \), then \( \alpha/\beta \) is a root of unity if \( \alpha/\beta \in \{\pm 1\} \), which leads to either \( u = 1, v = 0 \) or \( u = 0, v = 1 \). If \( u = 1, v = 0 \), then we get a contradiction with \( y \geq 3 \). If \( u = 0, v = 1 \), then \( y = d \) holds, which leads to a contradiction with \( \gcd(x,y) = 1 \). Thus

\[
L_n := \frac{(u + v \sqrt{-d})^n - (u - v \sqrt{-d})^n}{2v \sqrt{-d}}
\]

(9)

is a Lucas sequence.

Further, by (9) we have

\[
L_n = \frac{5^a 17^b}{v}
\]

for some non-negative integers \( a, b \). By Lemma 3 we get that \( L_n \) has a primitive divisor for \( n \geq 5 \) prime. Also the only prime divisors of \( L_n \) can be 5 or 17. By Lemma 2 we get that if \( p \) is a primitive divisor of \( L_n \), then \( p \equiv \pm 1 \pmod{n} \), so \( n \mid p \pm 1 \) holds. Since \( p \in \{5,17\} \), we have that one of the following cases holds:

\[
n \mid 4 = 2^2, \quad n \mid 6 = 2 \cdot 3, \quad n \mid 16 = 2^4, \quad n \mid 18 = 2 \cdot 3^2
\]

Since \( n \geq 5 \) we get a contradiction for all cases, which implies that (2) does not have a solution for \( n \geq 5 \).

Case 2: \( n = 3 \). At first, we point out that the usual method concerning the search for \( S \)-integral points on certain elliptic curves proves to be time consuming in this case, so we show a different approach.

By Lemma 1, we see that

\[
x + 5^a 17^b \sqrt{-d} = (u + v \sqrt{-d})^3
\]

(10)
holds, where $d \in \{1, 5, 17, 85\}$ and $u, v \in \mathbb{Z}$. After expanding the right hand side of equation (10), and comparing the imaginary parts, we get that

$$
5^a 17^b = v(3u^2 - dv^2).
$$

(11)

In (11) $\gcd(v, 3u^2 - dv^2) = 1$ holds, since otherwise we would get $\gcd(u, v) \neq 1$, which implies $\gcd(x, y) \neq 1$, which is clearly a contradiction. From this, we get the following type of equations:

$$
\begin{aligned}
3u^2 - dv^2 &= f \\
v &= g
\end{aligned}
$$

(12)

where

$$(f, g) \in \{(\pm 1, \pm 5^a 17^b), (\pm 5^a, \pm 17^b), (\pm 17^b, \pm 5^a), (\pm 5^a 17^b, \pm 1)\}.$$ 

Since $d \in \{1, 5, 17, 85\}$, we get a total of 16 cases, we have to deal with. We will illustrate the method in one of the more interesting cases, all the others can be done in the same way. Let $d = 5$, $f = \pm 17^b$, $g = \pm 5^a$. From this, we get that

$$3u^2 - 5^{2a+1} = \pm 17^b
$$

(13)

holds. Our main goal is to transform this to Ljunggren-type curves. To reduce the number of curves, and so the time of the computation we write (13) to the form of $Ax^2 + By^2 + Cz^2 = 0$. Now using Holzer’s theorem (see Lemma 4) we get, that (13) has a nontrivial solution if and only if $b$ is odd and $3u^2 - 5^{2a+1} = -17^b$ holds. Now we transform this to the following type.

$$
3 \left( \frac{u}{17^{2b_1}} \right)^2 = 5^{i+1} \left( \frac{5^{a_1}}{17^{b_1}} \right)^4 - 17^{j+1}
$$

(14)

where $i, j \in \{0, 2\}$, and $a = 4a_1 + i + 1$, $b = 4b_1 + j + 1$. So, the problem is reduced to finding all the $\{17\}$-integral points on quartics of the form of

$$
3Y^2 = 5^{i+1} X^4 - 17^{j+1}, \quad i, j \in \{0, 2\}, \quad \text{where } X = \frac{5^{a_2}}{17^{b_2}} \text{ and } Y = \frac{u}{17^{2b_2}}.
$$

Now, we can use MAGMA to determine all the solutions of the above equations. Repeating this for all the 16 cases we get that all the solutions of (2) with $n = 3$ are:

$$(x, y, k, l, n) \in \{(94, 21, 2, 1, 3), (2034, 161, 3, 2, 3)\}.$$ 

We point out that, in many of the above cases the method used can be combined with local methods to simplify the computations. AMdemo

**Case 3: $n = 4$.** If $n = 4$ holds, then we can write the following:

$$
y^4 - x^2 = 5^k 17^l
$$
On the diophantine equation \( x^2 + 5^k 17^l = y^n \)

which can be factored as

\[
(y^2 - x)(y^2 + x) = 5^k 17^l. \tag{15}
\]

In (15) \( \gcd(y^2 - x, y^2 + x) = 1 \) holds, else we would get a contradiction with \( \gcd(x, y) = 1 \). So, we get that

\[
\begin{cases}
y^2 - x = f \\
y^2 + x = g
\end{cases}
\]

where \( (f, g) \in \{(1, 5^k 17^l), (5^k, 17^l), (17^l, 5^k), (5^k 17^l, 1)\} \). Now, by adding the first equation to the second, we get, that

\[2y^2 = f + g\]

holds. Now using the same method as in the \( n = 3 \) case we get that with \( n = 4 \) all the solutions of (2) are

\[(x, y, k, l, n) \in \{(8, 3, 0, 1, 4)\}.

References


[18] D.Carmichael: On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. Math.* (2) 15 (1913) 30–70.


On the diophantine equation $x^2 + 5^k 17^l = y^n$

[35] M. Mignotte, B.M.M de Weger: On the equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$. 


[38] F.S.A. Muriefah, F. Luca, A. Togbe: On the diophantine equation $x^2 + 5^a 13^b = y^n$. 

Forensings Skifter 13 (1923) 65–82.

[40] T. Nagell: Contributions to the theory of a category of diophantine equations of the 
second degree with two unknowns. Nova Acta Reg. Soc. Upsal. IV Ser. 16, Uppsala 
(1955) 1–38.

[41] I. Pink: On the diophantine equation $x^2 + 2^a 3^b 5^c 7^d = y^n$. Publ. Math. Debrecen 


[46] T.N. Shorey, A.J. van der Poorten, R. Tijdeman, A. Schinzel: Applications of the 
Gel’fond-Baker method to Diophantine equations. In: Transcendence Theory: Advances 


291–304.


Authors’ addresses:
I. PINK, INSTITUTE OF MATHEMATICS, UNIVERSITY OF DEBRECEN, H-4010 DEBRECEN, 
P.O. BOX 12, HUNGARY
E-mail: pinki@math.klte.hu

Zs. RÁBAI, INSTITUTE OF MATHEMATICS, UNIVERSITY OF DEBRECEN, H-4010 DEBRECEN, 
P.O. BOX 12, HUNGARY
E-mail: zsrabai@gmail.com

Received: 23 July, 2010
Accepted for publication: 4 January, 2011
Communicated by: Attila Bérczes