ON THE EXPONENTIAL DIOPHANTINE EQUATION

\[ x^2 + p^m q^n = 2y^p \]

Kalyan Chakraborty and Azizul Hoque

(Received 29 April, 2023)

Abstract. We study the exponential Diophantine equation \( x^2 + p^m q^n = 2y^p \) in positive integers \( x, y, m, n \), and odd primes \( p \) and \( q \) using primitive divisors of Lehmer sequences in combination with elementary number theory. We discuss the solvability of this equation.

1. Introduction

The exponential Diophantine equation, so called generalized Lebesgue-Nagell equation

\[ x^2 + d = \lambda y^n, \quad x, y, n \in \mathbb{N}, \quad n \geq 3, \quad \lambda = 1, 2, 4, \quad (1.1) \]

has a long and rich history. Its study, for specific values of \( d, n \) and \( \lambda \), dates back to the works of Fermat and Euler. It was Lebesgue who first proved that (1.1) has no solution when \((d, \lambda) = (1, 1)\). Nowadays there are many results on the solutions of (1.1) for various values of \( d \), and also for \( d \) ranging in some infinite set of positive integers. A beautiful survey on this very interesting topic can be found in [17]. A generalization of (1.1), that is, the Diophantine equation,

\[ cx^2 + d^n = 4y^n, \quad x, y, n \in \mathbb{N}, \quad n \geq 3, \quad (1.2) \]

for given square-free positive integers \( c \) and \( d \), has been studied by several authors (cf. [4, 5, 7, 9, 13, 16]). In [4], Bilu studied (1.2) for ‘odd \( m \)’ under certain conditions. He pointed out that there is a flaw in [16] and a fortiori Bugeaud’s result in [5], and corrected that inaccuracy. In contrast, (1.2) has been studied in [9, 13] for ‘even \( m \)’. The authors completely solved (1.2) in [2, 7] when \( c = 1 \) and \( d = 1, 2, 3, 7, 11, 19, 43, 67, 163 \). Recently, the second author deeply investigated an analogous generalization of (1.1) in [14] when \( \lambda = 2 \). In [18], Patel deeply studied a similar generalization of (1.1) for \( \lambda = 1 \). More precisely, she presented a practical method for solving the Diophantine equation,

\[ cx^2 + d = y^n, \quad x, y, n \in \mathbb{N}, \quad \gcd(cx, d, y) = 1, \quad n \geq 3, \]

satisfying certain conditions.

Many authors considered (1.1) when \( d \) is a product of primes with different exponents and investigated their solutions (cf. [1, 6, 8, 12, 23]). In particular, Alan and Zengin [1] (res. Chakraborty et al. [8]) completely solved (1.1) when \( \lambda = 1 \) and \( d = 3^a 11^b \) (res. \( d = 2^a 11^b 19^c \)). In [12, 23], the equation (1.1) has
been solved when \( d = 2^n p^b \) with odd prime \( p \). Recently, Godinho and Neumann [15] obtained some conditions for the existence of the solutions of the following variation:

\[
x^2 + p^m q^n = y^p, \quad x, y, m, n \in \mathbb{N}, \quad \gcd(x, y) = 1,
\]

where \( p \) and \( q \) are distinct odd primes with \( p \geq 5 \). They used primitive divisors of certain Lucas sequences as well as the factorization of certain polynomials.

In this paper, we investigate the integer solutions \((x, y, m, n)\) of the slightly different variation of the above equation, viz.

\[
x^2 + p^m q^n = 2 y^p, \quad x, y, m, n \in \mathbb{N}, \quad \gcd(x, y) = 1,
\]

where \( p > 3 \) and \( q \geq 3 \) are distinct primes. This equation has been well investigated when either \( m = 0 \) or \( n = 0 \) (cf. [19, 22]). We consider both \( m \) and \( n \) to be positive integers and obtain the conditions for which (1.3) has no solution. The main result is:

**Theorem 1.1.** Let \( p > 3 \) and \( q \geq 3 \) be distinct primes. Assume that \( d \) is the square-free part of \( p^m q^n \) and \( h(-d) \) denotes the class number of \( \mathbb{Q}(\sqrt{-d}) \). If \( n \) is odd, \( d \not\equiv 7 \pmod{8} \) and \( \gcd(p, h(-d)) = 1 \), then (1.3) has no solution, except \((p, q, x, y, m, n) = (5, 17, 21417, 47, 3, 1)\). Further for even \( n \), (1.3) has no solution when \( q^{n/2} \not\equiv \pm 1 \pmod{p} \) and one of the following holds:

(i) \( m \) is even,
(ii) \( m \) is odd and \( p \not\equiv 7 \pmod{8} \).

**Remarks.** The following comments are worth to be noted.

(i) Let’s assume that \( N \) is a positive integer with \( p \mid N \) and consider the following extension of (1.1):

\[
x^2 + p^m q^n = 2 y^N, \quad x, y, m, n, N \in \mathbb{N}, \quad \gcd(x, y) = 1.
\]

Then Theorem 1.1 also holds for this equation too.

(ii) Let \( p \in \{13, 19, 43, 67, 163\} \) and \( q \in \{11, 19, 43, 67, 163\} \). For \( p \neq q \), (1.3) has no solution.

(iii) For the twin primes (both \( p \) and \( p + 2 \) are primes), then the Diophantine equation

\[
x^2 + p^m (p + 2)^2p = 2 y^p, \quad x, y, m, n \in \mathbb{N}, \quad \gcd(x, y) = 1
\]

has no solution.


2. Preliminary Descent

The following lemma is a part of [21, Corollary 3.1].

**Lemma 2.1.** For a given square-free positive integer \( d > 3 \), let \( k \geq 3 \) be an odd integer such that \( \gcd(k, h(-d)) = 1 \). Then all the positive integer solutions \((x, y, z)\) of the Diophantine equation

\[
x^2 + dy^2 = 2z^k, \quad \gcd(x, dy) = 1
\]

can be expressed as

\[
x + y\sqrt{-d} \over\sqrt{2} = \varepsilon_1 a + \varepsilon_2 b\sqrt{-d} \over\sqrt{2} \right)^k,
\]
where \( a \) and \( b \) are positive integers satisfying \( a^2 + b^2d = 2y, \gcd(a, bd) = 1, \) and \( \varepsilon_1, \varepsilon_2 \in \{-1, 1\} \).

Before proceeding further we need to recall some definitions. A pair of algebraic integers \( \alpha \) and \( \bar{\alpha} \) forms a Lehmer pair when \( (\alpha + \bar{\alpha})^2 \) and \( \alpha \bar{\alpha} \) are two non-zero coprime rational integers, and \( \alpha/\bar{\alpha} \) is not a root of unity. Given a positive integer \( t \), the \( t \)-th Lehmer number corresponds to the pair \( (\alpha, \bar{\alpha}) \) is defined as

\[
L_t(\alpha, \bar{\alpha}) = \begin{cases} 
\alpha^t - \bar{\alpha}^t & \text{when } t \text{ is odd}, \\
\alpha - \bar{\alpha} & \text{when } t = 1, \\
\alpha^t - \bar{\alpha}^t & \text{when } t \text{ is even}.
\end{cases}
\]

It is well known that all Lehmer numbers are non-zero rational integers. The pairs \( (\alpha_1, \bar{\alpha}_1) \) and \( (\alpha_2, \bar{\alpha}_2) \) are called equivalent if \( \alpha_1/\alpha_2 = \bar{\alpha}_1/\bar{\alpha}_2 \in \{\pm 1, \pm \sqrt{-1}\} \). A prime divisor \( p \) of \( L_k(\alpha, \bar{\alpha}) \) is primitive if \( p \nmid (\alpha^2 - \bar{\alpha}^2)^2L_1(\alpha, \bar{\alpha})L_2(\alpha, \bar{\alpha}) \cdots L_{k-1}(\alpha, \bar{\alpha}) \).

The following result about the primitive divisors of Lehmer numbers [3, Theorem 1.4] will be handy for us.

**Theorem A.** For any integer \( t > 30 \), the Lehmer numbers \( L_t(\alpha, \bar{\alpha}) \) have primitive divisors.

Assume that \( (\alpha, \bar{\alpha}) \) is a Lehmer pair. Then we can write \( \alpha = (\sqrt{a} \pm \sqrt{b})/2 \) and \( \bar{\alpha} = (\sqrt{a} \mp \sqrt{b})/2 \) by taking \( a = (\alpha + \bar{\alpha})^2 \) and \( b = (\alpha - \bar{\alpha})^2 \). The pair \( (a, b) \) is called the parameters corresponding to the Lehmer pair \( (\alpha, \bar{\alpha}) \). The next lemma is extracted from [20, Theorem 1].

**Lemma 2.2.** Let \( p \) be a prime such that \( 7 \leq p \leq 29 \). If the Lehmer numbers \( L_p(\alpha, \bar{\alpha}) \) have no primitive divisor, then up to equivalence, the parameters \( (a, b) \) of the corresponding Lehmer pair \( (\alpha, \bar{\alpha}) \) are given by:

(i) for \( p = 7 \), \( (a, b) = (1, -7), (1, -19), (3, -5), (5, -7), (13, -3), (14, -22) \);

(ii) for \( p = 13 \), \( (a, b) = (1, -7) \).

Let \( F_k \) (resp. \( L_k \)) be the \( k \)-th term in the Fibonacci (resp. Lucas) sequence defined as follows:

\[
\begin{align*}
F_{k+2} &= F_k + F_{k+1}, & F_0 = 0, & F_1 = 1, & k \geq 0, \\
L_{k+2} &= L_k + L_{k+1}, & L_0 = 2, & L_1 = 1, & k \geq 0.
\end{align*}
\]

Then the following lemma follows from [3, Theorem 1.3].

**Lemma 2.3.** Assume that the Lehmer numbers \( L_5(\alpha, \bar{\alpha}) \) have no primitive divisor.

Then up to equivalence, the parameters \( (a, b) \) of the corresponding pair \( (\alpha, \bar{\alpha}) \) are given by

\[
(a, b) = \begin{cases} 
(F_{k-2t}, F_{k-2t} - 4F_k) & \text{with } k \geq 3, \\
(L_{k-2t}, L_{k-2t} - 4L_k) & \text{with } k \neq 1;
\end{cases}
\]

where \( t \neq 0 \) and \( k \geq 0 \) are any integers and \( \varepsilon = \pm 1 \).

We also need some basic properties of Fibonacci numbers and Lucas numbers.

**Theorem B** ([11, Theorems 2 and 4]). For an integer \( k \geq 0 \), let \( F_k \) (resp. \( L_k \)) denote the \( k \)-th Fibonacci (resp. Lucas) number. Then

(i) if \( L_k = 2x^2 \), then \( (k, x) = (0, 1), (6, 3) \).
(i) if $F_k = 2x^2$, then $(k, x) = (0, 0), (3, 1), (6, 2)$.

It is not hard to prove the following lemma.

**Lemma 2.4.** Assume that $(k, d) = (7, 5), (47, 85)$. Then the solutions of the Diophantine equation

$$x^2 + dz^2 = 2 \times k^5, \ x, z \in \mathbb{N}$$

are given by

$$(x, z) = \begin{cases} (63, 77), (147, 49), (183, 5) & \text{if } (k, d) = (7, 5); \\ (21417, 5) & \text{if } (k, d) = (47, 85). \end{cases}$$

### 3. Proof of Theorem 1.1

Assume that $(x, y, m, n)$ is a positive integer solution of (1.3) for a given pair of distinct primes $p > 3$ and $q \geq 3$. Then (1.3) can be written as

$$x^2 + z^2d = 2y^p, \quad (3.1)$$

where

$$\begin{cases} z = p^{m_1}q^{n_1} \text{ with } m_1 = \left\lfloor \frac{m}{2} \right\rfloor \text{ and } n_1 = \left\lfloor \frac{n}{2} \right\rfloor, \\ d = 1, p, q, pq. \end{cases} \quad (3.2)$$

Since both $p$ and $q$ are odd primes, so that $x$ is odd. If $y$ is even then reading (3.1) modulo 8, we get $d \equiv 7 \pmod{8}$. This contradicts our assumption and thus $y$ is also odd.

Note that by the assumption, $\gcd(p, h(-d)) = 1$ when $n$ is odd. Again for even $n$, we have $d = 1$ when $m$ is even and $d = p$ when $m$ is odd. In the latter case, it follows from the Dirichlet class number formula that $1 \leq h(-p) < p$ (see [10, p. 67]). Thus, in either case, $\gcd(p, h(-d)) = 1$.

Here, $\gcd(dz, x) = 1$ as $\gcd(x, y) = 1$. Since $\gcd(p, h(-d)) = 1$ with $p$ odd, so that by Lemma 2.1 we have

$$\frac{x + z\sqrt{-d}}{\sqrt{2}} = \varepsilon_1 \left( a + \varepsilon_2b\sqrt{-d} \right)^p, \quad (3.3)$$

where $a$ and $b$ are positive coprime integers satisfying

$$a^2 + b^2d = 2y. \quad (3.4)$$

Here, $\varepsilon_1, \varepsilon_2$ are as defined in Lemma 2.1. Note that for $d = 3$, $\varepsilon_1$ satisfies $\varepsilon_1^6 = 1$ and hence it can be absorbed into the $p$-th power as $p > 3$.

Assume that

$$\begin{cases} \alpha = a + \varepsilon_2b\sqrt{-d} \sqrt{2}, \\ \bar{\alpha} = a - \varepsilon_2b\sqrt{-d} \sqrt{2}. \end{cases} \quad (3.5)$$

By (3.4), we see that $\alpha$ satisfies the polynomial $X^4 + 2(y - a^2)X^2 + y^2 \in \mathbb{Z}[X]$, and hence $\alpha$ is an algebraic integer and so is $\bar{\alpha}$. Since $\gcd(a, bd) = 1$, so that (3.4) gives $\gcd(a, y) = 1$, and thus $(\alpha + \bar{\alpha})^2 = 2a^2$ and $\alpha\bar{\alpha} = y$ are coprime (as $y$ is odd).

Now we have

$$\frac{2a^2}{y} = \frac{(\alpha + \bar{\alpha})^2}{\alpha\bar{\alpha}} = \frac{\alpha}{\bar{\alpha}} + \frac{\bar{\alpha}}{\alpha} + 2,$$
which implies that
\[ y \left( \frac{\alpha}{\alpha} \right)^2 + 2(y - a^2)\frac{\alpha}{\alpha} + y = 0. \]

Since \( \gcd(2(y - a^2), y) = \gcd(2\alpha, y) = 1 \), so that \( \alpha/\bar{\alpha} \) is not an algebraic integer and thus it is not a root of unity. Therefore, \( (\alpha, \bar{\alpha}) \) is a Lehmer pair.

As \( p \) is odd prime, the corresponding Lehmer numbers are given by
\[ L_p(\alpha, \bar{\alpha}) = \frac{\alpha^p - \bar{\alpha}^p}{\alpha - \bar{\alpha}}. \]
We use (3.1), (3.3) and (3.5) to get
\[ |L_p(\alpha, \bar{\alpha})| = \left| \frac{p^{m_1}q^{n_1}}{b} \right|. \]

Since \( L_p(\alpha, \bar{\alpha}) \in \mathbb{Z} \), so that \( b \mid p^{m_1}q^{n_1} \) which ensures that \( p \) and \( q \) are the only candidates for the primitive divisors of \( L_p(\alpha, \bar{\alpha}) \). However the fact 'if \( \ell \) is a primitive divisor of \( L_p(\alpha, \bar{\alpha}) \), then \( \ell \equiv \pm 1 \pmod{p} \)' helps us to remove \( p \) from the possibility of the primitive divisor.

Now if \( q \) is the primitive divisor of \( L_p(\alpha, \bar{\alpha}) \) then \( q \nmid (\alpha^2 - \bar{\alpha}^2)^2 \). Here, \( (\alpha^2 - \bar{\alpha}^2)^2 = -4a^2b^2d \) and thus \( q \) to be the primitive divisor of \( L_p(\alpha, \bar{\alpha}) \) only when \( n_1 \geq 1 \), \( b = p^{m_2} \) and \( d \in \{1, p\} \) with \( 0 \leq m_2 \leq m_1 \). Therefore, we can conclude by (3.6) that \( L_p(\alpha, \bar{\alpha}) \) has no primitive divisor except for the cases \( n_1 \geq 1 \), \( d \in \{1, p\} \) and \( b = p^{m_2} \) with \( 0 \leq m_2 \leq m_1 \). Thus by Theorem A, there is no Lehmer number \( L_p(\alpha, \bar{\alpha}) \) for \( p > 30 \) and hence (1.3) has no positive integer solution for \( p > 30 \) except for \( n_1 \geq 1 \), \( d \in \{1, p\} \) and \( b = p^{m_2} \) with \( 0 \leq m_2 \leq m_1 \).

Since \( (\alpha + \bar{\alpha})^2, (\alpha - \bar{\alpha})^2 \) are the parameters of the pair \( (\alpha, \bar{\alpha}) \), so that by Lemma 2.2 there is no Lehmer number \( L_p(\alpha, \bar{\alpha}) \) for \( p \geq 7 \). Therefore (1.3) has no positive integer solution for \( p \geq 7 \).

Now for \( p = 5 \), Lemma 2.3 gives us
(i) \( F_{k-2e} = 2a^2 \),
(ii) \( 4F_k - F_{k-2e} = 2b^2d \) with \( k \geq 3 \),
or,
(iii) \( L_{k-2e} = 2a^2 \),
(iv) \( 4L_k - L_{k-2e} = 2b^2d \) with \( k \neq 1 \).

Applying Theorem B in (i), we get \( (k, e, a) \in \{(2, 1, 0), (5, 1, 1), (4, -1, 2), (8, 1, 2)\} \). As \( a \) is positive odd integer, so that \( (k, e, a) = (5, 1, 1) \) and thus by (ii), we have \( 4F_k - F_3 = 2b^2d \). This implies that \( b^2d = 9 \), and hence by (3.4), we get \( (y, d) = (5, 1) \). Therefore (3.1) becomes \( x^2 + z^2 = 2 \times 5^3 \), which gives \( (x, z) = (3, 79), (79, 3) \) as \( \gcd(x, y) = 1 \). These solutions lead to \( m = 0 \), which is out of our consideration. Nevertheless, these solutions are listed in Table 1.

As before, by Theorem B we get \( (k, e, a) \in \{(4, -1, 3), (8, 1, 3)\} \), and thus (ii) gives \( (a, b, d) \in \{(3, 1, 5), (3, 1, 85)\} \). Therefore using (3.4), we get \( (d, y) \in \{(5, 7), (85, 47)\} \), and hence (3.1) and Lemma 2.4 together give us \( (x, y, z, d) = (183, 7, 5, 5), (21417, 47, 5, 85) \). As \( dz^2 = p^nq^n \) (see (3.2)), so that \( (x, y, z, d) = (183, 7, 5, 5) \) implies that \( n = 0 \) which is not possible as \( n \geq 1 \). Similarly, \( (x, y, z, d) = (21417, 47, 5, 85) \) gives \( (p, q, m, n) = (5, 17, 3, 1) \). Thus \( (p, q, x, y, m, n) = (5, 17, 21417, 47, 3, 1) \), which is a solution of (1.3). These solutions are listed in Table 1.
ensures that

Now we consider the case when $d = 1$. In this case, $m_1 = m/2$ and hence $m_1 = m/2$. Thus (3.7) implies that

If $m_2 = 0$, then the above equation can be reduced to

This implies that $m = 0$, which contradicts to our assumption. Therefore $m_2 \geq 1$ and hence reading (3.8) modulo $p^2$, we arrive at

This can be further reduced to $p^{m_2-1}q^{n/2} \equiv \pm 1 \pmod{p}$, which implies that $m_2 = m/2 - 1$ and $q^{n/2} \equiv \pm 1 \pmod{p}$. This contradicts the assumption.

Now we consider the final case, that is $d = p$. In this case, (3.7) implies that

This further implies that

Table 1: All the solutions of (1.3)

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
<th>$p$</th>
<th>$q$</th>
<th>$m$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>5</td>
<td>5</td>
<td>79</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>79</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>183</td>
<td>7</td>
<td>5</td>
<td>q</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>21417</td>
<td>47</td>
<td>5</td>
<td>17</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>
ON THE EXPONENTIAL DIOPHANTINE EQUATION \( x^2 + p^m q^n = 2y^n \)  

Since \( \sum_{j=1}^{(p-1)/2} \left( \frac{p}{2j+1} \right) p^{2j-2} q^{2m_2} (-p)^{j-1} \equiv 0 \pmod{p} \), so that the above equation implies that 

\[
p^{m_1 - m_2 - 1} q^{n/2} \equiv \pm 1 \pmod{p}.
\]

This further implies that \( q^{n/2} \equiv \pm 1 \pmod{p} \) with \( m_1 = m_2 + 1 \), which contradicts our hypothesis. Thus we complete the proof.

Acknowledgements. The authors are thankful to Professor Andrzej Dabrowski for providing a copy of [12]. The authors are grateful to the anonymous referee for careful reading and valuable comments which have helped to improve this paper.

References


Kalyan Chakraborty
Department of Mathematics
SRM University AP
Neerukonda, Mangalagiri Mandal
Guntur-522240
Andhra Pradesh,
India.
kalyan.c@srmap.edu.in

Azizul Hoque
Department of Mathematics,
Faculty of Science, Rangapara College,
Rangapara, Sonitpur-784505,
Assam,
India.
ahoque.ms@gmail.com