ON THE GENERALIZED RAMANUJAN-NAGELL EQUATION $x^2 - D = 2^{n+2}$

LE MAOHUA

Abstract. Let $D$ be a positive integer which is odd. In this paper we prove that the equation $x^2 - D = 2^{n+2}$ has at most three positive integer solutions $(x, n)$ except when $D = 2^{2m} - 3 \cdot 2^{m+1} + 1$, where $m$ is a positive integer with $m \geq 3$.

1. Introduction

Let $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$ be the sets of integers, positive integers and rational numbers respectively. Let $D \in \mathbb{N}$ be odd, and let $N(D)$ denote the number of solutions $(x, n)$ of the generalized Ramanujan-Nagell equation

\[ x^2 - D = 2^{n+2}, \quad x > 0, \, n > 0. \]

In [1], Beukers proved that $N(D) \leq 4$. Simultaneously, he showed that if $N(D) > 3$, then $D$ must be among the following types:

(I) $D = 2^{2m} - 3 \cdot 2^{m+1} + 1$, $m \in \mathbb{N}$, $m \geq 3$.

(II) $D = ((2^{m+1} - 17)/3)^2 - 32$, $m \in \mathbb{N}$, $m \geq 3$.

(III) $D = 2^{2m_2} + 2^{2m_1} - 2^{m_3+m_4+1} - 2^{m_4+1} - 2^{m_1+1} + 1$, $m_1, m_2 \in \mathbb{N}$, $m_2 > m_1 + 1 > 2$.

Moreover, equation (1) has exactly four solutions $(x, n) = (2^m - 3, 1)$, $(2^m - 1, m)$, $(2^m + 1, m + 1)$, and $(3 \cdot 2^m - 1, 2m + 1)$ if $D$ is of type I. In this paper, we completely determine all $D$ for which $N(D) = 4$.

Theorem. If $D$ is of type I, then $N(D) = 4$ otherwise $N(D) \leq 3$.

2. Preliminaries

Lemma 1 [3, Formula 1.76]. For any $m \in \mathbb{N}$ and any complex numbers $\alpha$, $\beta$, we have

\[ \alpha^m + \beta^m = \sum_{i=0}^{[m/2]} (-1)^i \binom{m}{i} (\alpha + \beta)^{m-2i} (\alpha \beta)^i, \]

Received by the editors March 30, 1990 and, in revised form, September 18, 1990.


1 Throughout this paper, “solution” and “positive solution” are the abbreviations for “integer solution” and “positive integer solution” respectively.

2 In [1] there is a misprint in this expression.
where
\[
\left[ \frac{m}{i} \right] = \frac{(m - i - 1)!m}{(m - 2i)!i!}, \quad i = 0, \ldots, \left\lfloor \frac{m}{2} \right\rfloor,
\]
are positive integers. □

Lemma 2 [2, Theorem 6.10.3]. Let \(a/b, a'/b', a''/b'' \in \mathbb{Q}\) be positive with \(ab' - a'b = \pm 1\). If \(a''/b''\) lies in the interval \((a/b, a'/b')\), then there exist positive integers \(c, c'\) such that
\[
a'' = ca + c'a', \quad b'' = cb + c'b'. \quad \square
\]

Lemma 3. If \((U, V)\) is a positive solution of the equation
\[
U^2 - 2V^2 = 1
\]
with \(2^{m+1}|V\) for some \(m \in \mathbb{N}\), then \(U + V\sqrt{2} = (3 + 2\sqrt{2})^t\) for some \(t \in \mathbb{N}\).

Proof. Since \(3 + 2\sqrt{2}\) is the fundamental solution of equation (2), we have \(U + V\sqrt{2} = (3 + 2\sqrt{2})^\gamma\) for some \(\gamma \in \mathbb{N}\). Then
\[
V = \sum_{i=0}^{((r-1)/2)} \left( \frac{\gamma}{2i + 1} \right)^{2^j} 2^{3j+i+1}.
\]
If \(2^{m+1}|V\), then from (3) we see that \(2|\gamma\). Further, if \(2^\lambda||\gamma\), since
\[
\left( \frac{\gamma}{2j + 1} \right) 2^{3j+1} = \gamma \left( \frac{\gamma - 1}{2j} \right) 2^{3j+1} \equiv 0 \pmod{2^{k+2}} \quad \text{for } j > 0,
\]
we obtain \(\lambda \geq m\) by (3). The lemma is proved. □

Let \(d \in \mathbb{N}\) be nonsquare, and let \(k \in \mathbb{Z}\) with \(\gcd(k, d) = 1\).

Lemma 4 [2, Theorem 10.8.2]. If \(|k| < \sqrt{d}\) and \((X, Y)\) is a positive solution of the equation
\[
X^2 - dY^2 = k, \quad \gcd(X, Y) = 1,
\]
then \(X/Y\) is a convergent of \(\sqrt{d}\). □

It is a well-known fact that the simple continued fraction of \(\sqrt{d}\) can be expressed as \([a_0, a_1, \ldots, a_s]\), where \(a_0 = (\sqrt{d})\), \(a_s = 2a_0\), and \(a_i < 2a_0\) for \(i = 0, \ldots, s - 1\).

Lemma 5. For any nonnegative integer \(j\), let \(p_j/q_j\) and \(\gamma_j\) denote the \(j\)th convergent and complete quotient of \(\sqrt{d}\) respectively. Further let
\[
k_j = (-1)^{j-1}(p_j^2 - dq_j^2) \quad \text{and} \quad \Delta_j = (-1)^j(p_{j-1}p_j - dq_{j-1}q_j).
\]
Then we have:
(i) \(k_j > 0, \quad \Delta_j > 0, \quad \text{and} \)
\[
a_{j+1} = \left[ \frac{\Delta_j + \sqrt{d}}{k_j} \right].
\]
(ii) \(k_j = 1\) if and only if \(a_{j+1} = 2a_0\).
(iii) Let
\[
t = \begin{cases} 
   s - 1, & \text{if } 2|s, \\
   2s - 1, & \text{if } 2 \nmid s.
\end{cases}
\]
Then \( p_t + q_t \sqrt{d} \) is the fundamental solution of the equation

\[ u^2 - dv^2 = 1. \]

(iv) For any \( m \in \mathbb{N} \), \( k_{m+1} = k_m \) (i = 0, \ldots, s - 1).

(v) If \( 1 < k < \sqrt{d} \), \( 2d \neq 0 \mod k \) and equation \((4)\) has solutions \((X, Y)\), then it has at least two positive solutions such that

\[ X < p_t, \quad Y < q_t. \]

**Proof.** Since \( \frac{q_0}{p_0} < \cdots < \frac{q_{2m}}{p_{2m}} < \frac{q_{2m+2}}{p_{2m+2}} < \cdots < \sqrt{d} < \cdots < \frac{q_{2m+1}}{p_{2m+1}} < \frac{p_{2m-1}}{q_{2m-1}} < \cdots < \frac{p_1}{q_1} \)

for any \( m \in \mathbb{N} \), we get \( k_j > 0 \) and \( \Delta_j > 0 \). Since \( p_{j-1}q_j - p_jq_{j-1} = (-1)^j \), we have

\begin{align*}
(8) & \quad p_j = \Delta_j q_j + k_j q_{j-1}, \quad d q_j = \Delta_j p_j + k_j p_{j-1}, \\
(9) & \quad d = \Delta_j^2 + k_j k_{j-1}.
\end{align*}

So we obtain

\begin{align*}
(10) & \quad \gamma_{j+1} = -\frac{p_{j-1} - q_{j-1} \sqrt{d}}{p_j - q_j \sqrt{d}} = \frac{(p_{j-1} - q_{j-1} \sqrt{d})(p_j + q_j \sqrt{d})}{(p_j - q_j \sqrt{d})(p_j + q_j \sqrt{d})} = \frac{\Delta_j + \sqrt{d}}{k_j}.
\end{align*}

Since \( a_{j+1} = [\gamma_{j+1}] \), \((5)\) is proved by \((10)\).

If \( k_j = 1 \), then from \((8)\) we get

\begin{align*}
(11) & \quad p_j/q_j = \Delta_j + q_{j-1}/q_j.
\end{align*}

From

\[ \left[ \begin{array}{c}
q_j - 1 \\
q_j
\end{array} \right] = \left\{ \begin{array}{ll}
1, & \text{if } j = 1 \text{ and } q_0 = q_1 = 1, \\
0, & \text{otherwise,}
\end{array} \right. \]

we obtain \( \Delta_j = a_0 \) by \((11)\), and \( a_{j+1} = 2a_0 \) by \((5)\). On the other hand, if \( a_{j+1} = 2a_0 \), since \( \Delta_j < \sqrt{d} \) by \((9)\), then we have \( k_j = 1 \) by \((5)\). Thus \((ii)\) is proved.

By \((ii)\), \((iii)\) is clear. In addition, \((iv)\) is Theorem 10.8.3 of [2].

Let \((X, Y)\) be a solution of equation \((4)\). Since \( k > 1 \) implies \( XY \neq 0 \), then \( (|X|, |Y|) \) is a positive solution of equation \((4)\). By Lemma 4, \(|X|/|Y|\) is a convergent of \( \sqrt{d} \) since \( 0 < k < \sqrt{d} \). Hence \( |X|/|Y| = p_{2r+1}/q_{2r+1} \) (\( r \geq 0 \)). Then there exists the integers \( a, i \) such that \( a \geq 0, 2|a|s, 2 \dagger i \), and \( 0 < i < t \), since \( k > 1 \). By \((iv)\), we have \( k_i = k \). It follows that \((p_i, q_i)\) is a positive solution of equation \((4)\) with \((7)\). Let

\begin{align*}
(12) & \quad X' = p_i p_t - d q_i q_t, \quad Y' = p_i q_t - p_t q_i.
\end{align*}

Then \( X', Y' \) are coprime integers. From

\[ X'^2 - d Y'^2 = (p_i^2 - d q_i^2)(p_t^2 - d q_t^2) = k, \]

we see that \((X', Y')\) is a solution of equation \((4)\). Further, \((X', Y')\) is a positive solution by

\[ 0 < X' - Y' \sqrt{d} = (p_i + q_i \sqrt{d})(p_t - q_t \sqrt{d}) = \frac{p_i + q_i \sqrt{d}}{p_t + q_t \sqrt{d}} < 1. \]

By Lemma 4, \( X'/Y' \) is a convergent of \( \sqrt{d} \). From

\[ X' + Y' \sqrt{d} = (p_i - q_i \sqrt{d})(p_t + q_t \sqrt{d}) < p_t + q_t \sqrt{d}, \]
we get $X' < p_i$ and $Y' < q_i$. If $(X', Y') = (p_i, q_i)$, since $\gcd(p_i, q_i) = 1$, then from (12) we get

$$p_i - 1 = c_1 q_i, \quad d q_i = c_1 p_i, \quad p_i + 1 = c_2 p_i, \quad q_i = c_2 q_i, \quad c_1, c_2 \in \mathbb{N}.$$ 

Since $c_1 p_i = c_2 d q_i$, we have $c_1 = c q_i, \quad c_2 d = c p_i$, where $c \in \mathbb{N}$. Hence

$$2d = c d p_i - c q_i = c(p_i^2 - d q_i^2) = c k \equiv 0 \pmod{k},$$

a contradiction. Therefore $(X', Y') \neq (p_i, q_i)$, (v) is proved. \quad \square

Let $I(d) = \{(d_1, d_2) \mid d_1, d_2 \in \mathbb{N}, \quad d_1 d_2 = d, \quad \gcd(d_1, d_2) = 1\}$, and let $I'(d) = I(d) \setminus \{(1, d)\}$.

**Lemma 6** [4]. There exists at most one pair $(d_1, d_2) \in I'(d)$ which make the equation

$$d_1 u'^2 - d_2 v'^2 = 1 \tag{13}$$

has solutions $(u', v')$. \quad \square

**Lemma 7** [2, Theorems 11.4.1 and 11.4.2]. Let $(d_1, d_2) \in I(d)$. If $(X, Y)$ is a solution of the equation

$$d_1 X^2 - d_2 Y^2 = k, \quad \gcd(X, Y) = 1, \tag{14}$$

then there exists a unique integer $l$ such that

$$l = d_1 \alpha X - d_2 \beta Y, \quad 0 < l \leq |k|,$$

where $\alpha, \beta \in \mathbb{Z}$ with $\beta X - \alpha Y = 1$. Such $l$ is called the characteristic number of the solution $(X, Y)$, and it will be denoted by $(X, Y)$. If $(X, Y) = l$, then we have

$$d_1 X \equiv -lY \pmod{k}, \quad l^2 \equiv d \pmod{k}, \quad \gcd(k, 2l, \frac{l^2 - d}{k}) = 1. \quad \square$$

**Lemma 8** [2, Theorem 11.4.2]. Let $(X_1, Y_1), (X_2, Y_2)$ be solutions of equation (14). Then $(X_1, Y_1) = (X_2, Y_2)$ if and only if

$$X_2 \sqrt{d_1} + Y_2 \sqrt{d_2} = (X_1 \sqrt{d_1} + Y_1 \sqrt{d_2})(u + v \sqrt{d}),$$

where $(u, v)$ is a solution of equation (6). \quad \square

**Lemma 9.** If $2 \nmid d$ and the congruence

$$l^2 \equiv d \pmod{2^{m+2}}, \quad 0 < l \leq 2^{m+2}, \quad \gcd(2^{m+2}, 2l, \frac{l^2 - d}{2^{m+2}}) = 1, \tag{15}$$

has a solution $l$ for $m \in \mathbb{N}$, then it has exactly one solution $l' = 2^{m+2} - l$ with $l' \neq l$.

**Proof.** Let $l'$ be a solution of (15) with $l' \neq l$. Since $2 \nmid d$ implies $2 \nmid ll'$, we get from $l^2 \equiv l'^2 \equiv d \pmod{2^{m+2}}$ that $l' = \delta l \pmod{2^{m+1}}$, where $\delta \in \{-1, 1\}$. If $\delta = 1$, then $l' = l + 2^{m+1} t$ for some $t \in \mathbb{Z}$. Notice that $2 \nmid (l^2 - d)/2^{m+2}$ and $2 \nmid (l'^2 - d)/2^{m+2}$. From

$$\frac{l'^2 - d}{2^{m+2}} = \frac{l^2 - d}{2^{m+2}} + lt + 2^m t^2,$$
we get $2 \mid t$, and so $l' = l$ since $0 < l$, $l' \leq 2^{m+2}$. This is a contradiction. Hence $\delta = -1$. Then $l' = -l + 2^{m+1}t$ for some $t \in \mathbb{Z}$. From
\[ \frac{l'^2 - d}{2^{m+2}} = \frac{l^2 - d}{2^{m+2}} - lt + 2^m t^2, \]
we obtain $l' = 2^{m+2} - l$ since $0 < l$, $l' \leq 2^{m+2}$. The lemma is proved. □

Lemma 10. Let $m \in \mathbb{N}$, and let $(d_1, d_2) \in I(d)$. If $2 \nmid d$ and $(X_0, Y_0)$ is a solution of the equation
\[ d_1 X^2 - d_2 Y^2 = 2^{m+2}, \quad \gcd(X, Y) = 1, \]
then all the solutions of equation (16) are given by
\[ X\sqrt{d_1} + Y\sqrt{d_2} = (X_0\sqrt{d_1} + Y_0\sqrt{d_2})(u + v\sqrt{d}), \]
where $(u, v)$ is an arbitrary solution of equation (6).

Proof. Under the assumption, $(X_0, -Y_0)$ is a solution of equation (16) too. Let $l = \langle X_0, Y_0 \rangle$. Then $\langle X_0, -Y_0 \rangle \equiv -l \pmod{2^{m+2}}$. By Lemma 9, we have either $\langle X, Y \rangle = \langle X_0, Y_0 \rangle$ or $\langle X, Y \rangle = \langle X_0, -Y_0 \rangle$ for any solution $(X, Y)$ of equation (16). Thus, by Lemma 8, the lemma is proved. □

Lemma 11. If $2 \nmid d$ and the equation
\[ X^2 - dY^2 = 2^{s+2}, \quad \gcd(X, Y) = 1, \quad Z > 0, \]
has solutions $(X, Y, Z)$, then it has a unique positive solution $(X_1, Y_1, Z_1)$ such that
\[ Z_1 \leq Z, \quad 1 < \frac{X_1 + Y_1\sqrt{d}}{X_1 - Y_1\sqrt{d}} < (u_1 + v_1\sqrt{d})^2, \]
where $Z$ runs over all solutions of equation (17), $u_1 + v_1\sqrt{d}$ is the fundamental solution of equation (6). Such $(X_1, Y_1, Z_1)$ is called the least solution of equation (17). Moreover, all solutions of equation (17) are given by
\[ Z = Z_1 t, \quad \frac{X + Y\sqrt{d}}{2} = \left(\frac{X_1 \pm Y_1\sqrt{d}}{2}\right)^t (u + v\sqrt{d}), \]
where $t$ is an arbitrary positive integer, $(u, v)$ is an arbitrary solution of equation (6).

Proof. Let $(X_0, Y_0, Z_1)$ be a solution of equation (17) with $Z_1 \leq Z$. By Lemma 10, all solutions of equation (17) with $Z = Z_1$ are given by
\[ X + Y\sqrt{d} = (X_0 \pm Y_0\sqrt{d})(u + v\sqrt{d}). \]
Since $u + v\sqrt{d} = \pm(u_1 + v_1\sqrt{d})^\gamma$ ($\gamma \in \mathbb{Z}$), we see from (19) that equation (17) has a unique positive solution $(X_1, Y_1, Z_1)$ which satisfy (18).

For any $t \in \mathbb{N}$, let
\[ \frac{X_t + Y_t\sqrt{d}}{2} = \left(\frac{X_1 + Y_1\sqrt{d}}{2}\right)^t, \]
and let
\[ \varepsilon = \frac{X_1 + Y_1\sqrt{d}}{2}, \quad \bar{\varepsilon} = \frac{X_1 - Y_1\sqrt{d}}{2}. \]

By Lemma 1, we have
\[ X_i = \varepsilon^i + \bar{\varepsilon}^i = \sum_{i=0}^{[t/2]} (-1)^i \binom{t}{i} (\varepsilon + \bar{\varepsilon})^{t-i}\varepsilon^i, \]
\[ Y_i = \frac{\varepsilon^i - \bar{\varepsilon}^i}{\sqrt{d}} = \begin{cases} \varepsilon^i - \bar{\varepsilon}^i & \text{if } t \equiv 0 \pmod{2}, \\ \frac{t}{2} \binom{2i+1}{i} \binom{t}{i} (dY_1^2)^{t-i}Z^{t-i}, & \text{if } t \equiv 1 \pmod{2}. \end{cases} \]

Since \( 2 \nmid X_1Y_1 \) implies \( 2 \nmid X_iY_i \), we see that \((X_i, Y_i, Z_i)\) is a solution of equation (17). Further, by Lemma 10, all solutions of equation (17) with \( Z_1 \mid Z \) are given by
\[ Z = Z_1t, \quad \frac{X + Y\sqrt{d}}{2} = \left( \frac{X_1 \pm Y_1\sqrt{d}}{2} \right) (u + v\sqrt{d}). \]

Let \((X', Y', Z')\) be a solution of equation (17) with \( Z_1 \parallel Z' \). Then \( Z' = Z_1t + Z_0 \), where \( t, Z_0 \in \mathbb{N} \) satisfy \( Z_0 < Z_1 \). Let \( l = (X_1, Y_1) \), and let \( l' = (X', Y') \). By Lemma 7, we have
\[ l^2 \equiv d \pmod{2z^t+2}, \quad l'^2 \equiv d \pmod{2z'^t+2}, \]
\[ X_i \equiv -lY_i \pmod{2z^t+2}, \quad X' \equiv -l'Y' \pmod{2z'+2}. \]

Since \( 2 \nmid ll' \), we get \( l' \equiv \delta l \pmod{2z^t+2} \), where \( \delta \in \{-1, 1\} \). From (20),
\[ X_iX' - \delta dY_iY' \equiv 0 \pmod{2z^t+2}, \quad X_iY' - \delta X'Y_i \equiv 0 \pmod{2z^t+2}. \]

There exists the integers \( X'', Y'' \) such that
\[ X_iX' - \delta dY_iY' = 2z^t+2X'', \quad X_iY' - \delta X'Y_i = 2z^t+2Y''. \]

Then
\[ X'Y'(X_i^2 - dY_i^2) \equiv 0 \pmod{\gcd(2z^t+2X'', 2z^t+2Y'') \gcd(2z^t+2X'', 2z^t+2Y'')}. \]

Since \( 2 \nmid X'Y' \), we get \( 2 \nmid \gcd(X'', Y'') \). From (21) and
\[ 2z^{t+1} = (X_i^2 - dY_i^2)(X'^2 - dY'^2) = (X_iX' - \delta dY_iY')^2 - d(X_iY' - \delta X'Y_i)^2, \]
we have

\[ X''^2 - d Y''^2 = 2z_0. \]

Since \( d \equiv 1 \pmod{8} \) implies \( Z_0 > 2 \), we see that \((X'', Y'', Z_0 - 2)\) is a solution of equation (17) with \( Z < Z_1 \), a contradiction. The lemma is proved. \( \square \)

**Lemma 12.** Let \((d_1, d_2) \in I'(d)\). If \( 2 \nmid d \) and the equation

\[
(22) \quad d_1 X'^2 - d_2 Y'^2 = 2z'^{t+2}, \quad \gcd(X', Y') = 1, \quad Z' > 0,
\]

has solutions \((X', Y', Z')\) then equation (17) has solutions \((X, Y, Z)\). Moreover, if equation (13) has solutions \((u', v')\), then all solutions of equation (22) are given by

\[
(23) \quad Z' = Z, \quad X' \sqrt{d_1} + Y' \sqrt{d_2} = (X + Y \sqrt{d})(u' \sqrt{d_1} + v' \sqrt{d_2}),
\]

where \((X, Y, Z)\) and \((u', v')\) are arbitrary solutions of equations (17) and (13) respectively. If equation (13) has no solution, then all solutions of equation (22) are given by

\[
(24) \quad Z' = Z_1', \quad \frac{X' \sqrt{d_1} + Y' \sqrt{d_2}}{2} = \left( \frac{X'_1 \sqrt{d_1} \pm Y'_1 \sqrt{d_2}}{2} \right)^{t'} (u + v \sqrt{d})
\]

where \( t' \) is an arbitrary positive integer with \( 2 \nmid t' \), \((u, v)\) is an arbitrary solution of equation (6), \((X'_1, Y'_1, Z'_1)\) is a unique positive solution of equation (22) such that

\[
(25) \quad Z'_1 = \frac{Z_1}{2}, \quad 1 < \frac{X'_1 \sqrt{d_1} + Y'_1 \sqrt{d_2}}{X'_1 \sqrt{d_1} - Y'_1 \sqrt{d_2}} < (u_1 + v_1 \sqrt{d})^2,
\]

where \((X_1, Y_1, Z_1)\) is the least solution of equation (17), \( u_1 + v_1 \sqrt{d} \) is the fundamental solution of equation (6). Such \((X'_1, Y'_1, Z'_1)\) is called the least solution of equation (22).

**Proof.** Let \((X', Y', Z')\) be a solution of equation (22). Then

\[
\left( \frac{d_1 X'^2 + d_2 Y'^2}{2} \right)^2 - d(X' Y')^2 = 2z'^{t+2},
\]

where \((d_1 X'^2 + d_2 Y'^2)/2\) and \(X' Y'\) are coprime integers. It follows that equation (17) has solutions.

If equation (13) has solutions, then (23) gives out all solutions of equation (22) clearly.

If equation (13) has no solution, by Lemma 10, equation (22) has a unique positive solution \((X'_1, Y'_1, Z'_1)\) satisfies \( Z'_1 \leq Z' \) and

\[
1 < \frac{X'_1 \sqrt{d_1} + Y'_1 \sqrt{d_2}}{X'_1 \sqrt{d_1} - Y'_1 \sqrt{d_2}} < (u_1 + v_1 \sqrt{d})^2,
\]

where \( Z' \) runs over all solutions of equation (22). Since \(((d_1 X'_1^2 + d_2 Y'_1^2)/2, X'_1 Y'_1, 2Z'_1)\) is a solution of equation (17), by Lemma 11, we have \( 2Z'_1 = Z_1 t \) for some \( t \in \mathbb{N} \). If \( t > 1 \), then \( Z'_1 \geq Z_1 \). By such that same argument as in the proof of Lemma 11, there exists the integers \( X'', Y'' \) satisfy

\[
d_1 X''^2 - d_2 Y''^2 = 2z_i - z_1, \quad \gcd(X'', Y'') = 1.
\]
Recalling that $Z_1' \leq Z_1'$ and equation (13) has no solution. It is impossible. Therefore $t = 1$ and (25) is proved.

Finally, by such the same argument as in the proof of Lemma 11, we can prove that all solutions of equation (22) are given by (24). The proof is complete.

**Lemma 13.** If $2 \nmid d$, then there exists at most two distinct pairs $(d_1', d_2') \in I(d)$ which make equation (16) have solutions $(X, Y)$.

**Proof.** Let $(d_1, d_2)$, $(d_1', d_2') \in I(d)$ with $(d_1, d_2) \neq (d_1', d_2')$. We assume that the equations
\begin{align*}
(26) \quad d_1 X^2 - d_2 Y^2 &= 2^{m+2}, \quad \gcd(X, Y) = 1, \\
(27) \quad d_1' X'^2 - d_2' Y'^2 &= 2^{m+2}, \quad \gcd(X', Y') = 1,
\end{align*}

have solutions $(X, Y)$ and $(X', Y')$ respectively. Let $l = \langle X, Y \rangle$ and $l' = \langle X', Y' \rangle$. By Lemma 9, we have $l' \equiv \delta l \pmod{2^{m+2}}$, where $\delta \in \{-1, 1\}$. Further, by Lemma 7, we have
\[d_1 X \equiv -lY \pmod{2^{m+2}}, \quad d_1' X' \equiv -l'Y' \equiv -\delta l Y' \pmod{2^{m+2}}.\]

Hence
\[d_1 d_1' X X' \equiv \delta l_2 Y Y' \equiv \delta d_1 Y Y' \pmod{2^{m+2}}, \quad d_1 d_1' X X' \equiv \delta l_2 Y Y' \pmod{2^{m+2}}.\]

Let $d_{11} = \gcd(d_1, d_1')$, $d_{12} = \gcd(d_1, d_2')$, $d_{21} = d_1'/d_{11}$, $d_{22} = d_2'/d_{12}$. Since $d_1 d_2 = d_1' d_2' = d$, then $d_1 = d_{11} d_{12}$, $d_2 = d_{21} d_{22}$, $d_1' = d_{11} d_{21}$, $d_2' = d_{12} d_{22}$. Notice that $2 \nmid d l l'$. We obtain from (28) that
\[d_{11} X X' - \delta d_{22} Y Y' \equiv d_{12} X Y' - \delta d_{21} X' Y \equiv 0 \pmod{2^{m+2}},\]

whence we get
\[d_{11} X X' - \delta d_{22} Y Y' = 2^{m+2} X'', \quad d_{12} X Y' - \delta d_{21} X' Y = 2^{m+2} Y'',\]
where $X'', Y'' \in \mathbb{Z}$. By (26) and (27),
\[2^{2m+4} = (d_1 X^2 - d_2 Y^2)(d_1' X'^2 - d_2' Y'^2) = d_1''(d_{11} X X' - \delta d_{22} Y Y')^2 - d_2''(d_{12} X Y' - \delta d_{21} X' Y)^2,\]

where $d_1'' = d_{11} d_{21}$, $d_2'' = d_{12} d_{22}$ with $d_1'' d_2'' = d$. Substituting (29) into (30), we get
\[d_1'' X X''^2 - d_2'' Y Y''^2 = 1.\]

Since $(d_1, d_2) \neq (d_1', d_2')$ implies $d_{12} > 1$, $d_1'' > 1$, and $(d_1'', d_2'') \in I'(d)$. From (31), such $(d_1'', d_2'')$ is unique by Lemma 6. We note that if $(d_1, d_2)$ is fixed, then the corresponding $(d_1'', d_2'')$ are different for some distinct $(d_1', d_2')$. This implies the lemma. \(\square\)

### 3. Further Preliminary Lemmas

Throughout this section, we assume that $D$ is a nonsquare. Notice that the least solution of the equation
\[X^2 - D Y^2 = 2^{z+2}, \quad \gcd(X, Y) = 1, \quad Z > 0,\]
is unique. By Lemmas 12 and 13, the following two lemmas are clear.
Lemma 14. If there exists two distinct pairs \((D_1, D_2) \in I'(D)\) which make the equation
\[
D_1X'^2 - D_2Y'^2 = 2Z'^2, \quad \gcd(X', Y') = 1, \quad Z' > 0
\]
have solutions \((X', Y', Z')\), then the least solution \((X_1, Y_1, Z_1)\) of equation (32) satisfies \(2|Z_1\).

Lemma 15. There exists at most three distinct pairs \((D_1, D_2) \in I'(D)\) which make equation (33) have solutions \((X', Y', Z')\). \(\Box\)

Lemma 16 [1, Lemma 7]. Suppose there exist integers \(a, b, A, B, m\) such that
\[
\frac{A + B\sqrt{D}}{2} = \left(\frac{a + b\sqrt{D}}{2}\right)^m, \quad m > 1, b \neq 0, a \equiv Db \pmod{2}.
\]
If \(D > 1\) and \(D \equiv 1 (\pmod{8})\), then \(|B| > 1\) except when \(m = 2\) and \(a, b \in \{-1, 1\}\). \(\Box\)

Lemma 17. If \((x, n)\) is a solution of equation (1), then \((x, 1, n)\) is a solution of equation (32). Let \((X_1, Y_1, Z_1)\) be the least solution of equation (32), and let \(u_1 + v_1\sqrt{D}\) be the fundamental solution of the equation
\[
u^2 - D\nu^2 = 1.
\]
Further let
\[
\varepsilon = \frac{X_1 + Y_1\sqrt{D}}{2}, \quad \bar{\varepsilon} = \frac{X_1 - Y_1\sqrt{D}}{2},
\]
\[
\rho = u_1 + v_1\sqrt{D}, \quad \bar{\rho} = u_1 - v_1\sqrt{D}.
\]
Then
\[
n = Z_1t, \quad \frac{x + \delta\sqrt{D}}{2} = \varepsilon^t\bar{\rho}^s, \quad \delta \in \{-1, 1\},
\]
where \(s, t \in \mathbb{Z}\) satisfy
\[
s \geq 0, \quad t > 0, \quad \gcd(s, t) = \begin{cases} 2, & \text{if } 2|s, 2|t \text{ and } x = \frac{D+1}{2}, \\ 1, & \text{otherwise}. \end{cases}
\]
Proof. By Lemma 11, (36) holds for some \(s, t \in \mathbb{Z}\) with \(s \geq 0\) and \(t > 0\). Moreover, by Lemma 16, \(s\) and \(t\) satisfy (37). The lemma is proved. \(\Box\)

Lemma 18. Under the assumption of Lemma 17, we have \(\delta \equiv xY_1/X_1 \pmod{4}\).
Proof. Let
\[
\frac{X + Y\sqrt{D}}{2} = \varepsilon^t, \quad u - v\sqrt{D} = \bar{\rho}^s.
\]
By Lemma 1, we have \(X, Y \in \mathbb{Z}\) satisfy
\[
X = \varepsilon^t + \bar{\varepsilon}^t = \sum_{i=0}^{[t/2]}(-1)^i \binom{t}{\frac{t}{2}} (\varepsilon + \bar{\varepsilon})^{t-2i}(\varepsilon\bar{\varepsilon})^i = \sum_{i=0}^{[t/2]}(-1)^i \binom{t}{\frac{t}{2}} X_1^{t-2i} 2Z_1^i
\]
\[
\implies \begin{cases} X_1^i - 2tX_1^{i-2} \pmod{4}, & \text{if } Z_1 = 1, \\ X_1^i \pmod{4}, & \text{if } Z_1 > 1, \end{cases}
\]
\begin{align*}
Y = \frac{e^t - e^{-t}}{\sqrt{D}} \equiv \begin{cases} 
Y_1^t + 2tY_1^{-t-2} \pmod{4}, & \text{if } Z_1 = 1, 2 \nabla t, \\
(Y_1^t + 2tY_1^{-t-2})(X_1^t - 2tX_1^{-t-2}) \pmod{4}, & \text{if } Z_1 > 1, 2 \nabla t, \\
Y_1^t \pmod{4}, & \text{if } Z_1 > 1, 2 \nabla t, \\
Y_1^t X_1^{-t} \pmod{4} & \text{if } Z_1 > 1, t = 2^\alpha t', \alpha > 0, 2 \nabla t',
\end{cases}
\end{align*}

since \( D \equiv 1 \pmod{8} \). Notice that \( 4 \mid \nu \) when \( D \equiv 1 \pmod{8} \). Then from

\begin{align*}
\frac{x + \delta \sqrt{D}}{2} = \frac{X + Y \sqrt{D}}{2} (u - v \sqrt{D}),
\end{align*}

we get \( x = X u - D Y v \equiv X u \pmod{4} \) and \( \delta = Y u - X v \equiv Y u \pmod{4} \), and so

\begin{align*}
\delta \equiv x \frac{Y}{X} \pmod{4}.
\end{align*}

Since \( X_1^2 \equiv DY_2^2 \pmod{8} \), substituting (39) and (40) into (42), the lemma is proved. □

**Lemma 19.** If \((x, n)\) is a solution of equation (1) with \(2 \mid n\), then \(2^n < D^2/16\).

**Proof.** Under the assumption, we have \(x + 2n/2+x = Dx\) and \(x - 2n/2+1 = D^n\), where \((D_1, D_2) \in I(D)\). It follows that \(2n/2+2 = D^n - D_2 \leq D - 1 < D\). Thus the lemma. □

**Lemma 20.** If \((x, n)\) is a solution of equation (1) with \(2 \nmid n\), then \(2 \nmid Z_1 t\) and \((x, 2Z_1((t-1)/2))\) is a solution of the equation

\begin{align*}
x'^2 - 2Z_1+2y'^2 = D, \quad \gcd(x', y') = 1,
\end{align*}

satisfying

\begin{align*}
\langle x', 2Z_1((t-1)/2) \rangle \equiv \begin{cases} 
-X_1 \pmod{D}, & \text{if } 2 \nmid s, \\
-X_1 u_1 \pmod{D}, & \text{if } 2 \nabla s.
\end{cases}
\end{align*}

**Proof.** By Lemma 7, we have

\begin{align*}
\langle x, 2Z_1((t-1)/2) \rangle \equiv -\frac{x}{2^{z_1((t-1)/2)}} \pmod{D}.
\end{align*}

From (38) and (41), we get

\begin{align*}
x \equiv X u \equiv \frac{X_1 u_1^t}{2^{t-1}} \equiv 2^{z_1((t-1)/2)} X_1 u_1^t
\equiv \begin{cases} 
2^{z_1((t-1)/2)} X_1 \pmod{D}, & \text{if } 2 \nmid s, \\
2^{z_1((t-1)/2)} X_1 u_1 \pmod{D}, & \text{if } 2 \nabla s,
\end{cases}
\end{align*}

since \(2 \nmid Z_1 t\), \(X_1^2 \equiv 2^{z_1+2} \pmod{D}\) and \(u_1^2 \equiv 1 \pmod{D}\). Substituting (45) into (44), we obtain the lemma. □

**Lemma 21.** Let \((X_1, Y_1, Z_1)\) be the least solution of equation (32). If \(2^{r^{z_1+2}} < \sqrt{D}\) for some \(r \in \mathbb{N}\), then the fundamental solution \(p = u_1 + v_1 \sqrt{D}\) of equation (34) satisfies \(p > D^{r^2}/2^{2r-2}\).

**Proof.** By Lemma 11, there exists \(X_i, Y_i \in \mathbb{Z}\ \ (i = 1, \ldots, r)\) such that

\begin{align*}
X_i^2 - DY_i^2 = 2^{z_1+2}, \quad \gcd(X_i, Y_i) = 1, \quad i = 1, \ldots, r.
\end{align*}
Since $2^{r_1+2} < \sqrt{D}$, by (v) of Lemma 5, $\sqrt{D}$ has $2r$ convergents $p_{s_i}/q_{s_i}$ and $p_{t_i}/q_{t_i}$ ($i = 1, \ldots, \gamma$) such that

$$k_{s_i} = k_{t_i} = 2^{z_i+2}, \quad 2 \uparrow s_i, t_i, 0 < s_i, t_i < t, i = 1, \ldots, \gamma,$$

where $t$ was defined in (iii) of Lemma 5. Therefore, by (i) of Lemma 5, we have

$$a_{s_{i+1}} = \left[ \frac{\Delta_{s_i} + \sqrt{D}}{k_{s_i}} \right] > \frac{\sqrt{D}}{2^{z_i+2}}, \quad i = 1, \ldots, r.$$

Notice where $p_0 = a_0 \geq 2, p_1 = a_0a_1 + 1$, and $p_{j+2} = a_{j+2}p_{j+1} + p_j$ for $j \geq 0$. By (iii) of Lemma 5, we deduce from (46) that

$$\rho > u_1 = p_1 > \prod_{j=0}^{l} a_j \geq a_0 \prod_{i=1}^{\gamma} a_{s_i} a_{t_i},$$

$$> a_0 \left( \prod_{i=1}^{\gamma} \frac{\sqrt{D}}{2^{z_i+2}} \right)^2 = \frac{a_0 D^r}{2^{r(r+1)z_1+4r}} > \frac{D^{r/2}}{2^{2r-2}},$$

since $a_0 = \lfloor \sqrt{D} \rfloor$. The lemma is proved. □

**Lemma 22** [1, Lemma 6 and the proof of Theorem 3]. Let $(x, n)$, $(x', n')$, $(x'', n'')$ be three solutions of equation (1) with $n'' > n' > n$. We have:

(i) If $x' - x = 2$, then either $D$ is of type I or $D$ is of type III and $(x, x') = (2^{m_2} - 2^{m_1} - 1, 2^{m_2} - 2^{m_1} + 1)$.

(ii) If $x' - x = 4$, then $D$ is of type I.

(iii) If $D$ is of type II and $(x, x', x'') = (2^{2m+1} - 17)/3, (2^{2m+1} + 1)/3, (17 \cdot 2^{2m+1} - 1)/3$, then $n'' = 2n' + 3$.

(iv) With the exception of above cases, $x' - x \geq 6$ and $n'' \geq 2n' + 53$. □

**Lemma 23** [1, Corollaries 1 and 2]. If $(x, n)$ is a solution of equation (1), then $n < 433 + (10 \log D)/\log 2$. Moreover, if $D < 2^{96}$, then $n < 16 + (2 \log D)/\log 2$. □

### 4. Proof of theorem

By Theorems 3 and 4 of [1], it suffices to prove that $N(D) = 3$ while $D \geq 10^{12}$ and $D$ is of types II or III. Moreover, if $D$ is a square, then $N(D) \leq 1$. We may assume that $D$ is not a square.

**Assertion 1.** If $D$ is of type II, then $N(D) = 3$.

**Proof.** In this case, equation (1) has three solutions

$$(x_1, n_1) = \left( \frac{2^{2m+1} - 17}{3}, 3 \right), \quad (x_2, n_2) = \left( \frac{2^{2m+1}}{3}, 2m + 1 \right), \quad (x_3, n_3) = \left( \frac{17 \cdot 2^{2m+1} - 1}{3}, 4m + 5 \right).$$
By the proof of Theorem 3 of [1], if $N(D) > 3$, then equation (1) has another solution $(x_4, n_4)$ with $n_4 > n_3$. By Lemmas 19 and 22, we see that $2 \nmid n_4$. Let $(X_1, Y_1, Z_1)$ be the least solution of (32), and let $\epsilon, \bar{\epsilon}, \rho, \bar{\rho}$ be defined as in (35). Then, by Lemma 17, we have

$$n_i = Z_i t_i, \quad \frac{x_i + \delta_i \sqrt{D}}{2} = \epsilon^i \bar{\rho}^i, \quad \delta_i \in \{-1, 1\}, \quad i = 1, \ldots, 4,$$

where $s_i, t_i \in \mathbb{Z}$ $(i = 1, \ldots, 4)$ satisfy

$$s_i \geq 0, \quad t_i > 0, \quad \gcd(s_i, t_i) = 1, \quad i = 1, \ldots, 4.$$

We see from (47) and (48) that equation (43) has three solutions $(x_j, 2^{z_1((t_j-1)/2)})$ $(j = 2, 3, 4)$. Let $l_j = (x_j, 2^{z_1((t_j-1)/2)})$ $(j = 2, 3, 4)$. By Lemma 7, we get from (47) and (48) that

$$l_2 - l_3 \equiv -\frac{2^{2m+1} + 1}{3 \cdot 2^{z_1((t_2-1)/2)}} + \frac{17 \cdot 2^{2m+1} - 1}{3 \cdot 2^{z_1((t_3-1)/2)}} \cdot 2^{(z_1-1)/2}$$

$$\equiv -\frac{2^{2m+2} (2^{3m+3} - 17 \cdot 2^{2m+1} + 2^m + 1) \not\equiv 0 \pmod{D}}{3 \cdot 2^{2m+2}}.$$

It follows that $l_2 \neq l_3$. Further, by Lemma 20, we have either $l_4 = l_2$ or $l_4 = l_3$. Furthermore, by Lemma 8, we get

$$x_4 + 2^{z_1((t_4-1)/2)} \sqrt{2^{z_1+2}}$$

$$= \begin{cases} (x_2 + 2^{z_1((t_2-1)/2)} \sqrt{2^{z_1+2}} (U' + V' \sqrt{2^{z_1+2}}), & \text{if } l_4 = l_2, \\ (x_3 + 2^{z_1((t_3-1)/2)} \sqrt{2^{z_1+2}} (U' + V' \sqrt{2^{z_1+2}}), & \text{if } l_4 = l_3, \end{cases}$$

and hence

$$2^{z_1((t_4-1)/2)} = \begin{cases} x_2 V' + 2^{z_1((t_2-1)/2)} U', & \text{if } l_4 = l_2, \\ x_3 V' + 2^{z_1((t_3-1)/2)} U', & \text{if } l_4 = l_3, \end{cases}$$

where $(U', V')$ is a positive solution of the equation

$$U'^2 - 2^{z_1+2} V'^2 = 1.$$ 

Since $t_3 > t_2$, we obtain

$$2^{z_1((t_2-1)/2)} \mid V'$$

by (50). On applying Lemma 3 with (52), we have

$$U' + V' \sqrt{2^{z_1+2}} = (3 + 2 \sqrt{2}) 2^{m_5}, \quad \gamma \in \mathbb{N},$$

since $Z_1 t_2 = 2m + 1$. From (53), we deduce $2U' > 25^{5 \cdot 2^{m-1}}$ and

$$n_4 > 2m + 1 + 5 \cdot 2^m$$

by (47), (48), and (50). On the other hand, by Lemma 23, we have

$$n_4 < 433 + 10 \frac{\log D}{\log 2} < 433 + 40m$$

since $D < 2^{4m}$. The combination of (54) and (55) yields $m \leq 7$ and $D < 2^{4m} \leq 2^{28} < 10^{12}$. Thus the assertion is proved. \qed
Assertion 2. If $D$ is of type III, then $N(D) = 3$.

Proof. In this case, equation (1) has three solutions

$$(x_1, n_1) = (2^{m_2} - 2^{m_1} - 1, m_1),$$

$$(x_2, n_2) = (2^{m_2} - 2^{m_1} + 1, m_2),$$

$$(x_3, n_3) = (2^{m_2} + 2^{m_1} - 1, m_2 + m_1).$$

If $N(D) > 3$, then equation (1) has another solution $(x_4, n_4)$ with $n_4 > n_3$. Moreover, then (48) and (49) still hold by Lemma 17.

When $2|m_1$ and $2|m_2$, we get from (56) that

$$D_{11} - D_{12} = 2^{m_1/2+2}, \quad D_{21} - D_{22} = 2^{m_2/2+2},$$

where

$$D_{11} = 2^{m_2} - 2^{m_1} + 2^{m_1/2+1} - 1, \quad D_{12} = 2^{m_2} - 2^{m_1} - 2^{m_1/2+1} - 1,$$

$$D_{21} = 2^{m_2} - 2^{m_2/2+1} - 2^{m_1} + 1, \quad D_{22} = 2^{m_2} - 2^{m_2/2+1} - 2^{m_1} + 1.$$ 

Since $(D_{11}, D_{12}), (D_{21}, D_{22})$ belongs to $I'(D)$ and $(D_{11}, D_{12}) \neq (D_{21}, D_{22})$, by Lemma 14, the least solution of equation (32) satisfies $2|Z_1$. Therefore, $2|n_4$ by (48). Then we have

$$D_{31} - D_{32} = 2^{(m_2+m_1)/2+2}, \quad D_{41} - D_{42} = 2^{n_4/2+2},$$

where

$$D_{31} = 2^{m_2} + 2^{(m_2+m_1)/2+1} + 2^{m_1} - 1, \quad D_{32} = 2^{m_2} - 2^{(m_2+m_1)/2+1} + 2^{m_1} - 1,$$

$$D_{41} = x_4 + 2^{n_4/2+1}, \quad D_{42} = x_4 - 2^{n_4/2+1}.$$ 

Since $(D_{31}, D_{32}), (D_{41}, D_{42}) \in I'(D)$ and $(D_{31}, D_{32})$ $(i = 1, \ldots, 4)$ are different, this implies that there exist four distinct pairs $(D_1, D_2) \in I'(D)$ which make equation (33) have solutions. By Lemma 15, it is impossible.

When $2|m_1$ and $2 \nmid m_2$, we have $2 \nmid Z_1$ by (48). If $2|n_4$, since $2|m_1$, we see from Lemma 14 that $2|Z_1$, a contradiction. Therefore $2|n_4$ and equation (43) has three solutions $(x_j, 2^{z_1((t_j-1)/2)})$ $(j = 2, 3, 4)$. Let

$$l_j = (x_j, 2^{z_1((t_j-1)/2)}) \quad (j = 2, 3, 4).$$

From (56), we get

$$l_2 - l_3 \equiv -\frac{2^{m_2} - 2^{m_1} + 1}{2^{z_1 ((t_2-1)/2)}} + \frac{2^{m_2} + 2^{m_1} - 1}{2^{z_1 ((t_3-1)/2)}} \equiv \frac{2^{(z_1-1)/2}}{2^{(m_2+m_1-1)/2}} (-2^{m_2/2} (2^{m_2} - 2^{m_1} + 1) + (2^{m_2} + 2^{m_1} - 1) \not\equiv 0 \pmod{D}).$$

It follows that $l_2 \neq l_3$ and either $l_4 = l_2$ or $l_4 = l_3$ by Lemma 20. By such the same argument as in the proof of Assertion 1, then (50) and (52) still hold. Hence

$$U' + V' \sqrt{2^{z_1+2}} = (3 + 2 \sqrt{2}) 2^{(m_2-1)/2} \gamma, \quad \gamma \in \mathbb{N},$$

whence we get $2U' > 2^{5/2} 2^{(m_2-3)/2}$. On applying this with (50), we obtain

$$n_4 > m_2 + 5 \cdot 2^{(m_2-3)/2}. \quad (57)$$

On the other hand, since $\sqrt{D} < 2^{m_2}$, we have

$$n_4 < 433 + 10 \frac{\log D}{\log 2} < 433 + 20m_2 \quad (58)$$
by Lemma 23. The combination of (57) and (58) yields \( m_2 \leq 17 \) and \( D < 2^{34} < 10^{12} \), which is in contradiction with the assumption.

Let \( 2 \nmid m_1 m_2 \) and \( 3.6 m_1 \leq m_2 \). Since \( 2 \nmid m_2 + m_1 \), we have \( 2 \nmid n_4 \), and equation (43) has three solutions \( (x_j, 2^{z_1((t_4-1)/2)}) \) \( (j = 1, 2, \ldots, 4) \). Let \( l_j = (x_j, 2^{z_1((t_4-1)/2)}) \) \( (j = 1, 2, 4) \). By Lemma 7, we obtain \( l_1 \neq l_2 \). Furthermore, by Lemma 20, we have either \( l_4 = l_1 \) or \( l_4 = l_2 \). By such the same argument as in the case that \( 2 \nmid m_1 \) and \( 2 \nmid m_2 \), we can prove \( l_4 \neq l_2 \). If \( l_4 = l_1 \), we have

\[
\begin{align*}
& x_4 + 2^{z_1((t_4-1)/2)}\sqrt{2z_1+2} = (2^{m_2} - 2^{m_1} - 1 + 2^{z_1((t_4-1)/2)}\sqrt{2z_1+2})(U' + V'\sqrt{2z_1+2}),
\end{align*}
\]

whence we get

\[
2^{z_1((t_4-1)/2)} = (2^{m_2} - 2^{m_1} - 1)V' + 2^{z_1((t_4-1)/2)}U',
\]

where \( U', V' \in \mathbb{N} \) satisfy (51). Hence \( 2^{z_1((t_4-1)/2)}|U' \) and

\[
2^{z_1((t_4-1)/2)} = (2^{m_2} - 2^{m_1} - 1)\frac{V'}{2^{z_1((t_4-1)/2)}} + U'.
\]

Further, by Lemma 3, we have

\[
U' + V'\sqrt{2z_1+2} = (3 + 2\sqrt{2})2^{(m_1-1)/2}y, \quad y \in \mathbb{N},
\]

since \( m_1 = Z_1 t_1 \) and \( 2 \nmid Z_1 \). Furthermore, we see from (60) that \( U' \equiv 1 \) (mod 8) and

\[
\frac{V'}{2^{z_1((t_4-1)/2)}} \equiv 3(2^{(m_1-1)/2} - 1) \equiv 3r \quad (\text{mod } 8)
\]

since \( m_1 \geq 3 \). Hence, we obtain \( y \equiv 3 \) (mod 8) by (59). It implies that \( y \geq 3 \) and

\[
2U' > 215 \cdot 2^{(m_1-3)/2}
\]

by (60). On applying this with (59), we get

\[
n_4 > m_1 + 15 \cdot 2^{(m_1-1)/2} - 2.
\]

On the other hand, by Lemma 23,

\[
n_4 < 433 + 10\log_2 D < 433 + 20m_2 \leq 433 + 72m_1.
\]

The combination of (61) and (62) yields \( m_1 \leq 13 \) and \( D < 2^{2m_2} < 2^{7.2m_1} < 2^{96} \). On applying Lemma 23 again, we have

\[
n_4 < 16 + 2\log_2 D < 16 + 4m_2 \leq 16 + 14.4m_1.
\]

On combining this with (61), we get \( m_1 \leq 5 \) and \( D < 2^{36} < 10^{12} \). Thus \( N(D) = 3 \).

Using the same method, we can prove the assertion for the case that \( 2 \nmid m_1 \), \( 2 \nmid m_2 \), and \( m_2 \leq 3.6m_1 \).

Let \( 2 \nmid m_1 \) and \( m_2 > 3.6m_1 \). We obtain from (48) that

\[
(\frac{x_2 + \delta_2\sqrt{D}}{2})^{t_1} \rho^{s_1t_1} = (\frac{x_3 + \delta_3\sqrt{D}}{2})^{t_2} \rho^{s_2t_2}.
\]

Since \( x_2 \equiv 1 \) (mod 4) and \( x_3 \equiv -1 \) (mod 4), we have

\[
\delta_2 = -\delta_3
\]
by Lemma 18. Since \(2^{m_2} - 2^{m_1} - 2 < \sqrt{D} < 2^{m^2} - 2^{m_1} - 1\), we have

\[
t_3 \log \frac{x_2 + \sqrt{D}}{2} + t_2 \log \frac{x_3 + \sqrt{D}}{2} > t_2 t_3 \log 2^{z_1}
\]

by (48) and (56). Hence, from (63) and (64),

(65)

\[
|s_2 t_3 - s_3 t_2| \log \rho = t_3 \log \frac{x_2 + \sqrt{D}}{2} + t_2 \log \frac{x_3 + \sqrt{D}}{2} - t_2 t_3 \log 2^{z_1}
\]

by (48) and (56). Hence, from (63) and (64),

\[
< t_3 \log \frac{1}{2} ((2^{m_2} - 2^{m_1} + 1) + (2^{m_2} - 2^{m_1} - 1)) + t_2 \log \frac{1}{2} ((2^{m_2} + 2^{m_1} - 1) + (2^{m_2} - 2^{m_1} - 1)) - t_3 \log 2^{m_2}
\]

< t_2 \log 2^{m_2}.

Notice that only one of \(n_2\) and \(n_3\) is even. We see from (49) that \(2 \not| s_2 t_3 - s_3 t_2\).

If \(|s_2 t_3 - s_3 t_2| > 1\), then \(|s_2 t_3 - s_3 t_2| > 3\) and

(66)

\[
3 \log \rho < t_2 \log 2^{m_2}
\]

by (65). Recalling that \(m_2 = Z_1 t_2\) and \(2 \not| Z_1\). Since \(2^{m_2 - 1} < \sqrt{D} < 2^{m_2}\), we get

\[
\sqrt{D} > \begin{cases} 2^{(t_2 - 3)z_1 + 2}, & \text{if } Z_1 = 1, \\ 2^{(t_2 - 1)z_1 + 2}, & \text{if } Z_1 > 1. \end{cases}
\]

By Lemma 21, we have

(67)

\[
\log \rho > \begin{cases} (t_2 - 3) \log \sqrt{D} - (t_2 - 4) \log 4, & \text{if } Z_1 = 1, \\ (t_2 - 1) \log \sqrt{D} - (t_2 - 2) \log 4, & \text{if } Z_1 > 1. \end{cases}
\]

Recalling that \(D \geq 10^{12}\). The combination of (66) and (67) yields

\[
t_2 \leq \begin{cases} 4, & \text{if } Z_1 = 1, \\ 2, & \text{if } Z_1 > 1, \end{cases}
\]

a contradiction. Thus

(68)

\[
s_2 t_3 - s_3 t_2 = \pm 1.
\]

Let \(\alpha = (\log(e/\varepsilon))/\log \rho^2\), and let

\[
\Lambda(x, n) = \log \frac{x + \sqrt{D}}{x - \sqrt{D}},
\]

for any solution \((x, n)\) of equation (1). Then we have

(69)

\[
\alpha - \frac{s_i}{t_i} = \frac{\delta_i \Lambda(x_i, n_i)}{t_i \log \rho^2}, \quad i = 1, \ldots, 4,
\]

by (48). We see from (64) that \(\alpha\) lies in the interval \((s_2/t_2, s_3/t_3)\). Moreover, since \(t_4 > t_j\) and \(\Lambda(x_4, n_4) < \Lambda(x_j, n_j)\) for \(j = 2, 3\), we see from (69) that \(s_4/t_4\) lies in the interval \((s_2/t_2, s_3/t_3)\) too. By Lemma 2, we get from (68) that

(70)

\[
t_4 = c t_2 + c' t_3, \quad s_4 = c s_2 + c' s_3, \quad c, c' \in \mathbb{N}.
\]
From (48) and (70), we have

\[ \frac{x_4 + \delta_4 \sqrt{D}}{2} = e^4 \bar{e}^4 = \left( \frac{x_2 + \delta_2 \sqrt{D}}{2} \right)^c \left( \frac{x_3 + \delta_3 \sqrt{D}}{2} \right)^{c'} . \]

Let

\[ \frac{X_2 + Y_2 \sqrt{D}}{2} = \left( \frac{x_2 + \delta_2 \sqrt{D}}{2} \right)^c, \quad \frac{X_3 + Y_3 \sqrt{D}}{2} = \left( \frac{x_3 + \delta_3 \sqrt{D}}{2} \right)^{c'} . \]

Then \( X_2, Y_2, X_3, Y_3 \) are integers. Let \( \varepsilon_2 = (x_2 + \delta_2 \sqrt{D})/2 \), and \( \bar{\varepsilon}_2 = (x_2 - \delta_2 \sqrt{D})/2 \). Since \( \varepsilon_2 + \bar{\varepsilon}_2 = x_2 \equiv 1 - 2^m_1 \pmod{2^m_2} \) and \( \varepsilon_2 \bar{\varepsilon}_2 = 2^m_2 \equiv 0 \pmod{2^m_3} \), by Lemma 1, we have

\[ e_2^m + \bar{e}_2^m = \sum_{i=0}^{[m/2]} (-1)^i \binom{m}{i} (e_2 + \bar{e}_2)^m - 2^i (e_2 \bar{e}_2)^i \equiv (1 - 2^m_1)^m \pmod{2^m_2} \]

for any \( m \in \mathbb{N} \). It follows that \( X_2 \equiv (1 - 2^m_1)^c \pmod{2^m_2} \). Simultaneously, we have

\[ Y_2 = \frac{e_2^c - \bar{e}_2^c}{\sqrt{D}} = \frac{e_2^c - \bar{e}_2^c}{e_2 - \bar{e}_2} = \delta_2 \left( e_2^{c - 1} + \bar{e}_2^{c - 1} \right) + \varepsilon_2 \bar{e}_2 \left( \frac{e_2^{c - 2} - \bar{e}_2^{c - 2}}{e_2 - \bar{e}_2} \right) \equiv \delta_2 (e_2^{c - 1} + \bar{e}_2^{c - 1}) \equiv \delta_2 (1 - 2^m_1)^{c - 1} \pmod{2^m_2}. \]

By the same argument, we can get \( X_3 \equiv (-1 + 2^m_1)^{c'} \pmod{2^m_2} \) and \( Y_3 \equiv \delta_3 (-1 + 2^m_1)^{c' - 1} \pmod{2^m_2} \), since \( x_3 = 2^m_2 + 2^m_1 - 1 \). From (64), (71) and (72),

\[ 2\delta_4 = X_2 Y_3 + X_3 Y_2 \]
\[ \equiv \delta_3 (1 - 2^m_1)^c (-1 + 2^m_1)^{c' - 1} + \delta_2 (1 - 2^m_1)^{c' - 1} (-1 + 2^m_1)^c' \]
\[ \equiv (-1)^c' 2\delta_2 (1 - 2^m_1)^{c + c' - 1} \pmod{2^m_2}. \]

It follows that

\[ \pm 1 \equiv (1 - 2^m_1)^{c + c' - 1} \pmod{2^m_2 - 1}, \]

whence we deduce that \( c + c' - 1 \equiv 0 \pmod{2^m_2 - 1} \). Since \( m_1 \geq 3 \) and \( m_2 > 3.6 m_1 \), we have \( c + c' - 1 > 2^{2.6 m_1 - 1} > 2^{6.8} > 96 \). Hence, from (48), (56) and (70), we get

\[ n_4 = cm_2 + c'(m_2 + m_1) > (c + c') m_2 > 96 m_2 > 48 \frac{\log D}{\log 2}, \]

since \( \sqrt{D} < 2^{m_2} \). On applying Lemma 23 with (73), we obtain \( D < 2^{20} < 10^{12} \). Thus \( N(D) = 3 \). All cases are considered and the assertion is proved.

The combination of Assertions 1 and 2 yields the theorem.

**Acknowledgment**

The author would like to thank Professor A. Schinzel and the referee for their valuable suggestions.
REFERENCES


Research Department, Changsha Railway Institute, Changsha, Hunan, Peoples Republic of China