ACTA ARITHMETICA
LX.2 (1991)

On the number of solutions of the generalized Ramanujan–Nagell equation $x^2 - D = 2^{n+2}$

by

MAOHUA LE (Changsha)

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

$$x^2 - D = 2^{n+2}, \quad x > 0, \ n > 0 \ (^1). \tag{1}$$

In [1], Beukers proved that $N(D) \le 4$. At the same time, he showed that if $N(D) > 3$, then D must be of one of the following types:

$$D = 2^{2m} - 3 \cdot 2^{m+1} + 1, \quad m \in \mathbb{N}, \ m \ge 3. \tag{I}$$

$$D = \left(\frac{2^{2m+1} - 17}{3}\right)^2 - 32, \quad m \in \mathbb{N}, \ m \ge 3. \tag{II}$$

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

Moreover, equation (1) has exactly four solutions

$$(x, n) = (2^m - 3, 1), \ (2^m - 1, m), \ (2^m + 1, m + 1), \ (3 \cdot 2^m - 1, 2m + 1)$$

when D is of type I, and it has at most three solutions when D is of type II or type III. In this paper, we completely determine all D which make $N(D) = 4$ as follows.

THEOREM 1. *If D is of type* I, *then $N(D) = 4$, otherwise $N(D) \le 3$.*

Recently, Beukers asked if $N(D) \le 2$ for the remaining cases. In this respect, we prove the following result.

THEOREM 2. *If D is not of one of the above types and the equation*

$$u'^2 - Dv'^2 = -1 \tag{2}$$

(^{1}) Throughout this paper, "solution" and "positive solution" are abbreviations for "integer solution" and "positive integer solution" respectively.

(^{2}) In the original there is a slip of pen.

has solutions (u', v'), *then* $N(D) \le 2$.

2. Preliminaries

LEMMA 1 ([5; Formula 1.76]). *For any* $m \in \mathbb{N}$ *and any complex numbers* α, β, *we have*

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

where

$$\begin{bmatrix} m \\ i \end{bmatrix} = \frac{(m-i-1)!m}{(m-2i)!i!}, \qquad i = 0, \ldots, [m/2],$$

are positive integers. ■

LEMMA 2 ([3; 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*

$$a'' = ca + c'a', \qquad b'' = cb + c'b'. \ ■$$

LEMMA 3. *If* (U, V) *is a positive solution of the equation*

$$U^2 - 2V^2 = 1 \tag{3}$$

with $2^{m+1} | V$ *for some* $m \in \mathbb{N}$, *then* $U + V\sqrt{2} = (3 + 2\sqrt{2})^{2^m t}$ *for some* $t \in \mathbb{N}$.

Proof. This follows immediately from [2]. ■

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

LEMMA 4 ([3, Theorem 10.8.2]). *If* $|k| < \sqrt{d}$ *and* (X, Y) *is a positive solution of the equation*

$$X^2 - dY^2 = k, \qquad \gcd(X, Y) = 1, \tag{4}$$

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 $i = 1, \ldots, s-1$.

LEMMA 5. *For any* $j \in \mathbb{Z}$ *with* $j \ge 0$, *let* p_j/q_j *and* r_j *denote the* j-*th convergent and complete quotient of* $\sqrt{d}$ *respectively. Further, let* $k_j = (-1)^{j-1}(p_j^2 - dq_j^2)$. *Then we have*:

(i) $k_j > 0$ *and* $a_{j+1} = [(\Delta_j + \sqrt{d})/k_j]$ *for a suitable* $\Delta_j \in \mathbb{N}$.

(ii) *Let*

$$t = \begin{cases} s-1 & \text{if } 2 \mid s, \\ 2s-1 & \text{if } 2 \nmid s. \end{cases}$$

Then $p_t + q_t\sqrt{d}$ *is the fundamental solution of the equation*

$$u^2 - dv^2 = 1. \tag{5}$$

(iii) *If* $1 < k < \sqrt{d}$, $2d \not\equiv 0 \pmod{k}$ *and equation* (4) *has solutions* (X, Y), *then it has at least two solutions* (p_i, q_i) *and* (p_{t-i-1}, q_{t-i-1}), *where* $0 < i < t-1$, $i \neq (t-1)/2$.

Proof. The lemma follows from Satz 10 and Satz 18 of [6; Chapter III] and from various results scattered in [6, §26]. ■

Let $I(d) = \{(d_1, d_2) \mid d_1, d_2 \in \mathbb{N},\ d_1d_2 = d,\ \gcd(d_1, d_2) = 1\}$, and let $I'(d) = I(d) \setminus \{(1, d)\}$.

LEMMA 6 ([7]). *There exists at most one pair* $(d_1, d_2) \in I'(d)$ *which makes the equation*

$$d_1u'^2 - d_2v'^2 = 1 \tag{6}$$

have solutions (u', v'). *Moreover*, *if* (u'_1, v'_1) *is the least positive solution of* (6), *then* $(u'_1\sqrt{d_1} + v'_1\sqrt{d_2})^2 = u_1 + v_1\sqrt{d}$ *is the fundamental solution of* (5). ■

LEMMA 7 ([3; 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*

$$d_1X^2 - d_2Y^2 = k, \qquad \gcd(X, Y) = 1, \tag{7}$$

then there exists a unique integer l *such that*

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

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

$$d_1X \equiv -lY \pmod{k}, \qquad l^2 \equiv d \pmod{k}, \qquad \gcd\left(k, 2l, \frac{l^2 - d}{k}\right) = 1. \ ■$$

LEMMA 8 ([3; Theorem 11.4.2]). *Let* (X_1, Y_1), (X_2, Y_2) *be solutions of* (7). *Then* $\langle X_1, Y_1\rangle = \langle X_2, Y_2\rangle$ *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* (5). ■

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

$$l^2 \equiv d \pmod{2^{m+2}}, \qquad 0 < l \leq 2^{m+2}, \qquad \gcd\left(2^{m+2}, 2l, \frac{l^2 - d}{2^{m+2}}\right) = 1, \tag{8}$$

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

P r o o f. Let l' be a solution of (8) with $l' \neq l$. Since $2 \nmid d$ implies $2 \nmid ll'$, we deduce from $l^2 \equiv l'^2 \equiv d \pmod{2^{m+2}}$ that $l' \equiv \delta l \pmod{2^{m+1}}$, 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 $0 < l,\ l' \le 2^{m+2}$. 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 $0 < l,\ l' \le 2^{m+2}$. 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*

$$(9) \qquad d_1 X^2 - d_2 Y^2 = 2^{m+2}, \quad \gcd(X, Y) = 1,$$

then all the solutions of (9) *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 (5).

P r o o f. Under our assumption, $(X_0, -Y_0)$ is also a solution of (9). 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 (9). Thus, by Lemma 8, the lemma is proved. ■

LEMMA 11. *If $2 \nmid d$ and the equation*

$$(10) \qquad X^2 - dY^2 = 2^{Z+2}, \quad \gcd(X, Y) = 1, \ Z > 0,$$

has solutions (X, Y, Z), then it has a unique positive solution (X_1, Y_1, Z_1) such that

$$(11) \qquad Z_1 \le Z, \quad 1 < \frac{X_1 + Y_1\sqrt{d}}{X_1 - Y_1\sqrt{d}} < (u_1 + v_1\sqrt{d})^2,$$

where Z runs over all solutions of (10), *$u_1 + v_1\sqrt{d}$ is the fundamental solution of* (5). *(X_1, Y_1, Z_1) is called the* l e a s t s o l u t i o n *of* (10). *Moreover, all solutions of* (10) *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 and (u, v) is an arbitrary solution of (5).

Proof. Let (X_0, Y_0, Z_1) be a solution of (10) with $Z_1 \le Z$. By Lemma 10, all solutions of (10) with $Z = Z_1$ are given by

$$X + Y\sqrt{d} = (X_0 \pm Y_0\sqrt{d})(u + v\sqrt{d}). \tag{12}$$

Since $u + v\sqrt{d} = \pm(u_1 + v_1\sqrt{d})^r$ $(r \in \mathbb{Z})$, we see from (12) that (10) has a unique positive solution (X_1, Y_1, Z_1) which satisfies (11).

For any $t \in \mathbb{N}$, let

$$(X_t + Y_t\sqrt{d})/2 = ((X_1 + Y_1\sqrt{d})/2)^t,$$

and let

$$\varepsilon = (X_1 + Y_1\sqrt{d})/2, \quad \overline{\varepsilon} = (X_1 - Y_1\sqrt{d})/2.$$

By Lemma 1, we have

$$X_t = \varepsilon^t + \overline{\varepsilon}^t = \sum_{i=0}^{[t/2]} (-1)^i \begin{bmatrix} t \\ i \end{bmatrix} (\varepsilon + \overline{\varepsilon})^{t-2i}(\varepsilon\overline{\varepsilon})^i = \sum_{i=0}^{[t/2]} (-1)^i \begin{bmatrix} t \\ i \end{bmatrix} X_1^{t-2i} 2^{Z_1 i},$$

$$Y_t = \frac{\varepsilon^t - \overline{\varepsilon}^t}{\sqrt{d}}$$

$$= \begin{cases} \dfrac{\varepsilon - \overline{\varepsilon}}{\sqrt{d}} \displaystyle\sum_{i=0}^{(t-1)/2} \begin{bmatrix} t \\ i \end{bmatrix} (\varepsilon - \overline{\varepsilon})^{t-2i-1}(\varepsilon\overline{\varepsilon})^i \\ \qquad = Y_1 \displaystyle\sum_{i=0}^{(t-1)/2} \begin{bmatrix} t \\ i \end{bmatrix} (dY_1^2)^{(t-1)/2-i} 2^{Z_1 i} & \text{if } 2 \nmid t, \\ \dfrac{\varepsilon^{t'} - \overline{\varepsilon}^{t'}}{\sqrt{d}} \displaystyle\prod_{j=0}^{\alpha-1} (\varepsilon^{2^j t'} + \overline{\varepsilon}^{2^j t'}) = \Bigg(Y_1 \displaystyle\sum_{i=0}^{(t'-1)/2} \begin{bmatrix} t' \\ i \end{bmatrix} (dY_1^2)^{(t'-1)/2-i} 2^{Z_1 i} \Bigg) \\ \quad \times \displaystyle\prod_{j=0}^{\alpha-1} \Bigg(\sum_{i=0}^{[2^j t'/2]} (-1)^i \begin{bmatrix} 2^j t' \\ i \end{bmatrix} X_1^{2^j t' - 2i} 2^{Z_1 i} \Bigg) & \text{if } t = 2^\alpha t',\ \alpha > 0,\ 2 \nmid t'. \end{cases}$$

Since $2 \nmid X_1 Y_1$ implies $2 \nmid X_t Y_t$, we see that $(X_t, Y_t, Z_1 t)$ is a solution of (10). Further, by Lemma 10, all solutions of (10) with $Z_1 \mid Z$ are given by

$$Z = Z_1 t,$$
$$\frac{X + Y\sqrt{d}}{2} = \left(\frac{X_t \pm Y_t\sqrt{d}}{2}\right)(u + v\sqrt{d}) = \left(\frac{X_1 \pm Y_1\sqrt{d}}{2}\right)^t (u + v\sqrt{d}).$$

Let (X', Y', Z') be a solution of (10) with $Z_1 \nmid Z'$. Then $Z' = Z_1 t + Z_0$, where $t, Z_0 \in \mathbb{N}$ satisfy $Z_0 < Z_1$. Let $l = \langle X_t, Y_t \rangle$, and let $l' = \langle X', Y' \rangle$. By Lemma 7, we have

$$l^2 \equiv d \pmod{2^{Z_1 t + 2}}, \quad l'^2 \equiv d \pmod{2^{Z' + 2}},$$
$$X_t \equiv -lY_t \pmod{2^{Z_1 t + 2}}, \quad X' \equiv -l'Y' \pmod{2^{Z'+2}}. \tag{13}$$

Since $2\nmid ll'$, we get

$$l' \equiv \delta l \pmod{2^{Z_1 t+2}}, \qquad \delta \in \{-1,1\}.$$

From (13),

$$X_t X' - \delta d Y_t Y' \equiv 0 \pmod{2^{Z_1 t+2}}, \qquad X_t Y' - \delta X' Y_t \equiv 0 \pmod{2^{Z_1 t+2}}.$$

There exist integers X'', Y'' such that

$$X_t X' - \delta d Y_t Y' = 2^{Z_1 t+2} X'', \qquad X_t Y' - \delta X' Y_t = 2^{Z_1 t+2} Y''. \tag{14}$$

Then

$$X'Y'(X_t^2 - dY_t^2) \equiv 0 \pmod{\gcd(2^{Z_1 t+2} X'', 2^{Z_1 t+2} Y'')}.$$

Since $2\nmid X'Y'$, we get $2\nmid \gcd(X'', Y'')$. From (14) and

$$2^{Z'+Z_1 t+4} = (X_t^2 - dY_t^2)(X'^2 - dY'^2) = (X_t X' - \delta d Y_t Y')^2 - d(X_t Y' - \delta X' Y_t)^2,$$

we have

$$X''^2 - dY''^2 = 2^{Z_0}.$$

Since $d \equiv 1 \pmod 8$ implies $Z_0 > 2$, we see that $(X'', Y'', Z_0 - 2)$ is a solution of (10) with $Z < Z_1$, a contradiction. The lemma is proved. ∎

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

$$d_1 X'^2 - d_2 Y'^2 = 2^{Z'+2}, \qquad \gcd(X', Y') = 1,\ Z' > 0, \tag{15}$$

has solutions (X', Y', Z'), then (10) has solutions (X, Y, Z). Moreover, if (6) has solutions (u', v'), then all solutions of (15) are given by

$$Z' = Z, \qquad X'\sqrt{d_1} + Y'\sqrt{d_2} = (X + Y\sqrt{d})(u'\sqrt{d_1} + v'\sqrt{d_2}), \tag{16}$$

where (X, Y, Z) and (u', v') are arbitrary solutions of (10) and (6) respectively. If (6) has no solution, then all solutions of (15) are given by

$$Z' = Z_1' t', \qquad \frac{X'\sqrt{d_1} + Y'\sqrt{d_2}}{2} = \left(\frac{X_1'\sqrt{d_1} \pm Y_1'\sqrt{d_2}}{2}\right)^{t'} (u + v\sqrt{d}), \tag{17}$$

where t' is an arbitrary positive integer with $2\nmid t'$, (u, v) is an arbitrary solution of (5), (X_1', Y_1', Z_1') is a unique positive solution of (15) such that

$$Z_1' = \frac{Z_1}{2}, \qquad 1 < \frac{X_1'\sqrt{d_1} + Y_1'\sqrt{d_2}}{X_1'\sqrt{d_1} - Y_1'\sqrt{d_2}} < (u_1 + v_1\sqrt{d})^2, \tag{18}$$

where (X_1, Y_1, Z_1) is the least solution of (10), $u_1 + v_1\sqrt{d}$ is the fundamental solution of (5). (X_1', Y_1', Z_1') is called the least solution *of (15).*

Proof. Let (X', Y', Z') be a solution of (15). Then

$$\left(\frac{d_1 X'^2 + d_2 Y'^2}{2}\right)^2 - d(X'Y')^2 = 2^{2Z'+2},$$

where $(d_1X'^2+d_2Y'^2)/2$ and $X'Y'$ are coprime integers. It follows that (10) has solutions.

If (6) has solutions, then (16) clearly gives all solutions of (15).

If (6) has no solution, then by Lemma 10, (15) has a unique positive solution (X_1', Y_1', Z_1') that satisfies $Z_1' \le Z'$ 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 (15). Since $((d_1X_1'^2+d_2Y_1'^2)/2, X_1'Y_1', 2Z_1')$ is a solution of (10), by Lemma 11 we have $2Z_1' = Z_1 t$ for some $t \in \mathbb{N}$. If $t > 1$, then $Z_1' \ge Z_1$. By much the same argument as in the proof of Lemma 11, there exist integers X'', Y'' satisfying

$$d_1X''^2 - d_2Y''^2 = 2^{Z_1'-Z_1}, \quad \gcd(X'', Y'') = 1.$$

Recalling that $Z_1' \ge Z_1$ and (6) has no solution, we obtain a contradiction. Therefore $t = 1$ and (18) is proved.

Finally, by much the same argument as in the proof of Lemma 11, we can prove that all solutions of (15) are given by (17). The proof is complete. ∎

LEMMA 13. *If $2\nmid d$, then there exist at most two distinct pairs $(d_1, d_2) \in I(d)$ which make* (9) *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

$$d_1X^2 - d_2Y^2 = 2^{m+2}, \qquad \gcd(X, Y) = 1, \tag{19}$$

and

$$d_1'X'^2 - d_2'Y'^2 = 2^{m+2}, \quad \gcd(X', Y') = 1\,, \tag{20}$$

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

$$d_1X \equiv -lY \pmod{2^{m+2}}, \quad d_1'X' \equiv -l'Y' \equiv -\delta lY' \pmod{2^{m+2}}.$$

Hence

$$\begin{aligned} d_1d_1'XX' &\equiv \delta l^2YY' \equiv \delta dYY' \pmod{2^{m+2}},\\ d_1\delta lXY' &\equiv d_1'lX'Y \pmod{2^{m+2}}. \end{aligned} \tag{21}$$

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 $d_1d_2 = d_1'd_2' = d$, we have $d_1 = d_{11}d_{12}$, $d_2 = d_{21}d_{22}$, $d_1' = d_{11}d_{21}$, $d_2' = d_{12}d_{22}$. Notice that $2\nmid dll'$. We find from (21) that

$$d_{11}XX' - \delta d_{22}YY' \equiv d_{12}XY' - \delta d_{21}X'Y \equiv 0 \pmod{2^{m+2}},$$

whence we get

$$d_{11}XX' - \delta d_{22}YY' = 2^{m+2}X'', \quad d_{12}XY' - \delta d_{21}X'Y = 2^{m+2}Y'', \tag{22}$$

where $X'', Y'' \in \mathbb{Z}$. By (19) and (20),

$$\begin{aligned}(23)\quad 2^{2m+4} &= (d_1X^2 - d_2Y^2)(d_1'X'^2 - d_2'Y'^2)\\ &= d_1''(d_{11}XX' - \delta d_{22}YY')^2 - d_2''(d_{12}XY' - \delta d_{21}X'Y)^2,\end{aligned}$$

where $d_1'' = d_{12}d_{21}$, $d_2'' = d_{11}d_{22}$ with $d_1''d_2'' = d$. Substituting (22) into (23), we get

$$(24)\qquad d_1''X''^2 - d_2''Y''^2 = 1.$$

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 (24), such a (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. ∎

3. Further preliminary lemmas. Throughout this section, we assume that D is non-square. Notice that the least solution of the equation

$$(25)\qquad X^2 - DY^2 = 2^{Z+2}, \quad \gcd(X, Y) = 1,\ Z > 0,$$

is unique. By Lemmas 12 and 13, the following two lemmas are clear.

LEMMA 14. *If there exist two distinct pairs $(D_1, D_2) \in I'(D)$ which make the equation*

$$(26)\qquad D_1X'^2 - D_2Y'^2 = 2^{Z'+2}, \quad \gcd(X', Y') = 1,\ Z' > 0,$$

have solutions (X', Y', Z'), then the least solution (X_1, Y_1, Z_1) of (25) *satisfies $2 \mid Z_1$.* ∎

LEMMA 15. *There exist at most three distinct pairs $(D_1, D_2) \in I'(D)$ which make* (26) *have solutions (X', Y', Z').* ∎

LEMMA 16 ([1; Lemma 7]). *Suppose there exist integers a, b, A, B, m such that*

$$\frac{A + B\sqrt{D}}{2} = \left(\frac{a + b\sqrt{D}}{2}\right)^m, \qquad m > 1,\ b \neq 0,\ a \equiv Db \pmod 2.$$

If $D > 1$ and $D \equiv 1 \pmod 8$, then $|B| > 1$ except when $m = 2$ and $a, b \in \{-1, 1\}$. ∎

LEMMA 17. *If (x, n) is a solution of* (1), *then $(x, 1, n)$ is a solution of* (25). *Let (X_1, Y_1, Z_1) be the least solution of* (25), *and let $u_1 + v_1\sqrt{D}$ be the fundamental solution of the equation*

$$(27)\qquad u^2 - Dv^2 = 1.$$

Further, let

$$(28)\qquad \begin{aligned}\varepsilon &= (X_1 + Y_1\sqrt{D})/2, & \overline{\varepsilon} &= (X_1 - Y_1\sqrt{D})/2,\\ \varrho &= u_1 + v_1\sqrt{D}, & \overline{\varrho} &= u_1 - v_1\sqrt{D}.\end{aligned}$$

Then

$$n = Z_1 t, \qquad \frac{x+\delta\sqrt{D}}{2} = \varepsilon^t \overline{\varrho}^s, \qquad \delta \in \{-1, 1\}, \tag{29}$$

where $s, t \in \mathbb{Z}$ *satisfy*

$$\begin{gathered} s \geq 0, \qquad t > 0, \\ \gcd(s,t) = \begin{cases} 2 & \text{if } 2 \mid s,\ 2 \mid t \text{ and } x = (D+1)/2, \\ 1 & \text{otherwise.} \end{cases} \end{gathered} \tag{30}$$

P r o o f. By Lemma 11, (29) holds for some $s, t \in \mathbb{Z}$ with $s \geq 0$ and $t > 0$. Moreover, by Lemma 16, s and t satisfy (30). The lemma is proved. ∎

LEMMA 18. *Under the assumption of Lemma* 17, $\delta \equiv xY_1/X_1 \pmod 4$.

P r o o f. Let

$$(X + Y\sqrt{D})/2 = \varepsilon^t, \qquad u - v\sqrt{D} = \overline{\varrho}^s. \tag{31}$$

By Lemma 1, $X, Y \in \mathbb{Z}$ satisfy

$$\begin{aligned} X &= \varepsilon^t + \overline{\varepsilon}^t \\ &= \sum_{i=0}^{[t/2]} (-1)^i \begin{bmatrix} t \\ i \end{bmatrix} (\varepsilon + \overline{\varepsilon})^{t-2i} (\varepsilon\overline{\varepsilon})^i = \sum_{i=0}^{[t/2]} (-1)^i \begin{bmatrix} t \\ i \end{bmatrix} X_1^{t-2i} 2^{Z_1 i} \\ &\equiv \begin{cases} X_1^t - 2tX_1^{t-2} \pmod 4 & \text{if } Z_1 = 1, \\ X_1^t \pmod 4 & \text{if } Z_1 > 1, \end{cases} \end{aligned} \tag{32}$$

$$\begin{aligned} Y &= \frac{\varepsilon^t - \overline{\varepsilon}^t}{\sqrt{D}} \\ &\equiv \begin{cases} Y_1^t + 2tY_1^{t-2} \pmod 4 & \text{if } Z_1 = 1,\ 2 \nmid t, \\ (Y_1^{t'} + 2t'Y_1^{t'-2})(X_1^{t'} - 2t'X_1^{t'-2}) \pmod 4 & \\ & \text{if } Z_1 = 1,\ t = 2^\alpha t',\ \alpha > 0,\ 2 \nmid t', \\ Y_1^t \pmod 4 & \text{if } Z_1 > 1,\ 2 \nmid t, \\ Y_1^{t'} X_1^{t-t'} \pmod 4 & \text{if } Z_1 > 1,\ t = 2^\alpha t',\ \alpha > 0,\ 2 \nmid t', \end{cases} \end{aligned} \tag{33}$$

since $D \equiv 1 \pmod 8$. Notice that $4 \mid v$ when $D \equiv 1 \pmod 8$. Then from

$$\frac{x + \delta\sqrt{D}}{2} = \left(\frac{X + Y\sqrt{D}}{2}\right)(u - v\sqrt{D}), \tag{34}$$

we get $x = Xu - DYv \equiv Xu \pmod 4$ and $\delta = Yu - Xv \equiv Yu \pmod 4$, and so

$$\delta \equiv \frac{xY}{X} \pmod 4. \tag{35}$$

Since $X_1^2 \equiv DY_1^2 \pmod 8$, substituting (32) and (33) into (35), we obtain the lemma. ∎

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

P r o o f. Under our assumption, we have $x + 2^{n/2+1} = D_1$ and $x - 2^{n/2+1} = D_2$, where $(D_1, D_2) \in I(D)$. It follows that $2^{n/2+2} = D_1 - D_2 \le D - 1 < D$, which completes the proof. ∎

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

$$x'^2 - 2^{Z_1+2} y'^2 = D, \quad \gcd(x', y') = 1, \tag{36}$$

satisfying

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

P r o o f. By Lemma 7, we have

$$\langle x, 2^{Z_1(t-1)/2} \rangle \equiv -\frac{x}{2^{Z_1(t-1)/2}} \pmod{D}. \tag{37}$$

From (31) and (34), we get

$$\begin{aligned} x \equiv Xu \equiv \frac{X_1^t u_1^s}{2^{t-1}} &\equiv 2^{Z_1(t-1)/2} X_1 u_1^s \\ &\equiv \begin{cases} 2^{Z_1(t-1)/2} X_1 \pmod{D} & \text{if } 2 \mid s, \\ 2^{Z_1(t-1)/2} X_1 u_1 \pmod{D} & \text{if } 2 \nmid s, \end{cases} \end{aligned} \tag{38}$$

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 (38) into (37), we obtain the lemma. ∎

LEMMA 21. *Let (X_1, Y_1, Z_1) be the least solution of (25). If $2^{rZ_1+2} < \sqrt{D}$ for some $r \in \mathbb{N}$, then the fundamental solution $\varrho = u_1 + v_1\sqrt{D}$ of (27) satisfies $\varrho > D^{r/2}/2^{2r-2}$.*

P r o o f. By Lemma 11, there exist $X_i, Y_i \in \mathbb{Z}$ $(i = 1, \ldots, r)$ such that

$$X_i^2 - DY_i^2 = 2^{Z_1 i+2}, \quad \gcd(X_i, Y_i) = 1, \; i = 1, \ldots, r.$$

Since $2^{rZ_1+2} < \sqrt{D}$, by Lemma 5(iii), $\sqrt{D}$ has $2r$ convergents p_{s_i}/q_{s_i} and p_{t_i}/q_{t_i} $(i = 1, \ldots, r)$ such that

$$k_{s_i} = k_{t_i} = 2^{Z_1 i+2}, \quad 2 \nmid s_i t_i, \quad 0 < s_i, t_i < t, \quad i = 1, \ldots, r,$$

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

$$\begin{aligned} a_{s_i+1} &= \left[\frac{\Delta_{s_i} + \sqrt{D}}{k_{s_i}}\right] > \frac{\sqrt{D}}{2^{Z_1 i+2}}, \\ a_{t_i+1} &= \left[\frac{\Delta_{t_i} + \sqrt{D}}{k_{t_i}}\right] > \frac{\sqrt{D}}{2^{Z_1 i+2}}, \quad i = 1, \ldots, r. \end{aligned} \tag{39}$$

Notice that $p_0 = a_0$, $p_1 = a_0 a_1 + 1$ and $p_{j+2} = a_{j+2} p_{j+1} + p_j$ for $j \ge 0$. By

Lemma 5(ii), we deduce from (39) that

$$\varrho > u_1 = p_t > \prod_{j=0}^{t} a_j \geq a_0 \prod_{i=1}^{r} a_{s_i} a_{t_i}$$
$$> a_0 \biggl(\prod_{i=1}^{r} \frac{\sqrt{D}}{2^{Z_1 i+2}} \biggr)^2 = \frac{a_0 D^r}{2^{r(r+1)Z_1+4r}} > \frac{D^{r/2}}{2^{2r-2}},$$

since $a_0 = [\sqrt{D}]$. 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* (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) *Except in the above cases*, $x' - x \geq 6$ *and* $n'' \geq 2n' + 53$. ■

Lemma 23 ([1; Theorem 1]). *Let* M *be an odd power of* 2. *Then for all* $x \in \mathbb{Z}$,

$$\left| \frac{x}{\sqrt{M}} - 1 \right| > \frac{2^{-43.5}}{M^{0.9}}. \ ■$$

Lemma 24 ([1; Corollary 1]). *If* (x,n) *is a solution of* (1), *then* $n < 433 + (10 \log D)/\log 2$. *Moreover*, *if* $D < 2^{96}$, *then* $n < 16 + (2 \log D)/\log 2$. ■

Lemma 25 ([8]). *Let* q *be a power of a prime. The equation*

$$y^2 = 4q^n + 4q + 1, \quad y > 0, n > 0,$$

has the only solution $(y,n) = (2q+1, 2)$ *except for* $q = 3$ *and* $(y,n) = (5,1)$, $(7,2)$, $(11,3)$. *The equation*

$$y^2 = 4q^n + 4q^2 + 1, \quad y > 0,\ n > 0,\ 2 \nmid n,$$

has the only solution $(y,n) = (2q+1, 1)$ *except for* $q = 2$ *and* $(y,n) = (5,1)$, $(7,3)$, $(23,7)$. ■

Lemma 26 ([4]). *Let* q *be a power of a prime. The equation*

$$y^2 = 4q^n + 4q^m + 1, \quad y > 0,\ n > m > 2,\ \gcd(n,m) = 1\,,$$

has no solution (y,n,m). ■

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

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

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

$$(40)\qquad \begin{gathered}(x_1,n_1)=\left(\frac{2^{2m+1}-17}{3},3\right),\qquad (x_2,n_2)=\left(\frac{2^{2m+1}+1}{3},2m+1\right),\\ (x_3,n_3)=\left(\frac{17\cdot 2^{2m+1}-1}{3},4m+5\right).\end{gathered}$$

By the proof of Theorem 3 of [1], if $N(D)>3$, then (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 (25), and let $\varepsilon,\overline{\varepsilon},\varrho,\overline{\varrho}$ be defined as in (28). Then, by Lemma 17, we have

$$(41)\qquad n_i=Z_1t_i,\qquad \frac{x_i+\delta_i\sqrt{D}}{2}=\varepsilon^{t_i}\overline{\varrho}^{s_i},\qquad \delta_i\in\{-1,1\},\qquad i=1,\ldots,4,$$

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

$$(42)\qquad s_i\ge 0,\qquad t_i>0,\qquad \gcd(s_i,t_i)=1,\qquad i=1,\ldots,4.$$

We see from (40) and (41) that (36) has three solutions $(x_j,2^{Z_1(t_j-1)/2})$ $(j=2,3,4)$. Let $l_j=\langle x_j,2^{Z_1(t_j-1)/2}\rangle$ $(j=2,3,4)$. By Lemma 7, we deduce from (40) and (41) that

$$\begin{aligned}l_2-l_3&\equiv-\frac{2^{2m+1}+1}{3\cdot 2^{Z_1(t_2-1)/2}}+\frac{17\cdot 2^{2m+1}-1}{3\cdot 2^{Z_1(t_3-1)/2}}\\ &\equiv-\frac{2^{(Z_1-1)/2}}{3\cdot 2^{2m+2}}(2^{3m+3}-17\cdot 2^{2m+1}+2^{m+2}+1)\not\equiv 0 \pmod{D}.\end{aligned}$$

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

$$\begin{aligned}x_4&+2^{Z_1(t_4-1)/2}\sqrt{2^{Z_1+2}}\\ &=\begin{cases}(x_2+2^{Z_1(t_2-1)/2}\sqrt{2^{Z_1+2}})(U'+V'\sqrt{2^{Z_1+2}}) & \text{if } l_4=l_2,\\ (x_3+2^{Z_1(t_3-1)/2}\sqrt{2^{Z_1+2}})(U'+V'\sqrt{2^{Z_1+2}}) & \text{if } l_4=l_3,\end{cases}\end{aligned}$$

and hence

$$(43)\qquad 2^{Z_1(t_4-1)/2}=\begin{cases}x_2V'+2^{Z_1(t_2-1)/2}U' & \text{if } l_4=l_2,\\ x_3V'+2^{Z_1(t_3-1)/2}U' & \text{if } l_4=l_3,\end{cases}$$

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

$$(44)\qquad U'^2-2^{Z_1+2}V'^2=1.$$

Since $t_3>t_2$, we obtain

$$(45)\qquad 2^{Z_1(t_2-1)/2}\mid V'$$

by (43). On applying Lemma 3 together with (45), we have

$$(46)\qquad U'+V'\sqrt{2^{Z_1+2}}=(3+2\sqrt{2})^{2^m r},\qquad r\in\mathbb{N},$$

since $Z_1 t_2 = 2m+1$. From (46), we deduce $2U' > 2^{5\cdot 2^{m-1}}$ and

$$n_4 > 2m + 1 + 5 \cdot 2^m \tag{47}$$

by (40), (41) and (43). On the other hand, by Lemma 24, we have

$$n_4 < 433 + 10\frac{\log D}{\log 2} < 433 + 40m \tag{48}$$

since $D < 2^{4m}$. The combination of (47) and (48) yields $m \le 7$ and $D < 2^{4m} \le 2^{28} < 10^{12}$. Thus the proposition is proved. ∎

Proposition 2. *If D is of type* III, *then* $N(D) = 3$.

P r o o f. In this case, (1) has three solutions

$$\begin{gathered}(x_1, n_1) = (2^{m_2} - 2^{m_1} - 1, m_1), \quad (x_2, n_2) = (2^{m_2} - 2^{m_1} + 1, m_2),\\ (x_3, n_3) = (2^{m_2} + 2^{m_1} - 1, m_2 + m_1).\end{gathered} \tag{49}$$

If $N(D) > 3$, then (1) has another solution (x_4, n_4) with $n_4 > n_3$. Moreover, then (41) and (42) still hold by Lemma 17.

When $2 \mid m_1$ and $2 \mid m_2$, we find from (49) that

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

where

$$\begin{aligned} D_{11} &= 2^{m_2} - 2^{m_1} + 2^{m_1/2+1} - 1, \quad & D_{12} &= 2^{m_2} - 2^{m_1} - 2^{m_1/2+1} - 1,\\ D_{21} &= 2^{m_2} + 2^{m_2/2+1} - 2^{m_1} + 1, \quad & D_{22} &= 2^{m_2} - 2^{m_2/2+1} - 2^{m_1} + 1.\end{aligned}$$

Since (D_{11}, D_{12}), $(D_{21}, D_{22}) \in I'(D)$ and $(D_{11}, D_{12}) \ne (D_{21}, D_{22})$, by Lemma 14, the least solution of (25) satisfies $2 \mid Z_1$. Therefore, $2 \mid n_4$ by (41). 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

$$\begin{gathered} D_{31} = 2^{m_2} + 2^{(m_2+m_1)/2+1} + 2^{m_1} - 1, \quad D_{32} = 2^{m_2} - 2^{(m_2+m_1)/2+1} + 2^{m_1} - 1,\\ D_{41} = x_4 + 2^{n_4/2+1}, \quad D_{42} = x_4 - 2^{n_4/2+1}.\end{gathered}$$

Since (D_{31}, D_{32}), $(D_{41}, D_{42}) \in I'(D)$ and (D_{i1}, D_{i2}) $(i = 1, \ldots, 4)$ are different, this implies that there exist four distinct pairs $(D_1, D_2) \in I'(D)$ which make (26) have solutions. By Lemma 15, that is impossible.

When $2 \mid m_1$ and $2 \nmid m_2$, we have $2 \nmid Z_1$ by (41). If $2 \mid n_4$, since $2 \mid m_1$, we see from Lemma 14 that $2 \mid Z_1$, a contradiction. Therefore $2 \nmid n_4$, and (36) has three solutions $(x_j, 2^{Z_1(t_j-1)/2})$ $(j = 2, 3, 4)$. Let $l_j = \langle x_j, 2^{Z_1(t_j-1)/2}\rangle$

($j = 2, 3, 4$). From (49), we get

$$\begin{aligned} l_2 - l_3 &\equiv -\frac{2^{m_2} - 2^{m_1} + 1}{2^{Z_1(t_2-1)/2}} + \frac{2^{m_2} + 2^{m_1} - 1}{2^{Z_1(t_3-1)/2}} \\ &\equiv \frac{2^{(Z_1-1)/2}}{2^{(m_2+m_1-1)/2}}(-2^{m_1/2}(2^{m_2} - 2^{m_1} + 1) + (2^{m_2} + 2^{m_1} - 1)) \\ &\not\equiv 0 \pmod{D}. \end{aligned}$$

It follows that $l_2 \neq l_3$ and either $l_4 = l_2$ or $l_4 = l_3$ by Lemma 20. By much the same argument as in the proof of Proposition 1, (43) and (45) still hold. Hence

$$U' + V'\sqrt{2^{Z_1+2}} = (3 + 2\sqrt{2})^{2^{(m_2-1)/2}r}, \quad r \in \mathbb{N},$$

whence we get

$$2U' > 2^{5\cdot 2^{(m_2-3)/2}}.$$

On applying this together with (43), we obtain

$$n_4 > m_2 + 5 \cdot 2^{(m_2-3)/2}. \tag{50}$$

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

$$n_4 < 433 + 10\frac{\log D}{\log 2} < 433 + 20m_2 \tag{51}$$

by Lemma 24. The combination of (50) and (51) yields $m_2 \leq 17$ and $D < 2^{34} < 10^{12}$, which contradicts our assumption.

Let $2 \nmid m_1 m_2$ and $3.6m_1 \geq m_2$. Since $2 \mid m_2 + m_1$, we have $2 \nmid n_4$, and (36) has three solutions $(x_j, 2^{Z_1(t_j-1)/2})$ ($j = 1, 2, 4$). Let $l_j = \langle x_j, 2^{Z_1(t_j-1)/2}\rangle$ ($j = 1, 2, 4$). 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 much the same argument as in the case of $2 \mid m_1$ and $2 \nmid m_2$, we can prove $l_4 \neq l_2$. If $l_4 = l_1$, we have

$$\begin{aligned} &x_4 + 2^{Z_1(t_4-1)/2}\sqrt{2^{Z_1+2}} \\ &\qquad = (2^{m_2} - 2^{m_1} - 1 + 2^{Z_1(t_1-1)/2}\sqrt{2^{Z_1+2}})(U' + V'\sqrt{2^{Z_1+2}}), \end{aligned}$$

whence we get

$$2^{Z_1(t_4-1)/2} = (2^{m_2} - 2^{m_1} - 1)V' + 2^{Z_1(t_1-1)/2}U',$$

where $U', V' \in \mathbb{N}$ satisfy (44). Hence $2^{Z_1(t_1-1)/2} \mid V'$ and

$$2^{Z_1(t_4-t_1)/2} = (2^{m_2} - 2^{m_1} - 1)\frac{V'}{2^{Z_1(t_1-1)/2}} + U'. \tag{52}$$

Further, by Lemma 3, we have

$$U' + V'\sqrt{2^{Z_1+2}} = (3 + 2\sqrt{2})^{2^{(m_1-1)/2}r}, \quad r \in \mathbb{N}, \tag{53}$$

since $m_1 = Z_1 t_1$ and $2 \nmid Z_1$. Furthermore, we see from (53) that $U' \equiv 1 \pmod 8$ and

$$\frac{V'}{2^{Z_1(t_1-1)/2}} \equiv 3^{2^{(m_1-1)/2}r-1} r \equiv 3r \pmod 8$$

since $m_1 \ge 3$. Hence, we obtain $r \equiv 3 \pmod 8$ by (52). This implies that $r \ge 3$ and

$$2U' > 2^{15\cdot 2^{(m_1-3)/2}}$$

by (53). On combining this with (52), we get

$$n_4 > m_1 + 15 \cdot 2^{(m_1-1)/2} - 2. \tag{54}$$

On the other hand, by Lemma 24,

$$n_4 < 433 + 10\frac{\log D}{\log 2} < 433 + 20m_2 \le 433 + 72m_1. \tag{55}$$

The combination of (54) and (55) yields $m_1 \le 13$ and $D < 2^{2m_2} \le 2^{7.2m_1} < 2^{96}$. On applying Lemma 24 again, we have

$$n_4 < 16 + 2\frac{\log D}{\log 2} < 16 + 4m_2 \le 16 + 14.4m_1.$$

On combining this with (54), we get $m_1 \le 5$ and $D < 2^{36} < 10^{12}$. Thus $N(D) = 3$.

Using the same method, we can prove the proposition in the case that $2 \nmid m_1$, $2 \mid m_2$ and $m_2 \le 3.6m_1$.

Let $2 \nmid m_1$ and $m_2 > 3.6m_1$. We deduce from (41) that

$$\left(\frac{x_2 + \delta_2\sqrt{D}}{2}\right)^{t_3} \varrho^{s_2 t_3} = \left(\frac{x_3 + \delta_3\sqrt{D}}{2}\right)^{t_2} \varrho^{s_3 t_2}. \tag{56}$$

Since $x_2 \equiv 1 \pmod 4$ and $x_3 \equiv -1 \pmod 4$, we have

$$\delta_2 = -\delta_3 \tag{57}$$

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 (41) and (49). Hence, from (56) and (57),

$$\begin{aligned}(58)\quad & |s_2 t_3 - s_3 t_2| \log \varrho \\ &= \left| t_3 \log \frac{x_2 + \delta_2\sqrt{D}}{2} - t_2 \log \frac{x_3 + \delta_3\sqrt{D}}{2} \right| \\ &= t_3 \log \frac{x_2 + \sqrt{D}}{2} + t_2 \log \frac{x_3 + \sqrt{D}}{2} - t_2 t_3 \log 2^{Z_1} \\ &< t_3 \log \tfrac{1}{2}((2^{m_2} - 2^{m_1} + 1) + (2^{m_2} - 2^{m_1} - 1))\end{aligned}$$

$$+ t_2 \log \tfrac{1}{2}((2^{m_2} + 2^{m_1} - 1) + (2^{m_2} - 2^{m_1} - 1)) - t_3 \log 2^{m_2}$$
$$< t_2 \log 2^{m_2}.$$

Notice that only one of n_2 and n_3 is even. We see from (42) that $2 \nmid s_2 t_3 - s_3 t_2$. If $|s_2 t_3 - s_3 t_2| > 1$, then $|s_2 t_3 - s_3 t_2| \ge 3$ and

$$3 \log \varrho < t_2 \log 2^{m_2} \tag{59}$$

by (58). Recalling that $m_2 = Z_1 t_2$ and $2 \nmid Z_1$, 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

$$\log \varrho > \begin{cases} (t_2 - 3)\log\sqrt{D} - (t_2 - 4)\log 4 & \text{if } Z_1 = 1, \\ (t_2 - 1)\log\sqrt{D} - (t_2 - 2)\log 4 & \text{if } Z_1 > 1. \end{cases} \tag{60}$$

Recalling that $D \ge 10^{12}$, the combination of (59) and (60) yields

$$t_2 \le \begin{cases} 4 & \text{if } Z_1 = 1, \\ 2 & \text{if } Z_1 > 1, \end{cases}$$

a contradiction. Thus

$$s_2 t_3 - s_3 t_2 = \pm 1. \tag{61}$$

Let $\alpha = (\log(\varepsilon/\overline{\varepsilon}))/\log \varrho^2$, and let

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

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

$$\alpha - \frac{s_i}{t_i} = \frac{\delta_i \Lambda(x_i, n_i)}{t_i \log \varrho^2}, \qquad i = 1, \ldots, 4, \tag{62}$$

by (41). We see from (57) that $\alpha \in (s_2/t_2, s_3/t_3)$. Moreover, since $t_4 > t_j$ and $\Lambda(x_4, n_4) < \Lambda(x_j, n_j)$ for $j = 2, 3$, we see from (62) that also $s_4/t_4 \in (s_2/t_2, s_3/t_3)$. By Lemma 2, we find from (61) that

$$t_4 = c t_2 + c' t_3, \qquad s_4 = c s_2 + c' s_3, \qquad c, c' \in \mathbb{N}. \tag{63}$$

From (41) and (63), we have

$$\frac{x_4 + \delta_4\sqrt{D}}{2} = \varepsilon^{t_4}\overline{\varrho}^{s_4} = \left(\frac{x_2 + \delta_2\sqrt{D}}{2}\right)^{c}\left(\frac{x_3 + \delta_3\sqrt{D}}{2}\right)^{c'}. \tag{64}$$

Let

$$\frac{X_2 + Y_2\sqrt{D}}{2} = \left(\frac{x_2 + \delta_2\sqrt{D}}{2}\right)^{c}, \qquad \frac{X_3 + Y_3\sqrt{D}}{2} = \left(\frac{x_3 + \delta_3\sqrt{D}}{2}\right)^{c'}. \tag{65}$$

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

$$\varepsilon_2^m + \overline{\varepsilon}_2^m = \sum_{i=0}^{[m/2]} (-1)^i \begin{bmatrix} m \\ i \end{bmatrix} (\varepsilon_2 + \overline{\varepsilon}_2)^{m-2i} (\varepsilon_2\overline{\varepsilon}_2)^i \equiv (1 - 2^{m_1})^m \pmod{2^{m_2}}$$

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

$$\begin{aligned} Y_2 &= \frac{\varepsilon_2^c - \overline{\varepsilon}_2^c}{\sqrt{D}} = \delta_2 \frac{\varepsilon_2^c - \overline{\varepsilon}_2^c}{\varepsilon_2 - \overline{\varepsilon}_2} = \delta_2 \left((\varepsilon_2^{c-1} + \overline{\varepsilon}_2^{c-1}) + \varepsilon_2\overline{\varepsilon}_2 \left(\frac{\varepsilon_2^{c-2} - \overline{\varepsilon}_2^{c-2}}{\varepsilon_2 - \overline{\varepsilon}_2} \right) \right) \\ &\equiv \delta_2(\varepsilon_2^{c-1} + \overline{\varepsilon}_2^{c-1}) \equiv \delta_2(1 - 2^{m_1})^{c-1} \pmod{2^{m_2}}. \end{aligned}$$

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 (57), (64) and (65),

$$\begin{aligned} 2\delta_4 &= X_2Y_3 + X_3Y_2 \\ &\equiv \delta_3(1 - 2^{m_1})^c(-1 + 2^{m_1})^{c'-1} + \delta_2(1 - 2^{m_1})^{c-1}(-1 + 2^{m_1})^{c'} \\ &\equiv (-1)^{c'} 2\delta_2(1 - 2^{m_1})^{c+c'-1} \pmod{2^{m_2}}. \end{aligned}$$

It follows that $\pm 1 \equiv (1 - 2^{m_1})^{c+c'-1} \pmod{2^{m_2-1}}$, whence we deduce that $c + c' - 1 \equiv 0 \pmod{2^{m_2-m_1-1}}$. Since $m_1 \geq 3$ and $m_2 > 3.6m_1$, we have $c + c' - 1 > 2^{2.6m_1-1} > 2^{6.8} > 96$. Hence, from (41), (49) and (63), we get

$$n_4 = cm_2 + c'(m_2 + m_1) > (c + c')m_2 > 96m_2 > 48\frac{\log D}{\log 2}, \tag{66}$$

since $\sqrt{D} < 2^{m_2}$. On combining Lemma 24 with (66), we obtain $D < 2^{20} < 10^{12}$. Thus $N(D) = 3$. All cases are considered and the proposition is proved. ∎

The combination of Propositions 1 and 2 yields the theorem.

5. Proof of Theorem 2. Clearly, D is non-square while (2) has solutions. Now we suppose that $N(D) > 2$. Then (1) has three solutions (x_i, n_i) $(i = 1, 2, 3)$ such that $n_3 > n_2 > n_1$. By Lemma 17, we have

$$n_i = Z_1 t_i, \quad t_i \in \mathbb{N},\ i = 1, 2, 3. \tag{67}$$

First we consider the case that one of n_1, n_2, n_3 is even, say $2 \mid n_j$ $(1 \leq j \leq 3)$. Then we have $x_j + 2^{n_j/2+1} = D_{1j}$ and $x_j - 2^{n_j/2+1} = D_{2j}$, where $(D_{1j}, D_{2j}) \in I'(D)$ satisfies

$$D_{1j} - D_{2j} = 2^{n_j/2+2}. \tag{68}$$

If $(D_{1j}, D_{2j}) = (D, 1)$, then $D = 2^{n_j/2+2} + 1$ and

$$x_i^2 = 4 \cdot 2^{n_i} + 4 \cdot 2^{n_j/2} + 1, \quad i = 1, 2, 3, \tag{69}$$

from (1). By Lemmas 25 and 26, we see from (69) that if $D \neq 17$ then $n_j/2 = 2n_i$ for each i such that $1 \leq i \leq 3$ and $i \neq j$. Since $n_3 > n_2 > n_1$, this is impossible for $D \neq 17$. Notice that $D = 17$ is of type I. Therefore $(D_{1j}, D_{2j}) \neq (D, 1)$.

Under the assumption that (2) has solutions, by Lemma 6, the equation

$$D_{1j} u'^2 - D_{2j} v'^2 = 1$$

has no solution (u', v'). Hence, by Lemma 12, we get $2 \mid Z_1$. It follows from (67) that $2 \mid n_i$ $(i = 1, 2, 3)$. Then we have

$$D_{1i} - D_{2i} = 2^{n_i/2+2}, \quad (D_{1i}, D_{2i}) \in I'(D), \quad (D_{1i}, D_{2i}) \neq (D, 1), \quad i = 1, 2, 3. \tag{70}$$

On the other hand, since (2) has solutions, the equation

$$DX'^2 - Y'^2 = 2^{Z'+2}, \quad \gcd(X', Y') = 1, \ Z' > 0, \tag{71}$$

has solutions (X', Y', Z') by Lemma 12. From (70) and (71), there exist four distinct pairs $(D_1, D_2) \in I'(D)$ which make (26) have solutions. But, by Lemma 15, that is impossible.

Next we consider the case that $2 \nmid n_i$ $(i = 1, 2, 3)$. Then $(x_i, 2^{Z_1(t_i-1)/2})$ $(i = 1, 2, 3)$ are positive solutions of (36). Let $l_i = \langle x_i, 2^{Z_1(t_i-1)/2} \rangle$ $(i = 1, 2, 3)$. By Lemma 20, we get either $l_i \equiv -X_1 \pmod{D}$ or $l_i \equiv -X_1 u_1 \pmod{D}$ $(1 \leq i \leq 3)$. Recalling that (2) has solutions, by Lemma 6, we have $u_1 \equiv -1 \pmod{D}$. This implies $l_i \equiv \pm X_1 \pmod{D}$, and $l_3 \equiv \lambda l_2 \pmod{D}$, where $\lambda \in \{-1, 1\}$. By Lemma 7, $(x_2, 2^{Z_1(t_2-1)/2}\lambda)$ is a solution of (36) such that $\langle x_2, 2^{Z_1(t_2-1)/2}\lambda \rangle \equiv \lambda l_2 \pmod{D}$. Hence, by Lemma 8, we obtain

$$x_3 + 2^{Z_1(t_3-1)/2}\sqrt{2^{Z_1+2}} = (x_2 + 2^{Z_1(t_2-1)/2}\lambda\sqrt{2^{Z_1+2}})(U' + V'\sqrt{2^{Z_1+2}}), \tag{72}$$

where (U', V') is a positive solution of (44). From (72),

$$2^{Z_1(t_3-1)/2} = x_2 V' + 2^{Z_1(t_2-1)/2}\lambda U'.$$

This implies $2^{Z_1(t_2-1)/2} \mid V'$. Hence, by Lemma 3, we have

$$U' + V'\sqrt{2^{Z_1+2}} \geq (3 + 2\sqrt{2})^{2^{(n_2-1)/2}}. \tag{73}$$

Let $\alpha = \log 2^{n_2+2}/\log D$. By Lemma 4, we see that $\alpha \geq 1/2$. By Lemma 23, we find from (72) and (73) that

$$2^{0.4(n_3+2)+43.5} D > \frac{D}{x_3 - 2^{n_3/2+1}} = x_3 + 2^{n_3/2+1} = x_3 + 2^{Z_1(t_3-1)/2}\sqrt{2^{Z_1+2}} \tag{74}$$

$$\begin{aligned}
&\geq (x_2 - 2^{Z_1(t_2-1)/2}\sqrt{2^{Z_1+2}})(U' + V'\sqrt{2^{Z_1+2}}) \\
&= (x_2 - 2^{n_2/2+1})(U' + V'\sqrt{2^{Z_1+2}}) \\
&> \frac{(3+2\sqrt{2})^{2^{(n_2-1)/2}}}{2^{0.4(n_2+2)+43.5}} = \frac{(3+2\sqrt{2})^{2^{-3/2}D^{\alpha/2}}}{2^{43.5}D^{0.4\alpha}}.
\end{aligned}$$

On applying Lemma 24, (74) yields

$$2^{218.3}D^5 > \frac{(3+2\sqrt{2})^{2^{-3/2}D^{\alpha/2}}}{2^{43.5}D^{0.4\alpha}},$$

whence we get

$$184 + (5 + 0.4\alpha)\log D > 0.7D^{\alpha/2}. \tag{75}$$

Recalling that $\alpha > 1/2$, we conclude from (75) that $D < 10^{12}$. Thus, by Theorem 4 of [1], the theorem is proved.

Acknowledgement. The author would like to thank Professor A. Schinzel for his valuable suggestions. Were it not for him, this paper would not exist.

References

[1] F. Beukers, *On the generalized Ramanujan–Nagell equation I*, Acta Arith. 38 (1981), 389–410.

[2] P. G. L. Dirichlet, *Sur une propriété des formes quadratiques à déterminant positif*, J. Math. Pures Appl. (2) 1 (1856), 76–79.

[3] L.-K. Hua, *Introduction to Number Theory*, Springer, Berlin 1982.

[4] M.-H. Le, *The diophantine equation* $x^2 = 4q^n + 4q^m + 1$, Proc. Amer. Math. Soc. 106 (1989), 599–604.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.

[6] O. Perron, *Die Lehre von den Kettenbrüchen*, Teubner, Leipzig 1929.

[7] K. Petr, *Sur l'équation de Pell*, Časopis Pest. Mat. Fys. 56 (1927), 57– 66 (in Czech).

[8] N. Tzanakis and J. Wolfskill, *The diophantine equation* $x^2 = 4q^{a/2} + 4q + 1$*, with an application to coding theory*, J. Number Theory 26 (1987), 96–116.

RESEARCH DEPARTMENT
CHANGSHA RAILWAY INSTITUTE
CHANGSHA, HUNAN, CHINA

Received on 7.9.1990
and in revised form on 11.2.1991 (2077)