ACTA ARITHMETICA
LXIV.1 (1993)

On the diophantine equation $D_1x^2 + D_2 = 2^{n+2}$

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 $D_1, D_2 \in \mathbb{N}$ be odd, and let $N(D_1, D_2)$ denote the number of solutions (1) (x, n) of the equation

$$D_1x^2 + D_2 = 2^{n+2}, \quad x > 0,\ n > 0. \tag{1}$$

There are many papers concerned with upper bounds for $N(D_1, D_2)$ when $\min(D_1, D_2) = 1$. The known results include the following:

1 (Nagell [12]). $N(1, 7) = 5$.

2 (Apéry [1]). If $D_2 \neq 7$, then $N(1, D_2) \leq 2$.

3 (Beukers [5]). $N(1, 23) = N(1, 2^{r+2} - 1) = 2$ for $r > 1$, otherwise $N(1, D_2) \leq 1$ for $D_2 \neq 7$.

4 (Le [8]). $N(7, 1) = 2$, otherwise $N(D_1, 1) \leq 1$.

We have not been able to find similar results for the case $\min(D_1, D_2) > 1$. In this paper we prove a general result as follows:

Theorem 1. *If* $\min(D_1, D_2) > 1$ *and* $(D_1, D_2) \neq (3, 5)$, *then* $N(D_1, D_2) \leq 2$.

By [4], we see that $N(3, 5) = 3$. On the other hand, we notice that if D_1, D_2 satisfy

$$D_1X_1^2 = 2^{Z_1} - (-1)^{(D_2-1)/2}, \quad D_2 = 3 \cdot 2^{Z_1} + (-1)^{(D_2-1)/2}, \quad X_1, Z_1 \in \mathbb{N},\ Z_1 > 1, \tag{2}$$

then (1) has two solutions

$$(x, n) = (X_1, Z_1), \quad ((2^{Z_1+1} + (-1)^{(D_2-1)/2})X_1, 3Z_1). \tag{3}$$

Supported by the National Natural Science Foundation of China.

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

Such a pair (D_1, D_2) will be called *exceptional*. By Theorem 1, if $(D_1, D_2) \neq (3,5)$ and (D_1, D_2) is exceptional, then $N(D_1, D_2) = 2$. For the remaining cases, we have:

THEOREM 2. *If* $\min(D_1, D_2) > 1$, $\max(D_1, D_2) > \exp\exp\exp 105$ *and* (D_1, D_2) *is not exceptional, then* $N(D_1, D_2) \leq 1$.

This theorem determines all but a finite number of (D_1, D_2) for which $N(D_1, D_2) > 1$.

2. Preliminaries

LEMMA 1 ([10, Formula 1.76]). *For any* $m \in \mathbb{N}$ *and any complex numbers* α *and* 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

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

LEMMA 2. *If* p *is an odd prime with* $p > 3$, $t \in \mathbb{N}$, $t > 2$, $t(t-1) = p^r s$, $r, s \in \mathbb{N}$ *and* $p \nmid s$, *then*

$$\binom{t}{2i} p^i \equiv 0 \pmod{p^{r+2}}$$

for $i > 1$.

Proof. Let $p^{\alpha_i} \parallel 2i(2i-1)$. Since $p \geq 5$ and $\gcd(2i, 2i-1) = 1$, we get $\alpha_i \leq [\operatorname{Log} 2i / \operatorname{Log} p] \leq i-2$. From

$$\binom{t}{2i} p^i = p^2 t(t-1) \binom{t-2}{2i-2} \frac{p^{i-2}}{2i(2i-1)} ,$$

the lemma follows. $\blacksquare$

LEMMA 3. *Let* $a, a', b, r, s \in \mathbb{N}$ *be such that* $a' > a \geq b$, $r > 1$ *and* $a' \equiv a \pmod{2^s}$. *Then*

$$\left(\binom{a'}{b} - \binom{a}{b} \right) 2^{br} \equiv 0 \pmod{2^{r+s}} .$$

Proof. Clearly, the lemma holds for $b = 1$. If $b>1$, let $E(z) = \prod_{i=0}^{b-1} (z-i)$. Then

$$\binom{a'}{b} = \frac{E(a')}{b!} , \qquad \binom{a}{b} = \frac{E(a)}{b!} ,$$

and $E(a') - E(a) \equiv 0 \pmod{a' - a}$. Hence $E(a') - E(a) \equiv 0 \pmod{2^s}$ as $a' \equiv a \pmod{2^s}$. Let $2^{\gamma_b} \,\|\, b!$. From

$$\gamma_b = \sum_{i=1}^{\infty} \left[\frac{b}{2^i}\right] < \sum_{i=0}^{\infty} \frac{b}{2^i} = b$$

we get $\gamma_b \le b - 1$. This implies that

$$\left(\binom{a'}{b} - \binom{a}{b}\right) 2^{br} = 2^r (E(a') - E(a)) \frac{2^{(b-1)r}}{b!} \equiv 0 \pmod{2^{r+s}}. \ \blacksquare$$

LEMMA 4. *Let* $t, t', r, s \in \mathbb{N}$ *be such that* $t' > t > 1$ *and* $t' \equiv t \pmod{2^s}$. *Then*

$$\binom{t' - i - 1}{i} 2^{ri} \equiv 0 \pmod{2^{r+s}}, \qquad \frac{t+1}{2} \le i \le t - 1.$$

Proof. For $(t+1)/2 \le i \le t-1$, we have $t' - 2i < t' - t \le t' - i - 1$. This implies that $\prod_{j=0}^{i-1} (t' - i - j - 1) \equiv 0 \pmod{2^s}$ as $t' \equiv t \pmod{2^s}$. Let $2^{\gamma_i} \,\|\, i!$. Since $\gamma_i \le i - 1$, we get

$$\binom{t' - i - 1}{i} 2^{ri} = 2^r \frac{2^{r(i-1)}}{i!} \prod_{j=0}^{i-1} (t - i - j - 1) \equiv 0 \pmod{2^{r+s}}. \ \blacksquare$$

LEMMA 5. *If* $\min(D_1, D_2) > 1$ *and the equation*

$$D_1X^2 + D_2Y^2 = 2^{Z+2}, \quad \gcd(X, Y) = 1, \ Z > 0, \tag{4}$$

has solutions (X, Y, Z), *then all solutions of* (4) *are given by*

$$Z = Z_1 t, \qquad \frac{X\sqrt{D_1} + Y\sqrt{-D_2}}{2} = \lambda \left(\frac{X_1\sqrt{D_1} + \lambda' Y_1 \sqrt{-D_2}}{2} \right)^t, \qquad \lambda, \lambda' \in \{-1, 1\},$$

where $t \in \mathbb{N}$ *with* $2 \nmid t$, (X_1, Y_1, Z_1) *is a unique positive solution of* (4) *such that* $Z_1 \le Z$ *for all solutions of* (4). (X_1, Y_1, Z_1) *is called the least solution of* (4).

Proof. Notice that the only solutions of the equation $u^2 - (-D_1D_2)v^2 = 1$ are $(u, v) = (\pm 1, 0)$. By much the same argument as in the proof of Lemmas 11 and 12 of [9], we can prove the lemma without difficulty. $\blacksquare$

LEMMA 6. *Let* a_1, a_2 *be complex numbers with* $a_2 \ne 0$. *The solution of the difference equation*

$$u_{m+2} = a_1 u_{m+1} + a_2 u_m, \qquad m \ge 0,$$

with given initial conditions u_0, u_1 *is*

$$u_m = u_0 F(m) + (u_1 - a_1 u_0) F(m-1), \qquad m \ge 0,$$

where

$$F(m)=\begin{cases}0 & \text{if } m<0,\\ 1 & \text{if } m=0,\\ \displaystyle\sum_{\substack{r_1+2r_2=m\\ r_1,r_2\ge 0}}\binom{r_1+r_2}{r_1}a_1^{r_1}a_2^{r_2} & \text{if } m>0.\end{cases}$$

Proof. By the definition of $F(m)$,

$$F(m)=\sum_{r_2=0}^{[m/2]}\binom{m-r_2}{r_2}a_1^{m-2r_2}a_2^{r_2}\,,\qquad m\ge 0\,.$$

Since

$$\binom{m+2-r_2}{r_2}=\binom{m+1-r_2}{r_2}+\binom{m-(r_2-1)}{r_2-1},\qquad r_2\ge 0\,,$$

we have

$$F(m+2)=a_1F(m+1)+a_2F(m)\,,\qquad m\ge 0\,.$$

Clearly, the lemma holds for $m=0$ or 1. Now we assume that it holds for some m with $m>1$. Then we have

$$\begin{aligned}u_{m+1}&=a_1u_m+a_2u_{m-1}\\ &=a_1(u_0F(m)+(u_1-a_1u_0)F(m-1))\\ &\quad+a_2(u_0F(m-1)+(u_1-a_1u_0)F(m-2))\\ &=u_1F(m)+a_2u_0F(m-1)\\ &=u_1F(m)+u_0(F(m+1)-a_1F(m))\\ &=u_0F(m+1)+(u_1-a_1u_0)F(m)\,.\end{aligned}$$

Thus, by induction on m, the lemma is proved. ∎

Let α be a nonzero algebraic number with the defining polynomial

$$a_0z^r+a_1z^{r-1}+\ldots+a_r=a_0(z-\sigma_1\alpha)\ldots(z-\sigma_r\alpha)\,,\qquad a_0>0\,,$$

where $\sigma_1\alpha,\ldots,\sigma_r\alpha$ are all the conjugates of α. Then

$$h(\alpha)=\frac{1}{r}\Big(\operatorname{Log}a_0+\sum_{i=1}^{r}\operatorname{Log}\max(1,|\sigma_i\alpha|)\Big)$$

is called *Weil's height* of α.

Lemma 7. *Let α be an algebraic number with degree* 2, *and let* $\log\alpha$ *be any nonzero determination of the logarithm of α. If $h(\alpha)\ge 2\pi e$ and $\Lambda=b_1\log\alpha-b_2\log(-1)\neq 0$ for some $b_1,b_2\in\mathbb{N}$ with* $\max(b_1,b_2)\ge 10^5$, *then*

$$|\Lambda|\ge\exp(-21590A(1+\operatorname{Log}B+\operatorname{Log}\operatorname{Log}2B)^2)\,,$$

where $A=h(\alpha)$, $B=\max(b_1,b_2)$.

P r o o f. Put $\alpha_1 = \alpha$ and $\alpha_2 = -1$. By the definitions of [11], we have $D = 2$, $f = 2e$, $a_1 = h(\alpha) + \operatorname{Log} 2$ and $a_2 = \pi e$. Since $h(\alpha) \ge 2\pi e$ and $B \ge 10^5$, we may choose $Z = 1.5$ and $G = 1 + \operatorname{Log} B + \operatorname{Log}\operatorname{Log} 2B$. Notice that α_1 and α_2 are multiplicatively dependent numbers. We see from Figure 4 of [11] that $C/Z^3 = 158$, $c_0 = 59.59$, $c_1 = 1.88$ and $c = 4.94$. Thus, by Theorem 5.11 of [11], the lemma is proved. ∎

LEMMA 8 ([6]). *Let F_m be the m-th Fibonacci number. If F_m is a power of* 2, *then* $m = 1, 2, 3$ *or* 6.

LEMMA 9 ([3]). *The only solutions of the equation*

$$X^3 + X^2Y - 2XY^2 - Y^3 = 1$$

are $(X, Y) = (1, 0)$, $(0, -1)$, $(-1, 1)$, $(2, -1)$, $(-1, 2)$, $(5, 4)$, $(4, -9)$ *and* $(-9, 5)$. ∎

LEMMA 10 ([2]). *Let $a \in \mathbb{Z}$ with $a \ne 0$, and let $f(X, Y) \in \mathbb{Z}[X, Y]$ be a homogeneous polynomial of degree $r \ge 3$ which is irreducible over $\mathbb{Q}$. Then all solutions (X, Y) of the equation*

$$f(X, Y) = a$$

satisfy

$$\max(|X|, |Y|) < \exp((rH)^{(10r)^5} + (\operatorname{Log}|a|)^{2r+2}),$$

where H is the height of $f(X, Y)$. ∎

R e m a r k. By some better estimates for the upper bound of solutions of Thue's equation (cf. Győry and Papp [7]), the bound $\max(D_1, D_2) > \exp\exp\exp 105$ in Theorem 2 can be improved.

3. Further preliminary lemmas. Notice that if $D_1 = d^2$ is a square and (x, n) is a solution of (1), then $(x', n') = (dx, n)$ is a solution of the equation

$$x'^2 + D_2 = 2^{n'+2}, \quad x' > 0, \ n' > 0.$$

We may assume that $\min(D_1, D_2) > 1$ and D_1 is not a square.

LEMMA 11. *Equation* (1) *has a solution* (x, n) *if and only if* (4) *has solutions* (X, Y, Z) *and its least solution* (X_1, Y_1, Z_1) *satisfies* $Y_1 = 1$.

P r o o f. If $Y_1 = 1$, then (1) has a solution $(x, n) = (X_1, Z_1)$. On the other hand, if (x, n) is a solution of (1), then $(x, 1, n)$ is a solution of (4). By Lemma 5, we have

$$(5) \qquad n = Z_1 t, \quad \frac{x\sqrt{D_1} + \sqrt{-D_2}}{2} = \lambda\left(\frac{X_1\sqrt{D_1} + \lambda' Y_1\sqrt{-D_2}}{2}\right)^t, \quad \lambda, \lambda' \in \{-1, 1\}, \ t \in \mathbb{N}, \ 2 \nmid t.$$

Let

$$\varepsilon_1 = \lambda \frac{X_1\sqrt{D_1} + \lambda' Y_1 \sqrt{-D_2}}{2}, \quad \overline{\varepsilon}_1 = \lambda \frac{X_1\sqrt{D_1} - \lambda' Y_1 \sqrt{-D_2}}{2}.$$

Since $D_1 X_1^2 + D_2 Y_1^2 = 2^{Z_1+2}$, by Lemma 1, from (5) we get

$$\begin{aligned} 1 &= \frac{\varepsilon_1^t - \overline{\varepsilon}_1^t}{\sqrt{-D_2}} = \lambda\lambda' Y_1 \frac{\varepsilon_1^t - \overline{\varepsilon}_1^t}{\varepsilon_1 - \overline{\varepsilon}_1} \\ &= \lambda\lambda' Y_1 \sum_{i=0}^{(t-1)/2} \begin{bmatrix} t \\ i \end{bmatrix} (\varepsilon_1 - \overline{\varepsilon}_1)^{t-2i-1} (\varepsilon_1 \overline{\varepsilon}_1)^i \\ &= \lambda\lambda' Y_1 \sum_{i=0}^{(t-1)/2} \begin{bmatrix} t \\ i \end{bmatrix} (-D_2 Y_1^2)^{\frac{t-1}{2}} 2^{Z_1 i}. \end{aligned}$$

This implies that $Y_1 = 1$. ∎

LEMMA 12. *Let*

$$\varepsilon = \frac{X_1\sqrt{D_1} + \sqrt{-D_2}}{2}, \quad \overline{\varepsilon} = \frac{X_1\sqrt{D_1} - \sqrt{-D_2}}{2}. \tag{6}$$

If $Z_1 > 1$, $2^\beta \parallel D_2 - (-1)^{(D_2-1)/2}$ *and* (1) *has a solution* (x, n) *with* $(x, n) \neq (X_1, Z_1)$, *then*

$$n = Z_1 t, \quad \frac{\varepsilon^t - \overline{\varepsilon}^t}{\varepsilon - \overline{\varepsilon}} = (-1)^{\frac{t-1}{2} \cdot \frac{D_2+1}{2}}, \tag{7}$$

where $t = 2^\alpha t_1 + 1$, $t_1 \in \mathbb{N}$, $2 \nmid t_1$, $\alpha = Z_1 - \beta + 1$.

Proof. By the proof of Lemma 11, we have $n = Z_1 t$ and

$$\frac{\varepsilon^t - \overline{\varepsilon}^t}{\varepsilon - \overline{\varepsilon}} = \lambda\lambda', \tag{8}$$

where $t \in \mathbb{N}$, $2 \nmid t$ and $t > 1$. By Lemma 1, we get

$$\lambda\lambda' = \sum_{i=0}^{(t-1)/2} \begin{bmatrix} t \\ i \end{bmatrix} (-D_2)^{\frac{t-1}{2} - i} 2^{Z_1 i} \equiv (-D_2)^{\frac{t-1}{2}} \pmod{2^{Z_1}},$$

whence we obtain

$$\frac{\varepsilon^t - \overline{\varepsilon}^t}{\varepsilon - \overline{\varepsilon}} = \sum_{i=0}^{(t-1)/2} \begin{bmatrix} t \\ i \end{bmatrix} (-D_2)^{\frac{t-1}{2} - i} 2^{Z_1 i} = (-1)^{\frac{t-1}{2} \cdot \frac{D_2+1}{2}} \tag{9}$$

since $Z_1 > 1$ and $D_2 - (-1)^{(D_2-1)/2} \equiv 0 \pmod 4$. If $t = 2^\alpha t_1 + 1$, $t_1 \in \mathbb{N}$ and $2 \nmid t_1$, then

$$(-D_2)^{\frac{t-1}{2}} - (-1)^{\frac{t-1}{2} \cdot \frac{D_2+1}{2}} \equiv 2^{\alpha+\beta-1} \pmod{2^{\alpha+\beta}}. \tag{10}$$

By (9) and (10), we get $\alpha = Z_1 - \beta + 1$. ∎

LEMMA 13. *If* $Z_1 > 1$ *and* (7) *holds for some* $t \in \mathbb{N}$ *with* $t > 1$ *and* $2 \nmid t$, *then* t *is an odd prime.*

Proof. Suppose that t is not a prime. Then t has an odd prime factor p with $p < t$. If $t = 2^{\alpha} t_1 + 1$, $p = 2^{\alpha'} t_2 + 1$ and $t/p = 2^{\alpha''} t_3 + 1$, where $t_1, t_2, t_3 \in \mathbb{N}$ with $2 \nmid t_1 t_2 t_3$, then

$$\alpha \begin{cases} = \min(\alpha', \alpha'') & \text{if } \alpha' \neq \alpha'', \\ > \alpha' & \text{if } \alpha' = \alpha''. \end{cases} \tag{11}$$

For any $m \in \mathbb{Z}$ with $m \geq 0$, let $Y_m = (\varepsilon^m - \overline{\varepsilon}^m)/(\varepsilon - \overline{\varepsilon})$. By Lemma 1, we have $Y_p, Y_{t/p} \in \mathbb{Z}$. If (7) holds, then

$$\begin{aligned} (-1)^{\frac{t-1}{2} \cdot \frac{D_2+1}{2}} &= \frac{\varepsilon^p - \overline{\varepsilon}^p}{\varepsilon - \overline{\varepsilon}} \cdot \frac{(\varepsilon^p)^{t/p} - (\overline{\varepsilon}^p)^{t/p}}{\varepsilon^p - \overline{\varepsilon}^p} \\ &= Y_p \sum_{j=0}^{(t/p-1)/2} \begin{bmatrix} t/p \\ j \end{bmatrix} (-D_2 Y_p^2)^{\frac{t/p-1}{2} - j} 2^{Z_1 p j} . \end{aligned}$$

This implies that $Y_p = \pm 1$ and $(|(\varepsilon^p + \overline{\varepsilon}^p)/(\varepsilon + \overline{\varepsilon})|, pZ_1)$ is a solution of (1). Therefore, by the proof of Lemma 12, we have $\alpha = \alpha' = \alpha'' = Z_1 - \beta + 1$, which contradicts (11). Thus t is an odd prime. ∎

LEMMA 14. *If* (7) *holds for some* $t \in \mathbb{N}$, *then* $t < 8.5 \cdot 10^6$.

Proof. For any complex number z, we have either $|e^z - 1| > 1/2$ or $|e^z - 1| \geq |z - k\pi\sqrt{-1}|/2$ for some $k \in \mathbb{Z}$. Hence

$$\operatorname{Log} |\varepsilon^t - \overline{\varepsilon}^t| \geq t \operatorname{Log} |\varepsilon| + \operatorname{Log} \left| t \log \frac{\overline{\varepsilon}}{\varepsilon} - k \log(-1) \right| - \operatorname{Log} 2 , \tag{12}$$

where $k \in \mathbb{Z}$ with $|k| \leq t$. Since

$$D_1 X_1^2 + D_2 = 2^{Z_1+2} , \tag{13}$$

we see from (6) that $\overline{\varepsilon}/\varepsilon$ satisfies

$$\begin{gathered} 2^{Z_1} \left(\frac{\overline{\varepsilon}}{\varepsilon} \right)^2 - \frac{1}{2}(D_1 X_1^2 - D_2) \frac{\overline{\varepsilon}}{\varepsilon} + 2^{Z_1} = 0 , \\ \gcd\left(2^{Z_1}, \frac{D_1 X_1^2 - D_2}{2} \right) = 1 . \end{gathered} \tag{14}$$

This implies that $\overline{\varepsilon}/\varepsilon$ is not a root of unity. Therefore, $\Lambda = t \log(\overline{\varepsilon}/\varepsilon) - k \log(-1) \neq 0$. From (13) and (14), $h(\overline{\varepsilon}/\varepsilon) = \operatorname{Log} 2^{Z_1/2}$ and the degree of $\mathbb{Q}(\overline{\varepsilon}/\varepsilon)$ is equal to 2. By Lemma 7, we have

$$|\Lambda| > \exp(-21590(\operatorname{Log} 2^{Z_1/2+1})(1 + \operatorname{Log} t + \operatorname{Log} \operatorname{Log} 2t)^2) .$$

Substituting this into (12) gives

$$\begin{aligned} &\operatorname{Log} |\varepsilon^t - \overline{\varepsilon}^t| \\ &\quad > t \operatorname{Log} |\varepsilon| - 21590(\operatorname{Log} 2^{Z_1/2+1})(1 + \operatorname{Log} t + \operatorname{Log} \operatorname{Log} 2t)^2 - \operatorname{Log} 2 . \end{aligned} \tag{15}$$

Notice that $|\varepsilon| = 2^{Z_1/2}$ and $|\varepsilon - \overline{\varepsilon}| = \sqrt{D_2} < 2^{(Z_1+2)/2}$. If (7) holds, then from (15) we get

$$\operatorname{Log} 2^{(Z_1+2)/2+1} + 21590(\operatorname{Log} 2^{Z_1/2+1})(1+\operatorname{Log} t+\operatorname{Log}\operatorname{Log} 2t)^2 > t \operatorname{Log} 2^{Z_1/2},$$

whence we obtain $t < 8.5 \cdot 10^6$. ■

4. Proofs

Assertion 1. $N(5,3) = 2$.

Proof. Since $5+3 = 2^3$, we see that $(1,1,1)$ is the least solution of the equation

$$5X^2 + 3Y^2 = 2^{Z+2}, \quad \gcd(X,Y) = 1, \ Z > 0.$$

By Lemma 5, if (x,n) is a solution of the equation

$$(16) \qquad 5x^2 + 3 = 2^{n+2}, \quad x > 0, \ n > 0,$$

with $(x,n) \neq (1,1)$, then there exist some $t \in \mathbb{N}$ such that

$$(17) \quad n = t, \quad \frac{x\sqrt{5}+\sqrt{-3}}{2} = \lambda\left(\frac{\sqrt{5}+\lambda'\sqrt{-3}}{2}\right)^t, \quad \lambda, \lambda' \in \{-1,1\}, \ t > 1, \ 2 \nmid t.$$

From (17), we get

$$(18) \qquad \pm 2^{t-1} = (-3)^{\frac{t-1}{2}} + \sum_{i=1}^{(t-1)/2} \binom{t}{2i} 5^i (-3)^{\frac{t-1}{2}-i}.$$

Since $2^2 \equiv 3^2 \equiv -1 \pmod 5$, we find from (18) that $t \equiv 1 \pmod 4$ and

$$(19) \qquad (-1)^{\frac{t-1}{4}} 4^{\frac{t-1}{2}} - 3^{\frac{t-1}{2}} = \sum_{i=1}^{(t-1)/2} \binom{t}{2i} 5^i (-3)^{\frac{t-1}{2}-i}.$$

Let $t = 2^\alpha 5^\beta t_1 + 1$, where $\alpha, t_1 \in \mathbb{N}$, $\beta \in \mathbb{Z}$, $\beta \ge 0$, $\gcd(10, t_1) = 1$. Notice that

$$(20) \qquad 5^{\beta+2} \parallel (-1)^{(t-1)/4} 4^{(t-1)/2} - 3^{(t-1)/2}.$$

If $\beta > 0$, then

$$5^{\beta+1} \,\Big\|\, \binom{t}{2} 5, \qquad 5^{\beta+1} \,\Big\|\, \sum_{i=1}^{(t-1)/2} \binom{t}{2i} 5^i (-3)^{\frac{t-1}{2}-i}$$

by Lemma 2. Hence (19) is impossible. If $\beta = 0$, then from (19) and (20) we get $5 \mid t$, since $3^2 + 4^2 = 5^2$. Let $t = 5^r t'$, where $r, t' \in \mathbb{N}$ with $\gcd(10, t') = 1$.

By Lemma 2, we have

$$5^{r+1} \,\Big\|\, \sum_{i=1}^{(t-1)/2} \binom{t}{2i} 5^i (-3)^{\frac{t-1}{2}-i} .$$

Therefore, $r = 1$ by (19) and (20). On the other hand, if $t' > 1$, then

$$2^{t'-1} = \sum_{j=0}^{(t'-1)/2} \binom{t'}{2j} 5^j (-3)^{\frac{t'-1}{2}-j}$$

by (17). By much the same argument as above, we can prove that $5 \mid t'$, a contradiction. Thus $t' = 1$ and $t = 5$. It follows from (17) that (16) has only one solution $(x, n) = (5, 5)$ with $(x, n) \neq (1, 1)$. ∎

Assertion 2. *If*

$$\begin{aligned}(D_1, D_2) = {} & (3,13),\ (5,11),\ (7,25),\ (9,23),\ (1,23),\ (15,49),\ (17,47),\\ & (31,97),\ (33,95),\ (63,193),\ (7,193),\ (65,191),\ (127,385),\\ & (129,383),\ (255,769),\ (257,767),\ (511,1537),\ (513,1535),\\ & (57,1535),\ (1023,3073),\ (1025,3071),\ (41,3071),\ (3,29),\\ & (21,11),\ (13,3),\end{aligned}$$

then $N(D_1, D_2) = 2$.

Proof. For the case $(D_1, D_2) = (3, 13)$, (1) has two solutions $(x, n) = (1, 2)$ and $(9, 6)$. Let $\varrho = (\sqrt{3} + \sqrt{-13})/2$, $\overline{\varrho} = (\sqrt{3} - \sqrt{-13})/2$, and let $k_m = (\varrho^{2m+1} - \overline{\varrho}^{2m+1})/(\varrho - \overline{\varrho})$ for any $m \in \mathbb{Z}$ with $m \geq 0$. Then $K = \{k_m\}_{m=0}^{\infty}$ is an integer sequence satisfying

$$(21) \qquad k_0 = 1\,, \quad k_1 = -1\,, \quad k_{m+2} = -5k_{m+1} - 16k_m\,, \quad m \geq 0\,.$$

By Lemma 12, if $N(3, 13) > 2$, then there exist some $t \in \mathbb{N}$ such that

$$(22) \qquad k_{(t-1)/2} = -1\,, \quad t > 3\,,\ 2 \nmid t\,.$$

Let p be an odd prime, and let $k_m^{(p)} \equiv k_m \pmod{p}$ with $0 \leq k_m^{(p)} < p$. By (21), we find that if $p = 17, 19, 23, 29, 37$ and 47, then $\{k_m^{(p)}\}_{m=0}^{\infty}$ are periodic sequences with periods $l = 36, 180, 132, 35, 342$ and 23 respectively. Moreover, $k_m^{(p)} \equiv -1 \pmod{p}$ if and only if $m \equiv 1 \pmod{l}$. This implies that if (22) holds, then $(t-1)/2 \equiv 1 \pmod{L}$, where $L = \mathrm{lcm}(36, 180, 132, 35, 342, 23) = 5782510 > 5 \cdot 10^6$. So we have $t > 10^7$. This is impossible by Lemma 14. Thus $N(3, 13) = 2$.

Using the same method, we can prove the other cases. The details of the proof will be given in: D.-Y. Jin and M.-H. Le, *Application of computers to number theory research I*, to appear. ∎

Assertion 3. *Let $\varepsilon, \overline{\varepsilon}$ be defined as in* (6). *If $Z_1 > 1$ and there exist $t_1, t_2 \in \mathbb{N}$ such that $t_2 > t_1 > 1$, $2 \nmid t_1 t_2$ and*

$$\left|\frac{\varepsilon^{t_l} - \overline{\varepsilon}^{t_l}}{\varepsilon - \overline{\varepsilon}}\right| = 1, \quad l = 1, 2, \tag{23}$$

then $t_2 > 2^{Z_1(t_1-1)+1}$.

Proof. If (23) holds, then (1) has two solutions. By Lemma 12, we have $t_1 \equiv t_2 \pmod 4$ and

$$\frac{\varepsilon^{t_l} - \overline{\varepsilon}^{t_l}}{\varepsilon - \overline{\varepsilon}} = (-1)^{\frac{t_1-1}{2}\cdot\frac{D_2+1}{2}}, \quad l = 1, 2. \tag{24}$$

For any $m \in \mathbb{Z}$ with $m \ge 0$, let $Y_m = (\varepsilon^m - \overline{\varepsilon}^m)/(\varepsilon - \overline{\varepsilon})$. Then

$$Y_0 = 0, \quad Y_1 = 1, \quad Y_{m+2} = X_1\sqrt{D_1}Y_{m+1} - 2^{Z_1}Y_m, \quad m \ge 0, \tag{25}$$

by (13). On applying Lemma 6 to (25), we get

$$Y_m = F(m-1), \quad m \ge 0, \tag{26}$$

where

$$F(m) = \begin{cases} 0 & \text{if } m < 0, \\ 1 & \text{if } m = 0, \\ \displaystyle\sum_{\substack{r_1+2r_2=m \\ r_1, r_2 \ge 0}} \binom{r_1+r_2}{r_1}(X_1\sqrt{D_1})^{r_1}(-2^{Z_1})^{r_2} & \text{if } m > 0. \end{cases} \tag{27}$$

Hence, from (24), (26) and (27), we get

$$\begin{aligned}(-1)^{\frac{t_1-1}{2}\cdot\frac{D_2+1}{2}} &= Y_{t_l} = F(t_l - 1) \\ &= (D_1X_1^2)^{\frac{t_l-1}{2}} + \sum_{i=1}^{(t_l-1)/2}\binom{t_l-i-1}{i}(D_1X_1^2)^{\frac{t_l-1}{2}-i}(-2^{Z_1})^i\end{aligned}$$

for $l = 1, 2$. It follows that

$$(-1)^{\frac{t_1-1}{2}\cdot\frac{D_2+1}{2}}((D_1X_1^2)^{(t_2-t_1)/2} - 1) + I_1 + I_2 + I_3 = 0, \tag{28}$$

where

$$I_1 = \sum_{i=1}^{(t_1-1)/2}\left(\binom{t_2-i-1}{i} - \binom{t_1-i-1}{i}\right)(D_1X_1^2)^{\frac{t_2-1}{2}-i}(-2^{Z_1})^i,$$

$$I_2 = \sum_{i=(t_1+1)/2}^{t_1-1}\binom{t_2-i-1}{i}(D_1X_1^2)^{\frac{t_2-1}{2}-i}(-2^{Z_1})^i,$$

$$I_3 = \sum_{i=t_1}^{(t_2-1)/2}\binom{t_2-i-1}{i}(D_1X_1^2)^{\frac{t_2-1}{2}-i}(-2^{Z_1})^i.$$

Let $2^\alpha \parallel t_1 - 1$, $2^\beta \parallel D_2 - (-1)^{(D_2-1)/2}$ and $2^s \parallel t_2 - t_1$. Recall that $\beta = Z_1 - \alpha + 1 < Z_1 + 2$ by Lemma 12. We have

$$2^\beta \parallel D_1X_1^2 - (-1)^{(D_2+1)/2} = -(D_2 - (-1)^{(D_2-1)/2}) + 2^{Z_1+2}.$$

Hence

$$2^{\beta+s-1} \parallel (D_1X_1^2)^{(t_2-t_1)/2} - 1.$$

This implies that

$$(29) \qquad 2^{Z_1-\alpha+s} \parallel (D_1X_1^2)^{(t_2-t_1)/2} - 1.$$

On the other hand, by Lemmas 3 and 4, we have $I_1 \equiv 0 \pmod{2^{Z_1+s}}$ and $I_2 \equiv 0 \pmod{2^{Z_1+s}}$ respectively. Therefore, by (29), if (28) holds, then

$$(30) \qquad 2^{Z_1-\alpha+s} \parallel I_3.$$

Since $I_3 \equiv 0 \pmod{2^{Z_1t_1}}$, from (30) we get $Z_1t_1 \le Z_1 - \alpha + s$. Hence $t_2 - t_1 \ge 2^s \ge 2^{Z_1(t_1-1)+1}$. ∎

Proof of Theorem 1. By Assertion 1, the theorem holds for $Z_1 = 1$. From now on we assume that $Z_1 > 1$.

By Lemmas 11–13, if $N(D_1, D_2) > 2$, then (24) holds for some odd primes t_1, t_2 with $t_2 > t_1$. Further, by Lemma 14 and Assertion 3, we have

$$(31) \qquad 8.5 \cdot 10^6 > t_2 > 2^{Z_1(t_1-1)+1}.$$

When $t_1 = 3$, from (9) we get $D_2 - (-1)^{(D_2-1)/2} = 3 \cdot 2^{Z_1}$. This implies that the pair (D_1, D_2) is exceptional. From (31), we get $Z_1 \le 10$. By Assertion 2, $N(D_1, D_2) = 2$.

When $t_1 = 5$, we have $(D_2 - 5 \cdot 2^{Z_1-1})^2 - 5 \cdot 2^{2(Z_1-1)} = 1$. Since $L_m^2 - 5F_m^2 = (-1)^m 4$ gives all solutions of the equation $u^2 - 5v^2 = \pm 4$, 2^{Z_1} is a Fibonacci number. Since $Z_1 > 1$, by Lemma 8, we find that $Z_1 = 3$ and $(D_1, D_2) = (3, 29)$ or $(21, 11)$. By Assertion 2, $N(D_1, D_2) = 2$.

When $t_1 = 7$, we have

$$(D_2 - 2^{Z_1+1})^3 + 2^{Z_1}(D_2 - 2^{Z_1+1})^2 - 2^{2Z_1+1}(D_2 - 2^{Z_1+1}) - 2^{3Z_1} = \pm 1.$$

By Lemma 9, we find that $Z_1 = 2$ and $(D_1, D_2) = (13, 3)$. Then $N(D_1, D_2) = 2$ by Assertion 2.

When $t_1 = 11$, we see from (31) that $Z_1 = 2$. Notice that (1) has no solution (x, n) with $n = 22$ for $(D_1, D_2) = (3, 13)$, $(5, 11)$, $(7, 9)$, $(11, 5)$ and $(13, 3)$. Hence (24) is impossible.

When $t_1 \ge 13$, (31) is impossible for $Z_1 > 1$. ∎

Proof of Theorem 2. According to the proof of Theorem 1, if $\max(D_1, D_2) > 29$, (D_1, D_2) is not exceptional and $N(D_1, D_2) > 1$, then (9) holds for some odd prime t with

$$(32) \qquad 8.5 \cdot 10^6 > t > 7.$$

Let

$$f(X,Y)=\sum_{i=0}^{(t-1)/2}\begin{bmatrix}t\\ i\end{bmatrix}X^{\frac{t-1}{2}-i}Y^i\,.$$

Notice that

$$\begin{bmatrix}t\\ 0\end{bmatrix}=1\,,\quad \begin{bmatrix}t\\ (t-1)/2\end{bmatrix}=t\,,\quad \begin{bmatrix}t\\ j\end{bmatrix}\equiv 0 \pmod t\,,\quad j=1,\ldots,(t-1)/2$$

for any odd prime t. By Eisenstein's theorem, $f(X,Y)$ is a homogeneous polynomial of degree $(t-1)/2$ with integer coefficients which is irreducible in $\mathbb{Q}$. From (9) we get

$$f(-D_2,2^{Z_1})=\pm 1\,. \tag{33}$$

Since

$$\max_{i=0,\ldots,(t-1)/2}\begin{bmatrix}t\\ i\end{bmatrix}<2^{t-1}\,,$$

if (33) holds for $t\ge 7$, then

$$\frac{1}{4}\max(D_1,D_2)<\max(D_2,2^{Z_1})<\exp\left(\left(2^{t-1}\left(\frac{t-1}{2}\right)\right)^{(5(t-1))^5}\right) \tag{34}$$

by Lemma 10. The combination of (32) and (34) yields $\max(D_1,D_2)<\exp\exp\exp 105$. ■

Acknowledgements. The author would like to thank the referee for his valuable suggestions.

References

[1] R. Apéry, *Sur une équation diophantienne*, C. R. Acad. Sci. Paris Sér. A 251 (1960), 1263–1264.

[2] A. Baker, *Contribution to the theory of diophantine equations I: On the representation of integers by binary forms*, Philos. Trans. Roy. Soc. London Ser. A 263 (1967), 273–297.

[3] V. I. Baulin, *On an indeterminate equation of the third degree with least positive discriminant*, Tul'sk. Gos. Ped. Inst. Uchen. Zap. Fiz.-Mat. Nauk Vyp. 7 (1960), 138–170 (in Russian).

[4] E. Bender and N. Herzberg, *Some diophantine equations related to the quadratic form* ax^2+by^2, in: Studies in Algebra and Number Theory, G.-C. Rota (ed.), Adv. in Math. Suppl. Stud. 6, Academic Press, San Diego 1979, 219–272.

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

[6] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. 39 (1964), 537–540.

[7] K. Győry and Z. Z. Papp, *Norm form equations and explicit lower bounds for linear forms with algebraic coefficients*, in: Studies in Pure Mathematics, Akadémiai Kiadó, Budapest 1983, 245–257.

[8] M.-H. Le, *The divisibility of the class number for a class of imaginary quadratic fields*, Kexue Tongbao (Chinese) 32 (1987), 724–727 (in Chinese).
[9] —, *On the number of solutions of the generalized Ramanujan–Nagell equation* $x^2 - D = 2^{n+2}$, Acta Arith. 60 (1991), 149–167.
[10] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.
[11] M. Mignotte and M. Waldschmidt, *Linear forms in two logarithms and Schneider's method III*, Ann. Fac. Sci. Toulouse 97 (1989), 43–75.
[12] T. Nagell, *The diophantine equation* $x^2 + 7 = 2^n$, Ark. Mat. 4 (1960), 185–187.

RESEARCH DEPARTMENT
CHANGSHA RAILWAY INSTITUTE
CHANGSHA, HUNAN
P. R. CHINA

Received on 23.1.1992
and in revised form on 28.10.1992 (2216)