Prenons $I_0 = I = R_K$ et notons $2L$ la longueur supposée paire du cycle d'idéaux réduits de I_0. Puisque $(I_L)^\sigma = (I^\sigma)_{-L} = I_{-L} = I_L$, I_L est réduit, invariant et distinct de I. L'idéal $(\sqrt{d})$ n'étant pas réduit (où $d \in R_k$ est libre de carré dans R_k et tel que $K = k(\sqrt{d})$), nous avons donc au moins quatre idéaux primitifs ramifiés principaux dans K, à savoir R_K, $(\sqrt{d})$, I_L et l'idéal J dual de ce dernier (défini par J est primitif et $(\sqrt{d})I_L = (m)J$, $m \in R_k$). Le sous-groupe $H_{\mathrm{reg}}(K)$ des classes régulières est donc d'ordre au plus 2^{t-2}. Le théorème 1 donne le résultat.

Ce résultat n'est que partiel et nous ne disposons pas encore de sa réciproque (la difficulté résultant de ce que contrairement au cas des corps quadratiques réels, ici les cycles d'idéaux réduits n'ont plus nécessairement même parité de longueur, et il n'est plus vrai qu'un idéal primitif ramifié ou son idéal dual soit réduit). Nous aborderons ailleurs de façon plus détaillée ces considérations.

Bibliographie

[1] H. Amara, *Groupe des classes et unité fondamentale des extensions quadratiques relatives à un corps quadratique imaginaire principal*, Pacific J. Math. 96 (1) (1981), 1–12.

[2] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Thompson, Washington, DC, 1967.

[3] C. Chevalley, *Sur la théorie du corps de classes*, J. Fac. Sci. Tokyo, Sec. 1, 1–2 (1933), 365–476. Plus spécialement, 402–406.

[4] H. Cohn, *Second Course in Number Theory*, Wiley, New York 1962.

[5] — *A Classical Invitation to Algebraic Numbers and Class Fields*, Universitext, Springer, 1978.

[6] Nguyen Quang Do Thong, *Unités de norme −1 d'un corps quadratique réel*, Séminaire Delange–Pisot–Poitou 1975/76, exposé G6.

[7] F. Gerth, *The 4-class ranks of quadratic extensions of certain imaginary quadratic fields*, Illinois J. Math. 33 (1) (1989), 132–142.

[8] G. Gras, *Etude du l-groupe des classes des extensions cycliques de degré l*, Séminaire Delange–Pisot–Poitou 1971/72, exposé 20.

[9] — *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l*, Ann. Inst. Fourier (Grenoble) 23 (3) (1973), 1–48; ibid. 23 (4) (1973), 1–44.

[10] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Graduate Texts in Math. 77, Springer, 1981.

[11] S. Louboutin, *Nombre de classes d'idéaux des extensions quadratiques du corps de Gauss*, preprint.

[12] — *Le groupe des classes ambiges (au sens strict)*, Séminaire de Théorie des Nombres, Paris 1987–88, Progr. Math. 81, Birkhäuser, Boston 1990, 147–153.

UNIVERSITÉ DE CAEN
U.F.R. SCIENCES
DÉPARTEMENT DE MATHÉMATIQUES
Esplanade de la Paix
14032 Caen Cedex, France

Reçu le 4.1.1990
et révisé le 3.4.1990 (1997)

ACTA ARITHMETICA
LVIII.3 (1991)

On the generalized Ramanujan–Nagell equation $x^2 - D = p^n$

by

MAOHUA LE (Changsha, China)

1. Introduction. Let Z, N, Q be the sets of integers, positive integers and rational numbers respectively. Let $D \in N$, and let p be an odd prime with $p \nmid D$. We denote the number of positive solutions(1) (x, n) of the generalized Ramanujan–Nagell equation

$$x^2 - D = p^n \tag{1}$$

by $N(D, p)$. In [1], Beukers proved that $N(D, p) \leqslant 4$. Simultaneously, he suspected that $N(D, p) \leqslant 3$. In this paper, we prove the following results.

THEOREM 1. *If* $\max(D, p) \geqslant 10^{100}$ *and*

$$p = \begin{cases} 3, \\ 4a^2+1; \end{cases} \qquad D = \begin{cases} \left(\dfrac{3^m+1}{4}\right)^2 - 3^m, & 2 \nmid m, \\ \left(\dfrac{p^m-1}{4a}\right)^2 - p^m, \end{cases} \qquad a, m \in N,\ m > 1, \tag{2}$$

then $N(D, p) = 3$.

THEOREM 2. *If* $\max(D, p) \geqslant 10^{240}$, *then* $N(D, p) \leqslant 3$.

2. Lemmas. By the proof of Theorem 2 of [1], we see that if D is a square, then $N(D, p) \leqslant 1$. From now on we assume that D is not a square.

LEMMA 1 ([1], Lemma 5). *Let* (x, n), (x', n'), (x'', n'') *be three positive solutions of* (1) *with* $n < n' < n''$. *Then* $n'' \geqslant 2n' + \max(3, n, 2(n'-1)/3)$ *except when* D, p *satisfy* (2) *and* $(n, n', n'') = (1, m, 2m+1)$. ∎

LEMMA 2 ([1], Theorem 1). *Let* (x, n), (x', n') *be two positive solutions of* (1) *with* $n < n'$. *Then* $p^n \leqslant \max(2 \cdot 10^6, 600D^2)$. ∎

LEMMA 3 ([3], Lemma 1). *Let* $u_1 + v_1\sqrt{D}$ *be the fundamental solution of the equation*

$$u^2 - Dv^2 = 1. \tag{3}$$

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

If the equation

$$(4)\qquad X^2-DY^2=p^Z,\quad \gcd(X,Y)=1,\quad Z>0$$

has solutions (X, Y, Z), *then it has a unique positive solution* (X_1, Y_1, Z_1) *which satisfies* $Z_1 \leqslant Z$ *and*

$$(5)\qquad 1<\frac{X_1+Y_1\sqrt{D}}{X_1-Y_1\sqrt{D}}<(u_1+v_1\sqrt{D})^2,$$

where Z *runs over all solutions of* (4). *Such* (X_1, Y_1, Z_1) *is called the least solution of* (4). *Then every solution* (X, Y, Z) *of* (4) *can be expressed as*

$$Z=Z_1t,\quad X+Y\sqrt{D}=(X_1\pm Y_1\sqrt{D})^t(u+v\sqrt{D}),$$

where $t\in \boldsymbol{N}$, (u, v) *is a solution of* (3). ∎

LEMMA 4. *Under the definitions in Lemma 3, let* $\varrho=u_1+v_1\sqrt{D}$, $\bar{\varrho}=u_1-v_1\sqrt{D}$, $\varepsilon=X_1+Y_1\sqrt{D}$, $\bar{\varepsilon}=X_1-Y_1\sqrt{D}$. *If* (x, n) *is a positive solution of* (1), *then we have*

$$(6)\qquad n=Z_1t,\quad x\pm\sqrt{D}=\varepsilon^t\bar{\varrho}^s,\quad t\in\boldsymbol{N},\ s\in\boldsymbol{Z},\ 0\leqslant s\leqslant t,\ \gcd(s,t)=1.$$

Proof. Clearly, if (x, n) is a positive solution of (1), then $(x, 1, n)$ is a solution of (4). By Lemma 3, we have

$$n=Z_1t,\quad x\pm\sqrt{D}=\varepsilon^t\bar{\varrho}^s,\quad t\in\boldsymbol{N},\ s\in\boldsymbol{Z}.$$

If $s<0$, then there exist positive integers a, b, c, d such that

$$\varepsilon^t=a+b\sqrt{D}\quad\text{and}\quad \bar{\varrho}^s=c+d\sqrt{D}.$$

It follows that $\pm 1=ad+bc>1$, a contradiction. Hence $s\geqslant 0$. Moreover, we see from Lemma 3 of [1] that $\gcd(s, t)=1$. If $x+\sqrt{D}=\varepsilon^t\bar{\varrho}^s$, then from (5) and

$$1<\frac{x+\sqrt{D}}{x-\sqrt{D}}=\left(\frac{\varepsilon}{\bar{\varepsilon}}\right)^t\bar{\varrho}^{2s}<\varrho^{2t-2s},$$

we obtain $s<t$. If $x-\sqrt{D}=\varepsilon^t\bar{\varrho}^s$, since $\varrho>2\sqrt{D}$ and

$$\frac{x}{\sqrt{D}}=\left(1+\frac{p^n}{D}\right)^{1/2}>\begin{Bmatrix}\sqrt{2}, & p^n>D\\ 1+\dfrac{p^n}{2D}>1+\dfrac{1}{D}, & p^n<D\end{Bmatrix}>\frac{\varrho^2+1}{\varrho^2-1},$$

we obtain

$$\frac{x+\sqrt{D}}{x-\sqrt{D}}=\left(\frac{\varepsilon}{\bar{\varepsilon}}\right)^{-t}\varrho^{2s}<\varrho^2,$$

and therefore $s<t+1$ by (5). Thus $s\leqslant t$. The lemma is proved. ∎

LEMMA 5. *Let* (x, n), (x', n') *be two positive solutions of* (1) *with* $p^n<p^{n'}<D^2$. *Then* $\log\varrho<5(\log D)^2$.

Proof. By Lemma 4, we have $n=Z_1t$, $n'=Z_1t'$, $x\pm\sqrt{D}=\varepsilon^t\bar{\varrho}^s$, $x'\pm\sqrt{D}=\varepsilon^{t'}\bar{\varrho}^{s'}$, where s, t, s', t' are integers satisfying $1\leqslant t<t'$ and $\gcd(s,t)=\gcd(s',t')=1$. It follows that $st'\neq s't$. If $x+\sqrt{D}=\varepsilon^t\bar{\varrho}^s$ and $x'+\sqrt{D}=\varepsilon^{t'}\bar{\varrho}^{s'}$, then

$$|t'\log(x+\sqrt{D})-t\log(x'+\sqrt{D})|=|s't-st'|\log\varrho\geqslant\log\varrho.$$

Since $p^n<p^{n'}<D^2$, we find

$$(7)\qquad \tfrac{5}{2}(\log D)^2>\frac{\log D^2}{\log p^{Z_1}}\log(1+\sqrt{D})^2$$
$$>\frac{\log p^{n'}}{\log p^{Z_1}}\log(p^{n'/2}+2\sqrt{D})>\frac{\log p^{n'}}{\log p^{Z_1}}\log(x'+\sqrt{D})$$
$$=t'\log(x'+\sqrt{D})>\max(t'\log(x+\sqrt{D}),\ t\log(x'+\sqrt{D}))$$
$$>|t'\log(x+\sqrt{D})-t\log(x'+\sqrt{D})|\geqslant\log\varrho.$$

The lemma holds for this case.

If $x+\sqrt{D}=\varepsilon^t\bar{\varrho}^s$ and $x'-\sqrt{D}=\varepsilon^{t'}\bar{\varrho}^{s'}$, then

$$|t'\log(x+\sqrt{D})-t\log(x'-\sqrt{D})|$$
$$=|t'\log(x+\sqrt{D})+t\log(x'+\sqrt{D})-t\log p^{n'}|\geqslant\log\varrho.$$

Since

$$t\log p^{n'}=\log p^n\cdot\log p^{n'}/\log p^{Z_1}<(\log p^{n'})^2<4(\log D)^2$$

and

$$t'\log(x+\sqrt{D})+t\log(x'+\sqrt{D})<2t'\log(x'+\sqrt{D})<5(\log D)^2$$

by (7), we get

$$\log\varrho<5(\log D)^2$$

immediately.

By the same way, the lemma holds for other cases. ∎

LEMMA 6 ([2], Theorem 10.7.2). *For any positive real number* α, *if* a/b *is an irreducible fraction satisfying* $|a/b-\alpha|<1/2b^2$, *then* a/b *is a convergent of* α. ∎

LEMMA 7. *Let* (x, n) *be a positive solution of* (1) *with* $p^n>D^{20/17}$, *and let* s, t, ε, $\bar{\varepsilon}$, ϱ, $\bar{\varrho}$ *be defined as in Lemma* 4. *Let* $\alpha=(\log(\varepsilon/\bar{\varepsilon}))/\log\varrho$. *If* $\gcd(2s, t)=\delta$, $2s=\delta a$, $t=\delta b$ *and* $D>10^{30}$, *then* a/b *is a convergent of* α.

Proof. Since $p^n > D^{20/17}$, we see from (6) that

$$(8)\qquad \left|\frac{a}{b}-\alpha\right| = \left|\frac{2s}{t}-\frac{\log(\varepsilon/\bar{\varepsilon})}{\log\varrho}\right| = \frac{1}{t\log\varrho}\log\frac{x+\sqrt{D}}{x-\sqrt{D}}$$

$$= \frac{2\sqrt{D}}{tx\log\varrho}\sum_{i=0}^{\infty}\frac{1}{2i+1}\left(\frac{D}{x^2}\right)^i < \frac{4\sqrt{D}}{tx\log\varrho}.$$

By Lemma 6, if a/b is not a convergent of α, then from (8) we get

$$(9)\qquad t > \frac{x\log\varrho}{8\sqrt{D}} = \frac{1}{8}\log\varrho\left(1+\frac{p^n}{D}\right)^{1/2}.$$

Let $r = \log p^n/\log D$. From (9),

$$(10)\qquad t > \tfrac{1}{8}\log\varrho(1+D^{r-1})^{1/2}.$$

Since $\varrho > 2\sqrt{D}$ and $t = \log p^n/\log p^{Z_1} < r\log D$, we see from (10) that $20r > (1+D^{r-1})^{1/2}$. This is impossible when $r > 20/17$ and $D > 10^{30}$. Hence the lemma. ■

Lemma 8. *Let p be an odd prime, and let $U_1+V_1\sqrt{p}$ be the fundamental solution of the equation*

$$(11)\qquad U^2-pV^2 = 1.$$

If $p \nmid V_1$ and (U, V) is a positive solution of (11) satisfying $p^r | V$ for some $r \in \mathbf{N}$, then $U+V\sqrt{p} = (U_1+V_1\sqrt{p})^{p^r t}$ for some $t \in \mathbf{N}$.

Proof. It is a well-known fact that $U+V\sqrt{p} = (U_1+V_1\sqrt{p})^l$ for some $l \in \mathbf{N}$. Then

$$(12)\qquad V = \sum_{i=0}^{[(l-1)/2]}\binom{l}{2i+1}p^i U_1^{l-2i-1}V_1^{2i+1}.$$

Since $p \nmid U_1V_1$, we see from (12) that if $p|V$ then $p|l$. If $p > 3$ and $p^\lambda \| l$, then

$$\binom{l}{2j+1}p^j = l\binom{l-1}{2j}\frac{p^j}{2j+1} \equiv 0 \pmod{p^{\lambda+1}}, \quad j \geqslant 1,$$

and hence $\lambda \geqslant r$ by (12). If $p = 3$ and $3^\lambda \| l$, then $U_1+V_1\sqrt{p} = 2+\sqrt{3}$,

$$\binom{l}{2j+1}3^j = l\binom{l-1}{2j}\frac{3^j}{2j+1} \equiv 0 \pmod{3^{\lambda+1}}, \quad j > 1,$$

and

$$\binom{l}{1}2^{l-1}+\binom{l}{3}2^{l-3}3 = 2^{l-4}l(8+(l-1)(l-2)) \not\equiv 0 \pmod{3^{\lambda+1}}.$$

So we have $\lambda \geqslant r$ by (12). The lemma is proved. ■

Let $d \in \mathbf{N}$ be non-square, and let $k \in \mathbf{Z}$ with $k \neq 0$ and $\gcd(k, d) = 1$.

Lemma 9 ([2], Theorem 10.8.2). *If $|k| < \sqrt{d}$ and (X, Y) is a positive solution of the equation*

$$(13)\qquad X^2-dY^2 = k, \quad \gcd(X, Y) = 1,$$

then X/Y is a convergent of $\sqrt{d}$. ■

Lemma 10 ([2], Theorem 11.4.1 and Formula 11.4.7). *For any fixed solution (X, Y) of (13), there exist unique integers α, β, l such that $\beta X-\alpha Y = 1$, $l = \alpha X-d\beta Y$, $0 < l \leqslant |k|$ and $X \equiv -lY \pmod{k}$. We call l the characteristic number of (X, Y), and denote it by $\langle X, Y\rangle$.* ■

Lemma 11 ([2], Theorem 11.4.2). *Let (X, Y), (X', Y') be solutions of equation (13). A necessary and sufficient condition for $\langle X, Y\rangle = \langle X', Y'\rangle$ is that $X'+Y'\sqrt{d} = (X+Y\sqrt{d})(U+V\sqrt{d})$ for some $U, V \in \mathbf{Z}$ with $U^2-dV^2 = 1$.* ■

Lemma 12. *If (x, n) is a positive solution of (1) with $2|n$, then $p^n < D^2/4$.*

Proof. If $2|n$, then we see from (1) that $x+p^{n/2} = D_1$ and $x-p^{n/2} = D_2$, where $D_1, D_2 \in \mathbf{N}$ with $D_1D_2 = D$. It follows that $2p^{n/2} = D_1-D_2 \leqslant D-1$. Hence the lemma. ■

Lemma 13. *Let (X_1, Y_1, Z_1) be the least solution of (4), and let $u_1+v_1\sqrt{D}$ be the fundamental solution of (13). Let $l_1, l_2 \in \mathbf{Z}$ with $l_1 \equiv -X_1 \pmod{D}$, $l_2 \equiv -X_1u_1 \pmod{D}$ and $0 < l_1, l_2 \leqslant D$. Let (x, n) be a positive solution of (1), and let $s, t, \varepsilon, \bar{\varepsilon}, \varrho, \bar{\varrho}$ be defined as in Lemma 4. If $2 \nmid n$, then $(x, p^{Z_1(t-1)/2})$ is a solution of the equation*

$$(14)\qquad X^2-p^{Z_1}Y^2 = D, \quad \gcd(X, Y) = 1,$$

which satisfies

$$\langle x, p^{Z_1(t-1)/2}\rangle = \begin{cases} l_1, & 2|s, \\ l_2, & 2\nmid s. \end{cases}$$

Proof. If $2 \nmid n$, then $2 \nmid Z_1t$ by (6). It follows that $(x, p^{Z_1(t-1)/2})$ is a solution of (14). Let $\varepsilon^t = A+B\sqrt{D}$, $\varrho^s = u+v\sqrt{D}$. Then A, B, u, v are integers satisfying $A \equiv X_1^t \pmod{D}$, $u \equiv u_1^s \pmod{D}$ and

$$(15)\qquad x = Au-DBv$$

by (6). Since $X_1^2 \equiv p^{Z_1} \pmod{D}$ and $u_1^2 \equiv 1 \pmod{D}$, we find from (15) that

$$(16)\qquad x \equiv Au \equiv X_1^t u_1^s \equiv \begin{cases} X_1p^{Z_1(t-1)/2} \pmod{D}, & 2|s, \\ X_1p^{Z_1(t-1)/2}u_1 \pmod{D}, & 2\nmid s. \end{cases}$$

By Lemma 10, we have

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

Therefore (16) yields the lemma. ■

LEMMA 14 ([4]). *Let $\beta, \alpha_1, \alpha_2$ be real algebraic numbers with degrees r_0, r_1, r_2 and heights H_0, H_1, H_2 respectively. Let $B = \max(H_0, e^{r_0})$ and $A_j = \max(H_j, |\alpha_j|)$ $(j = 1, 2)$. If $\Lambda = \beta \log \alpha_1 - \log \alpha_2 \neq 0$, then*

$$|\Lambda| > \exp(-5 \cdot 10^8 r^4 S_1 S_2 T^2),$$

where r is the degree of $\mathbf{Q}(\beta, \alpha_1, \alpha_2)$, $S_0 = r_0 + \log B$, $S_j = 1 + \log A_j/r_j$ $(j = 1, 2)$, $T = 4 + S_0/r_0 + \log r^2 S_1 S_2$. ∎

3. Proof of Theorem 1. In [1], Beukers showed that if D, p satisfy (2), then (1) has three positive solutions:

$$(x_1, n_1) = \begin{cases} \left(\frac{3^m-7}{4}, 1\right), & p = 3, \\ \left(\frac{p^m-1}{4a} - 2a, 1\right), & p \neq 3, \end{cases}$$

$$(17) \qquad (x_2, n_2) = \begin{cases} \left(\frac{3^m+1}{4}, m\right), & p = 3, \\ \left(\frac{p^m-1}{4a}, m\right), & p \neq 3, \end{cases}$$

$$(x_3, n_3) = \begin{cases} \left(2 \cdot 3^m - \frac{3^m+1}{4}, 2m+1\right), & p = 3, \\ \left(2a \cdot p^m + \frac{p^m-1}{4a}, 2m+1\right), & p \neq 3. \end{cases}$$

Now we suppose that $N(D, p) > 3$. By the proof of Theorem 2 of [1], equation (1) has a positive solution (x_4, n_4) with $n_4 > n_3 > n_2 > n_1$. By Lemma 1, we have $n_4 \geqslant 2n_3 + n_2 = 5m+2$, hence $p^{n_4} > D^2/4$ since $p^{2m-1} > 4D$ by (2). This implies $2 \nmid n_4$ by Lemma 12. Since $p^{n_1} = p < \sqrt{D}$ except when $(D, p, m) = (11, 5, 2)$, $x_1/1$ is a convergent of $\sqrt{D}$ by Lemma 9. Therefore, by the definition as in Lemma 3, then $(x_1, 1, 1)$ is the least solution of (4). Let $\varepsilon, \bar{\varepsilon}, \varrho, \bar{\varrho}$ be defined as in Lemma 4. Then we have

$$(18) \qquad x_i \pm \sqrt{D} = \varepsilon^{n_i} \bar{\varrho}^{s_i}, \quad i = 1, \ldots, 4,$$

where s_i $(i = 1, \ldots, 4)$ are integers satisfying

$$(19) \qquad 0 \leqslant s_i \leqslant n_i, \quad \gcd(s_i, n_i) = 1, \quad i = 1, \ldots, 4.$$

First we consider the case $2 \nmid m$. Then $(x_2, p^{(m-1)/2})$, (x_3, p^m) and $(x_4, p^{(n_4-1)/2})$ are solutions of the equation

$$(20) \qquad X^2 - pY^2 = D, \quad \gcd(X, Y) = 1.$$

By Lemma 10, we deduce from (17) that

$$\langle x_2, p^{(m-1)/2} \rangle - \langle x_3, p^m \rangle \equiv -\frac{x_2}{p^{(m-1)/2}} - \frac{x_3}{p^m}$$
$$= \left\{ \begin{array}{ll} \frac{1}{8 \cdot 3^m}(3^m+1)(3^m - 2 \cdot 3^{(m+1)/2} - 1), & p = 3 \\ \frac{1}{8a \cdot p^m}(p^m-1)(p^m - 2p^{(m+1)/2} + 1), & p \neq 3 \end{array} \right\} \not\equiv 0 \pmod{D},$$

and therefore $\langle x_2, p^{(m-1)/2} \rangle \neq \langle x_3, p^m \rangle$. By Lemma 13, we have either $\langle x_4, p^{(n_4-1)/2} \rangle = \langle x_2, p^{(m-1)/2} \rangle$ or $\langle x_4, p^{(n_4-1)/2} \rangle = \langle x_3, p^m \rangle$. Furthermore, by Lemma 11, we have

$$(21) \qquad x_4 + p^{(n_4-1)/2}\sqrt{p}$$
$$= \begin{cases} (x_2 + p^{(m-1)/2}\sqrt{p})(U + V\sqrt{p}), & \langle x_4, p^{(n_4-1)/2} \rangle = \langle x_2, p^{(m-1)/2} \rangle, \\ (x_3 + p^m\sqrt{p})(U + V\sqrt{p}), & \langle x_4, p^{(n_4-1)/2} \rangle = \langle x_3, p^m \rangle, \end{cases}$$

where (U, V) is a positive solution of (11). From (21),

$$(22) \qquad p^{(n_4-1)/2} = \begin{cases} x_2 V + p^{(m-1)/2} U, & \langle x_4, p^{(n_4-1)/2} \rangle = \langle x_2, p^{(m-1)/2} \rangle, \\ x_3 V + p^m U, & \langle x_4, p^{(n_4-1)/2} \rangle = \langle x_3, p^m \rangle. \end{cases}$$

Since $p \nmid x_2 x_3$ and $n_4 \geqslant 5m+2$, we see from (22) that $V \equiv 0 \pmod{p^{(m-1)/2}}$. Notice that

$$U_1 + V_1\sqrt{p} = \begin{cases} 2 + \sqrt{3}, & p = 3, \\ (2p-1) + 4a\sqrt{p}, & p \neq 3. \end{cases}$$

It follows that $p \nmid V_1$. Therefore, by Lemma 8, we have

$$U + V\sqrt{p} \geqslant (U_1 + V_1\sqrt{p})^{p^{(m-1)/2}}.$$

This implies

$$2U > (U_1 + V_1\sqrt{p})^{p^{(m-1)/2}} > (2\sqrt{p})^{p^{(m-1)/2}}.$$

Substitute this into (22) to get

$$(23) \qquad n_4 > m + p^{(m-1)/2}.$$

If $2 \nmid m$ and $m > 1$, then $m \geqslant 3$ and $p^{(m-1)/2} > D^{1/5}$ by (2). So from (23) we obtain

$$(24) \qquad n_4 > D^{1/5}.$$

On the other hand, since $p^{n_4} > D$, we deduce from (18) that

$$(25) \qquad \left| n_4 \log \frac{\varepsilon}{\bar{\varepsilon}} - 2s_4 \log \varrho \right| = \log \frac{x_4 + \sqrt{D}}{x_4 - \sqrt{D}} = \frac{2\sqrt{D}}{x_4} \sum_{i=0}^{\infty} \frac{1}{2i+1} \left(\frac{D}{x_4^2} \right)^i$$
$$< \frac{4\sqrt{D}}{x_4} < \frac{4\sqrt{D}}{p^{n_4/2}}.$$

Let $\beta = 2s_4/n_4$, $\alpha_1 = \varrho$, $\alpha_2 = \varepsilon/\bar{\varepsilon}$. Then α_1, α_2 satisfy $\alpha_1^2-2u_1\alpha_1+1=0$ and $p\alpha_2^2-2(x_1^2+D)\alpha_2+p=0$ respectively. As the definitions in Lemma 14, we have $r_0=1$, $r_1=r_2=r=2$, $A_1=2u_1$, $A_2=2(x_1^2+D)<6D$ and $B\leqslant 2n_4$ by (19). By Lemma 14, we have

$$(26)\quad \left|n_4\log\frac{\varepsilon}{\bar{\varepsilon}}-2s_4\log\varrho\right| > n_4\exp\big(-2\cdot 10^9(2+\log 2u_1)\times(2+\log 6D)(5+\log 2n_4+\log(2+\log 2u_1)(2+\log 6D))^2\big).$$

Since $p^{n_1}<p^{n_2}<D^2$ by (17), we see from Lemma 5 that $\log 2u_1 < 1+\log\varrho < 1+5(\log D)^2$. The combination of (25) and (26) yields

$$(27)\quad n_4 < 4\cdot 10^{11}(\log D)^3(\log\log D)^2.$$

On combining (27) with (24) we conclude $D<10^{100}$. Thus $N(D,p)=3$ if $\max(D,p)=D\geqslant 10^{100}$.

Next we consider the case $2\mid m$. Then $p\equiv 1 \pmod 4$ and $2\nmid D$ by (2), and $2\mid x_1$ by (17). Let

$$(28)\quad \begin{aligned} X_2+Y_2\sqrt{D} &= (x_1+\sqrt{D})^{n_2} = (x_1+\sqrt{D})^m,\\ u_2+v_2\sqrt{D} &= (u_1+v_1\sqrt{D})^{s_2}. \end{aligned}$$

Then, by (18), X_2, Y_2, u_2, v_2 are integers satisfying

$$x_2\pm\sqrt{D} = (X_2+Y_2\sqrt{D})(u_2-v_2\sqrt{D}).$$

Hence

$$(29)\quad \pm 1 = Y_2u_2-X_2v_2.$$

Since $2\mid m$ and $2\mid x_1$, we have $2\mid Y_2$ by (28). This implies $2\nmid v_2$ by (29), and $2\nmid v_1$, $2\mid u_1$ by (28). Let

$$(30)\quad X_4+Y_4\sqrt{D}=(x_1+\sqrt{D})^{n_4},\qquad u_4+v_4\sqrt{D}=(u_1+v_1\sqrt{D})^{s_4}.$$

Then $X_4, Y_4, u_4, v_4\in\mathbf{Z}$ with $x_4\pm\sqrt{D}=(X_4+Y_4\sqrt{D})(u_4-v_4\sqrt{D})$. Hence

$$(31)\quad x_4 = X_4u_4-DY_4v_4.$$

We observed that $2\mid x_4$, $2\mid x_1$, $2\nmid n_4$, $2\mid X_4$ and $2\nmid Y_4$. We find from (31) that $2\mid v_4$ and $2\nmid u_4$. Therefore $2\mid s_4$ since $2\mid u_1$. By Lemma 13, $(x_4, p^{(n_4-1)/2})$ is a solution of (20) which satisfies

$$\langle x_4, p^{(n_4-1)/2}\rangle \equiv -x_1 \equiv \langle x_1, 1\rangle \pmod D.$$

Hence $\langle x_4, p^{(n_4-1)/2}\rangle = \langle x_1, 1\rangle$. At the same time, we see from (17) that $\langle x_1, 1\rangle = \langle x_3, p^m\rangle$. Thus $\langle x_4, p^{(n_4-1)/2}\rangle = \langle x_3, p^m\rangle$ and

$$(32)\quad x_4+p^{(n_4-1)/2}\sqrt{p} = (x_3+p^m\sqrt{p})(U+V\sqrt{p})$$

by Lemma 11, where (U, V) is a positive solution of (11). According to the analysis for the case $2\nmid m$, we deduce from (32) that $p^m\mid V$ and $D<10^{100}$. The proof is complete.

4. Proof of Theorem 2. By Theorem 1, we now only consider the case of D, p not satisfying (2). Suppose that $N(D,p)>3$. Then (1) has four positive solutions (x_i, n_i) $(i=1,\dots,4)$ with $n_1<n_2<n_3<n_4$. Let $\varepsilon, \bar{\varepsilon}, \varrho, \bar{\varrho}$ be defined as in Lemma 4. We have

$$(33)\quad n_i = Z_1t_i,\quad x_i\pm\sqrt{D} = \varepsilon^{t_i}\bar{\varrho}^{s_i},\quad i=1,\dots,4$$

by Lemma 4, where s_i, t_i $(i=1,\dots,4)$ are integers satisfying

$$(34)\quad 0\leqslant s_i\leqslant t_i,\quad \gcd(s_i,t_i)=1,\quad i=1,\dots,4.$$

If $p^{Z_1}>\sqrt{D}$, then $p^{n_1}\geqslant p^{Z_1}>\sqrt{D}$ and $p^{n_2}\geqslant p^{2Z_1}>D$. By Lemmas 1 and 2, we have

$$\max(2\cdot 10^6, 600D^2) > p^{n_3}\geqslant p^{2n_2+n_1} > D^{5/2}.$$

This is impossible if $D>10^{240}$. Hence $p^{Z_1}<\sqrt{D}$ and $\max(D,p)=D$. Similarly, we have $p^{n_2}<D^2$ and $\log\varrho<5(\log D)^2$ by Lemma 5.

By Lemma 9, we have $p^{n_2}>\sqrt{D}$. Hence, by Lemma 1,

$$(35)\quad p^{n_3}\geqslant p^{2n_2+2(n_2-1)/3} > D^{4/3}p^{-2/3}.$$

If $p<D^{4/17}$, then from (35) we get

$$(36)\quad p^{n_3} > D^{20/17}.$$

If $p>D^{4/17}$, then $n_3\geqslant 2n_2+n_1\geqslant 5$ and (36) still holds. This implies $p^{n_4}>D^2$ by Lemma 1, hence $2\nmid n_4$ by Lemma 12.

Let $\delta=\gcd(2s_3,t_3)$, $2s_3=\delta s'$, $t_3=\delta t'$. By Lemma 7, we see from (36) that s'/t' and $2s_4/t_4$ are convergents of $\alpha=\log(\varepsilon/\bar{\varepsilon})/\log\varrho$ when $D\geqslant 10^{240}$. Since $t'<t_4$, by Theorem 10.2.4 of [2], we have

$$(37)\quad \left|\frac{s'}{t'}-\alpha\right| > \frac{1}{t'(t'+t_4)} \geqslant \frac{1}{t'(t_3+t_4)}.$$

From (33), we get

$$(38)\quad \left|\frac{s'}{t'}-\alpha\right| = \left|\frac{2s_3}{t_3}-\alpha\right| = \frac{1}{t_3\log\varrho}\log\frac{x_3+\sqrt{D}}{x_3-\sqrt{D}} = \frac{2\sqrt{D}}{t_3x_3\log\varrho}\sum_{i=0}^{\infty}\frac{1}{2i+1}\left(\frac{D}{x_3^2}\right)^i < \frac{4\sqrt{D}}{t_3x_3\log\varrho},$$

since $p^{n_3}>D$. The combination of (37) and (38) yields

$$(39)\quad t_3+t_4 > \frac{x_3\log\varrho}{4\sqrt{D}} = \frac{1}{4}\log\varrho\left(1+\frac{p^{n_3}}{D}\right)^{1/2}.$$

Substituting (36) into (39), we get

(40) $$t_3+t_4 > \tfrac{1}{4}D^{3/34}\log\varrho.$$

Let $\beta = 2s_4/t_4$, $\alpha_1 = \varrho$, $\alpha_2 = \varepsilon/\bar{\varepsilon}$. Then α_1, α_2 satisfy

$$\alpha_1^2-2u_1\alpha_1+1 = 0 \quad \text{and} \quad p^{Z_1}\alpha_2^2-2(X_1^2+DY_1^2)\alpha_2+p^{Z_1} = 0$$

respectively. The heights of α_1 and α_2 satisfy $H_1 = 2u_1$ and $H_2 = 2(X_1^2+DY_1^2) < 2\varrho^2 p^{Z_1}$ by (5). Recalling that $0 \leqslant s_4 \leqslant t_4$, by Lemma 14, we have

(41) $$\left|t_4\log\frac{\varepsilon}{\bar{\varepsilon}}-2s_4\log\varrho\right| > t_4\exp\big(-2\cdot 10^9(2+\log 2u_1)(2+\log 2\varrho^2 p^{Z_1}) \times(5+\log 2t_4+\log(2+\log 2u_1)(2+\log 2\varrho^2 p^{Z_1}))^2\big).$$

On the other hand, since $p^{n_4} > D$, we have

(42) $$\left|t_4\log\frac{\varepsilon}{\bar{\varepsilon}}-2s_4\log\varrho\right| = \log\frac{x_4+\sqrt{D}}{x_4-\sqrt{D}} < \frac{4\sqrt{D}}{x_4} < \frac{4\sqrt{D}}{p^{Z_1t_4/2}}.$$

The combination of (41) and (42) yields

(43) $$t_4 < 10^{11}(\log\varrho)(\log 2\varrho^2 p^{Z_1})(\log\log 2\varrho^2 p^{Z_1})^2.$$

Since $\varrho > 2\sqrt{D}$ and $t_3 = \log p^{n_3}/\log p^{Z_1} < \log p^{n_3} < \log 2\cdot 10^6 D^2$ by Lemma 2. From (39) and (43), we conclude that

(44) $$20+4\cdot 10^{11}(\log 2\varrho^2 p^{Z_1})(\log\log 2\varrho^2 p^{Z_1})^2 > D^{3/34}.$$

Recalling that $p^{Z_1} < \sqrt{D}$ and $\log\varrho < 5(\log D)^2$, we have $\log 2\varrho^2 p^{Z_1} < 11(\log D)^2$. Substituting this into (44), we conclude that $D < 10^{240}$. The theorem is proved.

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

References

[1] F. Beukers, *On the generalized Ramanujan–Nagell equation II*, Acta Arith. 39 (1981), 113–123.
[2] L.-K. Hua, *Introduction to Number Theory*, Springer-Verlag, Berlin 1982.
[3] M.-H. Le, *On the generalized Ramanujan–Nagell equation III* (Chinese), Dongbei Shuxue 4 (1988), 180–184.
[4] M. Mignotte and M. Waldschmidt, *Linear forms in two logarithms and Schneider's method*, Math. Ann. 231 (1978), 241–267.

RESEARCH DEPARTMENT
CHANGSHA RAILWAY INSTITUTE
Changsha, Hunan
China

Received on 9.1.1990
and in revised form on 7.6.1990 (2002)