Yuan-e Zhao; Tingting Wang

A note on the number of solutions of the generalized Ramanujan-Nagell equation $x^2 - D = p^n$

Czechoslovak Mathematical Journal, Vol. 62 (2012), No. 2, 381–389

Persistent URL: http://dml.cz/dmlcz/142835

Czechoslovak Mathematical Journal, 62 (137) (2012), 381–389

A NOTE ON THE NUMBER OF SOLUTIONS OF THE GENERALIZED RAMANUJAN-NAGELL EQUATION $x^2 - D = p^n$

Yuan-e Zhao, Yan'an, Tingting Wang, Xi'an

(Received December 14, 2010)

Abstract. Let D be a positive integer, and let p be an odd prime with $p \nmid D$. In this paper we use a result on the rational approximation of quadratic irrationals due to M. Bauer, M. A. Bennett: Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation. Ramanujan J. 6 (2002), 209–270, give a better upper bound for $N(D,p)$, and also prove that if the equation $U^2 - DV^2 = -1$ has integer solutions (U,V), the least solution (u_1, v_1) of the equation $u^2 - pv^2 = 1$ satisfies $p \nmid v_1$, and $D > C(p)$, where $C(p)$ is an effectively computable constant only depending on p, then the equation $x^2 - D = p^n$ has at most two positive integer solutions (x,n). In particular, we have $C(3) = 10^7$.

Keywords: generalized Ramanujan-Nagell equation, number of solution, upper bound

MSC 2010: 11D61

1. Introduction

Let $\mathbb{Z}, \mathbb{N}$ be the sets of all integers and positive integers respectively. Let D be a positive integer, and let p be an odd prime with $p \nmid D$. Further let $N(D,p)$ denote the number of solutions (x,n) of the generalized Ramanujan-Nagell equation

$$x^2 - D = p^n, \quad x, n \in \mathbb{N}. \tag{1.1}$$

By a classical result on the greatest prime divisor of $x^2 - D$ due to C. L. Siegel [7], we know that $N(D,p)$ is always finite. There are many papers concerned with upper bounds for $N(D,p)$. In 1981, using the hypergeometric method, F. Beukers [2] proved that $N(D,p) \leqslant 4$. Simultaneously, he proposed the following conjecture:

The research has been supported by N. S. F. (11071194) of P. R. China.

Conjecture 1.1. $N(D,p) \leqslant 3$.

In 1991, M. H. Le [3] basically verified Conjecture 1.1. Using the Baker method, he proved that if $\max(D,p) > 10^{240}$, then $N(D,p) \leqslant 3$. Conjecture 1.1 has been completely solved by M. Bauer and M. A. Bennett [1].

In this paper, using a result on the rational approximation of quadratic irrationals due to M. Bauer and M. A. Bennett [1], we give a better upper bound for $N(D,p)$ as follows.

Theorem. *If the equation*

$$U^2 - DV^2 = -1, \quad U, V \in \mathbb{Z} \tag{1.2}$$

has solutions (U,V), the least solution (u_1, v_1) of the equation

$$u^2 - pv^2 = 1, \quad u, v \in \mathbb{Z} \tag{1.3}$$

satisfies $p \nmid v_1$, and $D > C(p)$, where $C(p)$ is an effectively computable constant only depending on p, then $N(D,p) \leqslant 2$. In particular, we have $C(3) = 10^7$.

In [2], F. Beukers showed that if D and p satisfy

$$p = \begin{cases} 3, \\ 4a^2+1, \end{cases} \qquad D = \begin{cases} \left(\dfrac{3^m+1}{4}\right)^2 - 3^m, & 2 \nmid m, \\ \left(\dfrac{p^m-1}{4a}\right)^2 - p^m, & 2 \mid m, \end{cases} \qquad a, m \in \mathbb{N}, \ m > 1, \tag{1.4}$$

then (1.1) has three known solutions (x,n). The pair (D,p) is called exceptional or non-exceptional according as D and p satisfy (1.4) or not. So far we have not seen any non-exceptional pair (D,p) make $N(D,p) > 2$, so we propose the following conjecture:

Conjecture 1.2. *If (D,p) is a non-exceptional pair, then $N(D,p) \leqslant 2$.*

2. Preliminaries

Let d be a positive integer which is not a square. By the basic properties of Pell equations (see [6, Chapter 8]), we have the following two lemmas.

Lemma 2.1. *The equation*

$$u^2 - dv^2 = 1, \quad u, v \in \mathbb{Z} \tag{2.1}$$

has solutions (u, v) *with* $uv \neq 0$, *and it has a unique positive integer solution* (u_1, v_1) *satisfying* $u_1 + v_1\sqrt{d} \leqslant u + v\sqrt{d}$, *where* (u, v) *runs through all positive integer solutions of* (2.1). (u_1, v_1) *is called the least solution of* (2.1). *Then, every solution* (u, v) *of* (2.1) *can be expressed as*

$$u + v\sqrt{d} = \pm(u_1 + v_1\sqrt{d})^m, \quad m \in \mathbb{Z}.$$

Lemma 2.2. *If the equation*

$$U^2 - dV^2 = -1, \quad U, V \in \mathbb{Z} \tag{2.2}$$

has solutions (U, V), *then it has a unique positive integer solution* (U_1, V_1) *satisfying* $U_1 + V_1\sqrt{d} \leqslant U + V\sqrt{d}$, *where* (U, V) *runs through all positive integer solutions of* (2.2). (U_1, V_1) *is called the least solution of* (2.2). *Then we have* $u_1 + v_1\sqrt{d} = (U_1 + V_1\sqrt{d})^2$, *where* (u_1, v_1) *is the least solution of* (2.1).

Lemma 2.3 ([3, Lemma 8])**.** *Let* (u, v) *be a positive integer solution of* (1.3) *with* $p^r \mid v$, *where* r *is a positive integer. If the least solution* (u_1, v_1) *of* (1.3) *satisfies* $p \nmid v_1$, *then*

$$u + v\sqrt{p} = (u_1 + v_1\sqrt{p})^{p^r l}, \quad l \in \mathbb{N}.$$

Lemma 2.4 ([5, Lemma 3])**.** *If* $p \equiv 3 \pmod 4$, *then the least solution* (u_1, v_1) *of* (1.3) *satisfies* $u_1 + v_1\sqrt{p} > 2p - 3$.

Let k be an integer such that $|k| > 1$ and $\gcd(k, d) = 1$.

Lemma 2.5 ([3, Lemma 10])**.** *For any fixed solution* (A, B) *of the equation*

$$A^2 - dB^2 = k, \quad A, B \in \mathbb{Z}, \quad \gcd(A, B) = 1, \tag{2.3}$$

there exist unique integers α, β, l *such that* $\beta A - \alpha B = 1$, $l = \alpha A - d\beta B$ *and* $0 < l < |k|$. *We call* l *the characteristic number of the solution* (A, B), *and denote it by* $\langle A, B\rangle$. *Moreover, if* $\langle A, B\rangle = l$, *then* $l^2 \equiv d \pmod{|k|}$ *and* $A \equiv -lB \pmod{|k|}$.

Lemma 2.6 ([3, Lemma 11]). *Let (A_1, B_1) and (A_2, B_2) be two solutions of* (2.3). *A necessary and sufficient condition for $\langle A_1, B_1\rangle = \langle A_2, B_2\rangle$ is that*

$$A_2 + B_2\sqrt{d} = \big(A_1 + B_1\sqrt{d}\big)\big(u + v\sqrt{d}\big),$$

where (u, v) is a solution of (2.1).

Lemma 2.7. *If (A_1, B_1) is a solution of* (2.3) *with $\langle A_1, B_1\rangle = l$, then $(A_1, -B_1)$ is a solution of* (2.3) *with $\langle A_1, -B_1\rangle = |k| - l$.*

Proof. It is obvious that $(A_1, -B_1)$ is a solution of (2.3). Let $l' = \langle A_1, -B_1\rangle$. Since $\langle A_1, B_1\rangle = l$, by Lemma 2.5, we have $l' \equiv -A_1/-B_1 \equiv -l \pmod{|k|}$ and $0 < l, l' < |k|$. Thus, we get $l' = |k| - l$. The lemma is proved. □

Lemma 2.8 ([3, Lemma 3]). *If D is not a square and the equation*

$$X^2 - DY^2 = p^Z, \quad X, Y, Z \in \mathbb{Z}, \quad \gcd(X, Y) = 1, \quad Z > 0 \tag{2.4}$$

has solutions (X, Y, Z), then it has a positive integer solution (X_1, Y_1, Z_1) satisfying $Z_1 \leqslant Z$ and $1 < (X_1 + Y_1\sqrt{D})/(X_1 - Y_1\sqrt{D}) < (u_1 + v_1\sqrt{D})^2$, where Z runs through all solutions (X, Y, Z) of (2.4), *(u_1, v_1) is the least solution of the equation*

$$u^2 - Dv^2 = 1, \quad u, v \in \mathbb{Z}. \tag{2.5}$$

Moreover, every solution (X, Y, Z) of (2.4) *can be expressed as*

$$Z = Z_1 t, \; X + Y\sqrt{D} = \big(X_1 + \delta Y_1\sqrt{D}\big)^t\big(u + v\sqrt{D}\big), \quad t \in \mathbb{N}, \; \delta \in \{\pm 1\},$$

where (u, v) is a solution of (2.5).

Lemma 2.9 ([1, Corollary 1.6]). *For any fixed odd prime p and any positive integers r, s, we have*

$$\left|\frac{s}{p^r} - \sqrt{p}\right| > p^{-rC_1(p)},$$

where $C_1(p)$ is an effectively computable constant only depending on p with $0 < C_1(p) < 2$. In particular, we have $C_1(3) = 1.65$ if $r \neq 7$.

3. Further lemmas on (1.1)

Lemma 3.1 ([3, Lemma 4]). *Under the assumptions and the definitions as in Lemma* 2.8, *every solution* (x,n) *of* (1.1) *can be expressed as*

$$n = Z_1 t,\ x+\delta\sqrt{D} = \big(X_1+Y_1\sqrt{D}\big)^t\big(u_1-v_1\sqrt{D}\big)^s,\ t\in\mathbb{N},\ s\in\mathbb{Z},\ 0\leqslant s\leqslant t,\ \delta\in\{\pm1\}.$$

Lemma 3.2 ([3, Lemma 13]). *Under the assumptions and the definitions as in Lemmas* 2.5, 2.8 *and* 3.1, *if* (x,n) *is a solution of* (1.1) *with* $2\nmid n$, *then* $2\nmid Z_1$ *and the equation*

$$A^2 - p^{Z_1}B^2 = D,\quad A,B\in\mathbb{Z},\quad \gcd(A,B)=1 \tag{3.1}$$

has a solution $(A,B) = (x, p^{Z_1(t-1)/2})$ *with*

$$\langle x, p^{Z_1(t-1)/2}\rangle \equiv \begin{cases} -X_1 \pmod{D}, & \text{if } 2\mid s,\\ -X_1u_1 \pmod{D}, & \text{if } 2\nmid s.\end{cases}$$

Lemma 3.3. *Let* (x',n') *and* (x'',n'') *be two solutions of* (1.1) *with* $2\nmid n'n''$. *If* (1.2) *has solutions* (U,V), *then we have*

$$n' = Z_1t',\ n'' = Z_1t'',\quad t',t''\in\mathbb{N},\ 2\nmid t't'', \tag{3.2}$$

and

$$x'' + p^{Z_1(t''-1)/2}\sqrt{p^{Z_1}} = \big(x' + \lambda p^{Z_1(t'-1)/2}\sqrt{p^{Z_1}}\big)\big(u' + v'\sqrt{p^{Z_1}}\big),\ \lambda\in\{\pm1\}, \tag{3.3}$$

where (u',v') *is a solution of the equation*

$$u'^2 - p^{Z_1}v'^2 = 1,\quad u',v'\in\mathbb{Z}. \tag{3.4}$$

Proof. Since (1.2) has solutions, D is not a square. Hence, by Lemma 3.1, we get (3.2) immediately. Then, (3.1) has two solutions $(x', p^{Z_1(t'-1)/2})$ and $(x'', p^{Z_1(t''-1)/2})$. Let $l' = \langle x', p^{Z_1(t'-1)/2}\rangle$ and $l'' = \langle x'', p^{Z_1(t''-1)/2}\rangle$. If $l' = l''$, by Lemma 2.6, then (3.3) holds for $\lambda = 1$. If $l'\neq l''$, by Lemma 3.2, then we have

$$l'' \equiv l'u_1 \pmod{D}, \tag{3.5}$$

since $u_1^2\equiv 1 \pmod{D}$. Further, by Lemma 2.2, we have $u_1 \equiv U_1^2 + DV_1^2 \equiv U_1^2 \equiv -1 \pmod{D}$, where (U_1,V_1) is the least solution of (1.2). Therefore, we see from (3.5) that $l''\equiv -l' \pmod{D}$ and $l'' = D - l'$. Furthermore, by Lemma 2.7, $(x', -p^{Z_1(t'-1)/2})$ is a solution of (3.1) with $\langle x', -p^{Z_1(t'-1)/2}\rangle = D - l'$. Thus, applying Lemma 2.6 again, (3.3) holds for $\lambda = -1$. The lemma is proved. □

Lemma 3.4. *If* (1.2) *has solutions* (U, V), *then we have:*

(i) (D, p) *is a non-exceptional pair.*

(ii) *If* (1.1) *has solutions* (x, n), *then* $p \equiv 3 \pmod 4$ *and* $2 \nmid n$.

Proof. By (1.2), we have either $D \equiv 1 \pmod 4$ or $D \equiv 2 \pmod 8$. However, if (D, p) is an exceptional pair, then from (1.4) we get $D \equiv 6 \pmod 8$ for $p = 3$, and

$$D \equiv \begin{cases} 3 \pmod 4, & \text{if } 2 \mid a \text{ or } 2 \mid m, \\ 0 \pmod 4, & \text{otherwise,} \end{cases}$$

for $p = 4a^2 + 1$. Therefore, the conclusion (i) is proved.

Similarly, by (1.1), we have

$$p^n \equiv x^2 - D \equiv \begin{cases} 3 \pmod 4, & \text{if } D \equiv 1 \pmod 4, \\ 7 \pmod 8, & \text{if } D \equiv 2 \pmod 8. \end{cases}$$

This implies that $p \equiv 3 \pmod 4$ and $2 \nmid n$. Thus, the lemma is proved. □

Lemma 3.5 ([4, Proof of Assertion 7])**.** *Let* (D, p) *be a non-exceptional pair. If* (1.1) *has three solutions* $(x_1, n_1), (x_2, n_2)$ *and* (x_3, n_3) *with* $n_1 < n_2 < n_3$, *then* D *is not a square,* $p^{n_1} < \sqrt{D}$, $4\sqrt{D} < p^{n_2} < 600D^2$ *and* $p^{n_3} > \frac{4}{9}p^{8n_2/3}$.

Lemma 3.6. *Let* (x, n) *be a solution of* (1.1) *with* $2 \nmid n$. *Then we have*

$$D > C_2(p)p^{(2-C_1(p))n/2}, \tag{3.6}$$

where $C_2(p) = 2p^{(C_1(p)-1)/2}$ *and* $C_1(p)$ *is defined as in Lemma* 2.9.

Proof. We see from (1.1) that $x > p^{n/2}$ and

$$D = (x + p^{n/2})(x - p^{n/2}) > 2p^{n-1/2}\Big(\frac{x}{p^{(n-1)/2}} - \sqrt{p}\Big). \tag{3.7}$$

By Lemma 2.9, we have

$$\frac{x}{p^{(n-1)/2}} - \sqrt{p} > p^{-C_1(p)(n-1)/2}. \tag{3.8}$$

Substituting (3.8) into (3.7), we obtain (3.6) immediately. The lemma is proved. □

4. Proof of theorem

We now assume that (1.1) has three solutions $(x_1, n_1), (x_2, n_2)$ and (x_3, n_3) with $n_1 < n_2 < n_3$. Then, by Lemma 3.5, D is not a square. Since (1.2) has solutions (U, V), by Lemmas 3.1, 3.3 and 3.5, we have $p \equiv 3 \pmod 4$, $2 \nmid n_1 n_2 n_3$, (D, p) is a non-exceptional pair,

$$n_i = Z_1 t_i, \quad t_i \in \mathbb{N},\ i = 1, 2, 3,\ t_1 < t_2 < t_3,\ 2 \nmid t_1 t_2 t_3, \tag{4.1}$$

and

$$x_3 + p^{Z_1(t_3-1)/2}\sqrt{p^{Z_1}} = \big(x_2 + \lambda p^{Z_1(t_2-1)/2}\sqrt{p^{Z_1}}\big)\big(u' + v'\sqrt{p^{Z_1}}\big),\ \lambda \in \{\pm 1\}, \tag{4.2}$$

where (u', v') is a solution of (3.4). Hence, by (4.1) and (4.2), we get

$$x_3 + \sqrt{p^{n_3}} = \big(x_2 + \lambda\sqrt{p^{n_2}}\big)\big(u' + v'\sqrt{p^{Z_1}}\big). \tag{4.3}$$

Since $x_3 + \sqrt{p^{n_3}} > x_2 + \sqrt{p^{n_2}} \geqslant x_2 + \lambda\sqrt{p^{n_2}} > 0$, we see from (4.3) that (u', v') is a positive integer solution of (3.4). Further, since $2 \nmid Z_1$,

$$(u, v) = (u', p^{(Z_1-1)/2} v') \tag{4.4}$$

is a positive integer solution of (1.3).

By (4.3), we have

$$p^{(n_3-1)/2} = x_2 v' p^{(Z_1-1)/2} + \lambda u' p^{(n_2-1)/2}. \tag{4.5}$$

Since $p \nmid x_2$, we see from (4.1) and (4.5) that $p^{Z_1(t_2-1)/2} \mid v'$. Hence, by (4.4), we get

$$p^{(n_2-1)/2} \mid v. \tag{4.6}$$

Therefore, since $p \nmid v_1$, applying Lemma 2.3 to (4.6), we get from (4.4) that

$$u' + v'\sqrt{p^{Z_1}} = u + v\sqrt{p} = (u_1 + v_1\sqrt{p})^{p^{(n_2-1)/2} l} \geqslant (u_1 + v_1\sqrt{p})^{p^{(n_2-1)/2}}, \tag{4.7}$$

where (u_1, v_1) is the least solution of (1.3). Further, since $p \equiv 3 \pmod 4$, by Lemma 2.4, we have $u_1 + v_1\sqrt{p} > 2p - 3 \geqslant p$. Substituting it into (4.7), we get

$$u' + v'\sqrt{p^{Z_1}} > p^{p^{(n_2-1)/2}}. \tag{4.8}$$

By Lemma 3.5, we have $p^{n_2} < 600D^2$. It implies that

$$(4.9)\qquad x_2 + \lambda\sqrt{p^{n_2}} \geqslant x - \sqrt{p^{n_2}} = \frac{D}{x_2 + \sqrt{p^{n_2}}} > \frac{D}{\sqrt{600D^2 + D} + \sqrt{600D^2}} > \frac{1}{25}.$$

Moreover, since $p^{n_3} > \frac{4}{9}p^{8n_2/3}$ and $p^{n_2} > 4\sqrt{D}$, we have $p^{n_3} > 16D$ and

$$(4.10)\qquad x_3 + \sqrt{p^{n_3}} = \sqrt{p^{n_3} + D} + \sqrt{p^{n_3}} < \frac{51}{25}\sqrt{p^{n_3}}.$$

The combination of (4.3), (4.8), (4.9) and (4.10) yields

$$(4.11)\qquad 51\sqrt{p^{n_3}} > p^{p^{(n_2-1)/2}}.$$

On the other hand, by Lemma 3.6, we have

$$(4.12)\qquad D > (2p^{(C_1(p)-1)/2})p^{(2-C_1(p))n_3/2},$$

where $C_1(p)$ is defined as in Lemma 2.9. Since $p^{n_2} > 4\sqrt{D}$, by (4.11) and (4.12), we obtain

$$(4.13)\qquad \log D > C_3(p)D^{1/4} + C_4(D),$$

where

$$(4.14)\quad C_3(p) = \frac{2}{\sqrt{p}}(\log p)(2-C_1(p)),\ C_4(p) = \log(2p^{(C_1(p)-1)/2}) - (2-C_1(p))\log 51.$$

Since $C_1(p) < 2$ by Lemma 2.9, we find from (4.13) and (4.14) that $D < C(p)$. Thus, if $D > C(p)$, then (1.1) has at most two solutions (x, n).

In particular, since $C_1(3) = 1.65$ if $n_3 \neq 15$, we can deduce from (4.13) and (4.14) that $C(3) = 10^7$. The theorem is proved. □

References

[1] *M. Bauer, M. A. Bennett*: Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation. Ramanujan J. *6* (2002), 209–270.

[2] *F. Beukers*: On the generalized Ramanujan-Nagell equation II. Acta Arith. *39* (1981), 113–123.

[3] *M. H. Le*: On the generalized Ramanujan-Nagell equation $x^2 - D = p^n$. Acta Arith. *58* (1991), 289–298.

[4] *M. H. Le*: On the number of solutions of the generalized Ramanujan-Nagell equation $x^2 - D = p^n$. Publ. Math. Debrecen. *45* (1994), 239–254.

[5] *M. H. Le*: Upper bounds for class numbers of real quadratic fields. Acta Arith. *68* (1994), 141–144.

[6] *L. J. Mordell*: Diophantine Equations. London, Academic Press., 1969.
[7] *C. L. Siegel*: Approximation algebraischer Zahlen. Diss. Göttingen, Math. Zeitschr. *10* (1921), 173–213. (In German.)

Authors' addresses: Yuan-e Zhao, College of Mathematics and Computer Science, Yanan University, Yanan, Shaanxi, P. R. China; Tingting Wang, Department of Mathematics, Northwest University, Xi'an, Shaanxi, P. R. China, e-mail: tingtingwang126@126.com.