Bull. Math. Soc. Sci. Math. Roumanie
Tome 55(103) No. 3, 2012, 279–293

On the number of solutions of the generalized Ramanujan-Nagell equation $D_1x^2 + D_2^m = p^n$

by
Yongzhong Hu and Maohua Le

Abstract

Let D_1 and D_2 be coprime positive integers with $\min(D_1, D_2) > 1$, and let p be an odd prime with $p \nmid D_1D_2$. Further, let $N(D_1, D_2, p)$ denote the number of positive integer solutions (x, m, n) of the equation $D_1x^2 + D_2^m = p^n$. In this paper, we prove that $N(D_1, D_2, p) \leq 2$ except for $N(2, 7, 3) = N(10, 3, 13) = N(10, 3, 37) = N((3^{2l-1} - 1)/a^2, 3, 4 \cdot 3^{2l-1} - 1) = 3$, where a, l are positive integers.

Key Words: Exponential diophantine equation; generalized Ramanujan-Nagell equation; number of solutions; upper bound.
2010 Mathematics Subject Classification: Primary 11D61; Secondary 11D25.

1 Introduction

Let $\mathbb{Z}, \mathbb{N}$ be the sets of all integers and positive integers respectively. Let D_1, D_2 be coprime positive integers with $D_2 > 1$, and let p be an odd prime with $p \nmid D_1D_2$. In this paper, we deal with the number of solutions (x, m, n) of the equation

$$D_1x^2 + D_2^m = p^n, x, m, n \in \mathbb{N}, \tag{1.1}$$

which is an exponential extension of the Ramanujan-Nagell type equation. Let $N(D_1, D_2, p)$ denote the number of solutions of (1.1). For $D_1 = 1$, sum up the results of [5],[12] and [19], we have

Theorem A. *$N(1, D_2, p) \leq 2$ except for $N(1, 2, 3) = 4$ and $N(1, 2, 5) = N(1, 4, 5) = 3$.*

Recently, P.-Z. Yuan and Y.-Z. Hu[20] proved that if $4D_1+1$ is a power of p, then $N(D_1, 3D_1+1, p) = 2$ except for $N(1, 4, 5) = N(2, 7, 3) = 3$. In this paper, we prove a more general result as follows.

Supported by the National Natural Science Foundation of China(No.10971184)

Theorem B. *If $D_1 > 1$, then $N(D_1, D_2, p) \leq 2$ except for $N(2,7,3) = N(10,3,13) = N(10,3,37) = N((3^{2l-1}-1)/a^2, 3, 4\cdot 3^{2l-1}-1) = 3$, where $a, l \in \mathbb{N}$.*

2 Preliminaries

For any nonnegative integer k, let F_k and L_k denote the k-th Fibonacci number and Lucas number respectively.

Lemma 2.1 ([16],pp.60-61).

(i) $2|F_kL_k$ *if and only if* $3|k$.

(ii) $\gcd(F_k, L_k) = \begin{cases} 1, & \text{if } 3 \nmid k, \\ 2, & \text{if } 3|k. \end{cases}$

(iii) $F_{2k} = F_kL_k$.

(iv) $L_k^2 - 5F_k^2 = (-1)^k 4$.

(v) *Every solution (u, v) of the equation*

$$u^2 - 5v^2 = \pm 4, u, v \in \mathbb{N}$$

can be expressed as $(u, v) = (L_k, F_k)$, where $k \in \mathbb{N}$.

Lemma 2.2 ([7]). *The equation*

$$F_k = z^s, k, z, s \in \mathbb{N}, z > 1, s > 1$$

has only the solutions $(k, z, s) = (6, 2, 3)$ and $(12, 12, 2)$. The equation

$$L_k = z^s, k, z, s \in \mathbb{N}, z > 1, s > 1$$

has only the solution $(k, z, s) = (3, 2, 2)$.

Lemma 2.3 ([6]). *The equation*

$$F_k = 2^r z^s, k, z, r, s \in \mathbb{N}, 2 \nmid z, z > 1, s > 1$$

has only the solution $(k, z, r, s) = (12, 3, 4, 2)$. The equation

$$L_k = 2^r z^s, k, z, r, s \in \mathbb{N}, 2 \nmid z, z > 1, s > 1$$

has no solution (k, z, r, s).

Let d be a nonzero integer with $d \equiv 0$ or $1 \pmod 4$, and let $h(d)$ denote the class number of binary quadratic primitive forms with discriminant d.

Lemma 2.4 ([10],pp.321-322.Theorem 12.10.1). *If $d < 0$, then*

$$h(d) = \frac{\omega\sqrt{|d|}}{2\pi}K(d),$$

where $\omega = 2, 4$ or 6 according to $d < -4, d = -4$ or $d = -3$,

$$K(d) = \sum_{n=1}^{\infty}\left(\frac{d}{n}\right)_k \frac{1}{n},$$

where $(*/*)_k$ denote the Kronecker symbol.

Lemma 2.5 ([10],pp.322.Theorem 12.11.1 and 12.11.2). *Every discriminant d can be expressed as $d = fm^2$, where f is a fundamental discriminant, m is a positive integer. Then we have*

$$K(d) = K(f)\prod_{p|m}\left(1 - \left(\frac{f}{p}\right)_k \frac{1}{p}\right),$$

where $\prod_{p|m}$ denote the product through distinct prime divisors p of m.

Lemma 2.6 ([10],pp.324.Theorem 12.12.2). *If $d < 0$ is a fundamental discriminant, then*

$$K(d) = -\frac{\pi}{|d|^{3/2}}\sum_{r=1}^{|d|-1}\left(\frac{d}{r}\right)_k r.$$

Lemma 2.7 ([8],Lemma 1). *Let d_1, d_2 be coprime positive integers with $d_1d_2 > 1$, and let p be an odd prime with $p \nmid d_1d_2$. If The equation*

$$d_1X^2 + d_2Y^2 = p^Z, X, Y, Z \in \mathbb{Z}, \gcd(X, Y) = 1, Z > 0 \tag{2.1}$$

has solutions (X, Y, Z), then it has a unique positive integer solution (X_1, Y_1, Z_1) satisfying $Z_1 \le Z$, where Z through all solutions (X, Y, Z) of (2.1). Such (X_1, Y_1, Z_1) is called the least solution of (2.1). Then we have

(i) $h(-4d_1d_2) \equiv \begin{cases} 0 \pmod{Z_1}, & \text{if } d_1 = 1, \\ 0 \pmod{2Z_1}, & \text{if } d_1 > 1. \end{cases}$

(ii) *Every solution (X, Y, Z) of (2.1) can be expressed as*

$$Z = Z_1t, X\sqrt{d_1} + Y\sqrt{-d_2} = \lambda_1(X_1\sqrt{d_1} + \lambda_2Y_1\sqrt{-d_2})^t,$$

where $t \ge 1$ is an integer, $\lambda_2 \in \{-1, 1\}$. If $\min(d_1, d_2) > 1$, then t is odd. If $d_1d_2 \ne 3$, and $d_2 > 1$ or t is odd, then $\lambda_1 \in \{-1, 1\}$. If $d_1d_2 = 3$, then $\lambda_1 \in \{-1, 1, -i, i, \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}\}$.

By (ii) of Lemma 2.7, we can obtain the following lemma immediately.

Lemma 2.8 . *If* (X, Y, Z) *and* (X', Y', Z') *are positive integer solutions of* (2.1) *with* $(X, Y, Z) \neq (X', Y', Z')$*, then* $Z \neq Z'$.

Lemma 2.9 ([8],Theorem 1). *A necessary and sufficient condition that the equation*

$$d_1 y^2 + d_2 = p^z, y, z \in \mathbb{N} \tag{2.2}$$

has solutions (y, z) *is that* (2.1) *has solutions* (X, Y, Z) *and its least solution* (X_1, Y_1, Z_1) *satisfies* $Y_1 = 1$. *Moreover, if* $Y_1 = 1$*, then* (2.2) *has only the solution* $(y, z) = (X_1, Z_1)$ *except for* $3d_1X_1^2 - d_2 = \lambda$*, where* $\lambda \in \{-1, 1\}$*, and* (2.2) *has exactly two solutions* $(y, z) = (X_1, Z_1)$ *and* $(X_1(8d_1X_1^2 - 3\lambda), 3Z_1)$.

Lemma 2.10 *Let* $d_1 = 1$ *and* (X_1, Y_1, Z_1) *be the least solution of* (2.1). *If* (y, z) *is a solution of the equation*

$$1 + d_2 y^2 = p^z, y, z \in \mathbb{N}, \tag{2.3}$$

then one of the following conditions must be satisfied.

(i) $X_1 = 1, (y, z) = (Y_1, Z_1)$.

(ii) $|X_1^2 - d_2Y_1^2| = 1, (y, z) = (2X_1Y_1, 2Z_1)$.

(iii) $d_2 = 6, p = 7, X_1 = Y_1 = Z_1 = 1, (y, z) = (20, 4)$.

(iv) $d_2 = 2, p = 3, X_1 = Y_1 = Z_1 = 1, (y, z) = (11, 5)$.

Proof: This lemma can be immediately inferred from ([14],Theorem) and ([8],Theorem 1) for $d_2 = 2$ and $d_2 > 2$, respectively. ∎

Lemma 2.11 [15]. *The equation*

$$3x^2 = y^3 \pm 1, x, y \in \mathbb{N}$$

has no integer solution (x, y) .

Lemma 2.12 [11, 13]. *The equation*

$$x^2 - y^n = \lambda, x, y, n \in \mathbb{N}, n > 1, \lambda = \pm 1$$

has only the solution $(x, y, n) = (3, 2, 3)$.

Lemma 2.13 [17]. *The equation*

$$x^2 + 4 = y^n, x, y, n \in \mathbb{N}, \gcd(x, y) = 1, n > 1$$

has only the integer solution $(x, y, n) = (11, 5, 3)$.

Lemma 2.14 [3, 4]. *The equation*

$$x^2 + 3^m = y^n, x, y, m, n \in \mathbb{N}, \gcd(x, y) = 1, n > 1$$

has no integer solution (x, y, m, n) *with* $2 \not| m$.

Lemma 2.15 *The equation*

$$3^r + 4 = p^s, r, s \in \mathbb{N}, s > 1 \tag{2.4}$$

has no solution (r, s).

Proof: If $s > 1$, we infer from Lemma 2.13 that r is odd. Then, by Lemma 2.14, we know that (2.4) has no solution (r, s). The lemma is proved. □

Lemma 2.16 *The equation*

$$4 \cdot 3^r + \lambda = p^s, \lambda \in \{-1, 1\}, r, s \in \mathbb{N}, s > 1 \tag{2.5}$$

has no solution (r, s).

Proof: Since $p^s \equiv 4 \cdot 3^r + \lambda \equiv 3$ or $5 \pmod 8$, we get $2 \not| s$. Then, we infer from Lemma 2.12 that $2 \not| r$. Hence, by (2.5), we get

$$3 \cdot (2 \cdot 3^{(r-1)/2})^2 = 4 \cdot 3^r = p^s - \lambda = (p - \lambda) \left(\frac{p^s - \lambda}{p - \lambda} \right). \tag{2.6}$$

Notice that $\gcd(p-\lambda, \frac{p^s-\lambda}{p-\lambda})|s$ and $\frac{p^s-\lambda}{p-\lambda}$ is an odd. If $\gcd(p-\lambda, \frac{p^s-\lambda}{p-\lambda}) \neq 1$, then $3|s$ and a solution of the equation in Lemma 2.11 would be obtained, a contradiction. Hence, we get $\frac{p^s-\lambda}{p-\lambda} = 3^r$ or 1. If $\frac{p^s-\lambda}{p-\lambda} = 3^r$, then we get $p - \lambda = 4$, which means $p = 3, \lambda = -1$ or $p = 5, \lambda = 1$. By taking modulo 3 on (2.6), we get $0 \equiv p^s - \lambda \equiv -1$ or $1 \pmod 3$, this is impossible. If $\frac{p^s-\lambda}{p-\lambda} = 1$, then $s = 1$, a contradiction to $s > 1$. Thus, the lemma is proved. □

A Lehmer pair is a pair(α, β) of algebraic integers such that $(\alpha + \beta)^2$ and $\alpha\beta$ are non-zero coprime rational integers and α/β is not a root of unity. For a given Lehmer pair (α, β), one defines the corresponding sequence of Lehmer numbers by

$$u_n = u_n(\alpha, \beta) = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta}, & \text{if } 2 \not| n \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & \text{if } 2|n. \end{cases} \quad (n = 1, 2, \ldots). \tag{2.7}$$

Let (α, β)be a Lehmer pair. The prime number p is a primitive divisor of the Lehmer number $u_n(\alpha, \beta)$ if p divides $u_n(\alpha, \beta)$ but does not divide $(\alpha^2 - \beta^2)^2 u_1 ... u_{n-1}$.

A Lehmer pair (α, β) such that $u_n(\alpha, \beta)$ has no primitive divisors will be called n-defective Lehmer pair. Further, a positive integer n is totally non-defective if no Lehmer pair is n-defective.

Two Lehmer pair (α_1, β_1) and (α_2, β_2) are equivalent if $\alpha_1/\alpha_2 = \beta_1/\beta_2 \in \{\pm 1, \pm\sqrt{-1}\}$. For equivalent Lehmer pairs, we have $u_n(\alpha_1, \beta_1) = \pm u_n(\alpha_2, \beta_2)$. Therefore, one of them is n-defective if and only if the other is.

Lemma 2.17 [1, 18].

Let n satisfy $7 \le n \le 30$ and $2 \not| n$. Then, up to equivalence,all n-defective Lehmer pairs are of the form $(\sqrt{a}-\sqrt{b})/2, (\sqrt{a}+\sqrt{b})/2)$, where n, a, b are given below:

(i) $n = 7$, $(a,b) = (1,-7), (1,-19), (3,-5), (5,-7), (13,-3), (14,-22)$;

(ii) $n = 9$, $(a,b) = (5,-3), (7,-1), (7,-5)$;

(iii) $n = 13$,$(a,b) = (1,-7)$;

(iv) $n = 15$,$(a,b) = (7,-1), (10,-2)$.

Lemma 2.18 ([2], Theorem 1.4) *If $n > 30$, then n is totally non-defective.*

3 The solutions of (1.1) with $2 \not| m$

Let $\min(D_1, D_2) > 1$, and let (x, m, n) be a solution of (1.1) with $2 \not| m$. Then (2.1) has the solution

$$(X, Y, Z) = (x, D_2^{(m-1)/2}, n). \tag{3.1}$$

Since $\min(D_1, D_2) > 1$, by (ii) of Lemma 2.7, we get from (3.1) that

$$n = Z_1 t, t \in \mathbb{N}, 2 \not| t, \tag{3.2}$$

$$x\sqrt{D_1} + D_2^{(m-1)/2}\sqrt{-D_2} = \lambda_1 (X_1\sqrt{D_1} + \lambda_2 Y_1 \sqrt{-D_2})^t, \lambda_1, \lambda_2 \{-1, 1\}, \tag{3.3}$$

where (X_1, Y_1, Z_1) is the least solution of (2.1).

Lemma 3.1 $t \in \{1, 3\}$ *for* (3.2).

Proof: Let

$$\alpha = X_1\sqrt{D_1} + Y_1\sqrt{-D_2}, \beta = X_1\sqrt{D_1} - Y_1\sqrt{-D_2}. \tag{3.4}$$

Since

$$D_1 X_1^2 + D_2 Y_1^2 = p^{Z_1}, X_1, Y_1, Z_1 \in \mathbb{N}, \gcd(D_1 X_1^2, D_2 Y_1^2) = 1, \tag{3.5}$$

we see from (3.4) that α and β are roots of $z^4 - 2(D_1X_1^2 - D_2Y_1^2)z^2 + p^{2Z_1} = 0$, and hence, they are algebraic integers. Notice that $(\alpha+\beta)^2 = 4D_1X_1^2$ and $\alpha\beta = p^{Z_1}$ are coprime positive integers, $\alpha/\beta = ((D_1X_1^2 - D_2Y_1^2) + 2X_1Y_1\sqrt{-D_1D_2})/p^{Z_1}$ and it satisfies $p^{Z_1}(\alpha/\beta)^2 - 2(D_1X_1^2 - D_2Y_1^2)(\alpha/\beta) + p^{Z_1} = 0$, where $p^{Z_1} > 1$ and $\gcd(p^{Z_1}, 2(D_1X_1^2 - D_2Y_1^2)) = 1$, so α/β is not a root of unity. Therefore, (α, β) is a Lehmer pair with parameter $(a, b) = (4D_1X_1^2, -4D_2Y_1^2)$. Let $u_n(\alpha, \beta) (n \in \mathbb{N})$ be the corresponding Lehmer numbers defined as in (2.7). From (3.3) and (3.4), we get

$$D_2^{(m-1)/2} = Y_1 |u_t(\alpha, \beta)|. \tag{3.6}$$

Since $(\alpha^2 - \beta^2)^2 = -16D_1D_2X_1^2Y_1^2$, we see from (3.6) that the Lehmer number $u_t(\alpha, \beta)$ has no primitive divisor. Therefore, by Lemmas (2.17) and (2.18), we obtain $t \le 5$.

We are now to remove the case $t = 5$. For this case, by (3.2) and (3.3) we have $n = 5Z_1$ and

$$D_2^{(m-1)/2} = Y_1|5(D_1X_1^2)^2 - 10(D_1X_1^2)(D_2Y_1^2) + (D_2Y_1^2)^2|. \tag{3.7}$$

If $m = 1$, then from (3.7) we get $Y_1 = 1$. Hence, by (3.5), (2.2) has two solutions $(y, z) = (X_1, Z_1)$ and $(x, 5Z_1)$. But, by Lemma 2.9, it is impossible.

If $m > 1$ and $5 \nmid D_2$, since $\gcd(D_1X_1^2, D_2Y_1^2) = 1$, then from (3.7) we get $Y_1 = D_2^{(m-1)/2}$ and

$$4D_2^{2m} - 5(D_1X_1^2 - D_2^m)^2 = -1. \tag{3.8}$$

Notice that $D_2 > 1$ and $L_3 = 4$, we infer from Lemma 2.1 that $4D_2^m = L_{6l+3}$ for some positive integer l. Thus, we can simply exclude this case by applying Lemma 2.2 or 2.3 according to whether D_2 is a power of 2 or not.

If $m > 1$ and $5|D_2$, then we have $Y_1 = \frac{1}{5}D_2^{(m-1)/2}$ and

$$(D_1X_1^2 - D_2Y_1^2)^2 - 20(\frac{1}{5}D_2Y_1^2)^2 = 1. \tag{3.9}$$

Notice that $D_2 > 1$ and $F_6 = 8$, we infer from Lemma 2.1 that

$$\frac{4}{5}D_2Y_1^2 = \frac{4}{125}D_2^m = F_{6l+6}, l \in \mathbb{N}, \tag{3.10}$$

then we have $\min(\frac{1}{2}F_{3l+3}, \frac{1}{2}L_{3l+3}) > 1$. Using (ii) and (iii)of Lemma 2.1 on (3.10), we get either $F_{3l+3} = 2z^m$ or $L_{3l+3} = 2z^m$ with some positive integer $z > 1$. We can also exclude this case by applying Lemma 2.2 or 2.3 according to whether z is a power of 2 or not. Thus, we get $t \neq 5$ and $t \in \{1, 3\}$. The lemma is proved. □

Let $N_1(D_1, D_2, p)$ denote the number of solutions of (1.1) with $2 \nmid m$. Then we have

Lemma 3.2 $N_1(D_1, D_2, p) \leq 1$ *except for the following three cases:*

(i)

$$3D_1X_1^2 = D_2Y_1^2 + \lambda, Y_1 = D_2^l, \lambda \in \{-1, 1\}, l \in \mathbb{Z}, l \geq 0, \tag{3.11}$$

$$(x, m, n) \in \{(X_1, 2l + 1, Z_1), (X_1(8D_1X_1^2 - 3\lambda), 2l + 1, 3Z_1)\}.$$

(ii)

$$D_1X_1^2 = 3^l + 1, D_2 = 3, Y_1 = 1, p = 3^l + 4, l \in \mathbb{Z}, l \geq 0, \tag{3.12}$$

$$(x, m, n) \in \{(X_1, 1, 1), (X_1|3^l - 8|, 2l + 3, 3)\}.$$

(iii)

$$D_1X_1^2 = 3^{2l} + 1, D_2 = 3, Y_1 = 3^l, p = 4 \cdot 3^{2l} + 1, l \in \mathbb{Z}, l \geq 0, \tag{3.13}$$

$$(x, m, n) \in \{(X_1, 2l + 1, 1), (X_1(8 \cdot 3^{2l} - 1), 2l + 3, 3)\}.$$

Proof: By Lemmas 2.8 and 3.1, we have $N_1(D_1, D_2, p) \leq 2$. Moreover, by Lemma 3.1, if (1.1) has two solutions (x_1, m_1, n_1) and (x_2, m_2, n_2) with $n_1 < n_2$ and $2 \nmid m_1 m_2$, then

$$x_1 = X_1, Y_1 = D_2^{(m_1-1)/2}, n_1 = Z_1 \tag{3.14}$$

and

$$x_2 = X_1|3D_1X_1^2 - D_2Y_1^2|, D_2^{(m_2-1)/2} = Y_1|3D_1X_1^2 - D_2Y_1^2|, n_2 = 3Z_1. \tag{3.15}$$

By (3.14) and (3.15), we get

$$D_2^{(m_2-m_1)/2} = |3D_1X_1^2 - D_2^{m_1}|. \tag{3.16}$$

When $m_2 = m_1$, by (3.14) ,(3.15) and (3.16), we obtain the case (i) immediately.

When $m_2 > m_1$, we see from (3.16) that $3|D_2$ and

$$\frac{1}{3}D_2^{(m_2-m_1)/2} = |D_1X_1^2 - \frac{1}{3}D_2^{m_1}|. \tag{3.17}$$

Further, since $\gcd(D_1X_1^2, D_2Y_1^2) = 1$, we get from (3.17) that $D_2 = 3$ and either $m_1 = 1$ or $m_2 = m_1 + 2$.

If $m_1 = 1$, then from (3.14) and (3.17) we obtain

$$D_2Y_1^2 = 3, D_1X_1^2 = 3^l + 1, l = \frac{1}{2}(m_2 - m_1) - 1. \tag{3.18}$$

Substitute (3.18) into (3.5), we have

$$p^{Z_1} = 3^l + 4. \tag{3.19}$$

By applying Lemma 2.15 to (3.19), we get $Z_1 = 1$. Thus, by (3.18) and (3.19), we obtain the case (ii).

If $m_2 = m_1 + 2$, then from (3.14) and (3.17) we obtain

$$D_2Y_1^2 = 3^{2l+1}, D_1X_1^2 - 3^{2l} = \lambda, l = \frac{1}{2}(m_1 - 1), \lambda \in \{-1, 1\}. \tag{3.20}$$

Substitute (3.20) into (3.5), we have

$$p^{Z_1} = 4 \cdot 3^{2l} + \lambda. \tag{3.21}$$

Further, since p is an odd prime, if $\lambda = -1$, then from (3.21) we get $2 \cdot 3^l + 1 = p^{Z_1}$ and $2 \cdot 3^l - 1 = 1$. It implies that $l = 0$ and $p = 3$, which contradicts the assumption $p \nmid D_1 D_2$. So we have $\lambda = 1$. By applying Lemma 2.16 to (3.21), we get $Z_1 = 1$. Thus, we obtain the case (iii). The lemma is proved. □

4 The solutions of (1.1) with $2|m$

Let $\min(D_1, D_2) > 1$, and let (x, m, n) be a solution of (1.1) with $2|m$. Then the equation

$$D_1 X'^2 + D_2^2 Y'^2 = p^{Z'}, X', Y', Z' \in \mathbb{Z}, \gcd(X', Y') = 1, Z' > 0 \tag{4.1}$$

has the solution

$$(X', Y', Z') = (x, D_2^{(m-2)/2}, n). \tag{4.2}$$

Since $\min(D_1, D_2) > 1$, by applying Lemma 2.7 to (4.1) and (4.2), we have

$$n = Z_1' t', t' \in \mathbb{N}, 2 \not| t', \tag{4.3}$$

$$x\sqrt{D_1} + D_2^{(m-2)/2}\sqrt{-D_2^2} = \lambda_1 (X_1'\sqrt{D_1} + \lambda_2 Y_1'\sqrt{-D_2^2})^{t'}, \lambda_1, \lambda_2 \{-1, 1\}, \tag{4.4}$$

where (X_1', Y_1', Z_1') is the least solution of (4.1). Using the same method as in the proof of Lemma 3.1, we can prove a similar result as follows.

Lemma 4.1 $t' \in \{1, 3\}$ *for* (4.3).

Let $N_2(D_1, D_2, p)$ denote the number of solutions (x, m, n) of (1.1) with $2|m$. Then we have

Lemma 4.2 $N_2(D_1, D_2, p) \leq 1$ *except for*

$$D_1 X_1'^2 = 3^{2l-1} + \lambda, D_2 = 3, Y_1' = 3^{l-1}, p = 4 \cdot 3^{2l-1} + \lambda, \lambda \in \{-1, 1\}, \tag{4.5}$$

where l is a positive integer.

Proof: By Lemma 4.1, we have $N_2(D_1, D_2, p) \leq 2$. Moreover, If (1.1) has two solutions (x_1, m_1, n_1) and (x_2, m_2, n_2) such that $2|m_1$, $2|m_2$ and $n_1 < n_2$, then, from (4.4) we have

$$x_1 = X_1', Y_1' = D_2^{(m_1-2)/2}, n_1 = Z_1' \tag{4.6}$$

and

$$x_2 = X_1'|D_1 X_1'^2 - 3D_2^2 Y_1'^2|, D_2^{(m_2-2)/2} = Y_1'|3D_1 X_1'^2 - D_2^2 Y_1'^2|, n_2 = 3Z_1'. \tag{4.7}$$

By (4.6) and (4.7), we get

$$D_2^{(m_2-m_1)/2} = |3D_1 X_1'^2 - D_2^{m_1}|. \tag{4.8}$$

When $m_2 = m_1$, since $2|m_1$, by taking modulo 3 on two sides of (4.8), we obtain

$$3D_1 X_1'^2 = D_2^{m_1} - 1. \tag{4.9}$$

Since $D_1 X_1'^2 + D_2^2 Y_1'^2 = D_1 X_1'^2 + D_2^{m_1} = p^{Z_1'}$, we get from (4.9) that $3p^{Z_1'} = 4D_2^{m_1} - 1 = (2D_2^{m_1/2} + 1)(2D_2^{m_1/2} - 1)$. Further, since $\gcd(2D_2^{m_1/2} + 1, 2D_2^{m_1/2} - 1) = 1$ and $2D_2^{m_1/2} + 1 >$

$2D_2^{m_1/2}-1\geq 3$, we get $2D_2^{m_1/2}+1=p^{Z_1'}, 2D_2^{m_1/2}-1=3$. It implies that $D_2^{m_1/2}=2$ and $D_1=1$ by (4.9), a contradiction to $D_1>1$.

When $m_2>m_1$, we see from (4.8) that $D_2=3, m_2=m_1+2$ and

$$D_1{X_1'}^2=3^{m_1-1}+\lambda, \lambda\in\{-1,1\}. \tag{4.10}$$

Put $l=m_1/2$. By (4.6) and (4.10), we get the first three equalities of (4.5). Substituting them into (4.1), we get $4\cdot 3^{2l-1}+\lambda=p^{Z_1'}$. By Lemma 2.16, we have $Z_1'=1$, and the 4th equality of (4.5) follows. Thus, the lemma is proved. □

5 Further lemmas on the solutions of (1.1)

Lemma 5.1 *If D_1, D_2 and p satisfy* (3.11) *with $\lambda=1$, then $N_2(D_1,D_2,p)=0$.*

Proof: Under the assumption, we have $3D_1X_1^2=D_2^{2l+1}+1$ and

$$p^{Z_1}=4D_1X_1^2-1. \tag{5.1}$$

By (5.1), we get $p^{Z_1}\equiv 3 \pmod 4$, which implies that $p\equiv 3 \pmod 4$. We suppose that (1.1) has a solution (x,m,n) with $2|m$. Then we have $(-D_1/p)=1$, where $(*/*)$ denotes the Jacobi symbol. But, by (5.1) , we get

$$1=\left(\frac{-D_1}{p}\right)=-\left(\frac{D_1}{p}\right)=-\left(\frac{4D_1X_1^2}{p}\right)=-\left(\frac{p^{Z_1}+1}{p}\right)=-\left(\frac{1}{p}\right)=-1,$$

a contradiction. Thus, we have $N_2(D_1,D_2,p)=0$. The lemma is proved. □

Lemma 5.2 ([19]). *Let $a\in\mathbb{N}$. If $4a+1$ is a power of p, then the equation*

$$ax^2+(3a+1)^m=(4a+1)^n$$

has no solution (x,m,n) with $2|m$ except for $a=1$ or 2.

Lemma 5.3 . *The equation*

$$6u^2+1801^{2r}=7^s, u,r,s\in\mathbb{N} \tag{5.2}$$

has no solution (u,r,s).

Proof: We suppose that (5.2) has a solution (u,r,s). If $4|s$, then we have $6u^2\equiv 7^s-1801^{2r}\equiv 0 \pmod{200}$. It implies that $10|u$ and therefore $u=10v$, where $v\in\mathbb{N}$. Substitute it into (5.2) , we get $600v^2+1801^{2r}=7^s$. But, since $4|s, 1801=3\cdot 600+1$ and $4\cdot 600+1=7^4$, by Lemma 5.2, it is impossible.

If $2||s$, then we have $u^2\equiv 6u^2\equiv 7^s-1801^{2r}\equiv 3 \pmod 5$. But, since $(3/5)=-1$, it is impossible. Therefore, we obtain $2\nmid s$.

We see from (5.2) that the equation

$$X^2 + 6Y^2 = 7^Z, X, Y, Z \in \mathbb{Z}, \gcd(X, Y) = 1, Z > 0 \tag{5.3}$$

has the solution $(X, Y, Z) = (1801^r, u, s)$. Since the least solution of (5.3) is $(X_1, Y_1, Z_1) = (1, 1, 1)$, by (ii) of Lemma 2.7, we have

$$1801^r + u\sqrt{-6} = \lambda_1(1 + \lambda_2\sqrt{-6})^s, \lambda_1, \lambda_2 \in \{-1, 1\}. \tag{5.4}$$

Let $\theta = 1 + \sqrt{-6}$ and $\overline{\theta} = 1 - \sqrt{-6}$. By (5.4), we get

$$1801^r = \frac{1}{2}|\theta^s + \overline{\theta}^s|. \tag{5.5}$$

Notice that $\frac{1}{2}|\theta^3 + \overline{\theta}^3| = 17, \frac{1}{2}|\theta^5 + \overline{\theta}^5| = 121, 2 \not| s$ and 1801 is an odd prime. We find from (5.5) that

$$\gcd(30, s) = 1. \tag{5.6}$$

On the other hand, we see from (5.2) that the equation

$$6x^2 + (1801^2)^m = 7^n, x, m, n \in \mathbb{N} \tag{5.7}$$

has the solution $(x, m, n) = (u, r, s)$. Therefore, since $3 \not| s$, by Lemma 4.1, we have $s = Z_1'$, where (X_1', Y_1', Z_1') is the least solution of (4.1) for $(D_1, D_2, p) = (6, 1801, 7)$. By (i) of Lemma 2.7, we get $2Z_1'|h(-4 \cdot 6 \cdot 1801^2)$. But, by Lemmas 2.4 , 2.5 and 2.6, we can calculate that $h(-4 \cdot 6 \cdot 1801^2) = 3600$, a contradiction. Thus, the lemma is proved. □

Lemma 5.4 ([8],in the proof of Lemma 2). *The equation*

$$1 + 3x^2 = y^n, x, y, n \in \mathbb{N}, n > 2$$

has no solution (x, y, n).

Lemma 5.5 . *If positive integers* X, Z *satisfy*

$$1 + 12X^2 = p^Z, \tag{5.8}$$

then the equation

$$(9X^2 + 1)^m + 3x^2 = p^n, x, m, n \in \mathbb{N}, 2|m \tag{5.9}$$

has no solution (x, m, n).

Proof: By (5.8) and Lemma 5.4, we get $Z = 1$ or 2. Let (x, m, n) be a solution of (5.9). If $(1, 2X, Z)$ is the least solution of (2.1) for $d_1 = 1, d_2 = 3$, then $Z|n$. By (5.9), we have $X|x$. From Lemma 5.2 applied for $a = 3X^2$, we know that m must be odd, a contradiction. Arguing in the same way, we can prove that (5.9) has no solution with $2|n$.

Now, we suppose that n is odd. If $(1, 2X, Z)$ is not the least solution of (2.1) for $d_1 = 1, d_2 = 3$, by Lemma 2.8 we have

$$1 + 12X^2 = p^2 \tag{5.10}$$

and there are two positive integers A and B such that $(A, B, 1)$ is the least solution of (2.1) for $d_1 = 1, d_2 = 3$. Then

$$A^2 + 3B^2 = p. \tag{5.11}$$

If $2 \not| X$. By (5.9) we get $p \equiv -1 \pmod 8$ and therefore $p^2 \equiv 1 \pmod 8$. By (5.10) we get $p^2 \equiv 5 \pmod 8$, a contradiction.

If $2|X$. By (5.9) we get $p \equiv 1 \pmod 4$. By (5.10) we get $p^2 \equiv 1 \pmod{16}$. Thus, $p \equiv 1 \pmod 8$ and therefore $4|B$.

On using Lemma2.7, we have

$$1 + 2X\sqrt{-3} = \lambda_1'(A \pm \sqrt{-3}B)^2 \tag{5.12}$$

and

$$(9X^2 + 1)^{m/2} + x\sqrt{-3} = \lambda_1'{}'(A \pm \sqrt{-3}B)^n. \tag{5.13}$$

Notice that $4|B$ and $2 \not| n$, we can simple exclude $\lambda_1', \lambda_1'{}' \in \{\pm i, \pm\frac{1\pm\sqrt{-3}}{2}\}$. So we have $\lambda_1', \lambda_1'{}' \in \{-1, 1\}$.

Now,we can deduce from (5.12) and (5.13)that

$$A|X, A^2 - 3B^2 = \pm 1, \tag{5.14}$$

and any prime factor of A is a factor of $9X^2 + 1$. So we get $A = 1$ and $3B^2 = 0$ or 2, a contradiction. Thus, the lemma is proved. □

Lemma 5.6 . *Let $D_1 > 1$. If D_1, D_2 and p satisfy* (3.11) *with $\lambda = -1$, then $N_2(D_1, D_2, p) = 0$ except for $(D_1, D_2, p) = (2, 7, 3)$.*

Proof: Under the assumption, we have

$$3D_1X_1^2 = D_2^{2l+1} - 1, l > 0 \tag{5.15}$$

and

$$4D_1X_1^2 + 1 = p^{Z_1}. \tag{5.16}$$

We see from (5.16) that the equation

$$A^2 + D_1B^2 = p^C, A, B, C \in \mathbb{Z}, \gcd(A, B) = 1, C > 0 \tag{5.17}$$

has the solution $(A, B, C) = (1, 2X_1, Z_1)$. Let (A_1, B_1, C_1) be the least solution of (5.17), by Lemma 2.10, one of the following three conditions must be satisfied:

$$(A_1, B_1, C_1) = (1, 2X_1, Z_1); \tag{5.18}$$

$$(|A_1^2 - D_1B_1^2|, 2A_1B_1, 2C_1) = (1, 2X_1, Z_1); \tag{5.19}$$

$$D_1 = 6, p = 7, X_1 = 10, Z_1 = 4. \tag{5.20}$$

We now suppose that (1.1) has a solution (x, m, n) with $2|m$. Then (5.17) has the solution $(A, B, C) = (D_2^{m/2}, x, n)$. From (5.15) and (5.16) one can easily exclude $D_1 = 3$ for $l > 0$ or $l = 0$ by Lemma 2.12 and Lemma 5.5. By applying (ii) of Lemma 2.7, we get

$$n = C_1 t, t \in \mathbb{N}, \tag{5.21}$$

$$D_2^{m/2} + x\sqrt{-D_1} = \lambda_1(A_1 + \lambda_2 B_1\sqrt{-D_1})^t, \lambda_1, \lambda_2 \in \{-1, 1\}. \tag{5.22}$$

For the case (5.18), (5.21) and (5.22) can be written as

$$n = Z_1 t, t \in \mathbb{N}, \tag{5.23}$$

$$D_2^{m/2} + x\sqrt{-D_1} = \lambda_1(1 + 2\lambda_2 X_1\sqrt{-D_1})^t, \lambda_1, \lambda_2 \in \{-1, 1\} \tag{5.24}$$

respectively. By (5.24), we get $2X_1|x$. So we have $x = 2X_1 y$ with $y \in \mathbb{N}$. Substituting it into (1.1), we get

$$(D_1 X_1^2)(2y)^2 + D_2^m = p^n. \tag{5.25}$$

Hence, by (5.16), (5.23) and (5.25), we obtain

$$D_2^m \equiv 1 \pmod{D_1 X_1^2}. \tag{5.26}$$

Let $m = (2l + 1)q + \delta$, where $q, \delta \in \mathbb{Z}$ with $0 \le \delta < 2l + 1$. Since $D_2^{2l+1} \equiv 1 \pmod{D_1 X_1^2}$ by (5.15), we see from (5.26) that

$$D_2^\delta \equiv 1 \pmod{D_1 X_1^2}. \tag{5.27}$$

If $\delta > 0$, since $D_2 > 1$ and $\delta \le 2l$, then from (5.15) and (5.27) we get $D_2^{2l} - 1 \ge D_2^\delta - 1 \ge D_1 X_1^2 = \frac{1}{3}(D_2^{2l+1} - 1)$. It implies that $D_2^{2l}(3 - D_2) \ge 2$ and $D_2 = 2$. However, it is impossible by taking modulo 3 on (5.15).

If $\delta = 0$, then we have $2l + 1|m$. Hence, by (5.25), the equation

$$(D_1 X_1^2)x'^2 + (D_2^{2l+1})^{m'} = p^{n'}, x', m', n' \in \mathbb{N}$$

has the solution $(x', m', n') = (2y, m/(2l + 1), n)$ with $2|m'$ and $Z_1|n'$. But, since $D_2^{2l+1} = 3D_1 X_1^2 + 1$, from (5.16) and Lemma 5.2 applied for $a = D_1 X^2$, it is impossible except for $(D_1 X_1^2, D_2^{2l+1}, p) = (2, 7, 3)$. Thus, the lemma holds for the case (5.18).

For the case (5.19), we have

$$A_1^2 - D_1 B_1^2 = \lambda', \lambda' \in \{-1, 1\} \tag{5.28}$$

and

$$A_1 B_1 = X_1, C_1 = \frac{1}{2} Z_1. \tag{5.29}$$

From (5.21) and (5.29), we get

$$n = \frac{Z_1}{2} t, t \in \mathbb{N}. \tag{5.30}$$

If $2 \nmid t$, then from (5.22) we get $A_1 | D_2^{m/2}$. Further, since $\gcd(D_1 X_1^2, D_2 Y_1^2) = 1$, by (5.29), we obtain $A_1 = 1$ and $B_1 = X_1$. By (5.28), we have $D_1 = 2$ and $X_1 = 1$. Hence, by (5.15) and (5.16), we get $(D_1, D_2, p) = (2, 7, 3)$.

If $2|t$, since $(A_1 + B_1\sqrt{-D_1})^2 = \lambda' + 2X_1\sqrt{-D_1}$, then (5.22) can be written as

$$D_2^{m/2} + x\sqrt{-D_1} = \lambda_1(\lambda' + 2\lambda_2 X_1\sqrt{-D_1})^{t/2}, \frac{t}{2} \in \mathbb{N}, \lambda_1, \lambda_2, \lambda' \in \{-1, 1\}, \tag{5.31}$$

whence we get $2X_1|x$ and $x = 2X_1 y$ with $y \in \mathbb{N}$. Therefore, by (1.1), the solution (x, m, n) also satisfies (5.25). Further, by (5.16), (5.25) and (5.30), we obtain (5.26) again. Thus, using the same method as in the proof of the case (5.18), we can deduce that the lemma is true for the case.

For the case (5.20), by (5.15) and (5.16), we have $D_2 = 1801$. Then, by Lemma 5.3, (1.1) has no solution (x, m, n) with $2|m$. Thus, the lemma is proved. □

Using the same method as in the proof of Lemma 5.6, we can prove the following two lemmas.

Lemma 5.7 ([9],(ii) of Theorem 3.3.2). *If D_1, D_2 and p satisfy* (3.12) *or* (3.13)*, then $N_2(D_1, D_2, p) = 0$ except for $N_2(10, 3, 13) = N_2(10, 3, 37) = 1$.*

Lemma 5.8 ([9],(i) of Theorem 3.3.2). *If D_1, D_2 and p satisfy* (4.5)*, then $N_1(D_1, D_2, p) = 0$ for $\lambda = 1$, and $N_1(D_1, D_2, p) = 1, (x, m, n) = (2X_1', 1, 1)$ for $\lambda = -1$.*

6 Proof of Theorem B

Notice that the conditions (3.11),(3.12),(3.13) and (4.5) are independent from each other. Since $N(D_1, D_2, p) = N_1(D_1, D_2, p) + N_2(D_1, D_2, p)$, by Lemma 3.2 and 4.2, we have $N(D_1, D_2, p) \leq 3$. Further, by Lemmas 5.1, 5.6, 5.7 and 5.8, all the pairs (D_1, D_2, p) of $N(D_1, D_2, p) = 3$ are determined. Thus, the theorem is proved.

Acknowledgments

The authors are grateful to the referees for their valuable suggestions.

References

[1] M. Abouzaid, Les nombres de Lucas et Lehmer sans diviseur primitif, J. Number Theory de Bordeaux, 2006, **18(2):** 299-313.

[2] Y.Bilu, G.Hanrot and P.M.Voutier (with an appendix by M.Mignotte), Existence of primitive divisors of Lucas and Lehmer numbers, J Reine Angew Math., 2001, **539**:75-122.

[3] E.Brown, Diophantine equation of form $ax^2 + b^2D = y^p$, J.Reine Angew.Math., 1977, **291:**110-127.

[4] E.Brown, Diophantine equation of form $x^2 + D = y^n$, J.Reine Angew.Math., 1975, **274/275:**385-389.

[5] Y.Bugeaud, On some exponential diophantine equations, Monatsh.Math.,2001, **132(1):** 93-97.

[6] Y.Bugeaud, M.Mignotte and S.Siksek, Sur les nombres de Fibonacci de la forme $q^k y^p$, C.R.Math.Acad.Sci.Paris, 2004, **339(5):** 327-330.

[7] Y.Bugeaud, M.Mignotte and S.Siksek, Classical and modular approaches to exponential diophantine equations I:Fibonacci and Lucas perfect powers, Ann. Math. ,2006, **163(2):** 969-1018.

[8] Y.Bugeaud , T.N.Shorey, On the number of solutions of the generalized Ramanujan-Nagell equation, J.Reine Angew.Math., 2001, **539:**, 55-74.

[9] Y.-Z.Hu, Applications of the theorem about the existence of primitive divisors of Lucas and Lehmer numbers to exponential diophantine equations, PhD thesis, Central South University,2006.

[10] L.-G.Hua, Introduction to number theory, Berlin:Springer Verlag,1982.

[11] C.Ko, On the diophantine equation $x^2 = y^n + 1, xy \neq 0$, Sci Sinica, 1964, **14:** 457-460.

[12] M.-H. Le, The diophantine equation $x^2 + D^m = p^n$, Acta Arith, 1989, **52(3):** 255-265.

[13] V.A.Lebesgue, Sur l'impossibilite,en nombres entiers,de l'equation $x^m = y^2 + 1$, Nouv Ann Math., 1850, **9(1):**178-181.

[14] M.-G.Leu and G.-W.Li, The diophantine equation $2x^2 + 1 = 3^n$, Proc.Amer.Math.Soc., 2003, **131(12):** 3643-3645.

[15] W.Ljunggen, Einige Benerkungen uber die Darstellung genzer Zahlen durch binare kubische Formen mit positiver Diskriminante, Acta Math., 1942, **75(1):**1-21.

[16] L.J.Mordell, Diophantine equations, London: Academic Press,1969.

[17] T.Nagell, Contributions to the theory of a category of diophantine equations of the second degree with two unknowns, Nova Acta Regiae Soc Sci Upsaliensis(4), 1955, **16(2):** 1-38.

[18] P.M.Voutier, Primitive divisors of Lucas and Lehmer sequences, Math.Comp, 1995, **64**:869-888.

[19] P.-Z.Yuan and Y.-Z.Hu, On the diophantine equation $x^2 + D^m = p^n$, J.Number Theory, 2005, **111(2)**:144-153.

[20] P.-Z.Yuan and Y.-Z.Hu, On the diophantine equation $ax^2 + (3a + 1)^m = (4a + 1)^n$, Bull.Math.Soc.Sci.Math.Roumanie, 2010, **53(1)**:51-59.

Received: 09.09.2010, Revised:18.02.2012, Accepted: 02.03.2012.

Department of Mathematics, Foshan University, Foshan,Guangdong 528000,China,
E-mail: `huuyz@yahoo.com.cn`

Department of Mathematics, Zhanjiang Normal College, Zhanjiang,Guangdong 524048,China
E-mail: `lemaohua2008@163.com`