Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 4(4): 1170–1180.
DOI:10.3934/math.2019.4.1170
Received: 03 April 2019
Accepted: 14 July 2019
Published: 19 August 2019

Research article

On the Diophantine equations $x^2 - Dy^2 = -1$ and $x^2 - Dy^2 = 4$

Bingzhou Chen and Jiagui Luo*

School of Mathematics and Information, China West Normal University, Nanchong 637009, P. R. China

* **Correspondence:** Email: Luojg62@aliyun.com.

Abstract: In this paper, using only the Störmer theorem and its generalizations on Pell's equation and fundamental properties of Lehmer sequence and the associated Lehmer sequence, we discuss the Diophantine equations $x^2 - Dy^2 = -1$ and $x^2 - Dy^2 = 4$. We obtain the relation between a positive integer solution (x, y) of the Diophantine equation $x^2 - Dy^2 = -1$ and its fundamental solution if there is exactly one or two prime divisors of y not dividing D. We also obtain the relation between a positive integer solution (x, y) of the Diophantine equation $x^2 - Dy^2 = 4$ and its minimal positive solution if there is exactly two prime divisors of y not dividing D.

Keywords: Diophantine equations; Pell equations; minimal solutions; Lehmer sequences
Mathematics Subject Classification: 11D25, 11B39

1. Introduction

Throughout our paper, we let Z, N denote the sets of integers and positive integers respectively. We recall that the minimal positive solution of Diophantine equation

$$x^2 - Dy^2 = C, C \in \{-1, 4\} \tag{1.1}$$

is one of all positive integer solutions (x, y) such that $x + y\sqrt{D}$ is the smallest. One can easily find that the condition is equivalent to saying that (x, y) is a positive integer solutions of (1.1) such that x and y are the smallest. If $C = -1$, then such a solution is also called the fundamental solution of (1.1).

Störmer had ever obtained an important property on Pell's equation, called Störmer theory and stated it as follow

Theorem 1.1. (Störmer theorem [1]) *Let D be a positive nonsquare integer. Let (x_1, y_1) be a positive integer solution of Pell equation*

$$x^2 - Dy^2 = \pm 1. \tag{1.2}$$

If every prime factor of y_1 divides D, then $x_1 + y_1\sqrt{D}$ is the fundamental solution.

Consider the Diophantine equation

$$kx^2 - ly^2 = 1, \tag{1.3}$$

where $k > 1, l$ are relatively prime positive integers such that kl is not square. Qi Sun, Pingzhi yuan obtained the similar result with Störmer theorem.

Theorem 1.2. [10] *Let (x, y) be a positive integer solution of Diophantine equation (1.3).*
(i) If every prime factor x divides k, then

$$x\sqrt{k} + y\sqrt{l} = \varepsilon$$

or

$$x\sqrt{k} + y\sqrt{l} = \varepsilon^3,$$

and $x = 3^s x_1, 3^s + 3 = 4kx_1^2, 3 \nmid x_1, s \in \mathbb{N}, 2|s$, where $\varepsilon = x_1\sqrt{k} + y_1\sqrt{l}$ is the minimal positive solution of equation (1.3).
(ii) If every prime factor of y divides l, then

$$x\sqrt{k} + y\sqrt{l} = \varepsilon$$

or

$$x\sqrt{k} + y\sqrt{l} = \varepsilon^3,$$

and $y = 3^s y_1, 3^s - 3 = 4ly_1^2, 3 \nmid y_1, s \in \mathbb{N}, 2 \nmid s$.

Using the method of [10], Jiagui Luo proved the following

Theorem 1.3. [3] *Let (x, y) be a positive integer solution of Diophantine equation*

$$kx^2 - ly^2 = 2, \tag{1.4}$$

where k, l are odd positive integers such that kl is not square.
(i) If every prime factor of x divides k, then

$$x\sqrt{k} + y\sqrt{l} = \varepsilon$$

or

$$\frac{x\sqrt{k} + y\sqrt{l}}{\sqrt{2}} = \left(\frac{\varepsilon}{\sqrt{2}}\right)^3,$$

and $x = 3^s x_1, 3^s + 3 = 2kx_1^2$, where $\varepsilon = x_1\sqrt{k} + y_1\sqrt{l}$ is the minimal positive solution of equation (1.4), $s \in \mathbb{N}$.
(ii) If every prime factor of y divides l, then

$$x\sqrt{k} + y\sqrt{l} = \varepsilon$$

or

$$\frac{x\sqrt{k} + y\sqrt{l}}{\sqrt{2}} = \left(\frac{\varepsilon}{\sqrt{2}}\right)^3,$$

and $y = 3^s y_1, 3^s - 3 = 2ly_1^2, s \in \mathbb{N}$.

Theorem 1.4. [3] *Let (x, y) be a positive integer solution of Diophantine equation*

$$kx^2 - ly^2 = 4, \tag{1.5}$$

where k, l are odd positive integers such that kl is not square.
(i) If every prime factor of x divides k, then $x\sqrt{k} + y\sqrt{l} = \varepsilon$ is the minimal solution of equation (1.5) except for the case $(k, l, x, y) = (5, 1, 5, 11)$.
(ii) If every prime factor of y divides l, then $x\sqrt{k} + y\sqrt{l} = \varepsilon$ is the minimal solution of equation (1.5).

Remark From the proofs of Theorem 1.2, 1.3, 1.4 in [3, 10], one can easily find that the above Theorems are also true if every prime divisor of x divides one of k and x_1, so are done if every prime divisor of y divides one of l and y_1.

In 2011, Luo, Togbe and Yuan obtained the following

Theorem 1.5. [5] *Let D be a positive nonsquare integer such that the Diophantine equation*

$$x^2 - Dy^2 = 4, \tag{1.6}$$

is solvable in odd integers x and y. Let (x, y) be a positive integer solution of Pell equation (1.6) with $y = p^n y'$, where p is a prime not dividing D and $n \in \mathbb{N}$. If every prime factor of y' divides D, then $\frac{x+y\sqrt{D}}{2} = \frac{\varepsilon}{2}$ or $(\frac{\varepsilon}{2})^2$ or $(\frac{\varepsilon}{2})^3$ except for the case $(x, y, D) = (123, 55, 5)$, where $x_1 + y_1\sqrt{D} = \varepsilon$ is the minimal positive solution of (1.6).

In this paper, we prove the following

Theorem 1.6. *Let D be a positive nonsquare integer. Let (x, y) be a positive integer solution of Pell equation*

$$x^2 - Dy^2 = -1, \tag{1.7}$$

with $y = p^n y'$, where p is a prime not dividing D and $n \in \mathbb{N}$. If every prime factor of y' divides D, then $x + y\sqrt{D} = \varepsilon$ or ε^q, where $x_1 + y_1\sqrt{D} = \varepsilon$ is the fundamental solution of (1.7) and q is an odd prime which is not equal to p.

Theorem 1.7. *Let (x, y) be a positive integer solution of Pell equation with $y = p_1^{n_1} p_2^{n_2} y'$, where both p_1 and p_2 are primes not dividing D with $p_1 < p_2$ and $n_1, n_2 \in \mathbb{N}$. If every prime divisor of y' divides D, then $x + y\sqrt{D} = \varepsilon$ or ε^q or ε^{q^2}, where $x_1 + y_1\sqrt{D} = \varepsilon$ is the fundamental solution of (1.7) and q is an odd prime which is not equal to p_1 and p_2.*

Theorem 1.8. *Let (x, y) be a positive integer solution of Pell equation (1.6) with $y = p_1^{n_1} p_2^{n_2} y'$, where both p_1 and p_2 are primes not dividing D with $p_1 < p_2$ and $n_1, n_2 \in \mathbb{N}$. If every prime factor of y' divides D, then $\frac{x+y\sqrt{D}}{2} = \frac{\varepsilon}{2}$ or $(\frac{\varepsilon}{2})^2$ or $(\frac{\varepsilon}{2})^3$ or $(\frac{\varepsilon}{2})^4$ or $(\frac{\varepsilon}{2})^6$ or $(\frac{\varepsilon}{2})^q$, where $x_1 + y_1\sqrt{D} = \varepsilon$ is the minimal solution of (1.6), q is an odd prime different from p_1 and p_2.*

We organize this paper as follows. In Section 2, we present some lemmas which are needed in the proofs of our main results. Consequently, in Sections 3 to 5, we give the proofs of Theorem 1.6 to 1.8 respectively.

2. Lemmas

In this section, we present some lemmas that will be used later.

Lemma 2.1. [10] *All positive integer solutions of equation (1.7) are given by*

$$x + y\sqrt{D} = (x_1 + y_1\sqrt{D})^n, n \in \mathbb{N}, 2 \nmid n.$$

Lemma 2.2. [3] *All positive integer solutions of equation (1.6) are given by*

$$\frac{x + y\sqrt{D}}{2} = \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^n, n \in \mathbb{N}, 2 \nmid n.$$

Let $R > 0$, Q be nonzero coprime integers with $R - 4Q > 0$. Let α and β be the two roots of the trinomial $x^2 - \sqrt{R}x + Q$. The Lehmer sequence $\{P_n(R, Q)\}$ and the associated Lehmer sequence $\{Q_n(R, Q)\}$ with parameters R and Q are defined as follows:

$$P_n = P_n(R, Q) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta), & 2 \nmid n, \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2), & 2|n \end{cases}$$

and

$$Q_n = Q_n(R, Q) = \begin{cases} (\alpha^n + \beta^n)/(\alpha + \beta), & 2 \nmid n, \\ \alpha^n + \beta^n, & 2|n \end{cases}$$

For simplicity, in this paper we denote $(\alpha^{dr} - \beta^{dr})/(\alpha^d - \beta^d)$ and $(\alpha^r - \beta^r)/(\alpha - \beta)$ by $P_{r,d}$ and P_r respectively. Lehmer sequences and associated Lehmer sequences have many interesting properties and often raise in the study of exponential Diophantine equations. It is not difficult to see that P_n and Q_n are both positive integers for all positive integers n. The details can be seen in the references [2, 8, 11].

Lemma 2.3. [2] *Let m, n be positive integers and $d = \gcd(m, n)$. We have*

1. $\gcd(P_m, P_n) = P_d$.
2. $\gcd(Q_m, Q_n) = Q_d$ *if m/d and n/d are odd, and* 1 *or* 2 *otherwise.*
3. $\gcd(P_m, Q_n) = Q_d$ *if m/d is even, and* 1 *or* 2 *otherwise.*
4. *Let p be an odd prime. If $p^2|(\alpha - \beta)^2$, then $ord_p(P_n) = ord_p(n)$.*
5. *For odd integers r and d, we have* $\gcd(P_{r,d}, P_d)|r$.

Lemma 2.4. [2, 4] *If $2|P_n$, then we have*

1. $R = 4k, Q = 2l + 1, n = 2h$, *or*
2. $R = 2k, Q = 2l + 1, n = 4h$, *or*
3. $R = 4k \pm 1, Q = 2l + 1, n = 3h$.

Lemma 2.5. [6] *Assume that R and Q are all odd. If $Q_n = ku^2, k|n$, then $n = 1, 3, 5$. If $Q_n = 2ku^2, k|n$, then $n = 3$.*

Lemma 2.6. [7] *Let D be a positive nonsquare integer. Let $(x,\ y)$ be a positive integer solution of Pell equation*

$$x^2 - Dy^2 = 1, \tag{2.1}$$

with $y = p^n y'$, where p is a prime not dividing D and $n \in \mathbb{N}$. If every prime divisor of y' divides D, then $x + y\sqrt{D} = \varepsilon$ or ε^2 or ε^3, where $x_1 + y_1\sqrt{D} = \varepsilon$ is the fundamental solution of (2.1).

Lemma 2.7. [12] *The Diophantine equation*

$$x^m - y^n = 1, m, n \in \mathbb{N}, m > 1, n > 1 \tag{2.2}$$

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

Lemma 2.8. [9] *Let* (x, y) *be a positive integer solution of Diophantine equation (1.7). If every prime divisor of* y *divides* y_1*, then* $x + y\sqrt{D} = \varepsilon$*, where* $\varepsilon = x_1 + y_1\sqrt{D}$ *is the fundamental solution of equation (1.7).*

3. Proof of Theorem 1.6

By Lemma 2.1 we know that

$$x + y\sqrt{D} = (x_1 + y_1\sqrt{D})^m \tag{3.1}$$

for some odd integer m. If $m = 1$, there is nothing to do. Hence we may restrict ourself to $m > 1$. Let $\alpha = x_1 + y_1\sqrt{D}, \beta = x_1 - y_1\sqrt{D}$ and define

$$x_t + y_t\sqrt{D} = (x_1 + y_1\sqrt{D})^t, t \in \mathbb{N}.$$

We write $m = m_1 q^r$, where q is a prime factor of $m, \gcd(m_1, q) = 1, r \in \mathbb{N}$. By Lemma 2.8 we have p dos not divide y_1. We contend that p divides P_q. For otherwise every prime factor of $y_q = y_1 P_q$ divides D by the assumption. It follows from Theorem 1.1 that $q = 1$. This leads to a contradiction. By Lemma 2.3 we know that $\gcd(P_{m_1}, P_q) = P_{\gcd(m_1,q)} = P_1 = 1$. This implies that every prime factor of $y_{m_1} = y_1 P_{m_1}$ divides D because of $y_{m_1} | y_m = y = p^n y'$. Thus we obtain $m_1 = 1$ again by Theorem 1.1. Therefore, we have $m = q^r$. It is obvious that $q \neq p$ since

$$P_q = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} x_1^{q-2r-1} (D y_1^2)^r.$$

If $r > 1$, then

$$P_{q,q} = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} x_q^{q-2r-1} (D y_q^2)^r. \tag{3.2}$$

By Lemma 2.3, we know that $\gcd(P_q, P_{q,q}) | q$. Therefore we have p does not divide $P_{q,q}$, and thus every prime factor P of $P_{q,q}$ divides D. Then we get from (3.2) that $P | q x_q^{q-1}$, hence $P = q$. If $q > 3$, we contend that $P_{q,q} = q$. Otherwise we find from (3.2) that $q^2 | q x_q^{q-1}$ which is impossible. In another point, if $q > 3$, then we have

$$P_{q,q} = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} x_q^{q-2r-1} (D y_q^2)^r > q.$$

This leads to a contradiction. So we obtain that $q = 3$, whence $3 | D$. Since $x_q^2 - D y_q^2 = -1$, we get $-1 = (-1|3) = 1$, which is impossible. It follows that $r = 1$. This completes the proof of Theorem 1.6.

4. Proof of Theorem 1.7

By Lemma 2.1 we know that

$$x + y\sqrt{D} = (x_1 + y_1\sqrt{D})^m \tag{4.1}$$

for some odd integer m. It is enough to prove the result for the case $m > 1$ and $p_1 \nmid y_1, p_2 \nmid y_1$ by Theorem 1.6 and Lemma 2.8. Let $\alpha = x_1 + y_1\sqrt{D}, \beta = x_1 - y_1\sqrt{D}$ and define

$$x_t + y_t\sqrt{D} = (x_1 + y_1\sqrt{D})^t, t \in \mathbb{N}.$$

We write $m = m_1 q^r$, where q is a prime divisor of m, $\gcd(m_1, q) = 1, r \in \mathbb{N}$.

We first prove that $m_1 = 1$. Otherwise $m_1 > 1$, we get from Theorem 1.1 that $p_1|P_{m_1}, p_2|P_{q^r}$ or $p_2|P_{m_1}, p_1|P_{q^r}$. Without loss of generality, we assume that $p_1|P_{m_1}, p_2|P_{q^r}$. Then we get from Lemma 2.3 that $\gcd(P_{m_1}, P_{q^r}) = P_{\gcd(m_1,q^r)} = P_1 = 1$. Therefore we get from Theorem 1.6 that $q^r = q \neq p_2$ and that $m_1 = p$ is an odd prime other than p_1. So $m = pq$ and

$$y' p_1^{n_1} p_2^{n_2} = y_{pq} = y_1 P_q P_{p,q} = y_1 P_p P_{q,p}. \tag{4.2}$$

Let P be an arbitrary prime factor of P_q. It is easy to see that $P \neq p_1$ because of $p_1|P_p$ and $\gcd(P_p, P_q) = P_{\gcd(p,q)} = P_1 = 1$. If $P \neq p_2$, then we have $P|D$ by assumption. Hence we get from

$$P_q = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} x_1^{q-2r-1} (Dy_1^2)^r \tag{4.3}$$

that $P|qx_1^{\frac{q-1}{2}}$. It follows that $P = q$, whereas q^2 does not divide P_q. Conversely, if $q|D$, we can easily get from (4.3) that $ord_q(P_q) = 1$. We have shown that $P_q = q^\lambda p_2^t$, where $\lambda = 1$ or 0 depending $q|D$ or $q \nmid D$ and $t \leq n_2$. Let Q be an arbitrary prime factor of $P_{q,p}$ different from p_1 and p_2. Then we have $Q|D$ by assumption. Hence we get from

$$P_{q,p} = \sum_{r=0}^{(q-1)/2} \binom{p}{2r+1} x_p^{q-2r-1} (Dy_p^2)^r \tag{4.4}$$

that $Q|qx_1^{\frac{q-1}{2}}$. This implies that $Q = q$, whereas q^2 does not divide $P_{q,p}$. Conversely, if $q|D$, we can also get from (4.4) that $ord_q(P_{q,p}) = 1$. Similarly we can prove that $P_p = p^\mu p_1^s$, where $\mu = 1$ or 0 depending $p|D$ or $p \nmid D$ and $s \leq n_1$. A prime number P which is not equal to p_1 and p_2 divides $P_{p,q}$ if and only if $P = p$ and $p|D$ with the property $ord_p(P_{p,q}) = 1$. On the other hand, by Lemma 2.3(4),(5), we know that $\gcd(P_{q,p}, P_p)|q, \gcd(P_{p,q}, P_q)|p$ and

$$ord_{p_1}(P_{q,p}) = ord_{p_1}(q) = \begin{cases} 0 & q \neq p_1, \\ 1 & q = p_1. \end{cases} \quad ord_{p_2}(P_{p,q}) = ord_{p_2}(p) = \begin{cases} 0 & p \neq p_2, \\ 1 & p = p_2. \end{cases}$$

Therefore we get from (4.2) that

$$q \neq p_1, p \neq p_2, P_q = qp_2^{n_2}, q|D, P_{p,q} = pp_1^{n_1}, P_p = pp_1^{n_1}, p|D, P_{q,p} = qp_2^{n_2} \tag{4.5}$$

or

$$q \neq p_1, p \neq p_2, P_q = qp_2^{n_2}, q|D, P_{p,q} = p_1^{n_1}, P_p = p_1^{n_1}, p \nmid D, P_{q,p} = qp_2^{n_2} \tag{4.6}$$

or

$$q \neq p_1, p \neq p_2, P_q = p_2^{n_2}, q \nmid D, P_{p,q} = pp_1^{n_1}, P_p = pp_1^{n_1}, p|D, P_{q,p} = p_2^{n_2} \tag{4.7}$$

or

$$q \neq p_1, p \neq p_2, P_q = p_2^{n_2}, q \nmid D, P_{p,q} = p_1^{n_1}, P_p = p_1^{n_1}, p \nmid D, P_{q,p} = p_2^{n_2} \tag{4.8}$$

or

$$q \neq p_1, p = p_2, P_q = qp_2^{n_2-1}, q|D, P_{p_2,q} = p_2 p_1^{n_1}, P_{p_2} = p_1^{n_1}, P_{q,p_2} = qp_2^{n_2} \tag{4.9}$$

or

$$q \neq p_1, p = p_2, P_q = p_2^{n_2-1}, q \nmid D, P_{p_2,q} = p_2 p_1^{n_1}, P_{p_2} = p_1^{n_1}, P_{q,p_2} = p_2^{n_2} \tag{4.10}$$

or

$$q = p_1, p \neq p_2, P_{p_1} = p_2^{n_2}, P_{p,p_1} = pp_1^{n_1}, P_p = pp_1^{n_1-1}, p|D, P_{p_1,p} = p_1 p_2^{n_2} \tag{4.11}$$

or

$$q = p_1, p \neq p_2, P_{p_1} = p_2^{n_2}, P_{p,p_1} = p_1^{n_1}, P_p = p_1^{n_1-1}, p \nmid D, P_{p_1,p} = p_1 p_2^{n_2} \tag{4.12}$$

or

$$q = p_1, p = p_2, P_{p_1} = p_2^{n_2-1}, P_{p_2,p_1} = p_2 p_1^{n_1}, P_{p_2} = p_1^{n_1-1}, P_{p_1,p_2} = p_1 p_2^{n_2}. \tag{4.13}$$

Each of equation (4.5), (4.6), (4.7) and (4.8) implies that $P_q = P_{q,p}$, which is impossible. If $p_1 > p_2$, then we get from (4.9) that

$$y_{p_2} = P_{p_2} y_1 = p_1^{n_1} y_1 \geq p_1 y_1, x_{p_2}^2 = Dy_{p_2}^2 - 1 > p_1(Dy_1^2 - 1) = p_1 x_1^2.$$

Hence

$$qp_2^{n_2} = P_{q,p_2} = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} x_{p_2}^{q-2r-1} (Dy_{p_2}^2)^r >$$

$$p_1 \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} x_1^{q-2r-1} (Dy_1^2)^r = p_1 P_q = p_1 qp_2^{n_2-1} > qp_2^{n_2},$$

which is impossible. If $p_1 < p_2$, then we get from (4.9) that

$$y_q = P_q y_1 = qp_2^{n_2-1} y_1 \geq p_2 y_1, x_q^2 = Dy_q^2 - 1 > p_2(Dy_1^2 - 1) = p_2 x_1^2.$$

Hence

$$p_2 p_1^{n_1} = P_{p_2,q} = \sum_{r=0}^{(p_2-1)/2} \binom{p_2}{2r+1} x_q^{p_2-2r-1} (Dy_q^2)^r >$$

$$p_2 \sum_{r=0}^{(p_2-1)/2} \binom{p_2}{2r+1} x_1^{p_2-2r-1} (Dy_1^2)^r = p_2 P_{p_2} = p_2 p_1^{n_1},$$

which is also impossible. Similarly we can prove that equations (4.10), (4.11) and (4.12) cannot satisfied. For (4.13), without loss of generality, we assume that $p_1 > p_2$. Then we have that

$$y_{p_2} = P_{p_2} y_1 = p_1^{n_1-1} y_1 \geq p_1 y_1, x_{p_2}^2 = Dy_{p_2}^2 - 1 > p_1^2(Dy_1^2 - 1) = p_1^2 x_1^2.$$

Hence

$$p_1p_2^{n_2} = P_{p_1,p_2} = \sum_{r=0}^{(p_1-1)/2} \binom{p_{p_1}}{2r+1} x_{p_2}^{p_1-2r-1}(Dy_{p_2}^2)^r >$$

$$p_1^2 \sum_{r=0}^{(p_1-1)/2} \binom{p_{p_1}}{2r+1} x_1^{p_1-2r-1}(Dy_1^2)^r = p_1^2 P_{p_1} = p_1^2 p_2^{n_2-1} > p_1p_2^{n_2},$$

which is impossible. Therefore $m_1 = 1, m = q^r$ as desired.

We now prove $r \leq 2$. Otherwise $r > 2$, then we must have $p_1|P_{q^2}, p_2|P_{q^2}$ by Theorem 1.6 and

$$P_{q,q^2} = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} x_{q^2}^{q-2r-1}(Dy_{q^2}^2)^r. \tag{4.14}$$

Since $\gcd(P_{q,q^2}, P_{q^2})|q$, hence $p_1 \not| P_{q,q^2}, p_2 \not| P_{q,q^2}$. And thus every prime factor P of P_{q,q^2} divides D. Then we get from (4.14) that $P|qx_{q^2}^{q-1}$, and so $P = q$. If $q > 3$, we contend that $P_{q,q^2} = q$. Otherwise we find from (4.14) that $q^2|qx_{q^2}^{q-1}$ which is impossible. In another point, if $q > 3$, then we have

$$P_{q,q^2} = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} x_{q^2}^{q-2r-1}(Dy_{q^2}^2)^r > q.$$

This leads to a contradiction. So we obtain that $q = 3$, whence $3|D$. Since $x_q^2 - Dy_q^2 = -1$, we get $-1 = (-1|3) = 1$, which is impossible. Thus $r \leq 2$ as desired. The proof of Theorem 1.7 is complete.

5. Proof of Theorem 1.8

It is enough to prove the result for the case of p_1 not dividing y_1 and p_2 not dividing y_1 by the Remark of Theorem 1.4 and Theorem 1.6. By Lemma 2.2, we know that

$$\frac{x + y\sqrt{D}}{2} = (\frac{x_1 + y_1\sqrt{D}}{2})^m \tag{5.1}$$

for some positive integer m. If $m = 1$, there is nothing to do. Hence we may restrict ourself to $m > 1$. Let $\alpha = \frac{x_1+y_1\sqrt{D}}{2}, \beta = \frac{x_1-y_1\sqrt{D}}{2}$ and define

$$\frac{x_t + y_t\sqrt{D}}{2} = \left(\frac{x_1 + y_1\sqrt{D}}{2}\right)^t, t \in \mathbb{N}.$$

Case 1: We assume $2|m$. We write $m = 2m_1$. From (5.1) we get

$$\frac{x + y\sqrt{D}}{2} = (\frac{x_{m_1} + y_{m_1}\sqrt{D}}{2})^2.$$

Hence

$$x_{m_1}y_{m_1} = p_1^{n_1}p_2^{n_2}y'. \tag{5.2}$$

Since $x_{m_1}^2 - Dy_{m_1}^2 = 4$, we have that $\gcd(x_{m_1}, y_{m_1}) = 1$ or 2. If $\gcd(x_{m_1}, y_{m_1}) = 1$, then we have either $x_{m_1} = p_1^{n_1}, y_{m_1} = p_2^{n_2}y'$, or $x_{m_1} = p_2^{n_2}, y_{m_1} = p_1^{n_1}y'$. It follows that y_{m_1} satisfies the condition of

Theorem 1.5. Therefore we obtain that $m_1 = 1$ or 2 or 3, whence $m = 2$ or 4 or 6. If $\gcd(x_{m_1}, y_{m_1}) = 2$, then we have either

$$x_{m_1} = 2^{n_1-1}, y_{m_1} = 2p_2^{n_2}y' \tag{5.3}$$

or

$$x_{m_1} = 2p_2^{n_2}, y_{m_1} = 2^{n_1-1}y'. \tag{5.4}$$

From (5.3), we get that $Q_{m_1} = 2^t$. This implies that $m_1 = 3$ by Lemma 2.5. So we get that $x_1|2^{n_1-1} = x_3$, which is impossible since x_1 is an odd greater than 1. From (5.4), we get that $m_1 = 3$ by Lemma 2.4 and Theorem 1.5, whence $m = 6$. The result is true.

Case 2: Now we assume 2 does not divide m. We write $m = m_1q^r$, where q is a prime factor of $m, \gcd(m_1, q) = 1, r \in \mathbb{N}$. We divide the proof into three cases.

We first prove that $m_1 = 1$. Otherwise $m_1 > 1$, by Theorem 1.4 we get that $p_1|P_{m_1}, p_2|P_{q^r}$ or $p_2|P_{m_1}, p_1|P_{q^r}$. Without loss of generality, we assume that $p_1|P_{m_1}, p_2|P_{q^r}$. Then by Lemma 2.3, we have $\gcd(P_{m_1}, P_{q^r}) = P_{\gcd(m_1,q^r)} = P_1 = 1$. Hence we have that p_2 does not divide P_{m_1} and that p_1 does not divide P_{q^r}. So both $y_{m_1} = P_{m_1}y_1$ and $y_{q^r} = P_{q^r}y_1$ satisfy the condition of Theorem 1.5. We have $m = m_1q^r = 15, D = 5$. But a simple calculation shows that $y = y_{15} = 2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61$. Thus we have now shown that $m_1 = 1$.

We now prove that $r = 1$ and $\gcd(q, p_1p_2) = 1$ when $q > 3$. We claim $\gcd(q, p_1p_2) = 1$. Otherwise without loss generality, we may assume $p_1 = q|y_{q^r} = P_{q,q^{r-1}}y_{q^{r-1}}$. Since

$$P_{q,q^{r-1}} = \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} (x_{q^{r-1}}/4)^{q-2j-1} (Dy_{q^{r-1}}^2/4)^j,$$

so we have $p_1|y_{q^{r-1}}(Dy_{q^{r-1}}^2/4)^{\frac{q-1}{2}}$. It follows that $p_1|y_{q^{r-1}}$. Continue this step. We will get that $p_1|y_1(Dy_1^2/4)^{\frac{q-1}{2}}$, and so $p_1|y_1$, which contradicts with the beginning assumption. Hence $\gcd(q, p_1p_2) = 1$, as desired. If $r > 1$, then we have $p_1|P_q, p_2|P_q$ by Theorem 1.5. By Lemma 2.3, we know that $\gcd(P_{q^{r-1},q}, P_q)|q^{r-1}$. It follows that p_1 does not divide $P_{q^{r-1},q}$ and p_2 does not divide $P_{q^{r-1},q}$. Hence every prime factor of $P_{q^{r-1},q}$ divides D. Since $(Q_{q^{r-1},q}, P_{q^{r-1},q})$ is a positive integer solution of Pell equation $x_q^2X^2 - Dy_q^2Y^2 = 4$ and its minimal positive solution is $(1, 1)$, we have $P_{q^{r-1},q} = 1$ by Theorem 1.4, which is impossible. Thus we have now shown that $r = 1$.

Finally we prove that $r = 1$ and 3 does not divide p_1p_2 when $q = 3$. It is easy to prove that 3 does not divide p_1p_2 similarly as above. If $r > 1$, then by Lemma 2.4 we have

$$2^{n_1}p^{n_2}y' = y_{3^r} = y_1P_{3^{r-1},3}P_3, p_1 = 2, p_2 = p, 2|P_3.$$

According to Lemma 2.3, we have $\gcd(P_{3^{r-1},3}, P_3)|3^{r-1}$. It follows that 2 does not divide $P_{3^{r-1},3}$. Thus we have that $p|P_{3^{r-1},3}$ by Theorem 1.4. If $p|P_3$, then we have that $p = 3|P_3 = Dy_1^2 + 3$, whence $3|D$, which contradicts with the assumption. And so we have p does not divide P_3. If P is an odd prime divisor of P_3, then we have $P|D$. Hence $P|P_3 = Dy_1^2 + 3$, and so $P = 3$. Thus we have either

$$P_3 = Dy_1^2 + 3 = 2^{n_1}, 3 \nmid D \tag{5.5}$$

or

$$P_3 = Dy_1^2 + 3 = 2^{n_1}3^t, 3|D. \tag{5.6}$$

(5.5) leads that $x_1^2 = Dy_1^2 + 4 = 2^{n_1} + 1$. It follows that $(x_1, n_1, y_1, D) = (3, 3, 1, 5)$ by Lemma 2.7. By a simple calculation we get that $y_9 = 2^3 \cdot 17 \cdot 19$. This leads to a contradiction. (5.6) leads that $x_1^2 = Dy_1^2 + 4 = 2^{n_1}3^t + 1$. It is easy to see either 2 does not divide n_1 or 2 does not divide t. If 2 does not divide n_1 and 2 does not divide t, then by $x_1^2 = 2^{n_1}3^t + 1$ and Theorem 1.1 we get that $(x_1, n_1, t, y_1, D) = (5, 3, 1, 1, 21)$. By a simple calculation we get that $y_9 = 2^3 \cdot 3^2 \cdot 37 \cdot 109$. This also leads to a contradiction. If 2 does not divide n_1 and 2 divides t, then by $x_1^2 = 2^{n_1}3^t + 1$ and Lemma 2.6 we get

$$x_1 + 2^{\frac{n_1-1}{2}}3^{\frac{t}{2}}\sqrt{2} = 3 + 2\sqrt{2} \tag{5.7}$$

or

$$x_1 + 2^{\frac{n_1-1}{2}}3^{\frac{t}{2}}\sqrt{2} = (3 + 2\sqrt{2})^2 \tag{5.8}$$

or

$$x_1 + 2^{\frac{n_1-1}{2}}3^{\frac{t}{2}}\sqrt{2} = (3 + 2\sqrt{2})^3. \tag{5.9}$$

It is easy to see neither (5.7) nor (5.9) is true. From (5.8), we get that $(x_1, n_1, t, y_1, D) = (17, 5, 2, 1, 285)$. By a simple calculation we get that $y_9 = 2^5 \cdot 3^3 \cdot 1621 \cdot 4861$. Hence we know that the case 2 does not divide n_1 and 2 divides t are impossible. If 2 divides n_1 and 2 does not divide t, then by $x_1^2 = 2^{n_1}3^t + 1$ and Lemma 2.6 we get we get

$$x_1 + 2^{\frac{n_1}{2}}3^{\frac{t-1}{2}}\sqrt{3} = 2 + \sqrt{3} \tag{5.10}$$

or

$$x_1 + 2^{\frac{n_1}{2}}3^{\frac{t-1}{2}}\sqrt{3} = (2 + \sqrt{3})^2 \tag{5.11}$$

or

$$x_1 + 2^{\frac{n_1}{2}}3^{\frac{t-1}{2}}\sqrt{3} = (2 + \sqrt{3})^3. \tag{5.12}$$

It is easy to see neither (5.10) nor (5.12) is true. From (5.11), we get that $(x_1, n_1, t, y_1, D) = (7, 4, 1, 1, 45)$. By a simple calculation we get that $y_9 = 2^4 \cdot 3^2 \cdot 17 \cdot 19 \cdot 107$. Hence we have shown that 2 divide n_1 and 2 does not divide t are also impossible. Therefore $r = 1$, as desired. This finishes the proof of Theorem 1.8.

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. L. E. Dickson, *History of the Theory of Numbers*, Vol. II, Washington, Carnegie Institution of Washington, 1920.
2. D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math., **31** (1930), 419–448.
3. J. G. Luo, *Extensions and applications on störmer theory*, Journal of Sichuan University, **28** (1991), 469–474.

4. J. G. Luo, P. Z. Yuan, *On the solutions of a system of two Diophantine equations*, Science China Mathematics, **57** (2014), 1401–1418.
5. J. G. Luo, A. Togbe, P. Z. Yuan, *On some equations related to Ma's conjecture*, Integers, **11** (2011), 683–694.
6. J. G. Luo, P. Z. Yuan, *Square-classes in Lehmer sequences having odd parameters and their applications*, Acta Arith., **127** (2007), 49–62.
7. H. Mei, L. Mei, Q. fan, et al. *Extensions of störmer theorem*, Journal of Yuzhou University, **12** (1995), 25–27.
8. P. Ribenboim, *The Book of Prime Number Records*, Springer-Verlag, New York, 1989.
9. J. G. Luo, *On the Diophantine equation* $\frac{ax^m \pm 1}{ax \pm 1} = y^n$ *and* $\frac{ax^m \pm 1}{ax \pm 1} = y^n + 1$, Chinese Annals of Mathematics, Series A, **25** (2004), 805–808.
10. Q. Sun, P. Z. Yuan, *On the Diophantine equatins* $(ax^n - 1)/(ax - 1) = y^2$ *and* $(ax^n + 1)/(ax + 1) = y^2$, Journal of Sichuan University, **26** (1989), 20–24.
11. P. Z. Yuan, *A note on the divisibility of the generalized Lucas sequences*, Fibonacci Quarterly, **40** (2002), 153–156.
12. P. Mihäilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math., **572** (2004), 167–196.