

On some special forms of simultaneous Pell equations

by

ZHIGANG LI, JIANYE XIA and PINGZHI YUAN (Guangdong)

1. Introduction. In this paper, we investigate positive integer solutions (x, y, z) of some special forms of the simultaneous Pell equations

$$(1.1) \quad \begin{cases} ax^2 - by^2 = \delta_1, \\ cy^2 - dz^2 = \delta_2, \end{cases}$$

where a, b, c, d are positive integers, and δ_1, δ_2 are positive integers with $\gcd(ab, \delta_1) = \gcd(cd, \delta_2) = 1$. Thue [14] and Siegel [13] proved that if $(b, \delta_1) \neq k(d, \delta_2)$ with k an integer, then equations (1.1) have at most finitely many solutions. Anglin [1] described an algorithm for solving equations similar to (1.1).

For the special simultaneous Diophantine equations

$$(1.2) \quad x^2 - ay^2 = y^2 - bz^2 = 1,$$

where a and b are distinct integers, Yuan [20] proved that equations (1.2) have at most one positive integer solution if $a = 4m(m + 1)$ and m is a positive integer. Recently, Yuan [21] showed that equations (1.1) have at most two positive integer solutions if $\max(a, b, c, d) \geq 1.6 \cdot 10^{59}$ with $b \neq d$, and $\delta_i = 1$, $i = 1, 2$, and that equations (1.2) have at most two positive integer solutions if $a > 3.31 \cdot 10^{35}$. For more results on equations (1.1) and (1.2), see Walsh [17, 18], Bennett and Walsh [4], Bennett [3], Anglin [2], Yuan [22, 23], etc.

Using an elementary argument based on properties of Lucas sequences and existence of primitive prime factors of Lucas sequences, Yuan [20] showed that the number of positive solutions is at most one when equations (1.2) are of a special form. Ljunggren [7] proved that the equation $Ax^2 - By^4 = 1$,

2000 *Mathematics Subject Classification*: Primary 11D09, 11D25; Secondary 11B39, 11J13, 11J86.

Key words and phrases: simultaneous Pell equations, Lucas sequences, primitive prime factors.

Supported by National Natural Science Foundation of China (No. 10571180) and Guangdong Provincial Natural Science Foundation (No. 04009801).

$A > 0$, $B > 0$, has at most one positive solution, which will lead to a contradiction when one assumes equations (1.2) have at least two positive solutions. Yuan [20] just quoted this significant result of Ljunggren to complete his proofs.

In this paper, we shall study positive integer solutions of the special forms of the simultaneous Pell equations

$$(1.3) \quad \begin{cases} ax^2 - cy^2 = \delta, \\ y^2 - bz^2 = 1, \end{cases}$$

where a , b and c are positive integers with $(a, c) = 1$ and $(ac, \delta) = 1$, $\delta \in \{1, 4\}$. Yuan [20] has investigated the case $(a, c, \delta) = (1, 4m(m+1), 1)$. Following but developing the methods of Yuan [20], on the basis of properties of Lehmer sequences and primitive prime factors of Lehmer sequences, quoting other results ([7], [15], [9], [8]) on the equation $Ax^2 - Bx^4 = C$, $A, B, C > 0$, we will study the other two cases $(m+1, m, 1)$ and $(m+4, m, 4)$, and combine these techniques to prove:

THEOREM 1.1. *Let b and m be positive integers.*

- (1) *If $a = m + 1$, $c = m$, and $\delta = 1$, then equations (1.3) have at most one positive integer solution (x, y, z) .*
- (2) *If $a = m + 4$, $c = m$, $2 \nmid m$, and $\delta = 4$, then equations (1.3) have at most one positive integer solution (x, y, z) .*

The structure of the paper is as follows. In Section 2, we present the relevant lemmas on Lehmer sequences and their primitive prime factors. In Section 3, we quote the important theorems on $Ax^2 - By^4 = C$, and prove some corollaries. In Section 4, we prove Theorem 1.1.

2. Basic lemmas. First we consider the equation $ax^2 - cy^2 = \delta$ with square-free integers $a, c > 0$, $\delta = 1, 4$. We have

LEMMA 2.1 ([21, 16]). *Let $x_0^{(0)}\sqrt{a} + y_0^{(0)}\sqrt{c}$ be the fundamental solution of $ax^2 - cy^2 = \delta$, $\delta = 1, 4$ (i.e. the smallest positive integer solution). Then every positive integer solution (x, y) of this equation can be represented as*

$$\frac{x\sqrt{a} + y\sqrt{c}}{\sqrt{\delta}} = \left(\frac{x_0^{(0)}\sqrt{a} + y_0^{(0)}\sqrt{c}}{\sqrt{\delta}} \right)^n, \quad n > 0,$$

with $2 \nmid n$ if $\min(a, c) > 1$ or $(a, \delta) \neq (1, 1), (1, 4)$.

We consider (1.3). Suppose that integers a , b and c are positive and square-free. Let $x_0^{(1)}\sqrt{a} + y_0^{(1)}\sqrt{c}$ and $y_0^{(2)} + z_0^{(2)}\sqrt{b}$ be the fundamental solutions of $ax^2 - cy^2 = \delta$ and $y^2 - bz^2 = 1$, respectively. Put

$$\alpha = \frac{x_0^{(1)}\sqrt{a} + y_0^{(1)}\sqrt{c}}{\sqrt{\delta}}, \quad \beta = y_0^{(2)} + z_0^{(2)}\sqrt{b}.$$

Define

$$(2.4) \quad \begin{aligned} U_k &= \frac{\alpha^k - \alpha^{-k}}{2\sqrt{c/\delta}}, & V_k &= \frac{\alpha^k + \alpha^{-k}}{2\sqrt{a/\delta}}, \\ U'_l &= \frac{\beta^l - \beta^{-l}}{2\sqrt{b}}, & V'_l &= \frac{\beta^l + \beta^{-l}}{2}. \end{aligned}$$

The properties of Lehmer sequences play an important role in this paper. Since these properties are well known, we state the following lemma without proof.

LEMMA 2.2 ([10, 11]).

- (1) If $d = \gcd(m, n)$, then $\gcd(U_m, U_n) = U_d$.
- (2) If $d = \gcd(m, n)$, then $\gcd(V_m, V_n) = V_d$ if m/d and n/d are odd, and 1 otherwise.
- (3) If $d = \gcd(m, n)$, then $\gcd(U_m, V_n) = V_d$ if m/d is even, and 1 otherwise.
- (4) If $U_m \neq 1$, then $U_m \mid U_n$ if and only if $m \mid n$.
- (5) If $m > 1$, then $V_m \mid V_n$ if and only if n/m is an odd integer.
- (6) $(U_m, V_m) = 1$.

Next we look at positive integer solutions of (1.3). Assume that such solutions exist. Let (x_0, y_0, z_0) be the positive integer solution with the smallest positive y_0 , and (x, y, z) be any positive integer solution of (1.3). Then there exist positive integers k_0, l_0, k and l such that

$$(2.5) \quad y_0 = U_{k_0} = V'_{l_0}, \quad x_0 = V_{k_0}, \quad z_0 = U'_{l_0},$$

$$(2.6) \quad y = U_k = V'_l, \quad x = V_k, \quad z = U'_l.$$

To prove our theorem, we refer to two lemmas of [21].

LEMMA 2.3 ([21, Lemma 2.3]). *Let k_1, k_2, r and q be positive integers with $k_2 = 2qk_1 \pm r$, $0 \leq r \leq k_1$. Then $U_{k_2} \equiv \pm U_r \pmod{U_{k_1}}$.*

LEMMA 2.4 ([21, Lemma 2.4]). *Let the notations be as in (2.5) and (2.6). Then $y_0 \mid y$, $l_0 \mid l$ and $k_0 \mid k$. Furthermore, l/l_0 and k/k_0 are odd integers, which implies $x_0 \mid x$ and $z_0 \mid z$.*

Lemma 2.3 gives the relation between U_{k_1} and U_{k_2} in the sequence $\{U_k\}$. By Lemma 2.2(4), $U_{k_1} \mid U_{k_2}$ if and only if $k_1 \mid k_2$. But the relation in Lemma 2.3 is important in proving Lemma 2.8. By Lemma 2.4, we know that z/z_0 is an integer, which will be used in the proof of Lemma 2.7.

To prove our main theorem, we still need the following lemma.

LEMMA 2.5. *Let m and k be positive integers. Set*

$$U_k = \frac{\alpha^k - \alpha^{-k}}{2\sqrt{c/\delta}}, \quad V_k = \frac{\alpha^k + \alpha^{-k}}{2\sqrt{a/\delta}}.$$

- (1) If k is odd, and $(a, c, \delta) = (m + 1, m, 1)$, let $\alpha = \sqrt{m+1} + \sqrt{m}$, $\xi = 2m + 1 + 2\sqrt{m(m+1)}$, and $\bar{\xi} = 2m + 1 - 2\sqrt{m(m+1)}$, which implies $\alpha^2 = \xi$. Put

$$(2.7) \quad \tilde{x}_i = \frac{\xi^i + \xi^{-i}}{2}, \quad \tilde{y}_i = \frac{\xi^i - \xi^{-i}}{4\sqrt{m(m+1)}}, \quad i \in \{(k+1)/2, (k-1)/2\}.$$

Then

$$(2.8) \quad U_k^2 - 1 = 4(m+1) \cdot \tilde{y}_{(k+1)/2} \tilde{y}_{(k-1)/2}.$$

- (2) If k is odd, and $(a, c, \delta) = (m + 4, m, 4)$, let $\alpha = (\sqrt{m+4} + \sqrt{m})/2$, $\xi = (m + 2 + \sqrt{m(m+4)})/2$, and $\bar{\xi} = (m + 2 - \sqrt{m(m+4)})/2$, which implies $\alpha^2 = \xi$. Put

$$(2.9) \quad \tilde{x}_i = \xi^i + \xi^{-i}, \quad \tilde{y}_i = \frac{\xi^i - \xi^{-i}}{\sqrt{m(m+4)}}, \quad i \in \{(k+1)/2, (k-1)/2\}.$$

Then

$$(2.10) \quad U_k^2 - 1 = (m+4) \cdot \tilde{y}_{(k+1)/2} \tilde{y}_{(k-1)/2}.$$

Proof. (1) Since $\alpha^2 + \alpha^{-2} = 2(2m+1)$, we have

$$\begin{aligned} U_k^2 - 1 &= \frac{\alpha^{2k} + \alpha^{-2k} - 2}{4m} - 1 = \frac{\alpha^{2k} + \alpha^{-2k} - 2(2m+1)}{4m} \\ &= \frac{\alpha^{2k} + \alpha^{-2k} - (\alpha^2 + \alpha^{-2})}{4m} = \frac{(\alpha^{k+1} - \alpha^{-k-1})(\alpha^{k-1} - \alpha^{-k+1})}{4m} \\ &= \frac{((\alpha^2)^{(k+1)/2} - (\alpha^2)^{-(k-1)/2})((\alpha^2)^{(k-1)/2} - (\alpha^2)^{-(k+1)/2})}{4m} \\ &= \frac{(\xi^{(k+1)/2} - \xi^{-(k-1)/2})(\xi^{(k-1)/2} - \xi^{-(k+1)/2})}{4\sqrt{m(m+1)} \cdot 4\sqrt{m(m+1)}} \cdot 4(m+1). \end{aligned}$$

By the definitions of $\tilde{y}_{(k+1)/2}$, $\tilde{y}_{(k-1)/2}$, it follows that $U_k^2 - 1 = 4(m+1) \cdot \tilde{y}_{(k+1)/2} \tilde{y}_{(k-1)/2}$.

(2) Using similar methods to those in (1), we obtain (2.10) immediately. ■

REMARK. $2m+1+2\sqrt{m(m+1)}$ and $m+2+\sqrt{m(m+4)}$ are the smallest positive solutions of $x^2 - 4m(m+1)y^2 = 1$ and $x^2 - m(m+4)y^2 = 4$, respectively. In Lemma 2.5(1), keeping the definition of ξ , write

$$\tilde{V}_k = \frac{\xi^k + \xi^{-k}}{2}, \quad \tilde{U}_k = \frac{\xi^k - \xi^{-k}}{4\sqrt{m(m+1)}}, \quad k > 0.$$

Then $(\tilde{V}_k, \tilde{U}_k)$ is a positive integer solution of $x^2 - 4m(m+1)y^2 = 1$, and $\tilde{y}_{(k+1)/2} = \tilde{U}_{(k+1)/2}$, $\tilde{y}_{(k-1)/2} = \tilde{U}_{(k-1)/2}$. In Lemma 2.5(2), we can also set

$$\tilde{V}_k = \xi^k + \xi^{-k}, \quad \tilde{U}_k = \frac{\xi^k - \xi^{-k}}{\sqrt{m(m+4)}}, \quad k > 0.$$

Then $(\tilde{V}_k, \tilde{U}_k)$ is a positive integer solution of $x^2 - m(m+4)y^2 = 4$, and so $\tilde{y}_{(k+1)/2} = \tilde{U}_{(k+1)/2}$, $\tilde{y}_{(k-1)/2} = \tilde{U}_{(k-1)/2}$.

The $U_k^2 - 1$ in Lemma 2.5(1),(2) contains the factors $\tilde{y}_{(k+1)/2}, \tilde{y}_{(k-1)/2}$. We must clarify the relations between $\tilde{y}_{(k+1)/2}$ and $\tilde{y}_{(k-1)/2}$, which is the key step in proving Theorem 1.1.

LEMMA 2.6. *If $\tilde{x}_{(k+1)/2}, \tilde{x}_{(k-1)/2}, \tilde{y}_{(k+1)/2}$, and $\tilde{y}_{(k-1)/2}$ are defined as in (2.7) and (2.9), then $\gcd(\tilde{x}_{(k+1)/2}, \tilde{y}_{(k+1)/2}) = 1$, $\gcd(\tilde{x}_{(k-1)/2}, \tilde{y}_{(k-1)/2}) = 1$, $\gcd(\tilde{y}_{(k+1)/2}, \tilde{y}_{(k-1)/2}) = 1$, $\gcd(\tilde{x}_{(k+1)/2}, \tilde{x}_{(k-1)/2}) = 1$,*

$$\gcd(\tilde{x}_{(k+1)/2}, \tilde{y}_{(k-1)/2}) = \begin{cases} 1, & k \equiv 3 \pmod{4}, \\ \tilde{x}_1, & k \equiv 1 \pmod{4}, \end{cases}$$

$$\gcd(\tilde{x}_{(k-1)/2}, \tilde{y}_{(k+1)/2}) = \begin{cases} 1, & k \equiv 1 \pmod{4}, \\ \tilde{x}_1, & k \equiv 3 \pmod{4}. \end{cases}$$

Proof. From Lemma 2.2(6), $\gcd(\tilde{x}_{(k+1)/2}, \tilde{y}_{(k+1)/2}) = 1$ and $\gcd(\tilde{x}_{(k-1)/2}, \tilde{y}_{(k-1)/2}) = 1$. Since $\gcd((k+1)/2, (k-1)/2) = 1$, from Lemma 2.2(1), $\gcd(\tilde{y}_{(k+1)/2}, \tilde{y}_{(k-1)/2}) = \tilde{y}_1 = 1$. Notice that $(k+1)/2$ and $(k-1)/2$ have opposite parity. By Lemma 2.2(2), we have $\gcd(\tilde{x}_{(k+1)/2}, \tilde{x}_{(k-1)/2}) = 1$. If $k \equiv 1 \pmod{4}$, then $(k-1)/2$ is even and $(k+1)/2$ is odd. Thus by Lemma 2.2(3), $\gcd(\tilde{x}_{(k+1)/2}, \tilde{y}_{(k-1)/2}) = \tilde{x}_1$ and $\gcd(\tilde{x}_{(k-1)/2}, \tilde{y}_{(k+1)/2}) = 1$. Similarly, if $k \equiv 3 \pmod{4}$, then $\gcd(\tilde{x}_{(k+1)/2}, \tilde{y}_{(k-1)/2}) = 1$ and $\gcd(\tilde{x}_{(k-1)/2}, \tilde{y}_{(k+1)/2}) = \tilde{x}_1$. ■

For the solutions (x_0, y_0, z_0) and (x, y, z) , we shall prove that the ratio $(U_k^2 - 1)/(U_{k_0}^2 - 1)$ is a square whenever equations (1.3) are of special forms.

LEMMA 2.7. *Let the notations be as in (2.5), (2.6) and in Lemmas 2.5, 2.6.*

(1) *If $(a, c, \delta) = (m+1, m, 1)$, then*

$$(2.11) \quad \frac{\tilde{y}_{(k+1)/2}\tilde{y}_{(k-1)/2}}{\tilde{y}_{(k_0+1)/2}\tilde{y}_{(k_0-1)/2}} = \frac{\tilde{U}_{(k+1)/2}\tilde{U}_{(k-1)/2}}{\tilde{U}_{(k_0+1)/2}\tilde{U}_{(k_0-1)/2}} = \left(\frac{z}{z_0}\right)^2.$$

(2) *If $(a, c, \delta) = (m+4, m, 4)$, then*

$$(2.12) \quad \frac{\tilde{y}_{(k+1)/2}\tilde{y}_{(k-1)/2}}{\tilde{y}_{(k_0+1)/2}\tilde{y}_{(k_0-1)/2}} = \frac{\tilde{U}_{(k+1)/2}\tilde{U}_{(k-1)/2}}{\tilde{U}_{(k_0+1)/2}\tilde{U}_{(k_0-1)/2}} = \left(\frac{z}{z_0}\right)^2.$$

Proof. (1) By Lemma 2.1, both k_0 and k are odd. Then, by (2.8), Lemma 2.5(1), and Remark, we obtain

$$bz^2 = U_k^2 - 1 = 4(m+1) \cdot \tilde{U}_{(k+1)/2}\tilde{U}_{(k-1)/2} = 4(m+1) \cdot \tilde{y}_{(k+1)/2}\tilde{y}_{(k-1)/2},$$

$$bz_0^2 = U_{k_0}^2 - 1 = 4(m+1) \cdot \tilde{U}_{(k_0+1)/2}\tilde{U}_{(k_0-1)/2} = 4(m+1) \cdot \tilde{y}_{(k_0+1)/2}\tilde{y}_{(k_0-1)/2}.$$

Hence

$$\frac{\tilde{y}_{(k+1)/2}\tilde{y}_{(k-1)/2}}{\tilde{y}_{(k_0+1)/2}\tilde{y}_{(k_0-1)/2}} = \frac{\tilde{U}_{(k+1)/2}\tilde{U}_{(k-1)/2}}{\tilde{U}_{(k_0+1)/2}\tilde{U}_{(k_0-1)/2}} = \left(\frac{z}{z_0}\right)^2.$$

Since $z_0 \mid z$ by Lemma 2.4, $\tilde{y}_{(k+1)/2}\tilde{y}_{(k-1)/2}/\tilde{y}_{(k_0+1)/2}\tilde{y}_{(k_0-1)/2}$ is a square.

(2) As in (1), we can easily deduce (2.12). ■

To prove the theorem of this paper, we need the concept and the relevant theory of primitive prime factors of Lehmer sequences.

D. H. Lehmer [6], extending the theory of Lucas functions, studied a wide class of sequences, commonly referred to as *Lehmer sequences*. For a nonnegative integer n , the n th term in the Lehmer sequence $\{P_n\}$ is given by

$$P_n(\alpha, \beta) = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta} & \text{for } n \text{ odd,} \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{for } n \text{ even,} \end{cases}$$

where α and β are the roots of the trinomial $z^2 - L^{1/2}z + M$, and $L > 0$ and M are rational integers such that $L - 4M > 0$ and $\gcd(L, M) = 1$.

A prime p is called a *primitive prime factor* of the term P_n (of a Lehmer sequence or Lucas sequence) if $p \mid P_n$ but $p \nmid KLP_3 \cdots P_{n-1}$ (where $K = L - 4M$).

M. Ward [19] and L. K. Durst [5] (cf. [12, p. 214]) have proved the following result about primitive prime factors.

THEOREM W-D ([19, 5]). *Assume that, besides the restrictions on L , M stated as above,*

$$(L, M) = 1, \quad \langle L, M \rangle \neq \langle 1, 1 \rangle, \langle 2, 1 \rangle, \langle 3, 1 \rangle.$$

Then for $n \neq 1, 2, 3, 4, 6$, P_n has a primitive prime factor except for $K > 0$ if $n = 5$, $\langle L, M \rangle = \langle 1, -1 \rangle$, $n = 10$, $\langle L, M \rangle = \langle 5, 1 \rangle$, $n = 12$, $\langle L, M \rangle = \langle 1, -5 \rangle, \langle 5, 1 \rangle$.

LEMMA 2.8. *Put*

$$\widehat{P}_k = \begin{cases} \frac{\xi^k - \bar{\xi}^k}{\xi - \bar{\xi}} & \text{for } k \text{ odd,} \\ \frac{\xi^k - \bar{\xi}^k}{\xi^2 - \bar{\xi}^2} & \text{for } k \text{ even.} \end{cases}$$

If $\xi = 2m + 1 + 2\sqrt{m(m+1)}$ and $\bar{\xi} = 2m + 1 - 2\sqrt{m(m+1)}$, or $\xi = (m + 2 + \sqrt{m(m+4)})/2$ and $\bar{\xi} = (m + 2 - \sqrt{m(m+4)})/2$, then \widehat{P}_k has a primitive prime factor p for any $k > 2$. Moreover, if $p \mid \widehat{P}_n$, then $k \mid n$; conversely, if $k \mid n$, then $\widehat{P}_k \mid \widehat{P}_n$.

Proof. Consider first the case

$$\xi = 2m + 1 + 2\sqrt{m(m + 1)}.$$

Theorem W-D shows that if $k > 2$ and $k \neq 3, 4, 6$, then \widehat{P}_k has a primitive prime factor. So we only need to consider the indices $k = 3, 4$ and 6 . For $k = 3$, we have $\widehat{P}_3 = 16m^2 + 16m + 3 = (4m + 1)(4m + 3)$ and $KL = 64m(m + 1)(2m + 1)^2$. Since

$$KL \equiv -3 \pmod{\widehat{P}_3},$$

we see that if a prime number p divides \widehat{P}_3 and KL , then $p = 3$. It follows that \widehat{P}_3 is never a power of 3, since otherwise $4m + 1$ and $4m + 3$ would be powers of 3, which implies a contradiction. So there exists a prime number p such that $p \mid \widehat{P}_3$ and $p \neq 3$, and p is a primitive prime factor of \widehat{P}_3 .

For $k = 4$, we obtain $\widehat{P}_4 = 16m^2 + 16m + 2$ and $KL\widehat{P}_3 \equiv -4 \pmod{\widehat{P}_4}$. So only the prime $p = 2$ can divide both \widehat{P}_4 and $KL\widehat{P}_3$. Since $8m^2 + 8m + 1$ is odd, \widehat{P}_4 is never a power of 2; hence a prime factor $p > 2$ of \widehat{P}_4 is its primitive prime factor.

For $k = 6$, we have

$$\begin{aligned} \widehat{P}_5 &= (16m^2 + 12m + 1)(16m^2 + 20m + 5), \\ \widehat{P}_6 &= (16m^2 + 16m + 3)(16m^2 + 16m + 1), \end{aligned}$$

and

$$KL\widehat{P}_3\widehat{P}_4\widehat{P}_5 \equiv -3(16m^2 + 16m + 3) \pmod{\widehat{P}_6}.$$

Thus if a prime p divides \widehat{P}_6 and $KL\widehat{P}_3\widehat{P}_4\widehat{P}_5$, then $p = 3$ or $p \mid 16m^2 + 16m + 3$. It is also easy to see that $16m^2 + 16m + 1$ is never a power of 3. So a prime factor $p \neq 3$ of $16m^2 + 16m + 1$ is a primitive prime factor of \widehat{P}_6 . Therefore, if $\xi = 2m + 1 + 2\sqrt{m(m + 1)}$, then \widehat{P}_k ($k > 2$) has a primitive prime factor.

The argument for $\xi = (m + 2 + \sqrt{m(m + 4)})/2$ proceeds as in the first case.

If $p \mid \widehat{P}_n$, we can write $n = 2qk \pm r$, $0 \leq r \leq k$. By Lemma 2.3, $\widehat{P}_n \equiv \pm \widehat{P}_r \pmod{\widehat{P}_k}$, so $p \mid \widehat{P}_r$. Since p is a primitive prime factor of \widehat{P}_k , we have $r = 0$ or $r = k$. Hence $k \mid n$. By Lemma 2.2(4), we know that $\widehat{P}_k \mid \widehat{P}_n$ if and only if $k \mid n$ for any $k > 2$. ■

3. Corollaries for $Ax^2 - By^4 = C$ ($C = 1, 2, 4$). In this section we will introduce some theorems and corollaries for $Ax^2 - By^4 = C$ ($C = 1, 2, 4$).

THEOREM L-T ([7, 15]). *Let D be a positive nonsquare integer and $a_1 + b_1\sqrt{D}$ be the smallest positive integer solution of $x^2 - Dy^2 = 1$. Define*

$$a_k + b_k\sqrt{D} = (a_1 + b_1\sqrt{D})^k, \quad k > 0.$$

Then the equation

$$(3.13) \quad x^2 - Dy^4 = 1$$

has at most two positive integer solutions (x, y) . If two solutions (x_1, y_1) and (x_2, y_2) exist and $y_1 < y_2$, then $y_1 = \sqrt{b_1}$ and $y_2 = \sqrt{b_2}$, except if $D = 1785$ or $16 \cdot 1785$, in which case $y_1 = \sqrt{b_1}$ and $y_2 = \sqrt{b_4}$.

From Theorem L-T, with the above notations, we have the following corollary.

COROLLARY 3.1. *Let s and m be positive integers. Then the equation $x^2 - 4m(m+1)s^2y^4 = 1$ has two solutions if and only if $m = 84$ and $s = 1$, where $b_1 = 1$, $b_4 = (2 \cdot 13 \cdot 239)^2$.*

Proof. Since $a_2 + b_2\sqrt{D} = (a_1 + b_1\sqrt{D})^2$, we have $a_2 = a_1^2 + b_1^2D$ and $b_2 = 2a_1b_1$. If $y_1 = \sqrt{b_1}$ and $y_2 = \sqrt{b_2}$, then b_1 and b_2 are squares, which implies $2a_1$ is a square and $x_1 = a_1$ is even. Therefore, (x_1, y_1) is not a solution of the equation $x^2 - 4m(m+1)s^2y^4 = 1$, since x is odd. We may only take $m = 84$, $s = 1$ if $D = 1785$ or $16 \cdot 1785$, where $b_1 = 1$, $b_4 = (2 \cdot 13 \cdot 239)^2$. So $(x_1, y_1) = (169, 1)$ and $(x_2, y_2) = (6525617281, 6214)$ are two positive integer solutions of $x^2 - 4 \cdot 85 \cdot 86y^4 = 1$. ■

THEOREM L-Y ([9]). *Let A and B be odd positive integers and $u_1\sqrt{A} + v_1\sqrt{B}$ be the smallest positive integer solution of the equation $Ax^2 - By^2 = 4$ with $2 \nmid u_1v_1$. Define*

$$\frac{u_k\sqrt{A} + v_k\sqrt{B}}{2} = \left(\frac{u_1\sqrt{A} + v_1\sqrt{B}}{2} \right)^k, \quad k > 0.$$

If v_1 is not a square, then the equation

$$(3.14) \quad Ax^2 - By^4 = 4$$

has no positive integer solution except in the following two cases:

- (1) $v_1/3$ and $(Bv_1^2 + 3)/3$ are both squares; then $(x, y) = (u_3, \sqrt{v_3})$ is the only positive solution.
- (2) $v_1/5$ and $(B^2v_1^4 + 5Bv_1^2 + 5)/5$ are both squares; then $(x, y) = (u_5, \sqrt{v_5})$ is the only positive solution.

If v_1 is a square, then equation (3.14) has at most one positive integer solution other than $(x, y) = (u_1, \sqrt{v_1})$, which is given by either $(x, y) = (u_3, \sqrt{v_3})$ or $(x, y) = (u_2, \sqrt{v_2})$, the latter occurring if and only if u_1 and v_1 are both squares and $A = 1$, except for $A = 1$ and $B = 5$. If $A = 1$ and $B = 5$, the only two positive solutions of (3.14) are $(x, y) = (u_1, \sqrt{v_1}) = (3, 1)$ and $(x, y) = (u_6, \sqrt{v_6}) = (322, 12)$.

From Theorem L-Y, it is clear that equation (3.14) has two positive integer solutions if and only if v_1 is a square.

With the notations of Theorem L-Y, by computing, we have

COROLLARY 3.2. *If equation (3.14) has two positive integer solutions (x_1, y_1) and (x_2, y_2) with $\gcd(x_1, y_1) = 1$ and $\gcd(x_2, y_2) = 1$, then $A = 1$ and $B \neq 5$, and x_1 is a square, where $(x_1, y_1) = (u_1, \sqrt{v_1})$ and $(x_2, y_2) = (u_2, \sqrt{v_2})$ with $u_2 = u_1^2 - 2 = v_1^2 B + 2$ and $v_2 = u_1 v_1$.*

Proof. Since A and B are both odd, and $\gcd(x_1, y_1) = 1$, $\gcd(x_2, y_2) = 1$, it follows that x_1, y_1, x_2 , and y_2 are all odd.

If $A = 1$ and $B = 5$, then from Theorem L-Y, $(x_1, y_1) = (3, 1)$ and $(x_2, y_2) = (322, 12)$, which is impossible since $\gcd(x_2, y_2) = 2 > 1$. Expanding and computing

$$\frac{u_3\sqrt{A} + v_3\sqrt{B}}{2} = \left(\frac{u_1\sqrt{A} + v_1\sqrt{B}}{2} \right)^3,$$

we have $u_3 = u_1(v_1^2 B + 1) = u_1(u_1^2 A - 3)$ and $v_3 = v_1(u_1^2 A - 1) = v_1(v_1^2 B + 3)$, which is impossible since $x_1 = u_1, y_1 = \sqrt{v_1}, x_2 = u_3$, and $y_2 = \sqrt{v_3}$ are all odd. By Theorem L-Y, Corollary 3.2 is proved. ■

4. Proof of Theorem 1.1. Let (x_0, y_0, z_0) be the positive integer solution with the smallest positive y_0 , and (x, y, z) be any positive integer solution of (1.3), corresponding to positive integer pairs (k_0, l_0) and (k, l) in (2.5) and (2.6), respectively.

If $k_0 = 0$, then by (2.4) and (2.5), we have $y_0 = U_0 = 0$, which implies a contradiction, that is, there does not exist any integer z_0 such that $y_0^2 - bz_0^2 = 1$. If $k_0 = 1$, by (2.4) and (2.5), we have $x_0 = x_0^{(1)}, y_0 = y_0^{(1)} = y_0^{(2)}$, and $z_0 = z_0^{(2)}$. In Theorem 1.1(1) and (2), since $y = y_0^{(1)} = y_0^{(2)} = 1$, it follows that $z_0 = z_0^{(2)} = 0$. We know $(x_0, y_0, z_0) = (x_0^{(1)}, 1, 0)$ is not a positive integer solution of (1.3). So we may set $k_0 \geq 2$.

We first prove Theorem 1.1(1). Assume that Theorem 1.1(1) is not true, that is, the number of positive integer solutions (x, y, z) of equations (1.3) is greater than one. Since $a = m + 1 > 1$ in Theorem 1.1(1), from Lemma 2.1 we see that both k_0 and k are odd. So we set $k > k_0 \geq 3$ and consider the case $2 \nmid k_0$.

By Lemma 2.7(1), we know that

$$(4.15) \quad \frac{\tilde{y}_{(k+1)/2} \tilde{y}_{(k-1)/2}}{\tilde{y}_{(k_0+1)/2} \tilde{y}_{(k_0-1)/2}} = \frac{\tilde{U}_{(k+1)/2} \tilde{U}_{(k-1)/2}}{\tilde{U}_{(k_0+1)/2} \tilde{U}_{(k_0-1)/2}}$$

is a square. If $k_0 > 5$, then $(k_0 + 1)/2 > (k_0 - 1)/2 > 2$. By Lemma 2.8, $\tilde{U}_{(k_0+1)/2}$ and $\tilde{U}_{(k_0-1)/2}$ have primitive prime factors, and so we get

$$(4.16) \quad (k_0 + 1 \text{ divides } k + 1 \text{ or } k - 1) \quad \text{and} \quad (k_0 - 1 \text{ divides } k + 1 \text{ or } k - 1).$$

If $k_0 \leq 5$, since $z_0 > 0$, we have $k_0 = 3$, $k_0 = 5$. If $k_0 = 5$, by Lemma 2.8, $\tilde{U}_{(k_0+1)/2} = \tilde{U}_3$ has a primitive prime factor, and it is trivial that $(k_0 - 1)/2 = 2$ if $k_0 = 5$, and $(k_0 + 1)/2 = 2$, $(k_0 - 1)/2 = 1$ if $k_0 = 3$. Notice that either $(k + 1)/2$ or $(k - 1)/2$ is even. Thus (4.16) holds. We distinguish four possible cases according to (4.16).

(1) Assume that $k_0 + 1 \mid k + 1$ and $k_0 - 1 \mid k - 1$. By Lemma 2.6, $\gcd(\tilde{y}_{(k+1)/2}, \tilde{y}_{(k-1)/2}) = 1$ and $\gcd(\tilde{y}_{(k_0+1)/2}, \tilde{y}_{(k_0-1)/2}) = 1$. By (4.15) it follows that $\tilde{y}_{(k+1)/2}/\tilde{y}_{(k_0+1)/2} = F^2$ and $\tilde{y}_{(k-1)/2}/\tilde{y}_{(k_0-1)/2} = H^2$ for some positive integers F and H . Notice that $\tilde{x}_{(k_0+1)/2}^2 - 4m(m+1)\tilde{y}_{(k_0+1)/2}^2 = 1$, $\tilde{x}_{(k+1)/2}^2 - 4m(m+1)\tilde{y}_{(k+1)/2}^2 = 1$, $\tilde{x}_{(k_0-1)/2}^2 - 4m(m+1)\tilde{y}_{(k_0-1)/2}^2 = 1$, and $\tilde{x}_{(k-1)/2}^2 - 4m(m+1)\tilde{y}_{(k-1)/2}^2 = 1$. It is easy to see that $(\tilde{x}_{(k_0+1)/2}, 1)$ and $(\tilde{x}_{(k+1)/2}, F)$ are two solutions of the equation

$$(4.17) \quad x^2 - 4m(m+1)\tilde{y}_{(k_0+1)/2}^2 y^4 = 1,$$

and $(\tilde{x}_{(k_0-1)/2}, 1)$ and $(\tilde{x}_{(k-1)/2}, H)$ are two solutions of the equation

$$(4.18) \quad x^2 - 4m(m+1)\tilde{y}_{(k_0-1)/2}^2 y^4 = 1.$$

But by Corollary 3.1, equation (4.17) has at most one solution, since otherwise $\tilde{y}_{(k_0+1)/2} = 1$ and $k_0 = 1$, which is impossible. Also equation (4.18) has at most one solution, as otherwise $\tilde{y}_{(k_0-1)/2} = 1$ and $k_0 = 3$, so $\tilde{y}_{(k-1)/2} = 6214^2$, which is absurd. Therefore $F = H = 1$. Hence $k = k_0$.

(2) Assume that $k_0 + 1 \mid k - 1$ and $k_0 - 1 \mid k + 1$. We have $\tilde{y}_{(k-1)/2}/\tilde{y}_{(k_0+1)/2} = F^2$ and $\tilde{y}_{(k+1)/2}/\tilde{y}_{(k_0-1)/2} = H^2$ for some positive integers F and H . A similar discussion to (1) shows that $(\tilde{x}_{(k_0+1)/2}, 1)$ and $(\tilde{x}_{(k-1)/2}, F)$ are two solutions of (4.17), and $(\tilde{x}_{(k_0-1)/2}, 1)$ and $(\tilde{x}_{(k+1)/2}, H)$ are two solutions of (4.18). However, by Corollary 3.1 equations (4.17) and (4.18) have at most one solution each. Thus we have $F = H = 1$, and so $(k - 1)/2 = (k_0 + 1)/2$, $(k_0 - 1)/2 = (k + 1)/2$, which is a contradiction.

(3) Assume that $k_0 + 1 \mid k + 1$ and $k_0 - 1 \mid k + 1$. By Lemma 2.2, it follows that $\tilde{y}_{(k_0+1)/2} \mid \tilde{y}_{(k+1)/2}$, $\tilde{y}_{(k_0-1)/2} \mid \tilde{y}_{(k+1)/2}$, and $\gcd(\tilde{y}_{(k_0+1)/2}, \tilde{y}_{(k_0-1)/2}) = 1$, $\gcd(\tilde{y}_{(k+1)/2}, \tilde{y}_{(k-1)/2}) = 1$. This shows that $\tilde{y}_{(k-1)/2} = F^2$ for some positive integer F . Notice that $(2m + 1)^2 - 4m(m + 1) = 1$ and $\tilde{x}_{(k-1)/2}^2 - 4m(m + 1)\tilde{y}_{(k-1)/2}^2 = 1$. Thus $(2m + 1, 1)$ and $(\tilde{x}_{(k-1)/2}, F)$ are two positive solutions of

$$(4.19) \quad x^2 - 4m(m+1)y^4 = 1.$$

By Corollary 3.1, we have $F = 1$, so $k = 3$. Hence $k \leq k_0$.

(4) Assume that $k_0 + 1 \mid k - 1$ and $k_0 - 1 \mid k - 1$. Using similar arguments to those above, we get $\tilde{y}_{(k+1)/2} = H^2$ for some positive integer H . Thus $(2m + 1, 1)$ and $(\tilde{x}_{(k+1)/2}, H)$ are two solutions of (4.19). By Corollary 3.1, we have $H = 1$, and so $k = 3$, which implies $k \leq k_0$.

Next we consider Theorem 1.1(2). Since $a = m + 4 > 4$, by Lemma 2.1, k_0 and k are both odd, and so let $k > k_0 \geq 3$. We only consider the case $2 \nmid k_0$. The following discussion is analogous to that for Theorem 1.1(1), and by Lemmas 2.7(2) and 2.8, we obtain the same type of formulas (4.15) and (4.16). We also distinguish four possible cases.

(1') $k_0 + 1 \mid k + 1$ and $k_0 - 1 \mid k - 1$. By Lemma 2.6 and (4.15), it follows that $\tilde{y}_{(k+1)/2}/\tilde{y}_{(k_0+1)/2} = F^2$ and $\tilde{y}_{(k-1)/2}/\tilde{y}_{(k_0-1)/2} = H^2$ for some positive integers F and H . Then $(\tilde{x}_{(k_0+1)/2}, 1)$ and $(\tilde{x}_{(k+1)/2}, F)$ are two solutions of

$$(4.20) \quad x^2 - m(m + 4)\tilde{y}_{(k_0+1)/2}^2 y^4 = 4.$$

By Corollary 3.2, we have $u_2 = \tilde{x}_{(k+1)/2} = \tilde{x}_{(k_0+1)/2}^2 - 2$ and $v_2 = \tilde{x}_{(k_0+1)/2} = F^2$, the latter implying that $\tilde{y}_{(k+1)/2} = \tilde{y}_{(k_0+1)/2} \tilde{x}_{(k_0+1)/2} = \tilde{y}_{k_0+1}$, which yields $k + 1 = 2(k_0 + 1)$. Similarly, $(\tilde{x}_{(k_0-1)/2}, 1)$ and $(\tilde{x}_{(k-1)/2}, H)$ are two solutions of

$$(4.21) \quad x^2 - m(m + 4)\tilde{y}_{(k_0-1)/2}^2 y^4 = 4.$$

By Corollary 3.2, we have $k - 1 = 2(k_0 - 1)$. However, $k + 1 = 2(k_0 + 1)$ and $k - 1 = 2(k_0 - 1)$ cannot both hold.

(2') $k_0 + 1 \mid k - 1$ and $k_0 - 1 \mid k + 1$. By Lemma 2.6 and (4.15), we have $\tilde{y}_{(k-1)/2}/\tilde{y}_{(k_0+1)/2} = F^2$ and $\tilde{y}_{(k+1)/2}/\tilde{y}_{(k_0-1)/2} = H^2$ for some positive integers F and H . Then $(\tilde{x}_{(k_0+1)/2}, 1)$ and $(\tilde{x}_{(k-1)/2}, F)$ are two solutions of (4.20), and by Corollary 3.2 we have $\tilde{y}_{(k-1)/2} = \tilde{y}_{(k_0+1)/2} \tilde{x}_{(k_0+1)/2} = \tilde{y}_{k_0+1}$, which implies $k - 1 = 2(k_0 + 1)$. Since $(\tilde{x}_{(k_0-1)/2}, 1)$ and $(\tilde{x}_{(k+1)/2}, H)$ are two solutions of (4.21), by Corollary 3.2 we get $k + 1 = 2(k_0 - 1)$. But $k - 1 = 2(k_0 + 1)$ and $k + 1 = 2(k_0 - 1)$ contradict the assumptions on k_0 and k .

(3') $k_0 + 1 \mid k + 1$ and $k_0 - 1 \mid k + 1$. By a similar discussion to (3) above, we obtain $\tilde{y}_{(k-1)/2} = F^2$ for some positive integer F . It is trivial that $(m + 2, 1)$ and $(\tilde{x}_{(k-1)/2}, F)$ are two solutions of

$$(4.22) \quad x^2 - m(m + 4)y^4 = 4.$$

By Corollary 3.2, we have $\tilde{x}_{(k-1)/2} = m^2 + 4m + 2$ and $\tilde{y}_{(k-1)/2} = m + 2$. Thus $(k - 1)/2 = 2$ and hence $k = 5$. It is obvious that there is no odd positive k_0 such that $k_0 + 1 \mid 6$ and $k_0 - 1 \mid 6$.

(4') $k_0 + 1 \mid k - 1$ and $k_0 - 1 \mid k - 1$. We also have $\tilde{y}_{(k+1)/2} = H^2$ for some positive integer H . Thus $(2m + 1, 1)$ and $(\tilde{x}_{(k+1)/2}, H)$ are two solutions

of (4.22). By Corollary 3.2, we obtain $\tilde{x}_{(k+1)/2} = m^2 + 4m + 2$ and $\tilde{y}_{(k+1)/2} = m + 2$. Thus $(k + 1)/2 = 2$ and so $k = 3$, which contradicts $k > k_0 \geq 3$.

By the above discussion, the proof of Theorem 1.1 is complete. ■

References

- [1] W. S. Anglin, *Simultaneous Pell equations*, Math. Comp. 65 (1996), 355–359.
- [2] —, *The Queen of Mathematics: An Introduction to Number Theory*, Kluwer, Dordrecht, 1995.
- [3] M. A. Bennett, *On the number of solutions of simultaneous Pell equations*, J. Reine Angew. Math. 498 (1998), 173–199.
- [4] M. A. Bennett and P. G. Walsh, *Simultaneous Pell equations with few or no solutions*, Indag. Math. 11 (2000), 1–12.
- [5] L. K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math. 9 (1959), 437–441.
- [6] D. H. Lehmer, *An extended theory of Lucas functions*, Ann. of Math. 31 (1930), 419–438.
- [7] W. Ljunggren, *Ein Satz über die diophantische Gleichung $Ax^2 - By^4 = C$ ($C = 1, 2, 4$)*, in: Toltte Skandinaviska Matematikerkongressen (Lund, 1953), Lunds Univ. Mat. Inst., Lund, 1954, 188–194.
- [8] F. Luca and P. G. Walsh, *Squares in Lehmer sequences and some Diophantine applications*, Acta Arith. 100 (2001), 47–62.
- [9] J. G. Luo and P. Z. Yuan, *Square-classes in Lehmer sequences having odd parameters and their applications*, *ibid.* 127 (2007), 49–62.
- [10] W. L. McDaniel, *The g.c.d. in Lucas sequences and Lehmer number sequences*, Fibonacci Quart. 29 (1991), 24–29.
- [11] P. Ribenboim and W. L. McDaniel, *The square terms in Lucas sequences*, J. Number Theory 58 (1996), 104–123.
- [12] A. Schinzel, *On the primitive prime factors of Lehmer numbers I*, Acta Arith. 8 (1963), 213–223.
- [13] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. 1 (1929), 1–70.
- [14] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. 135 (1909), 284–305.
- [15] A. Togbe, P. M. Voutier and P. G. Walsh, *Solving a family of Thue equations with an application to the equation $x^2 - Dy^4 = 1$* , Acta Arith. 120 (2005), 39–58.
- [16] D. T. Walker, *On the Diophantine equation $mx^2 - ny^2 = \pm 1$* , Amer. Math. Monthly 74 (1967), 504–513.
- [17] P. G. Walsh, *On integer solutions to $x^2 - dy^2 = 1, z^2 - 2dy^2 = 1$* , Acta Arith. 82 (1997), 69–76.
- [18] —, *On two classes of simultaneous Pell equations with no solutions*, Math. Comp. 68 (1999), 385–388.
- [19] M. Ward, *The intrinsic divisors of Lehmer number*, Ann. of Math. (2) 62 (1955), 230–236.
- [20] P. Z. Yuan, *On the number of solutions of $x^2 - 4m(m+1)y^2 = y^2 - bz^2 = 1$* , Proc. Amer. Math. Soc. 132 (2004), 1561–1566.
- [21] —, *Simultaneous Pell equations*, Acta Arith. 115 (2004), 119–131.

- [22] P. Z. Yuan, *A note on the divisibility of the generalized Lucas sequences*, Fibonacci Quart. 40 (2002), 153–156.
- [23] —, *On the number of solutions of simultaneous Pell equations*, Acta Arith. 101 (2002), 215–221.

Zhigang Li and Pingzhi Yuan
Department of Mathematics
Sun Yat-sen University
Guangdong, Guangzhou 510275
P.R. China
E-mail: lizhigangfirst@sohu.com
zhigangli_cn@yahoo.com.cn
mcsypz@mai.sysu.edu.cn

Jianye Xia
Department of Applied Mathematics
Guangdong University of Finance
Guangdong, Guangzhou 510520
P.R. China
E-mail: tjcb43@gduf.edu.cn

*Received on 1.4.2006
and in revised form on 12.3.2007*

(5172)