ON THE NUMBER OF SOLUTIONS OF
\[ x^2 - 4m(m+1)y^2 = y^2 - bz^2 = 1 \]

PINGZHI YUAN

(Communicated by David E. Rohrlich)

Abstract. In this paper, using a result of Ljunggren and some results on primitive prime factors of Lucas sequences of the first kind, we prove the following results by an elementary argument: if \( m \) and \( b \) are positive integers, then the simultaneous Pell equations
\[ x^2 - 4m(m+1)y^2 = y^2 - bz^2 = 1 \]
possesses at most one solution \((x, y, z)\) in positive integers.

1. Introduction

Let \( a \) and \( b \) be nonzero positive integers. In this paper we study positive integer solutions \((x, y, z)\) of the simultaneous Pell equations
\[ x^2 - ay^2 = y^2 - bz^2 = 1. \]

By work of Thue [16] and Siegel [15], (1) has at most finitely many solutions, and all these solutions can be determined effectively by Baker [3]. Combining bounds for linear forms in logarithms of algebraic numbers with techniques from computational Diophantine approximations, all the solutions of (1) have been explicitly determined for certain values of \( a \) and \( b \) (see, e.g., [1], [3], [4], [7], [8], [9], and [13]). Anglin [2] devotes Section 4.6 of his textbook to the description of an algorithm for solving equations of forms similar to those of (1). Recently, Bennett [5], sharpening work of Masser and Rickert [12], applied techniques involving simultaneous Padé approximations of binomial functions, the theory of linear forms in two logarithms and some gap principles, to prove

Theorem 1.1 (Bennett [5], Th. 7.1). If \( a \) and \( b \) are distinct nonzero positive integers, then the simultaneous Diophantine equations (1) possess at most three solutions \((x, y, z)\) in positive integers.

By using a result of Ljunggren [11], results of Carmichael [6] and Voutier [17] concerning primitive prime factors of Lucas sequences of the first kind (see [6]), and properties of Lucas sequences, we shall prove

Theorem 1.2. If \( m \) and \( b \) are nonzero positive integers and \( a = 4m(m+1) \), then (1) possesses at most one solution \((x, y, z)\) in positive integers.

Received by the editors September 3, 2002.
2000 Mathematics Subject Classification. Primary 11D09; Secondary 11D25.
Key words and phrases. Simultaneous Diophantine equations, Pell equations, Lucas sequences.

©2004 American Mathematical Society
Notice that if $\alpha = 2m + 1 + 2\sqrt{m(m + 1)}$, $u_n = (\alpha^n - \alpha^{-n})/(\alpha - \alpha^{-1})$ and $b = u_n^2 - 1$, then (1) admits the solution $(x, y, z) = ((\alpha^n + \alpha^{-n})/2, u_n, 1)$. So the bound in Theorem 1.2 can be reached. We think that a much more general result is true:

**Conjecture 1.1.** For any nonzero positive integers $a$ and $b$, (1) possesses at most one positive integer solution $(x, y, z)$.

2. Some Lemmas

Suppose that $a$ and $b$ are nonzero positive integers, and neither $a$ nor $b$ is a perfect square. Let $\alpha$ and $\beta$ be the fundamental solutions of the Pell equations $x^2 - ay^2 = 1$ and $y^2 - bz^2 = 1$, respectively. Put

$$U_k = \frac{\alpha^k - \alpha^{-k}}{2\sqrt{\alpha}}, \quad V_k = \frac{\alpha^k + \alpha^{-k}}{2}, \quad V'_k = \frac{\beta^k + \beta^{-k}}{2}.$$  

The following lemma is fairly well known.

**Lemma 2.1** ([14]).

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 $U_m|U_n$ if and only if $m|n$.
5. If $m \geq 1$, then $V_m|V_n$ if and only if $n/m$ is an odd integer.
6. $U_{2m} = 2U_mV_m$.

**Lemma 2.2.** Let $k_0$, $k_1$, $k_2$ and $q$ be positive integers with $k_2 = 2qk_1 \pm k_0$, $0 \leq k_0 \leq k_1$. Then $U_{k_2} \equiv \pm U_{k_0}$ (mod $U_{k_1}$).

**Proof.** Since $U_{k_2} \equiv 2V_{k_1} \pm U_{k_0}$ (mod $U_{k_1}$) by direct computation, the lemma follows readily from Lemma 2.1 (4). $\square$

**Lemma 2.3.** Let $k_0$, $k_1$, $k_2$ and $q$ be positive integers with $k_2 = 2qk_1 \pm k_0$, $0 \leq k_0 \leq k_1$.

1. If $2|q$, then $V_{k_2} \equiv V_{k_0}$ (mod $V_{k_1}$).
2. If $2 \nmid q$, then $V_{k_2} \equiv -V_{k_0}$ (mod $V_{k_1}$).

**Proof.** If $q$ is even, then $V_{k_2} - V_{k_0} = 2aU_{k_1} \pm k_0u_{k_1}k_1$ and $V_{k_2}U_{2k_1}U_{qk_1}$, whence $V_{k_2} \equiv V_{k_0}$ (mod $V_{k_1}$). If $q$ is odd, then $V_{k_2} + V_{k_0} = 2V_{k_1} \pm v_{k_1}V_{qk_1}$, and $V_{k_1}V_{qk_1}$, whence $V_{k_2} \equiv -V_{k_0}$ (mod $V_{k_1}$). $\square$

Suppose that $(x, y, z)$ is a positive integer solution of (1). Then there exist positive integers $k$ and $l$ with

$$y = \frac{\alpha^k - \alpha^{-k}}{2\sqrt{\alpha}} = \frac{\beta^l + \beta^{-l}}{2}.$$  

Denote by $N(a, b)$ the number of positive solutions $(x, y, z)$ of (1). Let $(x_0, y_0, z_0)$ be the solution $(x, y, z)$ of (1) with the minimal positive integer $y$, and $k_0$, $l_0$ the corresponding $k$ and $l$ in (3), that is,

$$y_0 = \frac{\alpha^{k_0} - \alpha^{-k_0}}{2\sqrt{\alpha}} = \frac{\beta^{l_0} + \beta^{-l_0}}{2}.$$  

**Lemma 2.4.** If $(x, y, z)$ is a positive integer solution of (1), and $k$, $l$, $k_0$ and $l_0$ satisfy (3) and (4), then $y_0|y$, $l_0|l$ and $k_0|k$. Moreover, $l/l_0$ and $k/k_0$ are odd integers.
Proof. Notice that by Lemma 2.1 (5) we have that \( V'_0 | V'_1 \) if and only if \( l/l_0 \) is an odd integer. If \( U_{k_0} \neq 1 \), then \( U_{k_0}(U_k) \) if and only if \( k_0 | k \) and \( \text{ord}_2(U_k/U_{k_0}) = \text{ord}_2(k/k_0) \). So

\[ k_0 | k \implies y_0 | y \implies l_0 | l, \]

and \( l/l_0 \) and \( k/k_0 \) are odd. If \( l_0 | l \) and \( l/l_0 \) is odd, then \( y_0 | y, k_0 | k \), and \( k_0 | k_0 \) is odd. Otherwise, there are positive integers \( q, s, q_1 \) and \( t \), uniquely determined by \( k, l, k_0 \) and \( l_0 \), respectively, such that

\[ k = 2qk_0 + s, \quad 0 < s < k_0, \quad l = 2q_1l_0 + t, \quad 0 \leq t < l_0. \]

It follows from (6), Lemma 2.2 and Lemma 2.3 that

\[ y = U_k \equiv \pm U_s \pmod{U_{k_0}} \equiv \pm U_s \pmod{y_0}. \]

\[ y = V'_l \equiv \pm V'_s \pmod{V'_0} \equiv \pm V'_s \pmod{y_0}. \]

Since \( U_s < \frac{1}{4}U_{s+1} \leq \frac{1}{4}y_0 \) and \( V'_l < \frac{1}{4}V'_{l+1} \leq \frac{1}{4}y_0 \), we deduce a contradiction from (7) and (8).

In this paper, we confine our attention to the case of \( a = 4m(m+1) \). Hence \( \alpha = 2m + 1 + 2\sqrt{m(m+1)} \). Let \( \xi = \sqrt{m+1} + \sqrt{m}, \zeta = \sqrt{m+1} - \sqrt{m} \). Then \( \alpha \equiv \xi^2 \). Put

\[ x_k = \frac{\xi^k + \zeta^k}{2\sqrt{m+1}}, \quad y_k = \frac{\xi^k - \zeta^k}{2\sqrt{m}} \quad \text{if} \quad 2 \nmid k, \]

and

\[ x_k = V_{k/2}, \quad y_k = U_{k/2} \quad \text{if} \quad 2 | k. \]

Obviously, we have

\[ U_k = x_ky_k \quad \text{if} \quad 2 \nmid k \quad \text{and} \quad U_k = 2x_ky_k \quad \text{if} \quad 2 | k. \]

Lemma 2.5.

\[ U_k^2 - 1 = U_{k+1}U_{k-1} = \left\{ \begin{array}{ll} 4x_{k+1}y_{k+1}x_{k-1}y_{k-1} & \text{if} \quad 2 \nmid k, \\ x_{k+1}y_{k+1}x_{k-1}y_{k-1} & \text{if} \quad 2 | k \end{array} \right. \]

Proof. Since \( \alpha^2 = 8m(m+1) + 1 + 4(2m+1)\sqrt{m(m+1)} \), we have

\[ U_k^2 - 1 = \frac{\alpha^{2k} + \alpha^{-2k} - 2}{16m(m+1)} - 1 = \frac{\alpha^{2k} + \alpha^{-2k} - (\alpha^2 + \alpha^{-2})}{16m(m+1)} \]

\[ = \frac{(\alpha^{k+1} - \alpha^{-k-1})(\alpha^{k-1} - \alpha^{-k+1})}{16m(m+1)} = U_{k+1}U_{k-1} \]

\[ = \left\{ \begin{array}{ll} 4x_{k+1}y_{k+1}x_{k-1}y_{k-1} & \text{if} \quad 2 \nmid k, \\ x_{k+1}y_{k+1}x_{k-1}y_{k-1} & \text{if} \quad 2 | k \end{array} \right. \]

\[ \square \]

Lemma 2.6. (1) If \( k \) is even, then \( x_{k+1}, y_{k+1}, x_{k-1} \) and \( y_{k-1} \) are pairwise co-prime integers.

(2) If \( k \) is odd, then \( \gcd(x_{k+1}, x_{k-1}) = 1 \), \( \gcd(y_{k+1}, y_{k-1}) = 1 \),

\[ \gcd(x_{k+1}, y_{k-1}) = \left\{ \begin{array}{ll} 1 & \text{if} \quad k \equiv 3 \pmod{4}, \\ 2m + 1, & \text{if} \quad k \equiv 1 \pmod{4}. \end{array} \right. \]
Proof. (1) This is a special case of Theorem 1 of the author [18].

(2) If \( k \) is odd, then we derive the result from (10), Lemma 2.1 (3) and \( y_2 = V_1 = 2m + 1 \).

**Lemma 2.7** ([11]). For any positive integers \( A \) and \( B \), the Diophantine equation 
\[ Ax^2 - By^4 = 1 \]
has at most one positive integer solution \((x, y)\).

**Lemma 2.8.** If \( k > 2 \), then \( U_k \) has a primitive prime factor \( p \), and moreover, \( p | U_n \) if and only if \( k | n \).

Proof. The last assertion follows immediately from the definition of primitive prime factors. So it suffices to prove the first assertion. The results of Carmichael [6] and Voutier [17], concerning primitive prime factors of the first kind, imply the lemma if \( k \geq 5 \) and \( k \neq 6 \). The cases \( k = 3, 4, \) and \( 6 \) can be obtained by direct computation. If \( k = 3 \), then \( U_3 = \alpha^2 + \alpha^{-2} + 1 = 16m(m+1)+3 \) but \( 16m(m+1)+3 = 3^4 \) implies 
\[ (3^4 + 1)/(3+1) = □ \] (here and later \( □ \) stands for a perfect square of an integer), which is impossible. Therefore \( U_3 \) has a primitive prime factor. If \( k = 4 \), then \( (\alpha^2 + \alpha^{-2})/2 = 8m(m+1)+1 \), and its prime factors are primitive prime factors of \( U_4 \). Hence \( U_4 \) has a primitive prime factor. If \( k = 6 \), then \( \alpha^2 + \alpha^{-2} - 1 = 16m(m+1)+1 \neq 3^4 \), since otherwise \( 3^4 + 3 = 4C \), which is impossible. So \( U_6 \) has a primitive prime factor. This completes the proof. □

### 3. Proof of Theorem 1.2

Assume \( a = 4m(m+1) \). If \( N(a, b) > 1 \), let \((x_0, y_0, z_0)\) be the positive solution \((x, y, z)\) of (1) with minimal positive \( y \) value, and \((x, y, z)\) another positive integer solution of (1). Define \( k, l, k_0 \) and \( l_0 \) by (3) and (4). From Lemma 2.4 we know that \( l/l_0 \) and \( k/k_0 \) are odd integers, which implies \( z_0 | z \).

**Case I.** If \( 2 | k_0 \), then from the proof of Lemma 2.5 we have
\[ b^2 z_0^2 = U_{k_0}^2 - 1 = U_{k_0+1} U_{k_0-1} = x_{k_0+1} y_{k_0+1} x_{k_0-1} y_{k_0-1} \]
and
\[ b z^2 = U_k^2 - 1 = U_{k+1} U_{k-1} = x_{k+1} y_{k+1} x_{k-1} y_{k-1} \]
If \( k_0 > 3 \), by Lemma 2.8, \( U_{k+1} \) and \( U_{k-1} \) have primitive prime factors \( p \) and \( q \), respectively, and by combining \( z_0 | z \), (13), (14) and Lemma 2.8 we get
\[ k_0 + 1 \text{ divides } k + 1 \text{ or } k - 1 \text{ and } k_0 - 1 \text{ divides } k + 1 \text{ or } k - 1 . \]
If \( k_0 = 2 \), by Lemma 2.8, \( U_3 \) has a primitive prime factor \( p \). By \( k_0 - 1 = 1 \), \( z_0 | z \), (13), (14) and Lemma 2.8, (15) holds too. Since both \( k_0 \) and \( k \) are even, \( x_{k_0+1}, y_{k_0+1}, x_{k_0-1} \) and \( y_{k_0-1} \) are pairwise coprime integers by Lemma 2.6, and so are \( x_{k+1}, y_{k+1}, x_{k-1} \) and \( y_{k-1} \). Therefore if \( k_0 + 1 | k + 1 \) and \( k_0 - 1 | k - 1 \), then by (13), (14), Lemma 2.1 and Lemma 2.6 (1) we have
\[ x_{k+1}/x_{k_0+1} = A^2, \text{ } y_{k+1}/y_{k_0+1} = B^2, \text{ } x_{k-1}/x_{k_0-1} = C^2, \text{ } y_{k-1}/y_{k_0-1} = D^2 \]
for some positive integers \( A, B, C \) and \( D \). Notice that \( 2 \nmid (k_0+1)(k_0-1)(k+1)(k-1) \).
So by (9) and (16) we have
\[ (m+1)x_{k_0+1}^2 A^4 - my_{k_0+1}^2 B^4 = 1 \]
and

\[(m + 1)x_{k_0 - 1}^2 - my_{k_0 - 1}^2 D^4 = 1.\]

Note that \((m + 1)x_{k_0 + 1}^2 - my_{k_0 + 1}^2 = 1\) and \((m + 1)x_{k_0 - 1}^2 - my_{k_0 - 1}^2 = 1\) by (9). So by (17), (18) and Lemma 2.7 we have

\[k + 1 = k_0 + 1 \quad \text{and} \quad k - 1 = k_0 - 1,
\]

which implies that \(k = k_0\). If \(k_0 + 1\) divides \(k - 1\) and \(k_0 - 1\) divides \(k + 1\), then similarly to the above discussions we get

\[k + 1 = k_0 - 1 \quad \text{and} \quad k - 1 = k_0 + 1,
\]

which is impossible. If \(k_0 + 1\) divides \(k + 1\) and \(k_0 - 1\) divides \(k + 1\), then \((k_0 + 1)(k_0 - 1), k - 1) = 1.

So by (13), (14) and \(z_0 | z\) we have \(U_{k - 1} = x_{k - 1} y_{k - 1} = 1\). Hence \(x_{k - 1} = A^2\) and \(y_{k - 1} = B^2\) for some positive integers \(A\) and \(B\). So \((m + 1)A^4 - mB^4 = 1\). From \((m + 1) = 1\) and Lemma 2.7 we get \(k = 2\), which is impossible. Similarly, the case \(k_0 + 1\) divides \(k - 1\) and \(k_0 - 1\) divides \(k + 1\) is impossible.

Case II. If \(2 \nmid k_0\), then from the proof of Lemma 2.5 we have

\[(19) \quad b_k^2 = U_{k_0 + 1}^2 - 1 = U_{k_0 + 1} U_{k_0 - 1} = 4x_{k_0 + 1} y_{k_0 + 1} x_{k_0 - 1} y_{k_0 - 1}
\]

and

\[(20) \quad b_k^2 = U_{k - 1}^2 - 1 = U_{k - 1} U_{k - 1} = 4x_{k - 1} y_{k - 1} x_{k - 1} y_{k - 1}.
\]

If \(k_0 > 3\), then, by Lemma 2.8, \(U_{k_0 + 1}\) and \(U_{k_0 - 1}\) have primitive prime factors \(p\) and \(q\) respectively. Combining \(z_0 | z\), (19), (20) and Lemma 2.8, we have

\[(21) \quad k_0 + 1 \text{ divides } k + 1 \text{ or } k - 1 \quad \text{and} \quad k_0 - 1 \text{ divides } k + 1 \text{ or } k - 1.
\]

If \(k_0 \leq 3\), then \(k_0 = 3\) since \(z_0 > 0\). By Lemma 2.8, \(U_4\) has a primitive prime factor \(p\). Since \(k_0 - 1 = 2\), by \(z_0 | z\), (19), (20) and Lemma 2.8 we see that (21) holds too.

First we assume that \(k_0 + 1\) divides \(k + 1\) and \(k_0 - 1\) divides \(k - 1\). If \(2 | k_0 + 1\), then by (10) and Lemma 2.1 we have

\[(22) \quad x_{k - 1}/x_{k + 1} = A, \quad y_{k + 1}/y_{k - 1} = B^2, \quad 2m + 1|(x_{k + 1}, x_{k + 1})
\]

for some positive integers \(A\) and \(B\). This yields

\[x_{k + 1}^2 A^4 - y_{k + 1}^2 \cdot 4m(m + 1) B^4 = 1,
\]

and, by Lemma 2.7, \(A = B = 1\). Hence \(x_{k + 1}^2 - y_{k + 1}^2 \cdot 4m(m + 1) = 1\), and so \(k_0 + 1 = k + 1\), that is, \(k = k_0\). Similarly we derive that \(k = k_0\) in the case \(2 | k_0 - 1\), in which case, \(x_{k + 1}^2 = 4m(m + 1)y_{k + 1}^2 = 1\).

Next we assume that \(k_0 + 1|k - 1\) and \(k_0 - 1|k + 1\). If \(2 | k_0 + 1\), then as before \(k + 1|k_0 - 1\), that is, \(k = k_0 + 1\). By \(k_0 - 1|k + 1\) we obtain \(k_0 - 1|4\); so \(k_0 = 5\) and \(k = 7\). Then, by (19) and (20), \(U_5/U_4 = 2V_4\) is a perfect square, which is impossible. If \(2 | k_0 - 1\), we obtain similarly \(k_0 - 1 = k + 1\), which is impossible.

Now we assume that \(k_0 + 1|k + 1\) and \(k_0 - 1|k + 1\). Then \(U_{k_0 + 1} U_{k + 1}\) and \(U_{k_0 - 1} U_{k + 1}\). By Lemma 2.1, \(\gcd(U_{k_0 + 1}, U_{k_0 - 1}) = 2(2m + 1)\), since \(U_2 = 2(2m + 1)\). Therefore \(U_{k - 1} = 2x_{k - 1} y_{k - 1} = 2(2m + 1)\). Note that \((2m + 1)|x_{k - 1}\) and \((x_{k - 1}, y_{k - 1}) = 1\) by Lemma 2.6. Thus \(x_{k - 1} = A^2, y_{k - 1} = B^2\) for some positive integers \(A\) and \(B\). Therefore, by the definitions of \(x_{k - 1}\) and \(y_{k - 1}\), \((2m + 1)^2 A^4 - 4m(m + 1) B^4 = 1\). So by Lemma 2.7 and \((2m + 1)^2 - 4m(m + 1) = 1\) we have \(A = 1\) and \(B = 1\) or \(k = 2\), which is impossible. The solution of the last case \(k_0 + 1|k - 1\) and \(k_0 - 1|k - 1\) is just the same as the case \(k_0 + 1|k + 1\) and \(k_0 - 1|k + 1\). This completes the proof.
ACKNOWLEDGMENTS

This paper was rewritten in Leiden University when I was a visiting scholar. I am pleased to thank Robert Tijdeman for his encouragement and a number of helpful suggestions, and I would also like to thank Jan Hendrik Evertse and the Mathematical Institute for their hospitality.

REFERENCES


Department of Mathematics, ZHONGSHAN University, GUANGZHOU 510275, P.R. CHINA
E-mail address: yuanpz@csru.edu.cn
E-mail address: mcsypz@zsu.edu.cn
E-mail address: yuanpz@mail.csu.edu.cn