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

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

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.

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 α and β be the fundamental solutions of the Pell equations $x^2 - ay^2 = 1$ and $y^2 - bz^2 = 1$, respectively. Put

$$(2) \quad U_k = \frac{\alpha^k - \alpha^{-k}}{2\sqrt{a}}, \quad V_k = \frac{\alpha^k + \alpha^{-k}}{2}, \quad V'_l = \frac{\beta^l + \beta^{-l}}{2}.$$

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) $U_{2m} = 2U_m V_m$.

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 $U_{k_2} \equiv \pm U_{k_0} \pmod{U_{k_1}}$.

Proof. Since $U_{k_2} \mp U_{k_0} = 2V_{kq_1 \pm k_0} U_{qk_1}$ 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 $V_{k_2} \equiv V_{k_0} \pmod{V_{k_1}}$,

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

Proof. If q is even, then $V_{k_2} - V_{k_0} = 2aU_{kq_1 \pm k_0} U_{qk_1}$ and $V_{k_1} | U_{2k_1} | U_{qk_1}$, whence $V_{k_2} \equiv V_{k_0} \pmod{V_{k_1}}$. If q is odd, then $V_{k_2} + V_{k_0} = 2V_{kq_1 \pm k_0} V_{qk_1}$ and $V_{k_1} | V_{qk_1}$, whence $V_{k_2} \equiv -V_{k_0} \pmod{V_{k_1}}$. $\square$

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

$$(3) \quad y = \frac{\alpha^k - \alpha^{-k}}{2\sqrt{a}} = \frac{\beta^l + \beta^{-l}}{2}.$$

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,

$$(4) \quad y_0 = \frac{\alpha^{k_0} - \alpha^{-k_0}}{2\sqrt{a}} = \frac{\beta^{l_0} + \beta^{-l_0}}{2}.$$

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 $V'_{l_0} | V'_l$ 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

$$(5) \quad k_0 | k \quad \implies \quad y_0 | y \quad \implies \quad l_0 | l,$$

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/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

$$(6) \quad k = 2qk_0 \pm s, \quad 0 < s < k_0, \quad l = 2q_1l_0 \pm t, \quad 0 \leq t < l_0.$$

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

$$(7) \quad y = U_k \equiv \pm U_s \pmod{U_{k_0}} \equiv \pm U_s \pmod{y_0},$$

$$(8) \quad y = V'_l \equiv \pm V'_t \pmod{V'_{l_0}} \equiv \pm V'_t \pmod{y_0}.$$

Since $U_s < \frac{1}{2}U_{s+1} \leq \frac{1}{2}y_0$ and $V'_t < \frac{1}{2}V'_{t+1} \leq \frac{1}{2}y_0$, we deduce a contradiction from (7) and (8). $\square$

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 $\xi = \sqrt{m+1} + \sqrt{m}$, $\bar{\xi} = \sqrt{m+1} - \sqrt{m}$. Then $\alpha = \xi^2$. Put

$$(9) \quad x_k = \frac{\xi^k + \bar{\xi}^k}{2\sqrt{m+1}}, \quad y_k = \frac{\xi^k - \bar{\xi}^k}{2\sqrt{m}} \quad \text{if} \quad 2 \nmid k,$$

and

$$(10) \quad x_k = V_{k/2}, \quad y_k = U_{k/2} \quad \text{if} \quad 2 | k.$$

Obviously, we have

$$(11) \quad U_k = x_k y_k \quad \text{if} \quad 2 \nmid k \quad \text{and} \quad U_k = 2x_k y_k \quad \text{if} \quad 2 | k.$$

Lemma 2.5.

$$(12) \quad U_k^2 - 1 = U_{k+1}U_{k-1} = \begin{cases} 4x_{k+1}y_{k+1}x_{k-1}y_{k-1} & \text{if} \quad 2 \nmid k, \\ x_{k+1}y_{k+1}x_{k-1}y_{k-1} & \text{if} \quad 2 | k. \end{cases}$$

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

$$\begin{aligned} U_k^2 - 1 &= \frac{\alpha^{2k} + \alpha^{-2k} - 2}{16m(m+1)} - 1 = \frac{\alpha^{2k} + \alpha^{-2k} - (\alpha^2 + \alpha^{-2})}{16m(m+1)} \\ &= \frac{(\alpha^{k+1} - \alpha^{-k-1})(\alpha^{k-1} - \alpha^{-k+1})}{16m(m+1)} = U_{k+1}U_{k-1} \\ &= \begin{cases} 4x_{k+1}y_{k+1}x_{k-1}y_{k-1} & \text{if} \quad 2 \nmid k, \\ x_{k+1}y_{k+1}x_{k-1}y_{k-1} & \text{if} \quad 2 | k. \end{cases} \end{aligned}$$

$\square$

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

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

$$\gcd(x_{k+1}, y_{k-1}) = \begin{cases} 1, & k \equiv 3 \pmod{4}, \\ 2m+1, & k \equiv 1 \pmod{4}, \end{cases}$$

and

$$\gcd(y_{k+1}, x_{k-1}) = \begin{cases} 1, & k \equiv 1 \pmod{4}, \\ 2m+1, & k \equiv 3 \pmod{4}. \end{cases}$$

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 $y_2 = V_1 = 2m+1$. $\square$

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 $16m(m+1) + 3 = 3^s$ implies $(3^s + 1)/(3 + 1) = \square$ (here and later $\square$ 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 . So U_4 has a primitive prime factor. If $k = 6$, then $\alpha^2 + \alpha^{-2} - 1 = 16m(m+1) + 1 \neq 3^t$, since otherwise $3^t + 3 = 4\square$, which is impossible. So U_6 has a primitive prime factor. This completes the proof. $\square$

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

$$(13) \quad bz_0^2 = U_{k_0}^2 - 1 = U_{k_0+1}U_{k_0-1} = x_{k_0+1}y_{k_0+1}x_{k_0-1}y_{k_0-1}$$

and

$$(14) \quad bz^2 = U_k^2 - 1 = U_{k+1}U_{k-1} = x_{k+1}y_{k+1}x_{k-1}y_{k-1}.$$

If $k_0 > 3$, by Lemma 2.8, U_{k_0+1} and U_{k_0-1} have primitive prime factors p and q , respectively, and by combining $z_0|z$, (13), (14) and Lemma 2.8 we get

$$(15) \quad k_0 + 1 \text{ divides } k + 1 \text{ or } k - 1 \quad \text{and} \quad k_0 - 1 \text{ divides } k + 1 \text{ or } k - 1.$$

If $k_0 = 2$, 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

$$(16) \quad x_{k+1}/x_{k_0+1} = A^2, \quad y_{k+1}/y_{k_0+1} = B^2, \quad x_{k-1}/x_{k_0-1} = C^2, \quad y_{k-1}/y_{k_0-1} = D^2$$

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

$$(17) \quad (m+1)x_{k_0+1}^2A^4 - my_{k_0+1}^2B^4 = 1$$

and

$$(18) \quad (m+1)x_{k_0-1}^2 C^4 - my_{k_0-1}^2 D^4 = 1.$$

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 $k_0+1|k-1$ and $k_0-1|k+1$, 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 $k_0+1|k+1$ and $k_0-1|k+1$, then $((k_0+1)(k_0-1), k-1) = 1$. So by (13), (14) and $z_0|z$ we have $U_{k-1} = x_{k-1}y_{k-1} = \square$. 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 $(m+1) - m = 1$ and Lemma 2.7 we get $k = 2$, which is impossible. Similarly, the case $k_0+1|k-1$ and $k_0-1|k-1$ is impossible.

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

$$(19) \quad bz_0^2 = U_{k_0}^2 - 1 = U_{k_0+1}U_{k_0-1} = 4x_{k_0+1}y_{k_0+1}x_{k_0-1}y_{k_0-1}$$

and

$$(20) \quad bz^2 = U_k^2 - 1 = U_{k+1}U_{k-1} = 4x_{k+1}y_{k+1}x_{k-1}y_{k-1}.$$

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 $k_0+1|k+1$ and $k_0-1|k-1$. If $2||k_0+1$, then by (10) and Lemma 2.1 we have

$$(22) \quad x_{k+1}/x_{k_0+1} = A^2, \quad y_{k+1}/y_{k_0+1} = B^2, \quad 2m+1|(x_{k_0+1}, x_{k+1})$$

for some positive integers A and B . This yields

$$x_{k_0+1}^2 A^4 - y_{k_0+1}^2 \cdot 4m(m+1)B^4 = 1,$$

and, by Lemma 2.7, $A = B = 1$. Hence $x_{k_0+1}^2 - y_{k_0+1}^2 \cdot 4m(m+1) = 1$, 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, $x_{k_0-1}^2 - 4m(m+1)y_{k_0-1}^2 = 1$.

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, $k = k_0+2$. By $k_0-1|k+1$ we obtain $k_0-1|4$; so $k_0 = 5$ and $k = 7$. Then, by (19) and (20), $U_8/U_4 = 2V_4$ 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 $U_{k-1} = 2x_{k-1}y_{k-1} = 2(2m+1)\square$. 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 treatment of the last case $k_0+1|k-1$ and $k_0-1|k-1$ is just the same as of 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

- [1] W. S. Anglin, *Simultaneous Pell equations*, Math. Comp. **65** (1996), no. 213, 355-359. MR **96d**:11030
- [2] W. S. Anglin, *The Queen of Mathematics: An Introduction to Number Theory*, Kluwer, Dordrecht, 1995. MR **96c**:11001
- [3] A. Baker, *Linear forms in the logarithms of algebraic numbers, IV*, Mathematika, **15** (1968), 204-216. MR **41**:3402
- [4] A. Baker and H. Davenport, *The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$* , Quart. J. Math. Oxford Ser. (2) **20** (1969), 129-137. MR **40**:1333
- [5] M. A. Bennett, *On the number of solutions of simultaneous Pell equations*, J. reine angew. Math. **498** (1998), 173-199. MR **99c**:11029
- [6] R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$* , Ann. Math. (2) **15** (1913), 30-70.
- [7] E. Brown, *Sets in which $xy + k$ is always a square*, Math. Comp. **45** (1985), no. 172, 613-620. MR **86k**:11019
- [8] C. M. Grinstead, *On a method of solving a class of Diophantine equations*, Math. Comp. **32** (1978), no. 143, 936-940. MR **58**:10724
- [9] K. Kedlaya, *Solving constrained Pell equations*, Math. Comp. **67** (1998), no. 222, 833-842. MR **98g**:11147
- [10] D. H. Lehmer, *An extended theory of Lucas' function*, Ann. Math. **31** (1931), 419-449.
- [11] W. Ljunggren, *Ein Satz über die Diophantische Gleichung $Ax^2 - By^4 = C$ ($C = 1, 2, 4$)*, Tolfte Skand. Mat., Lund, 1953, 188-194. MR **16**:448a
- [12] D. W. Masser and J. H. Rickert, *Simultaneous Pell equations*, J. Number Theory **61** (1996), 52-66. MR **98c**:11023
- [13] R. G. E. Pinch, *Simultaneous Pellian equations*, Math. Proc. Cambridge Philos. Soc. **103** (1988), 35-46. MR **89a**:11029
- [14] P. Ribenboim and W. L. McDaniel, *The square terms in Lucas sequences*, J. Number Theory **58** (1996), 104-123. MR **97c**:11021
- [15] C. L. Siegel, *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. **1** (1929), 1-70.
- [16] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. reine angew. Math. **135** (1909), 284-305.
- [17] P. M. Voutier, *Primitive divisors of Lucas and Lehmer sequences*, Math. Comp. **64** (1995), no. 210, 869-888. MR **95f**:11022
- [18] P. Yuan, *A Note on the Divisibility of the Generalized Lucas Sequences*, Fibonacci Quart., **40** (2002), 153-156. MR **2003c**:11017

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