ACTA ARITHMETICA
101.3 (2002)

On the number of solutions of simultaneous Pell equations

by

Pingzhi Yuan (Changsha)

1. Introduction. In this paper, we shall investigate positive integer solutions (x, y, z) of the simultaneous Diophantine equations

$$x^2 - az^2 = y^2 - bz^2 = 1, \tag{1}$$

where a and b are distinct nonzero integers. These and related equations have connections with polygonal numbers, P_i-sets and elliptic curves. Here we refer the reader to [7], [8], [11] and [12].

Denote by $N(a, b)$ the number of solutions to (1) in positive integers (x, y, z). Let m be a positive integer,

$$n(l, m) = \frac{(m + \sqrt{m^2 - 1})^{2l} - (m - \sqrt{m^2 - 1})^{2l}}{4\sqrt{m^2 - 1}},$$

and let $N_{l,m} = N(a, b)$, where $(a, b) = (m^2 - 1, n^2(l, m) - 1)$. In [3] and [4], combining bounds for linear forms in logarithms of algebraic numbers with techniques from computational Diophantine approximation, Bennett, sharpening work of Masser and Rickert [10], proved

Theorem 1.1 ([3], Th.1.1). *If a and b are distinct positive integers, then the simultaneous equations* (1) *have at most three solutions (x, y, z) in positive integers.*

Theorem 1.2 ([4], Th.1.3). *If l and m are positive integers with $l \geq 2$ and $m \geq 3 \cdot 10^7 \sqrt{l} \log^2 l$, then $N_{l,m} = 2$.*

Bennett [4] also proposed

Conjecture 1.3. *If a and b are distinct positive integers, then $N(a, b) \leq 2$.*

In this paper, we prove

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

Key words and phrases: simultaneous Diophantine equations, Diophantine approximations, linear forms in logarithms, Lucas sequences.

Theorem 1.4. *If a and b are distinct positive integers with* $\max(a,b) \geq 1.4 \cdot 10^{57}$, *then* $N(a,b) \leq 2$.

This result provides an almost affirmative answer to Conjecture 1.3. Lower bounds for linear forms in the logarithms of (three) algebraic numbers allow one to effectively solve any given system of equations of the form (1), in conjunction with techniques from computational Diophantine approximation (see e.g. [1] where it is shown that (1) has at most one positive solution for $2 \leq a < b \leq 200$). That being said, the computations remaining to resolve Conjecture 1.3 appear to be highly nontrivial.

2. Some lemmas. Suppose that $b > a \geq 2$ are nonsquare integers. Let us first note (see [4] and later in this paper) that we can restrict ourselves to a and b of the form $a = m^2 - 1$ and $b = n^2 - 1$ $(m < n)$ without loss of generality (provided $N(a,b) \geq 1$). Henceforth, we assume that a and b are of this form and put $\alpha = m + \sqrt{m^2-1}$, $\beta = n + \sqrt{n^2-1}$,

$$U_k = \frac{\alpha^k - \alpha^{-k}}{2\sqrt{a}}, \qquad U'_k = \frac{\beta^k - \beta^{-k}}{2\sqrt{b}}, \qquad V_k = \frac{\alpha^k + \alpha^{-k}}{2}. \tag{2}$$

Lemma 2.1. *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 the well known fact that if $U_m \neq 1$, then $U_m \mid U_n$ if and only if $m \mid n$ (see [13]).

Suppose that (x,y,z) is a positive integer solution to (1). Then

$$z = \frac{\alpha^l - \alpha^{-l}}{2\sqrt{a}} = \frac{\beta^k - \beta^{-k}}{2\sqrt{b}} \tag{3}$$

for some positive integers l and k. Since $n > m$, from (3) it is readily seen that

$$\sqrt{b/a}\,\alpha^l > \beta^k > \alpha^l \tag{4}$$

and $(\beta/\alpha)^2 > b/a$, so if $k > 1$ and $l > 1$, then $l > k$.

Let

$$\Lambda = \tfrac{1}{2}\log(b/a) + l\log\alpha - k\log\beta. \tag{5}$$

Then (3) implies that

$$0 < \Lambda = \log(1-\beta^{-2k}) - \log(1-\alpha^{-2l}) < -\log(1-\alpha^{-2l}) < \frac{\alpha^2}{\alpha^2-1}\cdot\alpha^{-2l}.$$

It follows that

$$\log\Lambda < -2l\log\alpha + \log\frac{\alpha^2}{\alpha^2-1}. \tag{6}$$

Suppose that $N(a,b) \geq 3$. Then from Theorem 1.1 of [3], we have $N(a,b) = 3$. Let (x_i, y_i, z_i) $(i = 1, 2, 3)$ be positive solutions to (1). Then

$$z_i = \frac{\alpha^{l_i} - \alpha^{-l_i}}{2\sqrt{a}} = \frac{\beta^{k_i} - \beta^{-k_i}}{2\sqrt{b}}$$

for positive integers l_i and k_i $(i = 1, 2, 3)$ with $1 = k_1 < k_2 < k_3$ and $1 = l_1 < l_2 < l_3$. From the discussion above, we also have $(x_1, y_1, z_1) = (m, n, 1)$ and $l_i > k_i$ $(i = 2, 3)$.

LEMMA 2.2. *With the above notations, we have either* $l_2 \mid l_3$ *and* $k_2 \mid k_3$, *or* $l_3 = 2ql_2 \pm 1$ *and* $k_3 = 2q_1k_2 \pm 1$ *for some positive integers* q *and* q_1.

Proof. If $l_2 \mid l_3$, then $z_2 \mid z_3$, so $k_2 \mid k_3$. Conversely, if $k_2 \mid k_3$, then $l_2 \mid l_3$. Now assume that $l_2 \nmid l_3$, $k_2 \nmid k_3$, and let

$$l_3 = 2ql_2 \pm l_0, \quad 0 < l_0 < l_2, \quad k_3 = 2q_1k_2 \pm k_0, \quad 0 < k_0 < k_2 \tag{7}$$

for positive integers q, q_1, k_0 and l_0. By Lemma 2.1 we have $z_3 = U_{l_3} \equiv \pm U_{l_0} \pmod{z_2}$ and $z_3 = U'_{k_3} \equiv \pm U'_{k_0} \pmod{z_2}$, so

$$U_{l_0} \equiv \pm U'_{k_0} \pmod{z_2}. \tag{8}$$

Notice that $z_2 = U_{l_2} = U'_{k_2}$ and $\max(U_{l_0}, U'_{k_0}) < \frac{1}{2}\max(U_{l_2}, U'_{k_2}) = \frac{1}{2}z_2$, so (8) holds if and only if $U_{l_0} = U'_{k_0}$ and (7) takes the same plus or minus sign. From our assumptions, we thus have $l_0 = k_0 = 1$.

Note. With a similar argument as that in the above proof, if z_0 is the least positive integer z of the solution (x, y, z) of (1), then $z_0 \mid z$ for any solution (x, y, z) of (1). This justifies our restriction.

To deduce a lower bound of l_3, we require

LEMMA 2.3 ([6] or [14]). *The equation* $x^4 - Dy^2 = 1$ *has at most one solution in positive integers* x, y *unless* $D = 1785, 4\cdot 1785, 16\cdot 1785$ *in which case the equation has two positive integer solutions* $(x, y) = (13, 4), (239, 1352)$; $(x, y) = (13, 2), (239, 676)$; $(x, y) = (13, 1), (239, 338)$ *respectively. If the equation* $x^4 - Dy^2 = 1$ *has one solution* (x_1, y_1) *in positive integers, then* $x_1^2 = x_0$ *or* $x_1^2 = 2x_0^2 - 1$, *where* $x_0 + y_0\sqrt{D}$ *is the fundamental solution of the Pell equation* $x^2 - Dy^2 = 1$.

A result of Ljunggren [9] ensures that the equation $Ax^2 - By^4 = 1$ $(A > 1)$ has at most one positive integer solution. Let (u, v) be the solution in positive integers of $Ax^2 - By^2 = 1$ with u minimal, and put $\eta = u\sqrt{A} + v\sqrt{B}$. Let $v = k^2 l$ with l squarefree. If a solution to $Ax^2 - By^4 = 1$ exists, then $x\sqrt{A} + y^2\sqrt{B} = \eta^l$. With these results, we get

LEMMA 2.4. $k_2 \neq 3$.

Proof. If $k_2 = 3$, then $z_2 = U'_3 = 4n^2 - 1 = U_{l_2}$, from which it follows that l_2 is odd, say, $l_2 = 2l + 1$. Therefore $U_{l_2} + 1 = 2U_{l+1}V_l = 4n^2$. We claim that l is odd. In fact, if l is even, then $2\nmid V_l$ and $2\nmid U_{l+1}$, which contradicts $2V_lU_{l+1}=4n^2$. Since l is odd, we have $(V_l,U_{l+1})=m$. So $U_{l+1}/U_2=\square$ and $V_l/V_2=\square$ (hereafter $\square$ stands for a perfect square), that is, $U_{l+1}=2my^2$. Since $V_{l+1}^2-(m^2-1)U_{l+1}^2=1$, we have

$$V_{l+1}^2-4m^2(m^2-1)y^4=1. \tag{9}$$

Notice that $\alpha^2=2m^2-1+2m\sqrt{m^2-1}$, so

$$V_{l+1}\equiv\begin{cases}1 \pmod{4m^2(m^2-1)} & \text{if } 4\mid l+1,\\ -1 \pmod{2m^2} & \text{if } 4\nmid l+1.\end{cases} \tag{10}$$

Combining (9) with (10) leads to the following two possibilities.

Case I. If $4\mid l+1$, then $V_{l+1}-1=2m^2(m^2-1)A^4$ and $V_{l+1}-1=2B^4$ for some A and B. This leads to $B^4-m^2(m^2-1)A^4=1$, which is impossible by Lemma 2.3 since the fundamental solution of $x^2-m^2(m^2-1)y^2=1$ is $2m^2-1+2\sqrt{m^2(m^2-1)}$.

Case II. If $4\nmid l+1$, then $V_{l+1}-1=2(m^2-1)A^4$ and $V_{l+1}+1=2m^2B^4$ for some A and B. It follows that $m^2B^4-(m^2-1)A^4=1$ has a solution $(B,A)=(1,1)$. So by the above result of Ljunggren we have $y=1, l=1$ and $l_2=3$, which contradicts $l_2>k_2=3$. This completes the proof of Lemma 2.4.

Lemma 2.5. *If $b/a=\square$, then $N(a,b)=1$.*

Proof. Since $b/a=\square$, we have $\beta=\alpha^d$ for some positive integer d. If $N(a,b)>1$, then there are positive integers l and k with

$$z_2=U_l=U'_k=U_{kd}/U_d, \tag{11}$$

and hence $l\mid kd$. The lemma therefore follows from results of Carmichael [5] and Voutier [15] concerning primitive divisors of Lucas sequences.

Lemma 2.6. *If $k_2\neq 2$, then $l_3>2.8l_2\beta$.*

Proof. If $k_2\neq 2$, then by Lemma 2.4 we have $k_2\geq 4$, so $z_2=U'_{k_2}>\beta^3$. By Lemma 2.2 we can divide the proof of this lemma into two cases according as $l_2\mid l_3$ or not.

First if $l_2\mid l_3$, then by Lemma 2.2 we have $l_3=ql_2, k_3=q_1k_2$ for some positive integers q and q_1. Further

$$\frac{z_3}{z_2}=\frac{U_{ql_2}}{U_{l_2}}=\frac{U'_{q_1k_2}}{U'_{k_2}} \tag{12}$$

implies that $q>q_1$. Considering the second equality in (12) modulo z_2^2, we have

$$qx_2^{q-1}\equiv q_1y_2^{q_1-1} \pmod{z_2^2}. \tag{13}$$

Since $x_2^2 \equiv y_2^2 \equiv 1 \pmod{z_2^2}$, we have $q^2 \equiv q_1^2 \pmod{z_2^2}$ by (13). Hence $q > z_2 > \beta^3$ and

$$l_3 > l_2\beta^3.$$

Now if $l_2 \nmid l_3$, by Lemma 2.2 we have $l_3 = 2ql_2 \pm 1$ and $k_3 = 2q_1k_2 \pm 1$ for some positive integers q and q_1. From $z_3 = U'_{k_3} = U_{l_3}$, we have $q > q_1$. Notice that $\beta^{2k_2} = 2z_2^2(n^2-1) + 1 + 2y_2z_2\sqrt{n^2-1}$, so

$$z_3 = U'_{k_3} \equiv 2nq_1y_2z_2 \pm 1 \pmod{2z_2^2(n^2-1)}. \tag{14}$$

Similarly,

$$z_3 = U_{l_3} \equiv 2mqx_2z_2 \pm 1 \pmod{2z_2^2(m^2-1)}. \tag{15}$$

From (14) and (15) we have

$$mqx_2 \equiv nq_1y_2 \pmod{z_2}. \tag{16}$$

If k_2 is even, then $n \mid z_2$. From (16) and $x_2^2 \equiv y_2^2 \equiv 1 \pmod{z_2^2}$ we have $n \mid mq$ and $(mq/n)^2 \equiv q_1^2 \pmod{z_1/n}$. From $z_3 = U'_{k_3} = U_{l_3}$ it is easily seen that $mq \neq nq_1$. Hence

$$q_1 > \sqrt{\frac{z_2}{n}} \quad \text{or} \quad \frac{mq}{n} > \sqrt{\frac{z_2}{n}}. \tag{17}$$

Since $z_2 > \beta^3$ and $q > q_1$, we have

$$l_3 = 2ql_2 \pm 1 > 2\left(\sqrt{\frac{\beta^3}{n}} + 1\right)l_2\beta - 1 \geq 2.8l_2\beta. \tag{18}$$

If k_2 is odd, then $z_2 > \beta^4$. So from (16) and $x_2^2 \equiv y_2^2 \equiv 1 \pmod{z_2^2}$, we have

$$mq > \sqrt{z_2} \quad \text{or} \quad nq_1 > \sqrt{z_2}.$$

It follows that $q > q_1 > 2\beta$ and $l_3 = 2ql_2 \pm 1 \geq 3.8l_2\beta$. Lemma 2.6 is proved.

LEMMA 2.7. *If $k_2 = 2$ and $\beta > 1000$, then $n = n(l,m)$ for some positive integer l and $l_3 > 1.5l_2\beta^{2/3}$.*

Proof. Obviously, we just need to prove the latter conclusion. If $2 \mid k_3$, let $k_3 = 2q_1$ and $l_3 = l_2q$ for some positive integers q and q_1. We have

$$qx_2^{q-1} \equiv q_1y_2^{q_1-1} \pmod{z_2^2}.$$

Notice that $z_2 = 2n(l,m)$ and $x_2^2 \equiv y_2^2 \equiv 1 \pmod{z_2^2}$, so $q > z_2 = 2n(l,m) > \beta + 1$ and $l_3 = ql_2 > l_2(\beta+1)$. If $2 \nmid k_3$, let $k_3 = 4q_1 \pm 1$ and $l_3 = 2ql_2 \pm 1$ for some positive integers q and q_1. Similarly, we have

$$z_3 \equiv 2nq_1y_2z_2 \pm 1 \equiv \pm 1 \pmod{z_2^2}, \qquad z_3 \equiv 2mqx_2z_2 \pm 1 \pmod{z_2^2}. \tag{19}$$

From (19) and $(x_2, z_2) = 1$ we have $z_2 \mid 2mq$. So $q \geq z_2/(2m) = 2n(l,m)/(2m) > 0.759\beta^{2/3}$ and $l_3 \geq 2ql_2 - 1 > 1.5l_2\beta^{2/3}$ (provided $\beta > 1000$).

To prove Theorem 1.4, we still require an estimate for linear forms in the logarithms of (three) algebraic numbers. We use the following result of Baker and Wüstholz [2]. Let $\alpha_1, \ldots, \alpha_n$ (with $n \geq 2$) denote algebraic numbers not equal to 0 or 1. Let $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ and set $d = [K : \mathbb{Q}]$. Define a modified height by the formula

$$h_m(\alpha) = \max\{h(\alpha), |\log \alpha|/d, 1/d\},$$

where $h(\alpha)$ denotes the standard logarithmic Weil height of an algebraic number α.

THEOREM 2.8 (Baker–Wüstholz [2]). *Let $b_1, \dots, b_n$ be integers such that*

$$\Lambda = b_1 \log \alpha_1 + \dots + b_n \log \alpha_n$$

is nonzero. Then if $B = \max\{|b_1|, \dots, |b_n|\} \geq 3$ we have the inequality

$$\log |\Lambda| > -C_1 h_m(\alpha_1) \dots h_m(\alpha_n) \log B$$

with

$$C_1 = 18(n+1)! n^{n+1} (32d)^{n+2} \log(2nd).$$

3. Proof of Theorem 1.4. We apply Theorem 2.8 with

$$\alpha_1 = \sqrt{b/a}, \quad \alpha_2 = \alpha, \quad \alpha_3 = \beta, \quad b_1 = 1, \quad b_2 = l_3, \quad b_3 = -k_3, \quad n = 3.$$

By Lemma 2.5 we may take $d = 4$, and

$$h_m(\alpha_1) = \tfrac{1}{2} \log b < \beta, \quad h_m(\alpha_2) = \tfrac{1}{2} \log \alpha, \quad h_m(\alpha_3) = \tfrac{1}{2} \log \beta, \quad B = l_3.$$

Therefore by Theorem 2.8 we have

$$\log |\Lambda| > -9.56 \cdot 10^{14} \log \alpha \log^2 \beta \log l_3. \tag{20}$$

If $k_2 \neq 2$, combining (20) with (6), by Lemma 2.6 we have

$$l_3 < 4.78 \cdot 10^{14} \log^3 l_3.$$

It follows that $l_3 < 4.5 \cdot 10^{19}$. Therefore by Lemma 2.6 and $l_2 \geq 6$, we have

$$b < 1.8 \cdot 10^{36}.$$

If $k_2 = 2$, combining (20) and (6), by Lemma 2.7 we have

$$l_3 < 1.0775 \cdot 10^{15} \log^3 l_3.$$

It follows that $l_3 < 1.06 \cdot 10^{20}$. Therefore by Lemma 2.7 and $l_2 \geq 4$, we have

$$b < 1.4 \cdot 10^{57}.$$

This completes the proof.

Acknowledgements. I am grateful to the referee for his/her valuable suggestions.

References

[1] W. S. Anglin, *Simultaneous Pell equations*, Math. Comp. 65 (1996), 355–359.

[2] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. 442 (1993), 19–62.

[3] M. A. Bennett, *On the number of solutions of simultaneous Pell equations*, ibid. 498 (1997), 173–200.
[4] —, *Solving families of simultaneous Pell equations*, J. Number Theory 67 (1997), 246–251.
[5] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2) 15 (1913), 30–70.
[6] J. H. E. Cohn, *The Diophantine equation* $x^4 - Dy^2 = 1$, *II*, Acta Arith. 78 (1997), 401–403.
[7] M. Gardner, *Mathematical games*, *On the patterns and the unusual properties of figurate numbers*, Scientific American 231 (1974), 116–120.
[8] K. Kedlaya, *Solving constrained Pell equations*, Math. Comp. 67 (1998), 833–842.
[9] W. Ljunggren, *Ein Satz über die Diophantische Gleichung* $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$, Tolfte Skand. Matemheikerkongressen, Lund, 1953, 188–194.
[10] D. W. Masser and J. H. Rickert, *Simultaneous Pell equations*, J. Number Theory 61 (1996), 52–66.
[11] K. Ono, *Euler's concordant forms*, Acta Arith. 78 (1996), 101–123.
[12] R. G. E. Pinch, *Simultaneous Pellian equations*, Math. Proc. Cambridge Philos. Soc. 103 (1988), 35–46.
[13] P. Ribenboim and W. L. McDaniel, *The square terms in Lucas sequences*, J. Number Theory 58 (1996), 104–123.
[14] Q. Sun and P. Z. Yuan, *On the Diophantine equation* $x^4 - Dy^2 = 1$, Adv. in Math. (China) (1) 25 (1996), 85.
[15] P. M. Voutier, *Primitive divisors of Lucas and Lehmer sequences*, Math. Comp. 64 (1995), 869–888.

Department of Mathematics and Mechanics
Central South University (Tiedao Campus)
Hunan, Changsha 410075, P.R. China
E-mail: yuanpz@csru.edu.cn

Received on 28.2.2000
and in revised form on 21.5.2001 (3764)