On the number of solutions of simultaneous Pell equations

Michael A. Bennett

Abstract

It is proven that if a and b are distinct nonzero integers then the simultaneous Diophantine equations

$$x^2 - az^2 = 1, \quad y^2 - bz^2 = 1$$

possess at most three solutions in positive integers (x, y, z). Since there exist infinite families of pairs (a, b) for which the above equations have at least two solutions, this result is not too far from the truth. If, further, u and v are nonzero integers with $av - bu$ nonzero, then the more general equations

$$x^2 - az^2 = u, \quad y^2 - bz^2 = v$$

are shown to have $\ll 2^{\min\{\omega(u), \omega(v)\}} \log(|u| + |v|)$ solutions in integers, where $\omega(m)$ denotes the number of distinct prime factors of m and the implied constant is absolute. These results follow from a combination of techniques including simultaneous Padé approximation to binomial functions, the theory of linear forms in two logarithms and some gap principles, both new and familiar. Some connections to elliptic curves and related problems are briefly discussed.

1 Introduction

In this paper, we study positive integer solutions (x, y, z) of the simultaneous Diophantine equations

$$(1) \qquad x^2 - az^2 = u, \quad y^2 - bz^2 = v$$

where a, b, u and v are nonzero integers with $av \neq bu$. Individually, these Pell equations possess either no solutions or infinitely many, corresponding to units

in related quadratic fields. Taken together, they define an affine variety which, as the intersection of a pair of quadric surfaces in $\mathbb{R}^3$, is generically a curve of genus one. By the work of Thue [26] and Siegel [25], this curve contains at most finitely many integer points. Setting $w = xy$ and considering (1) as a hyperelliptic equation $w^2 = (az^2+u)(bz^2+v)$, we may apply the theory of linear forms in logarithms (see e.g. [4]) to effectively bound all solutions (x, y, z) to (1), though the dependence on the given coefficients (a, b, u, v) is a strong one (note here that the conditions on the coefficients guarantees the absence of repeated roots). Approaches similar to this, combining bounds for linear forms in logarithms of algebraic numbers with techniques from computational Diophantine approximation, have been successfully applied to the problem of explicitly determining all solutions to (1), for some fixed a, b, u and v (see e.g. [1], [5], [8], [14] and [21]). Indeed, Anglin [2] devotes Section 4.6 of his textbook to the decription of an algorithm for solving (1). A variety of classical algebraic and elementary approaches to this and similar problems can be found in the papers of Arwin [3], Boutin and Teilhet [7], Gloden [13] and Ljunggren [17] (where the last cited combines Skolem's p-adic method with information from related quadratic and quartic fields). For an elementary proof of the nonexistence of solutions to certain cases of (1), the reader is directed to the forthcoming paper of Walsh [28]. This result is in some sense an explicit characterization of Brauer-Manin obstruction for the intersections of particular quadric surfaces. A detailed and very general discussion of such obstruction to the Hasse principle, as it relates to these and other surfaces, may be found in [11] and [12].

We primarily focus our attention on the more specific equations

$$(2) \qquad\qquad x^2 - az^2 = 1, \quad y^2 - bz^2 = 1$$

where a and b are distinct positive integers. General results of Schlickewei [23] on S-unit equations and of Schlickewei and Schmidt [24] on common terms in recurrence sequences provide absolute (if large) bounds upon the number of solutions to such equations (to quote Masser and Rickert [18] : "it appears difficult to avoid numbers like $2^{2^{80}}$"). Anglin [1], however, has shown that these equations admit at most one positive solution (x, y, z) whenever $\max\{a, b\} \leq 200$, so it might be hoped that one could derive a rather small bound upon the number of solutions to (2) for arbitrary a and b (with a and b distinct and nonzero). Such a bound was recently achieved by Masser and Rickert [18] who applied the method of simultaneous Padé approximation to hypergeometric functions, in conjunction with suitable gap principles (to ensure that solutions to (2) are spread apart), to prove

Theorem (Masser-Rickert) If a and b are distinct nonzero integers, then the simultaneous equations (2) possess at most 16 solutions (x, y, z) in positive integers.

In what follows, we take an approach which is fundamentally similar to that of Masser and Rickert, but introduce a new gap principle which is powerful enough to allow application of recent bounds from the theory of linear forms in the logarithms of (two) algebraic numbers. Our main result is

Theorem 1.1 If a and b are distinct nonzero integers, then the simultaneous equations (2) possess at most three solutions (x, y, z) in positive integers.

As noted in [18] (see Section 5 for details), there exist infinite parametrized families of distinct positive integers a and b for which (2) has at least two positive solutions, so the above is not too far from best possible.

A fruitful way of viewing equations (1) and (2) is via a connection to elliptic curves. Indeed, since the study of rational solutions to (2) is equivalent to Euler's problem of concordant forms (see e.g. the paper of Ono [20]), this correspondence is analogous to that discovered by Tunnell [27] for congruent numbers. To be precise, as noted in [18] and [20], the affine variety defined by (2) may be birationally mapped to the elliptic curve

$$Y^2 = X (X + a) (X + b)$$

and a similar relationship connects the variety (1) with the curve

$$Y^2 = X (uX + a) (vX + b)$$

(with both of these maps extending to isomorphisms between their respective projective models). We may therefore derive information about rational points on certain elliptic curves from rational solutions to (1) or (2), and vice versa. In particular, Masser and Rickert used an argument similar to the proof of the "Taxicab" theorem (on representations of integers as sums of two cubes) to show that given a positive integer n, we can find integers u and v for which the equations

$$x^2 - 2z^2 = u, \quad y^2 - 3z^2 = v$$

possess at least n solutions in positive (x, y, z). In fact, defining the number of integer solutions (x, y, z) to (1) to be $N(a, b, u, v)$, their approach implies that

$$\sup_{u,v} N(2, 3, u, v) \gg \log^{1/3} (|u| + |v|)$$

3

where the supremum is taken over nonzero integers u and v with $2v \neq 3u$. Similarly, using the fact that the elliptic curve

$$Y^2 = X(X+3)(X+783)$$

has rank two, one can show that

$$\sup_{u,v} N(3, 783, u, v) \gg \log^{1/2}(|u| + |v|).$$

In the other direction, defining $\omega(m)$ to be the number of distinct prime factors of m, we prove

Theorem 1.2 If a, b, u and v are nonzero integers with $av \neq bu$, then

$$N(a, b, u, v) \ll 2^{\min\{\omega(u), \omega(v)\}} \log(|u| + |v|)$$

where the implied constant is absolute.

For further discussion of the connections between simultaneous Pell equations and elliptic curves, one may see [20], [21] and [29]. In the first of these, for example, this relationship is used to describe a number of infinite families of integers (a, b) for which (2) possesses no nontrivial integral solutions.

2 Some Gap Principles

Here and in the sequel, we will suppose, without loss of generality, that $b > a \geq 2$ are integers and consider simultaneous equations of the form (2). In this section, we prove a pair of results that ensure that solutions to (2) cannot lie too "close together". Suppose, for i an integer, that (x_i, y_i, z_i) is a positive solution to (2). From the theory of Pellian equations, it follows that

$$(3) \qquad\qquad z_i = \frac{\alpha^{j_i} - \alpha^{-j_i}}{2\sqrt{a}} = \frac{\beta^{k_i} - \beta^{-k_i}}{2\sqrt{b}}$$

where α and β are the fundamental solutions to the equations $x^2 - az^2 = 1$ and $y^2 - bz^2 = 1$ respectively (i.e. the fundamental units in $\mathbb{Q}(\sqrt{a})$ or $\mathbb{Q}(\sqrt{b})$, or their squares) and j_i and k_i are positive integers. If we assume that $z_{i+1} > z_i$, then (3) implies that

$$\frac{z_{i+1}}{z_i} = \frac{\beta^{k_{i+1}} - \beta^{-k_{i+1}}}{\beta^{k_i} - \beta^{-k_i}} > \beta^{k_{i+1} - k_i} \geq \beta > 2\sqrt{b}.$$

Lemma 2.1 If (x_i, y_i, z_i) are positive solutions to (2) for $1 \leq i \leq 3$, with $z_3 > z_2 > z_1$, then for k_i as in (3), we have $k_3 \geq k_2 + 3k_1 - 1$.

Proof: We follow Masser and Rickert [18] in considering the determinant

$$\Delta = \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = \begin{vmatrix} x_1 - \sqrt{a}z_1 & y_1 - \sqrt{b}z_1 & z_1 \\ x_2 - \sqrt{a}z_2 & y_2 - \sqrt{b}z_2 & z_2 \\ x_3 - \sqrt{a}z_3 & y_3 - \sqrt{b}z_3 & z_3 \end{vmatrix}.$$

Define, for $1 \leq i \leq j \leq 3$,

$$D_i = \left(x_i - \sqrt{a}y_i\right)^2 - \left(y_i - \sqrt{b}z_i\right)^2$$

and

$$E_{ij} = \left(x_i - \sqrt{a}z_i\right)^2 \left(y_j - \sqrt{b}z_j\right)^2 - \left(x_j - \sqrt{a}z_j\right)^2 \left(y_i - \sqrt{b}z_i\right)^2.$$

Expanding along the third column of Δ and using that

$$\left(x_i - \sqrt{a}z_i\right) = \frac{1}{2\sqrt{a}z_i} \left(1 - \left(x_i - \sqrt{a}z_i\right)^2\right)$$

and

$$\left(y_i - \sqrt{b}z_i\right) = \frac{1}{2\sqrt{b}z_i} \left(1 - \left(y_i - \sqrt{b}z_i\right)^2\right),$$

we have

$$\Delta = \frac{(z_1 z_2 z_3)^{-1}}{4\sqrt{ab}} \left(z_1^2 \left(D_3 - D_2 + E_{23}\right) + z_2^2 \left(D_1 - D_3 - E_{13}\right) + z_3^2 \left(D_2 - D_1 + E_{12}\right)\right).$$

Now the inequalities $z_{i+1} > 2\sqrt{b}z_i$ and $b > a \geq 2$ yield

$$|E_{ij}| < \frac{1}{576az_i^2}$$

and

$$\frac{0.2}{z_i^2} \left(\frac{1}{a} - \frac{1}{b}\right) < D_i < \frac{0.3}{z_i^2} \left(\frac{1}{a} - \frac{1}{b}\right).$$

Applying these, we may conclude (again using $z_{i+1} > 2\sqrt{b}z_i$) that

$$\frac{z_3}{24a\sqrt{ab}z_1^3 z_2} < |\Delta| < \frac{z_3}{12a\sqrt{ab}z_1^3 z_2}.$$

5

Since Δ is an integer, it follows that

$$(4) \qquad\qquad z_3 > 12a\sqrt{ab}z_1^3 z_2.$$

Now suppose $k_3 \leq k_2 + 3k_1 - 2$. Since $\beta \geq 2 + \sqrt{3}$, we have from (3) that

$$\frac{z_3}{z_1^3 z_2} < 12\ b\ \sqrt{b}\ \beta^{k_3 - k_2 - 3k_1} \leq 12\ b\ \sqrt{b}\ \beta^{-2}.$$

The inequality $\beta > 2\sqrt{b}$ therefore implies $z_3 < 3\sqrt{b}z_1^3 z_2$, contradicting (4). $\square$

We note that (4) may be sharpened by replacing 12 with $16 - \delta$ where $\delta = \delta(b)$ is positive and satisfies $\lim_{b \to \infty} \delta(b) = 0$. For our purposes, the above formulation is adequate and is of some use in proving the following much stronger gap principle, suggested to the author by C.L. Stewart:

Lemma 2.2 If (x_i, y_i, z_i) are positive solutions to (2) for $1 \leq i \leq 3$, with $z_3 > z_2 > z_1$, then for α, j_i and k_i as in (3), we have

$$(k_3 - k_2)(k_2 - k_1) > \alpha^{2j_1}.$$

Proof: Suppose that instead

$$(5) \qquad\qquad (k_3 - k_2)(k_2 - k_1) \leq \alpha^{2j_1}.$$

From (3), we have that the quantity $\left| \alpha^{j_{i+1} - j_i} - \beta^{k_{i+1} - k_i} \right|$ is bounded above by

$$\max\left\{ \left| \frac{\alpha^{j_{i+1} - 3j_i} - \alpha^{-j_{i+1} - j_i}}{1 - \alpha^{-2j_i}} \right|, \left| \frac{\beta^{k_{i+1} - 3k_i} - \beta^{-k_{i+1} - k_i}}{1 - \beta^{-2k_i}} \right| \right\}$$

for $1 \leq i \leq 2$. From the aforementioned work of Anglin [1], we may assume that $b > \max\{a, 200\}$ and hence $\beta \geq 15 + \sqrt{224}$ (and $\alpha \geq 2 + \sqrt{3}$). It follows that

$$(6) \qquad \left| \alpha^{j_{i+1} - j_i} - \beta^{k_{i+1} - k_i} \right| < \min\left\{ 1.078\ \alpha^{j_{i+1} - 3j_i}, 1.004\ \frac{b}{a}\ \beta^{k_{i+1} - 3k_i} \right\}$$

whence

$$(7) \qquad 0 < \left| \frac{\log \beta}{\log \alpha} - \frac{j_{i+1} - j_i}{k_{i+1} - k_i} \right| < \frac{1.004\ b}{a \log \alpha\ (k_{i+1} - k_i)}\ \beta^{-2k_i}$$

for $1 \leq i \leq 2$. To see the first of these inequalities, note that if $\alpha^{j_{i+1} - j_i} = \beta^{k_{i+1} - k_i}$ then the equality

$$\frac{\alpha^{j_{i+1}} - \alpha^{-j_{i+1}}}{\alpha^{j_i} - \alpha^{-j_i}} = \frac{\beta^{k_{i+1}} - \beta^{-k_{i+1}}}{\beta^{k_i} - \beta^{-k_i}}$$

6

implies that

$$\frac{\alpha^{-2j_i} - \alpha^{-2j_{i+1}}}{1 - \alpha^{-2j_i}} = \frac{\beta^{-2k_i} - \beta^{-2k_{i+1}}}{1 - \beta^{-2k_i}}$$

and so (again using $\alpha^{j_{i+1}-j_i} = \beta^{k_{i+1}-k_i}$)

$$\frac{\alpha^{-2j_i}}{1 - \alpha^{-2j_i}} = \frac{\beta^{-2k_i}}{1 - \beta^{-2k_i}}.$$

It follows that $\alpha^{j_i} = \beta^{k_i}$, contradicting (3) (since $a \neq b$).

Since $\alpha \geq 2 + \sqrt{3}$, we have

(8) $$\frac{a}{b}\, \beta^{2k_1} < \alpha^{2j_1} < 1.161 \frac{a}{b}\, \beta^{2k_1}.$$

Applying Lemma 2.1, it follows that $k_3 - k_2 \geq 3k_1 - 1 \geq 2$ and thus (5) implies

$$k_2 - k_1 < 0.581\, \frac{a}{b}\, \beta^{2k_1}.$$

Since $\alpha \geq 2 + \sqrt{3}$ and $k_2 \geq k_1 + 1$, we have

$$\left| \frac{\log \beta}{\log \alpha} - \frac{j_{i+1} - j_i}{k_{i+1} - k_i} \right| < \frac{1}{2\, (k_{i+1} - k_i)^2} \qquad (1 \leq i \leq 2)$$

and so both $\frac{j_2 - j_1}{k_2 - k_1}$ and $\frac{j_3 - j_2}{k_3 - k_2}$ are convergents to $\frac{\log \beta}{\log \alpha}$. If these are distinct this implies (see e.g. [15]) that either

$$\left| \frac{\log \beta}{\log \alpha} - \frac{j_2 - j_1}{k_2 - k_1} \right| > \frac{1}{(k_3 - k_1)\, (k_2 - k_1)}$$

or

$$\left| \frac{\log \beta}{\log \alpha} - \frac{j_3 - j_2}{k_3 - k_2} \right| > \frac{1}{(k_3 - k_1)\, (k_3 - k_2)}$$

depending on which of the two convergents provides a better approximant to $\frac{\log \beta}{\log \alpha}$. In each case, we have

$$k_3 - k_1 > \frac{a \log \alpha\; \beta^{2k_1}}{1.004\; b}.$$

On the other hand, (5) and (8) imply that

$$k_3 - k_1 \leq \alpha^{2j_1} + 1 < 1.161\, \frac{a}{b}\, \beta^{2k_1} + 1$$

7

which yields the desired contradiction (since $\frac{a}{b} \beta^{2k_1} > 4a \geq 8$).

It remains to consider when

(9)
$$\frac{j_2 - j_1}{k_2 - k_1} = \frac{j_3 - j_2}{k_3 - k_2}.$$

In this situation, the proof is rather delicate and we must tread warily. Since $b > a$, from (3) we have that $\alpha^{j_1} < \beta^{k_1}$. Now, by calculus, it is readily checked that the function

$$\frac{x^{k_2/k_1} - x^{-k_2/k_1}}{x - x^{-1}}$$

is strictly increasing on the interval $\left[\alpha^{j_1}, \beta^{k_1}\right]$ (where we use that $\alpha^{2j_1} > \frac{a}{b} \beta^{2k_1} > \frac{k_2 + k_1}{k_2 - k_1}$) and so the equality

$$\frac{\alpha^{j_2} - \alpha^{-j_2}}{\alpha^{j_1} - \alpha^{-j_1}} = \frac{\beta^{k_2} - \beta^{-k_2}}{\beta^{k_1} - \beta^{-k_1}}$$

implies that $j_2 > j_1 k_2 / k_1$ and thus

(10)
$$k_1 j_2 \geq j_1 k_2 + 1.$$

Define

$$\Phi = (z_2/z_1)^{k_3 - k_2}, \qquad \Psi = (z_3/z_2)^{k_2 - k_1}$$

and $\Omega = \Phi - \Psi$. We derive upper and lower bounds upon Ω in two different ways and then use (9) and (10) to deduce a contradiction. First, note that from (3), we may express Φ as

$$\Phi = \beta^{(k_2 - k_1)(k_3 - k_2)} \sum_{r=0}^{k_3 - k_2} \binom{k_3 - k_2}{r} \left(\frac{\beta^{-2k_1} - \beta^{-2k_2}}{1 - \beta^{-2k_1}}\right)^r.$$

Since $\beta \geq 15 + \sqrt{224}$ and (from Lemma 2.1) $k_3 - k_2 \geq 2$, inequalities (5) and (8) imply that

$$\Phi < \beta^{(k_2 - k_1)(k_3 - k_2)} \left(1 + (k_3 - k_2) \ \beta^{-2k_1} + (k_3 - k_2)^2 \ \beta^{-4k_1}\right).$$

Similarly, we have

$$\Psi = \beta^{(k_2 - k_1)(k_3 - k_2)} \sum_{r=0}^{k_2 - k_1} \binom{k_2 - k_1}{r} \left(\frac{\beta^{-2k_2} - \beta^{-2k_3}}{1 - \beta^{-2k_2}}\right)^r$$

and so

$$\Psi > \beta^{(k_2 - k_1)(k_3 - k_2)}.$$

8

It follows that

$$(11) \qquad \Omega < \beta^{(k_2-k_1)(k_3-k_2)} \left((k_3 - k_2) \ \beta^{-2k_1} + (k_3 - k_2)^2 \ \beta^{-4k_1} \right).$$

We next derive a lower bound upon Ω. From (3), we have

$$\Phi = \alpha^{(j_2-j_1)(k_3-k_2)} \sum_{r=0}^{k_3-k_2} \binom{k_3 - k_2}{r} \left(\frac{\alpha^{-2j_1} - \alpha^{-2j_2}}{1 - \alpha^{-2j_1}} \right)^r$$

so that

$$\Phi > \alpha^{(j_2-j_1)(k_3-k_2)} \left(1 + (k_3 - k_2) \left(\alpha^{-2j_1} - \alpha^{-2j_2} \right) \right).$$

Now

$$\Psi = \alpha^{(j_3-j_2)(k_2-k_1)} \sum_{r=0}^{k_2-k_1} \binom{k_2 - k_1}{r} \left(\frac{\alpha^{-2j_2} - \alpha^{-2j_3}}{1 - \alpha^{-2j_2}} \right)^r$$

and thus (5), (8) and $\alpha \geq 2 + \sqrt{3}$ give

$$\Psi < \alpha^{(j_3-j_2)(k_2-k_1)} \left(1 + 1.002 \, (k_2 - k_1) \, \alpha^{-2j_2} \right).$$

We therefore have, from (9), that

$$(12) \qquad \Omega > \alpha^{(j_2-j_1)(k_3-k_2)} \left((k_3 - k_2) \, \alpha^{-2j_1} - c_1 \alpha^{-2j_2} \right)$$

where $c_1 = (k_3 - k_2) + 1.002 \, (k_2 - k_1)$. Combining (6) and (11) and noting that Lemma 2.1 implies $(k_3 - k_2) (k_2 - k_1) \geq 2k_1$, we have

$$\begin{aligned} \Omega \quad < \quad & (k_3 - k_2) \left(\alpha^{j_2-j_1} (1 + \theta) \right)^{k_3-k_2-\frac{2k_1}{k_2-k_1}} + \\ & (k_3 - k_2)^2 \left(\alpha^{j_2-j_1} (1 + \theta) \right)^{k_3-k_2-\frac{2k_1}{k_2-k_1}} \left(\alpha^{j_2-j_1} (1 - \theta) \right)^{-\frac{2k_1}{k_2-k_1}} \end{aligned}$$

where $\theta = 1.078 \, \alpha^{-2j_1}$. In conjunction with (12), this yields

$$(13) \qquad \frac{c_1}{k_3 - k_2} \, \alpha^{-2(j_2-j_1)} + c_2 \, c_3 \, \alpha^{2j_1-2k_1 \left(\frac{j_2-j_1}{k_2-k_1} \right)} > 1$$

with

$$c_2 = 1 + (k_3 - k_2) \left(\alpha^{j_2-j_1} (1 - \theta) \right)^{-\frac{2k_1}{k_2-k_1}}$$

and

$$c_3 = (1 + \theta)^{k_3-k_2-\frac{2k_1}{k_2-k_1}}.$$

Now since $\alpha^{2j_1} > \frac{a}{b} \, \beta^{2k_1} > 4a \, \beta^{2(k_1-1)}$, it follows from $\beta \geq 15 + \sqrt{224}$ that

$$(1 - \theta)^{-\frac{2k_1}{k_2-k_1}} \leq \left(1 - 1.078 \, \alpha^{-2} \right)^{-2} < 1.2.$$

9

Applying (5), we therefore have

$$c_2 < 1 + \frac{1.2}{k_2 - k_1} \; \alpha^{2j_1 - 2k_1\left(\frac{j_2 - j_1}{k_2 - k_1}\right)}$$

and

$$c_3 < (1+\theta)^{\frac{\alpha^{2j_1}}{k_2 - k_1}} < 3^{\frac{1}{k_2 - k_1}}.$$

From (10), $j_1 < k_1 \left(\frac{j_2 - j_1}{k_2 - k_1}\right)$, so that

$$c_2 \, c_3 \, \alpha^{2j_1 - 2k_1\left(\frac{j_2 - j_1}{k_2 - k_1}\right)} < \left(\alpha^{-\frac{2}{k_2 - k_1}} + \frac{1.2}{k_2 - k_1}\alpha^{-\frac{4}{k_2 - k_1}}\right) 3^{\frac{1}{k_2 - k_1}}.$$

If $k_2 - k_1 \le 2$, since $k_3 - k_2 \ge 2$, it follows that the left hand side of (13) is less than

$$\frac{2}{\alpha} + \frac{4}{\alpha^2} < 1.$$

If, however, $k_2 - k_1 \ge 3$, we have

$$1 + \frac{1.2}{k_2 - k_1} \; \alpha^{-\frac{2}{k_2 - k_1}} < 1 + \frac{1.2}{k_2 - k_1}$$

and (since $\alpha \ge 2 + \sqrt{3}$)

$$\left(3/\alpha^2\right)^{\frac{1}{k_2 - k_1}} < 1 - \frac{1.2}{k_2 - k_1}$$

and so to conclude as stated, we need only show that

$$\frac{c_1}{k_3 - k_2} \; \alpha^{-2(j_2 - j_1)} < \frac{1}{(k_2 - k_1)^2},$$

contradicting (13). But (6) and the inequality $k_3 - k_2 \ge 2$ imply

$$\frac{c_1}{k_3 - k_2} \; \alpha^{-2(j_2 - j_1)} < (k_2 - k_1) \; \beta^{-2(k_2 - k_1)}$$

which, since $\beta \ge 15 + \sqrt{224}$, is smaller than $(k_2 - k_1)^{-2}$. $\square$

As we shall observe, this lemma is the key ingredient in our sharpening of the work of Masser and Rickert not only because it provides a doubly exponential rather than polynomial gap principle but also because its precise form permits use of bounds from the theory of linear forms in logarithms. Unfortunately, it does not appear that a similar result may be readily obtained for more general choices of u and v in (1), primarily since one requires an analogous bound to (10).

3 Application of the Hypergeometric Method

We next prove a result which provides a bound upon all solutions (x, y, z) to (2) solely in terms of a single "suitably large" solution, what one might term an "anti-gap principle". The argument here is fundamentally identical to that of Masser and Rickert [18] though we require a slightly more flexible version of their related Proposition. For more details on the technique of Padé approximation to hypergeoemtric functions, the reader is directed to [6], [10] and [22].

In [6], following Rickert [22], we considered the problem of obtaining simultaneous approximations to functions of the form

$$(1 + a_0 x)^{s/n}, \dots, (1 + a_m x)^{s/n}$$

where the a_i's are distinct integers with $a_j = 0$ for some j, $|a_i| < |x|^{-1}$ for $0 \le i \le m$ and s and n positive, relatively prime integers with $s < n$. We derived our approximants from the contour integral

$$I_i(x) = \frac{1}{2\pi i} \int_\gamma \frac{(1 + zx)^k (1 + zx)^{s/n}}{(z - a_i)(A(z))^k} \, dz \quad (0 \le i \le m)$$

where k is a positive integer,

$$A(z) = \prod_{i=0}^{m} (z - a_i)$$

and γ a closed, counter-clockwise contour enclosing the poles of the integrand. Cauchy's theorem implies that

$$I_i(x) = \sum_{j=0}^{m} p_{ij}(x)(1 + a_j x)^{s/n} \quad (0 \le i \le m)$$

where $p_{ij}(x) \in \mathbb{Q}[x]$ with degree at most k and by evaluating these polynomials at $x = 1/N$, we may deduce lower bounds for simultaneous rational approximation to the numbers

$$(1 + a_0/N)^{s/n}, \dots, (1 + a_m/N)^{s/n}$$

through application of the following lemma (a slight variant of Lemma 2.1 of [22]):

Lemma 3.1 Let $\theta_1, \dots \theta_m$ be arbitrary real numbers and $\theta_0 = 1$. Suppose there exist positive real numbers l, p, L and P $(L > 1)$ such that for each

positive integer k, we can find integers p_{ijk} $(0 \le i, j \le m)$ with nonzero determinant,

$$|p_{ijk}| \le pP^k \quad (0 \le i, j \le m)$$

and

$$\left| \sum_{j=0}^{m} p_{ijk}\theta_j \right| \le lL^{-k} \quad (0 \le i \le m).$$

Then we may conclude that

$$\max \left\{ \left| \theta_1 - \frac{p_1}{q} \right|, \ldots, \left| \theta_m - \frac{p_m}{q} \right| \right\} > c\, q^{-\lambda}$$

for all integers $p_1, \ldots, p_m$ and q, where

$$\lambda = 1 + \frac{\log(P)}{\log(L)}$$

and

$$c^{-1} = 2mpP\, (\max(1, 2l))^{\lambda-1}.$$

In our particular situation, we take $s = 1$, $n = m = 2$, $a_0 < a_1 < a_2$ with $a_j = 0$ for some $0 \le j \le 2$, $N > M^9$, where

$$M = \max_{0 \le i \le 2} \{|a_i|\}$$

and note that by Lemma 3.3 of [22], we may find C_k with $C_k\, p_{ij}(1/N) \in \mathbb{Z}$ and

$$C_k \le \left(4\, N \prod_{0 \le i < j \le 2} (a_j - a_i)^2 \right)^k.$$

Further, we have, for $0 \le i \le 2$,

$$\left| I_i \left(\frac{1}{N} \right) \right| = \frac{1}{\pi N^{3k}} \int_0^\infty \frac{x^{k+\frac{1}{2}}\, dx}{\left(x + 1 + \frac{a_i}{N} \right) B(x)^k}$$

where

$$B(x) = \prod_{j=0}^{2} \left(x + 1 + \frac{a_j}{N} \right).$$

It follows that

$$\left| I_i \left(\frac{1}{N} \right) \right| < \frac{\left(1 - \frac{M}{N} \right)^{-2k-1}}{\pi N^{3k}} \int_0^\infty \frac{x^{k+\frac{1}{2}}\, dx}{(x+1)^{3k+1}} < 0.43 \left(6.74 N^3 \right)^{-k}$$

12

where the latter inequality follows from $N > M^9$ and induction upon k.

It remains to find an upper bound upon $|p_{ij}(1/N)|$. Our argument is essentially the same as that in [18] (to which the reader is directed for more details). First, note that we may write

$$p_{ij}(x)\,(1 + a_j x)^{1/2} = \frac{1}{2\pi i}\int_{\Gamma_j}\frac{(1 + zx)^k(1 + zx)^{1/2}}{(z - a_i)\,(A(z))^k}\,dz \quad (0 \le i, j \le 2)$$

where Γ_j is defined by

$$|z - a_j| = \min_{i \neq j}\left\{\frac{|a_j - a_i|}{2}\right\}$$

oriented positively. We therefore have that

$$\left|p_{ij}\left(\frac{1}{N}\right)\right|\left(1 + \frac{a_j}{N}\right)^{1/2} \le \max_{z \in \Gamma_j}\left|\frac{\left(1 + \frac{z}{N}\right)^{k+\frac{1}{2}}}{(A(z))^k}\right|.$$

Minimizing the function

$$\left|\frac{A(z)}{z - a_j}\right|$$

on the contour Γ_j, using that $N > M^9$ and considering the cases with a_1 negative, zero and positive separately, we may conclude that

$$|p_{ij}(x)| < 1.01\,\left(\frac{8.01}{\zeta}\right)^k$$

where

$$\zeta = \begin{cases}(a_1 - a_0)^2\,(2a_2 - a_0 - a_1) & \text{if } a_2 - a_1 \ge a_1 - a_0 \\ (a_2 - a_1)^2\,(a_1 + a_2 - 2a_0) & \text{if } a_2 - a_1 < a_1 - a_0.\end{cases}$$

Applying Lemma 3.1, since Lemma 3.4 of [22] ensures that $\det(p_{ij}(1/N))$ does not vanish, we therefore have

Theorem 3.2 If a_i, p_i, q and N are integers for $0 \le i \le 2$, with $a_0 < a_1 < a_2$, $a_j = 0$ for some $0 \le j \le 2$, q nonzero and $N > M^9$, where

$$M = \max_{0 \le i \le 2}\{|a_i|\},$$

then we have

$$\max_{0 \le i \le 2}\left\{\left|\sqrt{1 + \frac{a_i}{N}} - \frac{p_i}{q}\right|\right\} > (130\,N\,\Upsilon)^{-1}\,q^{-\lambda}$$

13

where

$$\lambda = 1 + \frac{\log\left(33N\Upsilon\right)}{\log\left(1.7N^2 \ \prod_{0 \le i < j \le 2} \left(a_i - a_j\right)^{-2}\right)}$$

and

$$\Upsilon = \begin{cases} \frac{(a_2 - a_0)^2 (a_2 - a_1)^2}{2a_2 - a_0 - a_1} & \text{if } a_2 - a_1 \ge a_1 - a_0 \\ \frac{(a_2 - a_0)^2 (a_1 - a_0)^2}{a_1 + a_2 - 2a_0} & \text{if } a_2 - a_1 < a_1 - a_0. \end{cases}$$

From this result, we have

Corollary 3.3 If (x_i, y_i, z_i) are positive solutions to (2) for $1 \le i \le 2$, and if k_i is as defined in (3), then $k_1 \ge 9$ implies that

$$k_2 < \left(\frac{7k_1^2 + 17k_1 - 32}{k_1^2 - 9k_1 + 8}\right) k_1 \le 86k_1.$$

Proof: We apply the previous theorem with $a_0 = 0$, $a_1 = a$, $a_2 = b$, $N = abz_1^2$, $q = abz_1z_2$, $p_1 = ay_1y_2$ and $p_2 = bx_1x_2$. Since

(14)
$$z_1 = \frac{\beta^{k_1} - \beta^{-k_1}}{2\sqrt{b}} > \left(2\sqrt{b}\right)^{k_1 - 1} \ge 2^8 \, b^4$$

the inequality $N > M^9$ obtains. It follows that

$$\sqrt{1 + \frac{a_1}{N}} - \frac{p_1}{q} = \frac{y_1}{bz_1}\left(\sqrt{b} - \frac{y_2}{z_2}\right)$$

and

$$\sqrt{1 + \frac{a_2}{N}} - \frac{p_2}{q} = \frac{x_1}{az_1}\left(\sqrt{a} - \frac{x_2}{z_2}\right).$$

Since (x_1, y_1, z_1) and (x_2, y_2, z_2) are both solutions to (2), we therefore have

$$\max\left\{\left|\sqrt{1 + \frac{a_1}{N}} - \frac{p_1}{q}\right|, \left|\sqrt{1 + \frac{a_2}{N}} - \frac{p_2}{q}\right|\right\} < z_2^{-2}.$$

By calculus, $N\Upsilon \le \frac{1}{2}b^5 z_1^2$ and $N^2(ab(b-a))^{-2} > b^{-2}z_1^4$ and so (14) implies that

$$\lambda < \frac{3k_1}{2k_1 - 4}.$$

It follows from Theorem 3.2 and $k_1 \ge 9$ that

$$z_2^{k_1 - 8} \le 65^{2k_1 - 4} \, a^{3k_1} \, b^{13k_1 - 20} \, z_1^{7k_1 - 8}$$

14

and applying $b > a$ and inequality (14) therefore yields

$$z_2 < z_1^{\frac{7k_1^2+17k_1-32}{k_1^2-9k_1+8}}.$$

Noting that $k_2 \geq \sigma k_1$ implies, for σ a positive constant exceeding unity, that

$$\frac{z_2}{z_1^\sigma} > \beta^{k_2-\sigma k_1} \left(2\sqrt{b}\right)^{\sigma-1} > 1,$$

the first part of the corollary follows. The second inequality is a consequence of the fact that $\frac{7k_1^2+17k_1-32}{k_1^2-9k_1+8}$ is decreasing in k_1 and equal to 86 for $k_1 = 9$. □

We now have all the necessary machinery in place to show that (2) has at most four positive solutions. From Lemma 2.2, we have

$$(k_3 - k_2)(k_2 - k_1) > \alpha^{2j_1} \geq 7 + 4\sqrt{3}$$

which implies that $k_3 \geq 9$ in all cases. Further, if we have five solutions to (2), say (x_i, y_i, z_i) for $1 \leq i \leq 5$, then from (3) and Lemma 2.2,

$$(k_5 - k_4)(k_4 - k_3) > \alpha^{2j_3} > \frac{a}{b}\beta^{2k_3} > 2a\beta^{2(k_3-1)}.$$

Since $\beta \geq 2 + \sqrt{3}$ and $k_3 \geq 9$, this implies that $k_5 > 86k_3$, contradicting Corollary 3.3.

As a comment on Theorem 3.2, we note that the result may be sharpened somewhat through use of precise asymptotics for the contour integrals that occur in the proof, say via application of the saddle point method (see e.g. [6] for details). It does not appear, however, that such a sharpening is of use in the case at hand. To show that, in fact, there are at most three solutions in positive integers to (2), we require a result from the theory of linear forms in logarithms.

4 Linear Forms in Two Logarithms

In this section, we will suppose that we have four positive solutions (x_i, y_i, z_i) $(1 \leq i \leq 4)$ to (2) with α, β, j_i and k_i as in (3) and $z_{i+1} > z_i$ for $1 \leq i \leq 3$. We further suppose that $k_3 > 10^6$, an assumption we will justify in the next section. Also, we have $k_2 \leq 8$, since otherwise we may argue as at the end of the last section to deduce that there are at most three solutions to (2). From the recent work of Laurent, Mignotte and Nesterenko [16], we infer

Lemma 4.1 Let α and β be the fundamental solutions to

$$x^2 - ay^2 = 1 \quad \text{and} \quad y^2 - bz^2 = 1,$$

respectively, where $b > a \geq 2$ are integers, and, for j and k positive integers, define

$$\Lambda = j \log \alpha \ - \ k \log \beta.$$

Then if

$$h = \max \left\{ 12, 4 \log \left(\frac{k}{\log \alpha} + \frac{j}{\log \beta} \right) - 1.8 \right\},$$

either one has $\Lambda = 0$ or

$$
\begin{aligned}
\log |\Lambda| \ \geq \ & -61.2 \log \alpha \log \beta \ h^2 - 24.3 \left(\log \alpha + \log \beta \right) h - 2h \\
& -48.1 \left(\log \alpha \log \beta \right)^{1/2} h^{3/2} - \log \left(\log \alpha \log \beta \ h^2 \right) - 7.3.
\end{aligned}
$$

Proof: This is easily deduced from Théorème 2 of [16], taking $\alpha_1 = \alpha$, $\alpha_2 = \beta$, $b_1 = k$, $b_2 = j$, $D = 4$ and $\rho = 11$ and noting that the result follows readily if $\log \alpha$ and $\log \beta$ are $\mathbb{Q}$-linearly dependent with Λ nonzero. $\square$

We apply this lemma with $j = j_4 - j_3$ and $k = k_4 - k_3$. The inequalities in (7) imply the nonvanishing of Λ and, further, that

$$(15) \qquad \qquad \log |\Lambda| < -2 \left(k_3 - 1 \right) \ \log \beta.$$

To combine this bound with Lemma 4.1, we again depend upon Lemma 2.2 which, crucially for this argument, guarantees that the exponents k_i grow in terms of the fundamental units α and β, a property we have not explicitly used thus far.

It is convenient at this stage to make the following observation. If $\alpha = m + s\sqrt{a}$ is the fundamental solution to $x^2 - az^2 = 1$, then s divides z for any solution (x, y, z) to this equation. It follows that solutions to $x^2 - az^2 = 1$ are in one-to-one correspondence with those to $x^2 - (m^2 - 1) z_1^2 = 1$. A similar result holds for the equation $y^2 - bz^2 = 1$ and iterating this argument, if a and b are distinct positive integers such that (2) possesses positive solutions, then these correspond to solutions of a system of equations of the form

$$(16) \qquad \qquad X^2 - AY^2 = 1 \quad \text{and} \quad Y^2 - BZ^2 = 1$$

where $A = m^2 - 1$ and $B = n^2 - 1$ for integers m and n. Therefore, if we can prove that simultaneous equations of the form (16) have at most three positive solutions, then the same is true for (2) in general. We will thus assume that

16

a and b are each one less than squares and, in particular, that $\alpha < \beta$ (since $a < b$) and $j_1 = k_1 = 1$.

If $h = 12$ in Lemma 4.1, then applying

(17) $$\beta \geq \max \left\{ \alpha, 15 + \sqrt{224} \right\}$$

yields the inequality

$$\log |\Lambda| > - \left(8812.8 \log \alpha + 2594.1 \right) \, \log \beta.$$

Further, Lemma 2.2 implies, with $k_2 \leq 8$, that

(18) $$k_3 > \frac{1}{7} \, \alpha^{2j_1} = \frac{1}{7} \, \alpha^2.$$

Together with (15), we therefore have

$$k_3 < 2203.2 \log k_3 + 5585.3$$

which contradicts the choice of $k_3 > 10^6$. Next suppose that

$$h = 4 \log \left(\frac{k}{\log \alpha} + \frac{j}{\log \beta} \right) - 1.8.$$

From (6) and the inequality $\alpha \geq 2 + \sqrt{3}$, we have that $h < 4 \log k$. Application of Lemma 4.1 gives

(19) $$\log |\Lambda| > - \left(979.2 \log \alpha \log^2 k + 384.8 \log^{3/2} k + 197.0 \log k + 3.7 \right) \log \beta$$

where we have again used (17). Applying Corollary 3.3 and $k_3 > 10^6$, we therefore have

$$k = k_4 - k_3 < 6.01 k_3$$

and so (15), (18) and (19) yield

$$k_3 < 356.5 \log^3 k_3 + 231.1 \log^{3/2} k_3 + 111.3 \log k_3 + 2.9,$$

contradicting $k_3 > 10^6$.

5 A Class of Examples

In this section, we deal with a number of cases for which the associated fundamental units are small and discuss families of (a, b) for which (2) has at least

two positive solutions (x, y, z). As observed in the previous section, we may assume that

$$a = m^2 - 1, \ b = n^2 - 1, \ \alpha = m + \sqrt{m^2 - 1} \text{ and } \beta = n + \sqrt{n^2 - 1}$$

where $n > m \geq 2$ are integers. To complete the proof of Theorem 1.1, we must show that (2) has at most three positive solutions if k_i (as defined in (3)) satisfies $k_3 \leq 10^6$ and $2 \leq k_2 \leq 8$. If we assume the existence of four positive solutions, then Lemma 2.2 implies that the associated k_i satisfy

$$(20) \qquad (k_4 - k_3)(k_3 - k_2) > \alpha^{2j_2} > \frac{a}{b} \beta^{2k_2} > 4a\beta^{2(k_2-1)}.$$

Now $k_3 \geq 9$ implies, via Corollary 3.3, that $k_4 < 86k_3$. Together with (20) and the fact that $\beta \geq 15 + \sqrt{224}$, we have that $k_3 \geq 12$. Iterating this argument (using (20) and Corollary 3.3), we conclude that $k_3 \geq 35$ and so (from Corollary 3.3) $k_4 < 10k_3$. Since we are assuming that $k_3 \leq 10^6$, this, with (20), implies

$$(21) \qquad \sqrt{a} \ \beta^{k_2-1} < 1.5 \times 10^6.$$

Let us define integers $z_{m,i}$ by the recurrence relation

$$z_{m.i+1} = 2mz_{m,i} - z_{m,i-1}$$

where $z_{m,0} = 0$ and $z_{m,1} = 1$. It follows that the positive integers z for which the equation $x^2 - az^2 = 1$ has solutions are exactly those with $z = z_{m,i}$ for $i \geq 1$ (remembering that $a = m^2 - 1$). Since we have $m \geq 2$ and $n \geq 15$, inequality (21) shows that $2 \leq k_2 \leq 5$. We treat each of these possibilities in turn.

If $k_2 = 5$, then (21) implies that $m = 2$ and $n = 15$, whence $z_2 = 807301$. On the other hand, $z_{2,11} < 807301 < z_{2,12}$, so that this fails to be a solution to $x^2 - 3z^2 = 1$. Suppose next that $k_2 = 4$. If $m \geq 6$, then, from (21), we have $n \leq 31$ and so

$$z_{n,4} = 8n^3 - 4n \leq 238204.$$

However, $z_{m,6} \geq z_{6,6} = 241956$ and, since $z_{m,5}$ is odd, we may thus assume that $2 \leq m \leq 5$. Now, $m \geq 2$, $n \geq 15$ and (21) imply that $15 \leq n \leq 47$ and hence

$$26940 \leq z_{n,4} \leq 830396.$$

We conclude, for $k_2 = 4$, by noting that the only values of $z_{m,i}$ in this interval with $2 \leq m \leq 5$, $z_{m,i} \equiv 0 \ (mod \ 4)$ and $i > 4$ are $z_{2,10} = 151316$, $z_{3,8} = 235416$

18

and $z_{4,6} = 30744$, all of which are distinct from $z_{n,4}$ for $15 \leq n \leq 47$. If $k_2 = 3$, we argue similarly. Since $z_{m,i} \equiv 3 \ (mod \ 4)$ exactly when $i \equiv 3 \ (mod \ 4)$, we may restrict our attention to the equation $z_{m,i} = z_{n,3}$ with $i \equiv 3 \ (mod \ 4)$ and $i \geq 7$. If $m \geq 5$, then (21) gives $n \leq 276$ and so

$$z_{n,3} = 4n^2 - 1 \leq 304703$$

while $z_{m,7} \geq z_{5,7} = 950599$. For $m \geq 2$, (21) yields the inequality $n \leq 465$, whence

$$889 \leq z_{n,3} \leq 864899.$$

The only $z_{m,i}$ in this interval with $2 \leq m \leq 4$, $i \equiv 3 \ (mod \ 4)$ and $i \geq 7$ are $z_{2,7} = 2911$, $z_{2,11} = 564719$, $z_{3,7} = 40391$ and $z_{4,7} = 242047$, none of which are of the form $4n^2 - 1$.

It remains to consider when $k_2 = 2$. Since $z_{n,2} = 2n$ and $z_{m,i}$ is even precisely when i is even, it follows that pairs (a, b) with $a = m^2 - 1, b = n^2 - 1$ and $n > m \geq 2$ for which (2) possesses solutions with $k_1 = 1$ and $k_2 = 2$ are exactly those satisfying

$$(22) \qquad n = \frac{1}{2} \, z_{m,2j} = \frac{\left(m + \sqrt{m^2 - 1}\right)^{2j} - \left(m - \sqrt{m^2 - 1}\right)^{2j}}{4\sqrt{m^2 - 1}}$$

for some $j \geq 2$. The "smallest" member of one of these families corresponds to the equations

$$x^2 - 3z^2 = 1, \quad y^2 - 783z^2 = 1$$

with solutions $(x, y, z) = (2, 28, 1)$ and $(97, 1567, 56)$ (as noted in [18]). Similarly, the equations

$$x^2 - 2z^2 = 1, \quad y^2 - 3001556z^2 = 1$$

possess the solutions $(x, y, z) = (3, 3465, 2)$ and $(19601, 24012449, 13860)$ (derived from $m = 3$ and $n = 3465$). The author knows of no pair (a, b) for which (2) has even two positive solutions which is not induced by the above parameterized families (nor of any pair (a, b) for which (2) has three positive solutions).

To complete the proof of Theorem 1.1, we note that if $m \geq 21$, then (21) implies that $n \leq 35754$, but

$$\frac{1}{2} \, z_{m,2j} \geq \frac{1}{2} \, z_{m,4} = 4m^3 - 2m \geq 37002.$$

Similarly, (21) allows us to restrict our attention to $n = \frac{1}{2} \, z_{m,4}$ for $2 \leq m \leq 20$, $n = \frac{1}{2} \, z_{m,6}$ for $2 \leq m \leq 5$, $n = \frac{1}{2} \, z_{m,8}$ for $2 \leq m \leq 3$ and $n = \frac{1}{2} \, z_{2,10}$. For

19

each of these 26 cases, we compute the initial terms in the continued fraction expansion to $\frac{\log \beta}{\log \alpha}$. Arguing as in Section 2, we have, analogous to (7),

$$(23) \qquad \left| \frac{\log \beta}{\log \alpha} - \frac{j_4 - j_3}{k_4 - k_3} \right| < \frac{1.001 \, b}{a \log \alpha \, (k_4 - k_3)} \, \beta^{-2k_3}.$$

Now $\beta \geq 28 + \sqrt{783}$ so (21) implies that $k_3 \geq 65$, whence from Corollary 3.3, we have $k_4 - k_3 < 8k_3 < 10^7$. Inequality (23) therefore yields

$$\left| \frac{\log \beta}{\log \alpha} - \frac{j_4 - j_3}{k_4 - k_3} \right| < \frac{1}{10^{224} \, (k_4 - k_3)} < \frac{1}{10^{217} \, (k_4 - k_3)^2}$$

which implies the existence of a partial quotient a_{i+1} to $\frac{\log \beta}{\log \alpha}$ satisfying $a_{i+1} > 10^{216}$ for a corresponding convergent p_i/q_i with $q_i < 10^7$ (see e.g. [15]). For each of the 26 cases we are concerned with, the 17th convergent has denominator exceeding 10^7 and the largest of the first 18 partial quotients we encounter is $a_{16} = 17145$ for $m = 2$ and $n = 5432$. This concludes the proof of Theorem 1.1.

As a final comment in this section, we note that a result of Nemes and Pethő [19] allows us to strengthen Theorem 1.1 in the following sense:

Theorem 5.1 If a and b are positive integers then there exists an effective constant $b_0 = b_0(a)$ such that if $b \geq b_0$ then either (a, b) is equivalent to a pair $(m^2 - 1, n^2 - 1)$ of the form described in (22) or equation (2) possesses at most two solutions (x, y, z) in positive integers.

Proof: Let $a = m^2 - 1$ and $b = n^2 - 1$ for $n > m \geq 2$ and, for fixed m and $k_2 \geq 3$, consider the equation $z_{m,i} = z_{n,k_2}$, where $z_{m,i}$ is as defined in Section 5. Viewing z_{n,k_2} as a polynomial in n of degree $k_2 - 1$, Theorem 3 of [19] may be applied to show that this equation possesses at most finitely many solutions in integers i and n and, through the theory of linear forms in logarithms, to effectively bound their size (note that, in the terminology of Theorem 3 of [19], we have $q = -1/(4m^2 - 1) < 0$). Now, if $k_2 \geq 10^6$, the arguments of Section 4 (this time applied to the linear form $\Lambda = (j_3 - j_2) \log \alpha - (k_3 - k_2) \log \beta$) may be used to derive a contradiction. The theorem follows, therefore, by taking $b_0 = n_0^2 - 1$, where solutions to $z_{m,i} = z_{n,k_2}$ for $3 \leq k_2 < 10^6$ satisfy $n < n_0$. $\square$

6 The More General Situation

Let us now turn our attention to the simultaneous equations described in (1) (and hence Theorem 1.2) where a, b, u and v are nonzero integers with,

additionally, $av - bu$ nonzero. The theory of Pellian equations guarantees that if each of the equations in (1) possesses a solution, then a positive solution (x_i, y_i, z_i) to (1) satisfies

$$(24) \qquad z_i = \frac{\alpha^{j_i}\mu - \alpha^{-j_i}\overline{\mu}}{2\sqrt{a}} = \frac{\beta^{k_i}\nu - \beta^{-k_i}\overline{\nu}}{2\sqrt{b}}$$

where α and β are the fundamental solutions to $x^2 - az^2 = 1$ and $y^2 - bz^2 = 1$, respectively, μ and ν are "base" solutions to $x^2 - az^2 = u$ and $y^2 - bz^2 = v$ and $\overline{\mu}$ and $\overline{\nu}$ are their conjugates (by a base solution to an equation like $x^2 - az^2 = u$, we mean a minimal positive solution (if such a solution exists) corresponding to an integer l with $l^2 \equiv a \pmod{u}$ and $0 \le l < |u|$. For an explanation of these terms, the reader is directed to [9]. The only fact we will require regarding these "base" solutions is that there are at most $2^{\omega(u)}$ of them where, again, $\omega(u)$ denotes the number of distinct prime factors of u.). It follows that two positive solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) with $z_2 > z_1$, corresponding to a fixed pair of base solutions μ and ν, satisfy

$$\frac{z_2}{z_1} = \beta^{k_2 - k_1}\left(1 + \frac{\overline{\nu}}{\nu}\left(\frac{\beta^{-2k_1} - \beta^{-2k_2}}{1 - \beta^{-2k_1}\frac{\overline{\nu}}{\nu}}\right)\right) > 0.9\beta$$

where we use that $|\overline{\nu}/\nu| < 1$. The number of positive integer solutions (x, y, z) to the simultaneous equations (1) with $z < \max\{|u|, |v|\}^c$, for a fixed positive constant c is thus $\ll 2^{\min\{\omega(u),\omega(v)\}}\log(|u| + |v|)$. We will show that for c suitably large, the number of solutions to (1) with z exceeding $\max\{|u|, |v|\}^c$ is, for a fixed pair of base solutions to (1), absolutely bounded.

For convenience, set

$$M_1 = \max\{|a|, |b|\}, \quad M_2 = \max\{|u|, |v|\} \quad \text{and} \quad M_3 = \max\{M_1, M_2\}.$$

We have

Lemma 6.1 If (x_i, y_i, z_i) are positive solutions to (1) for $1 \le i \le 3$, belonging to a fixed pair of base solutions and satisfying $z_3 > z_2 > z_1 > M_2^3$, then $z_3 > z_1^3$.

Proof: We consider, again, the determinant Δ defined in the proof of Lemma 2.1, where this time the three solutions are to (1). We once again restrict our attention to a fixed pair of base solutions μ and ν to (1). As previously, we expand along the third column, define $\alpha_i = x_i + \sqrt{a}z_i$ and $\beta_i = y_i + \sqrt{b}z_i$ and find

$$\Delta = \frac{uv}{4\sqrt{ab}z_1z_2z_3}\sum_{1 \le i \le 3} z_i\,\delta_i$$

21

where

$$\delta_1 = u \left(\alpha_3^{-2} - \alpha_2^{-2} \right) + v \left(\beta_2^{-2} - \beta_3^{-2} \right) + uv \left((\alpha_2 \beta_3)^{-2} - (\alpha_3 \beta_2)^{-2} \right)$$

and similarly for δ_2 and δ_3. From $b > a \geq 2$ and $z_3 > z_2 > z_1$, it follows that

$$|\delta_i| < \frac{M_2}{2z_1^2} + \frac{M_2^2}{36z_1^4}$$

and thus $z_1 > M_2^3$ implies that

$$|\Delta| < \frac{M_2^3 z_3}{z_1^4} < \frac{z_3}{z_1^3}.$$

If $\Delta = 0$, however, arguing as in [18], then the solutions (x_i, y_i, z_i) lie in a proper subspace of $\mathbb{R}^3$, contradicting Bezout's theorem (since the (proper) intersection between this subspace and the affine variety defined by the equations in (1) would thus contain more than four points – namely $\pm(x_i, y_i, z_i)$ for $1 \leq i \leq 3$). Since Δ is an integer, it follows that $z_3 > z_1^3$ as desired. $\square$

We can now appeal to Theorem 3.2 to find a bound for large solutions in terms of a single one of suitable size:

Lemma 6.2 If (x_i, y_i, z_i) are positive solutions to (1) for $1 \leq i \leq 2$, belonging to a fixed pair of base solutions and satisfying $z_1 > 15 \times M_3^{10}$, then $z_2 < z_1^{80}$.

Proof: We apply Theorem 3.2 with $a_0 = 0$, $a_1 = av$, $a_2 = bu$ and N, q, p_1 and p_2 as in the proof of Corollary 3.3. Arguing as in this proof, we obtain

$$\max \left\{ \left| \sqrt{1 + \frac{a_1}{N}} - \frac{p_1}{q} \right|, \left| \sqrt{1 + \frac{a_2}{N}} - \frac{p_2}{q} \right| \right\} < M_2 \, z_2^{-2}.$$

Also, $N\Upsilon \leq M_1^5 M_2^3 z_1^2$ and

$$N^2 \prod_{0 \leq i < j \leq 2} (a_i - a_j)^{-2} \geq M_1^{-4} M_2^{-6} z_1^4$$

and so $z_1 > 15 \times M_3^{10}$ implies that $\lambda < 29/15$. It follows from Theorem 3.2 that

$$z_2 < 130^{15} M_1^{133} M_2^{60} z_1^{59} < z_1^{80}$$

where, again, the last inequality comes from $z_1 > 15 \times M_3^{10}$ and $M_3 \geq 3$. $\square$

Since this Lemma, together with Lemma 6.1, guarantees at most finitely many positive solutions (x, y, z) to (1), corresponding to μ and ν, with $z \gg \max\{|u|, |v|\}^{10}$, this completes the proof of Theorem 1.2.

7　Concluding Remarks

The techniques described in this paper may be modified somewhat to treat a number of similar problems connected to common values in recurrence sequences and produce strong bounds where applicable (though in rather less generality than [24]). For example, we can, through a result analogous to Lemma 2.2, prove

Theorem 7.1 If a and b are distinct nonzero integers, then the simultaneous Diophantine equations

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

possess at most three solutions (x, y, z) in positive integers.

This provides a quantitative version of a theorem of Ljunggren [17] (see also [3] for further work on simultaneous Pell equations of this type).

A question of some interest is whether the "correct" bound in Theorem 1.2 is two or three (positive solutions to (2) – or, if one likes, 20 or 28 integer solutions). As previously mentioned, the author does not know of any pairs (a, b) for which (2) possesses three positive solutions or of any with even two which are not essentially members of the families defined by equation (22). There does not appear to be particularly compelling evidence one way or the other and a conjecture at this stage might be a trifle rash. One may further note that each positive solution to (2) corresponds (see [20]) to a rational point of infinite order on the elliptic curve

$$Y^2 = X\,(X + a)\,(X + b)\,.$$

In fact, the pairs (a, b) defined by (22) may be readily shown to induce a family of elliptic curves with rank at least two.

Finally, it seems very likely that Theorem 1.2 may be improved, through a treatment of the simultaneous equations

$$P(x, y, z) = Q(x, y, z) = 1$$

where P and Q are ternary quadratic forms. The upper bound upon the number of solutions should, in all likelihood, depend only upon the number of prime factors of the integers u and v.

8　Acknowledgements

References

[1] W.S. Anglin. Simultaneous Pell equations. *Math. Comp.* **65** (1996), no. 213, 355-359.

[2] W.S. Anglin. The Queen of Mathematics: An Introduction to Number Theory. Kluwer, Dordrecht, 1995.

[3] A. Arwin. Common solutions to simultaneous Pell equations. *Ann. Math.* **52** (1922), 307-312.

[4] A. Baker. Linear forms in the logarithms of algebraic numbers. *Mathematika* **15** (1968), 204-216.

[5] A. Baker and H. Davenport. The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. *Quart. J. Math. Oxford* (2) **20** (1969), 129-137.

[6] M.A. Bennett. Simultaneous rational approximation to binomial functions. *Trans. Amer. Math. Soc.* **348** (1996), 1717-1738.

[7] A. Boutin and P.F. Teilhet. The form $6\beta^2 + 1$ is not a square if β is a root of $\gamma^2 - 3\beta^2 = 1$. *L'Intermédiare des mathématiciens* **XI** (1904), 68, 182.

[8] E. Brown. Sets in which $xy + k$ is always a square. *Math. Comp.* **45** (1985), 613-620.

[9] D.A. Buell. Binary Quadratic Forms : Classical Theory and Modern Computations. Springer-Verlag, 1989.

[10] G.V. Chudnovsky. On the method of Thue-Siegel. *Ann. of Math.,* II Ser. **117** (1983), 325-382.

[11] J.-L. Colliot-Thélène, J.-J. Sansuc and Sir P. Swinnerton-Dyer. Intersection of two quadrics and Châtelet surfaces. I. *J. reine angew. Math.* **373** (1987), 37-107.

[12] J.-L. Colliot-Thélène, J.-J. Sansuc and Sir P. Swinnerton-Dyer. Intersection of two quadrics and Châtelet surfaces. II. *J. reine angew. Math.* **374** (1987), 72-168.

[13] A. Gloden. Impossibilités Diophantiennes. *Euclides, Madrid* **9** (1949), 476.

[14] C.M. Grinstead. On a method of solving a class of Diophantine equations. *Math. Comp.* **32** (1978), 936-940.

[15] A. Khintchine. Continued Fractions. P. Noordhoff Ltd., Groningen, 1963, 3rd edition.

[16] M. Laurent, M. Mignotte and Y. Nesterenko. Formes linéaires en deux logarithms et déterminants d'interpolation. *J. Number Theory* **55** (1995), 285-321.

[17] W. Ljunggren. Litt om simultane Pellske ligninger. *Norsk Mat. Tidsskr.* **23** (1941), 132-138.

[18] D.W. Masser and J.H. Rickert. Simultaneous Pell equations. *J. Number Theory* to appear.

[19] I. Nemes and A. Pethő. Polynomial values in linear recurrences II. *J. Number Theory* **24** (1986), 47-53.

[20] K. Ono. Euler's concordant forms. *Acta Arith.* to appear.

[21] R.G.E. Pinch. Simultaneous Pellian equations. *Math. Proc. Cambridge Philos. Soc.* **103** (1988), 35-46.

[22] J.H. Rickert. Simultaneous rational approximations and related diophantine equations. *Proc. Cambridge Philos. Soc.* **113** (1993), 461-472.

[23] H.P. Schlickewei. S-unit equations over number fields. *Invent. Math.* **102** (1990), 95-107.

[24] H.P. Schlickewei and W.M. Schmidt. The intersection of recurrence sequences. *Acta Arith.* **72** (1995), 1-44.

[25] C.L. Siegel. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuss. Akad. Wiss.* (1929), 1.

[26] A. Thue. Über Annäherungenswerte algebraischen Zahlen. *J. reine angew. Math.* **135** (1909), 284-305.

[27] J. Tunnell. A classical Diophantine problem and modular forms of weight $\frac{3}{2}$. *Invent. Math.* **72** (1983), 323-334.

[28] P.G. Walsh. Elementary methods for solving simultaneous Pell equations. to appear.

[29] D. Zagier. Large integral points on elliptic curves. *Math. Comp.* **48** (1987), 425-436.

Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
E-mail address : mabennet@math.lsa.umich.edu