Simultaneous Pell Equations

D. W. Masser

Mathematisches Institut, Universität Basel, Rheinsprung 21, 4051 Basel, Switzerland

and

J. H. Rickert

Rose-Hulman Institute of Technology, 5500 Wabash Avenue, Terre Haute, Indiana 47803

Communicated by E. Bombieri

Received October 25, 1995

It is proved that if $a$ and $b$ are different non-zero rational integers then the “simultaneous Pell equations”

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

have at most 132 solutions in rational integers $x, y, z$.

1. INTRODUCTION

Let $a$ and $b$ be rational integers, and consider the Pell equations

$$x^2 - az^2 = 1, \quad y^2 - bz^2 = 1. \quad (1.1)$$

It is well-known that each equation separately can have infinitely many solutions in rational integers $x, z$ or $y, z$; in fact this happens as soon as $a$ or $b$ are positive non-squares. The object of this paper is to show that such behaviour changes drastically when the two equations are considered simultaneously.

**Theorem.** Suppose $a, b$ are distinct and non-zero. Then the simultaneous Pell equations (1.1) have at most 132 solutions in rational integers $x, y, z$. 

When $a, b$ are distinct and non-zero, it is easy to see that (1.1) has only finitely many solutions. For example, the quartic polynomial $P(z) = (az^2 + 1)(bz^2 + 1)$ is then squarefree, and any integral solution $(x, y, z)$ of $x^2 - az^2 = 1, y^2 - bz^2 = 1$ would have $P(z)$ squarefree.
(1.1) gives rise to an integral point \((z, Z)\) on the hyperelliptic curve 
\[ Z^2 = P(z) \] 
for \(Z = xy\). But Siegel’s Theorem implies that there are only finitely many such \((z, Z)\), so only finitely many \((x, y, z)\) as well.

Standard results for hyperelliptic curves (see for example [Ba2, p. 45]) now lead to effective estimates for the sizes of all solutions of (1.1); however, the bounds will depend on \(a\) and \(b\), and they will probably be quite large.

When we are interested instead in the number of solutions of (1.1), the work of Evertse [E] on \(S\)-units, as developed by Evertse and Silverman [ES], provides somewhat smaller estimates, but the bounds still depend on \(a\) and \(b\).

Uniform bounds independent of the coefficients, at least for the number of solutions of Thue equations, are provided by the method of Thue–Siegel–Roth; see for example the work of Bombieri and Schmidt [BS]. The celebrated generalization to simultaneous approximation due to Schmidt achieves something similar for norm form equations [Schm]. And Schlickewei’s developments for \(S\)-units (generalizing [E]) can in fact be applied directly to our equations (1.1). For example, with the four units 
\[ x \pm z \sqrt{a}, y \pm z \sqrt{b}, \] 
Theorem 1.1 (p. 96) of [Schl] gives an absolute bound \(C\) in our theorem in place of 132. But \(C\) seems to be quite large, and it appears difficult to avoid numbers like \(2^{50}\). This situation should soon improve with the use of Faltings’s Product Theorem (see [FW] and forthcoming work of Evertse and Ferretti independently).

In the present paper we return to the Padé Approximation approach also originated by Thue and taken up with great effect by both Baker [Ba1] and Evertse [E]. But of course we need to study simultaneous approximation. Our specific construction uses the integrals introduced in the second author’s paper [R]. Naturally we have to combine these with gap principles of a familiar kind.

The equations (1.1) may seem rather special, but if arbitrary constants in place of 1 are allowed, then we cannot hope to keep the uniformity. For example, we will prove the following fact.

**Remark.** Given any \(N\), there are rational integers \(u\) and \(v\) such that the equations

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

(1.2) have at least \(N\) solutions in rational integers \(x, y, z\).

Our paper is organized as follows. In Section 2 we prove our remark by explicitly writing (1.1) as an elliptic curve and imitating the proof of the “Taxicab Theorem” (terminology of [ST, p. 147]) that there are positive integers expressible in arbitrarily many ways as the sum of two integer cubes. The calculations here are also helpful in establishing a simple estimate of Bezout type that we shall need later for one of our gap principles.
In Section 3 we state a proposition on the simultaneous rational approximation of certain quadratic irrationals, very much in the style of \([R]\). This is proved in Sections 4–8. One feature is that our treatment of the arithmetic estimates parallels that of the analytic estimates in that we use \(p\)-adic analysis as well as complex analysis. A similar feature can be found in the articles \([V]\) and \([BV]\) of Väätäinen and Bundschuh. A minor technical difference is that we are able to avoid the Schnirelmann integral by formulating everything in terms of residues.

Finally, in Section 9 we state and prove our gap principles, and then in Section 10 we establish our theorem.

Almost certainly our bound 132 can be improved, probably by using the lemniscates in \([R]\) (the saddle-point method) or the positivity techniques of Lemma 4.2 of \([R]\) or the refined denominator estimates introduced by Chudnovsky \([C]\). For the use of some of these at the level of simultaneous approximation see a forthcoming paper of Bennett \([Be]\).

Anglin \([A]\) has calculated the complete set of solutions of (1.1) for every \(a, b\) with \(\max \{a, b\} \leq 200\), and he never finds more than 12 solutions. On the other hand, there is a family of examples, of which

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

is a member. This has at least 20 solutions \((x, y, z)\) given by

\[
(\pm 1, \pm 1, 0), \quad (\pm 2, \pm 28, \pm 1), \quad (\pm 97, \pm 1567, \pm 56)
\]

with all choices of signs.

2. ELLIPTIC CURVES

Let \(K\) be a field of characteristic zero, and let \(a, b\) be distinct non-zero elements of \(K\). The equations (1.1) define an affine curve \(C_0(a, b)\) of genus 1. This is the image of the elliptic curve \(E_0(a, b)\) defined by

\[
t^2 = 4s(s + a)(s + b)
\]

under the rational map

\[
x = (s^2 + 2as + ab)/D, \quad y = (s^2 + 2bs + ab)/D, \quad z = t/D
\]

for \(D = D(s) = s^2 - ab\). This map is birational, with inverse given by

\[
x = a(y + 1)/(x - 1) = b(x + 1)/(y - 1), \quad t = zD(s).
\]

These may be extended to isomorphisms between the respective projective models \(C(a, b)\) and \(E(a, b)\) obtained by homogenizing. Then the “trivial point”
Let $\lambda, \mu, \nu$ in $K$, not all zero, there are at most four points 
$(x, y, z)$ on $C(a, b)$ satisfying $\lambda x + \mu y + \nu z = 0$.

Proof. We can easily see that the function $f = \lambda x + \mu y + \nu z$ on $C(a, b)$ is not identically zero; for example, on $E(a, b)$ the function $D(s)f$ looks like
\[\lambda(s^2 + 2as + ab) + \mu(s^2 + 2bs + ab) + \nu t,\]
and since $1, s, s^2, t$ are linearly independent, equating to zero the coefficients of $s, s^2, t$ would lead to $\lambda = \mu = \nu = 0$. Now $f$ can have poles, at worst simple, only at the four points at infinity on $C(a, b)$; and so $f$ has at most four zeroes as well. This proves the lemma.

Here we prove the remark in Section 1 by imitating the well-known argument for $x^3 + y^3 = w$. We choose $a = 2, b = 6$; then the point $P = (s_1, t_1)$ cannot have finite order on $E(2, 6)$, otherwise $2P = (s_2, t_2) = (1/4, -15/4)$ would also have finite order, contradicting Lutz–Nagell (see for example [ST, p. 56]) on the integrality of $s_2$ and $t_2$.

In particular, there are infinitely many rational points on $E(2, 6)$, and therefore also on $C(2, 6)$. For a positive integer $N$ take $N$ different finite points on $C(2, 6)$ and express them with a common denominator $T$ as $T^{-1}(X_i, Y_i, Z_i)$ for rational integers $X_i, Y_i, Z_i$ $(1 \leq i \leq N)$. Now with $u = v = -2T^2$
the points
$(x, y, z) = (2Z_i, Y_i, X_i) \quad (1 \leq i \leq N)$
lie on (1.2). This establishes the remark.

3. SIMULTANEOUS APPROXIMATION

The proof of our theorem rests on the following result.

Proposition. Let $a_1, a_2$ be distinct positive integers with

\[M = \max\{a_1, a_2\} \geq 3,\]

SIMULTANEOUS PELL EQUATIONS
and let $N \geq M^{24}$ be an integer. Then for all integers $q \geq 1$, $p_1$, $p_2$ we have
\[
\max\{|\sqrt{1 + a_1/N} - p_1/q|, |\sqrt{1 + a_2/N} - p_2/q|\} \geq (200M^3N)^{-1} q^{-17/10}.
\]
This will be proved in the next five sections by constructing many good simultaneous approximations and applying the following general result.

**Lemma 3.1.** Let $\theta_1, \theta_2$ be real numbers, and suppose there are positive real numbers $l, p, L, P$ and a positive integer $D < L$ with the following properties. For each positive integer $k$ we can find rational numbers $p(\kappa)$, $(i, j) = 0, 1, 2)$, with non-zero determinant, such that the $D \kappa p(i, j)$ are integers $(i, j) = 0, 1, 2)$ and
\[
|p(i, j)| \leq p^k \quad (i, j = 0, 1, 2)
\]
\[
|p(10) + p(1) \theta_1 + p(2) \theta_2| \leq IL^{-k} \quad (i, j = 0, 1, 2).
\]
Then for all integers $q \geq 1$, $p_1$, $p_2$ we have
\[
\max\{|\theta_1 - p_1/q|, |\theta_2 - p_2/q|\} \geq cq^{-1 - \lambda},
\]
where
\[
\lambda = (\log V)/(\log U), \quad V = PD, \quad U = L/D
\]
and
\[
c^{-1} = 6PVC^{-1}, \quad C = \max\{1, 2\}.
\]

**Proof.** This is just Lemma 2.1 (p. 463) of [R] with $m = 2$ and $Q = d = f = 1$.

### 4. Laurent Series

Let $K$ be either the complex field $C (= C_p)$ or the $p$-adic analogue $C_p$ for a finite rational prime $p$. Denote by $|x|$ the standard norm of $x$ in $K$.

We shall be considering formal Laurent series $\varphi = \varphi(z) = \sum_{n=-\infty}^{\infty} c_n(z-a)^n$ with coefficients $c_n$ in some extension field $K'$ of $K$, and a point $a$ in $K$. We write
\[
c_{-1} = \text{res}\{\varphi, a\} = \text{res}\{\varphi(z), a\}
\]
for the residue. Suppose for the rest of this section that $K' = K$. If there exists $R_\varphi$ such that the series converges whenever $0 < |z - a| < R_\varphi$, then for any $R$ in the value group with $0 < R < R_\varphi$ we write $\sup\{\varphi, R, a\}$ for the supremum of $|\varphi|$ on $|z - a| = R$. 

56 MASSER AND RICKERT
Lemma 4.1. For any \( R \) with \( 0 < R < R_\varphi \), we have

\[ |\text{res}\{\varphi, a\}| \leq R \sup\{\varphi, R, a\}. \]

Proof. If \( p = \infty \) the estimate follows immediately from the representation of the residue as the complex integral of \( (2\pi i)^{-1} \varphi(z) \) over \( |z - a| = R \).

If \( p \neq \infty \) we could presumably use the Schnirelmann integral to the same effect. But it is quicker simply to observe that \( \sup\{\varphi, R, a\} \) is the supremum of the \( |c_a| R^n \) (see for example [DGS, Proposition 1.1, p. 114]) and in particular at least \( |c_{-1}| R^{-1} \). So we get what we want without Schnirelmann.

5. RESIDUES CONSTRUCTION

Let \( K \) be in the preceding section. We can define the formal Taylor series \( f(t) = \sqrt{1 + t} \) over \( K \), with constant coefficient 1. Let \( a_0, a_1, a_2 \) be distinct elements of \( K \), and define the polynomial

\[ A(z) = (z - a_0)(z - a_1)(z - a_2). \]

For a variable \( x \) the functions

\[ \sigma_j(x, z) = \sqrt{(1 + zx)/(1 + a_j x)} = \sqrt{1 + t} \quad (j = 0, 1, 2) \]

for \( t = (z - a_j) x/(1 + a_j x) \) are then formal Taylor series in \( z - a_j \) over the field \( \mathbb{K}(x) \). So if \( k \) is a non-negative integer the functions

\[ F^{(k)}_{ij}(x, z) = (1 + zx)^k \sigma_j(x, z)/((z - a_i)(A(z))^k) \quad (i, j = 0, 1, 2) \quad (5.1) \]

are formal Laurent series in \( z - a_j \) over \( \mathbb{K}(x) \). We define

\[ P^{(k)}_{ij}(x) = \text{res}\{F^{(k)}_{ij}(x, z), a_j\} \quad (i, j = 0, 1, 2) \quad (5.2) \]

as the residues at \( z = a_j \). These are the quantities \( p_{ij}(x) \) of [R, p. 465] with \( m = 2 \) and \( r = 1/2 \) (see also the remark at the beginning of the proof of Lemma 4.1, p. 467).

It follows from Lemma 3.4 of [R, p. 466] that the determinant of the \( P^{(k)}_{ij}(x) \) \( (i, j = 0, 1, 2) \) is non-zero for any non-zero \( x \) in \( K \) (note that a product sign in Eq. (3.10) of [R] has been wrongly printed as a summation sign).

We shall now fix \( a_0, a_1, a_2 \) as rational integers, and we also fix \( x \) as \( 1/N \) for a positive rational integer \( N \). So the quantities

\[ p^{(k)}_{ij} = P^{(k)}_{ij}(1/N) \]
are rational numbers with non-zero determinant. We will obtain the estimates necessary for Lemma 3.1 using the inequalities of Section 4, first for non-archimedean $p \neq \infty$ and then for archimedean $p = \infty$.

6. NON-ARCHIMEDEAN ESTIMATES

Here we assume $p \neq \infty$.

**Lemma 6.1.** We have

$$|p^{(k)}| \leq |D|^{-k} \quad (i, j = 0, 1, 2)$$

for $D = 4(a_0 - a_1)^2 (a_1 - a_2)^2 (a_2 - a_0)^2 N$.

**Proof.** By symmetry we may temporarily assume that $|a_0 - a_1| \leq |a_1 - a_2| \leq |a_2 - a_0|$. We use (5.2) and Lemma 4.1 with $|z - a_i| = R$ for some $R < |4| |N + a_i|$. This implies $|\sigma_i(x, z)| = 1$ for $x = 1/N$ in (5.1), because $\sqrt{1 + t}$ converges for $|t| < |4|$ (see for example [DGS, Proposition 7.3(ii, iii), p. 143]). Thus $|1 + xz| = |1 + a_j/N|$ in (5.1). We now treat $j = 0, 1, 2$ in turn.

Consider first $j = 0$. We take $R < |a_0 - a_i|$ as well. Then

$$|z - a_0| = R, \quad |z - a_1| = |a_0 - a_1|, \quad |z - a_2| = |a_2 - a_0|.$$ 

In particular, $|z - a_i| \geq R$ ($i = 0, 1, 2$), and so

$$|p^{(k)}(x, z)| \leq |N|^{-k} |N + a_j|^{k} R^{-k-1} |a_0 - a_i|^{-k} |a_2 - a_0|^{-k}. \quad (6.1)$$

So Lemma 4.1 gives

$$|p^{(k)}| \leq |N|^{-k} |N + a_j|^k R^{-k} |a_0 - a_1|^{-k} |a_2 - a_0|^{-k}.$$ 

We now split cases. If $|4| |N + a_j| \leq |a_0 - a_1|$ we may make $R \to |4| |N + a_j|$ to get the required result. If $|4| |N + a_j| \geq |a_0 - a_1|$, we may make $R \to |a_0 - a_1|$ and use $|N + a_j| \leq 1$ to get the same result.

Consider next $j = 1$. Here we also take $R < |a_0 - a_1|$. Now

$$|z - a_0| = |a_0 - a_1|, \quad |z - a_1| = R, \quad |z - a_2| = |a_1 - a_2|,$$

and we get (6.1) with $a_2 - a_0$ replaced by $a_1 - a_2$, so the same splitting of cases gives the result.

Finally, consider $j = 2$. We take $R < |a_1 - a_2|$. Now

$$|z - a_0| = |a_2 - a_0|, \quad |z - a_1| = |a_1 - a_2|, \quad |z - a_2| = R.$$
7. ARCHIMEDEAN ESTIMATES

Here we assume $p = \infty$. Now it is convenient to order the rational integers $a_0, a_1, a_2$ by

$$a_0 < a_1 < a_2,$$

and also to define

$$M = \max\{|a_0|, |a_1|, |a_2|\}.$$

Finally we assume $N \geq 2M$.

**Lemma 7.1.** We have

$$|p_i^{(k)}| \leq \sqrt{u_1} \cdot (8u_1/A)^k$$

where $u_1 = 1 + 2M/N$ and

$$A = (a_1 - a_0)^2 (2a_2 - 3a_1 + a_0) \quad (a_1 - a_0 \leq a_2 - a_1)$$

$$A = (a_2 - a_1)^2 (3a_1 - 2a_0 - a_2) \quad (a_1 - a_0 \geq a_2 - a_1).$$

**Proof.** Again we use (5.2) and Lemma 4.1, this time with $|z - a_j| = R$ for some $R \leq M$. This implies $|z| \leq 2M$, so $|1 + zx| \leq u_1$. Also,

$$|\sigma_j(x, z)|^2 = |1 + (z - a_j) x/(1 + a_j x)| \leq 1 + (R/N)/(1 - M/N)$$

which does not exceed $1/(1 - M/N) \leq u_1$. These dispose of the factors $U = \sqrt{u_1} \cdot u_i^{(k)}$ in (7.1). For the other factors we have to treat $j = 0, 1, 2$ in turn.

Consider first $j = 0$. We take $R = \frac{1}{4}(a_1 - a_0) \leq M$. Then

$$|z - a_0| = R, \quad |z - a_1| \geq R, \quad |z - a_2| \geq \frac{1}{2}(2a_2 - a_0 - a_1).$$

In particular, $|z - a_i| \geq R$ $(i = 0, 1, 2)$, and so

$$|p_i^{(k)}| \leq U(8/A_0)^k$$

(7.2)
with
\[ A_0 = (a_1 - a_0)^2 (2a_2 - a_0 - a_1). \]

Consider next \( j = 1 \). Unfortunately this needs two subcases, depending on whether \( a_1 \) is nearer \( a_0 \) or \( a_2 \).

If \( j = 1 \) and \( a_1 - a_0 \leq a_2 - a_1 \), we take \( R = \frac{1}{2}(a_1 - a_0) \) as above. Then
\[
|z - a_0| \geq R, \quad |z - a_1| = R, \quad |z - a_2| \geq \frac{1}{2}(2a_2 - 3a_1 + a_0).
\]
Again \( |z - a_i| \geq R (i = 0, 1, 2) \), so we get
\[
|p_{ij}^{(k)}| \leq U(8/A_0)^k \quad (7.3)
\]
with
\[ A_10 = (a_1 - a_0)^2 (2a_2 - 3a_1 + a_0). \]

If \( j = 1 \) and \( a_1 - a_0 \geq a_2 - a_1 \) we take \( R = \frac{1}{2}(a_2 - a_1) \leq M \). Then
\[
|z - a_0| \geq \frac{1}{2}(3a_1 - 2a_0 - a_2), \quad |z - a_1| = R, \quad |z - a_2| \geq R.
\]
Again \( |z - a_i| \geq R (i = 0, 1, 2) \), so we get
\[
|p_{ij}^{(k)}| \leq U(8/A_1)^k \quad (7.4)
\]
for
\[ A_12 = (a_2 - a_1)^2 (3a_1 - 2a_0 - a_2). \]

This completes the case \( j = 1 \).

Finally if \( j = 2 \) we take \( R = \frac{1}{2}(a_2 - a_1) \), so
\[
|z - a_0| \geq \frac{1}{2}(a_1 + a_2 - 2a_0), \quad |z - a_1| \geq R, \quad |z - a_2| = R.
\]
Again \( |z - a_i| \geq R (i = 0, 1, 2) \), so we get
\[
|p_{ij}^{(k)}| \leq U(8/A_2)^k \quad (7.5)
\]
for
\[ A_2 = (a_2 - a_1)^2 (a_1 + a_2 - 2a_0). \]

Collecting up (7.2), (7.3), (7.4), and (7.5), and comparing them with (7.1), we see that it remains only to check
\[
A_{10} \leq \min\{A_0, A_2\} \quad (7.6)
\]
if \(a_1 - a_0 \leq a_2 - a_1\); and

\[
A_{12} \leq \min\{A_0, A_2\} \tag{7.7}
\]

if \(a_1 - a_0 \geq a_2 - a_1\).

For this we go asymmetric. Since everything is a function of the differences between \(a_0, a_1, a_2\) we can assume \(a_0 = 0\). We write \(x = a_1/a_2\), so \(0 < x < 1\), and the two subcases above correspond to \(x \leq 1/2\) and \(x \geq 1/2\). We find

\[
A_0/A = x^2(2 - x), \quad A_2/A = (1 - x)^2(1 + x)
\]

and

\[
A_{10}/A = x^2(2 - 3x), \quad A_{12}/A = (1 - x)^2(3x - 1)
\]

for \(A = a_3^2\). Now (7.6) and (7.7) are straightforward (there is of course symmetry about \(x = 1/2\)). This completes the proof of Lemma 7.1.

Next we write

\[
\theta_j = \sqrt{1 + a_j/N} \quad (j = 0, 1, 2)
\]

for the positive square roots; these exist because of our assumption \(N \geq 2M\).

**Lemma 7.2.** We have

\[
\left| \sum_{j=0}^{2} p^{(k)}_j \theta_j \right| \leq \sqrt{2} \cdot u_2(2u_2^3/N^3)^k \quad (i = 0, 1, 2),
\]

where \(u_2 = N/(N - M)\).

**Proof.** Let \(x\) be any complex number with \(|x| < 1/M\). Then (5.1) and (5.2) give

\[
\sum_{j=0}^{2} P^{(k)}_j(x) \sqrt{1 + a_j x} \sum_{j=0}^{2} \text{res}\{F^{(k)}(x, z), a_j\} \tag{7.8}
\]

with

\[
F^{(k)}(x, z) = (1 + zx)^k \sqrt{1 + z/(z - a_j)(A(z))^k} \quad (i = 0, 1, 2).
\]

By the Residue Theorem this is the integral of \((2\pi i)^{-1} F^{(k)}(x, z)\) around \(|z| = R\) for any \(R\) with \(M < R < 1/|x|\). With \(x = 1/N\) we get the estimate
\[ \sqrt{2} \cdot 2^k R(R-M)^{-3k-1}. \] By making \( R \to N \) we obtain the result of the present lemma.

Underlying this result is of course the fact that the left-hand side of (7.8) has a zero of order at least \( 3k \) at \( x = 0 \) (compare with Lemma 3.1, p. 464 of [R]).

8. PROOF OF PROPOSITION

We take \( a_0 = 0 \) in Sections 6 and 7, so that \( \theta_0 = 1 \). We may assume \( M = \max\{a_1, a_2\} = a_2 \). We will check that the \( p_j^{(3)} \) satisfy the conditions of our Lemma 3.1. Applying Lemma 6.1 with all \( p \neq \infty \), we see that the value
\[ D = 4a_1^2a_2^2(a_2 - a_1)^2 \leq \frac{1}{4} M^6 N \]
is suitable for the denominators. Also by Lemma 7.1 we can take
\[ p = \sqrt{u_1}, \quad P = 8u_1/A \quad (u_1 = 1 + 2M/N), \]
and by Lemma 7.2 also
\[ I = \sqrt{2} \cdot u_2, \quad L = \frac{1}{2} N^3 u_2^3 \quad (u_2 = N(N - M)). \]
We certainly have \( D < L \); in fact, since \( N \geq M^{24} \) we even have
\[ U = L/D \geq 4L/(M^6 N) \geq U_0 \]
for \( U_0 = 2u_2^{3} N^{7/4} \). Because \( N \geq M^{24} \) this means that \( u_2 \) is practically 1 (to 10 significant figures), and so we see that \( U_0 > 1 \) with a lot to spare.

We claim that
\[ V = PD \leq 16u_1 M^3 N \leq V_0 \]
for \( V_0 = 16u_1 N^{3/8} \). The second inequality is clear. To check the first, note that if \( a_1 \leq \frac{1}{2} a_2 \) we have
\[ PD = 32u_1 M^3 N(1 - \alpha)^2/(2 - 3\alpha) \]
for \( 0 < \alpha = a_1/a_2 \leq 1/2 \), and this is indeed at most \( 16u_1 M^3 N \). The calculation for \( a_1 \geq \frac{1}{2} a_2 \) is similar because of symmetry about \( \alpha = \frac{1}{2} \).

Now we compute
\[ U_0^7/V_0^{10} = 2^{-33} u_1^{-10} u_2^{-21} N \geq 2^{-33} u_1^{-10} u_2^{-21} 3^{24} > 1 \]
because \( u_1 \) is also practically 1. It follows that
\[
\hat{\lambda} = \frac{\log V}{\log U} \leq (\log V_0)/(\log U_0) \leq 7/10.
\]
Also \( C = 2^{3/2} u_2 \) so finally
\[
c^{-1} = 6pV C^2 \leq 96u_1^{3/2} C^{7/9} M^3 N < 200M^3 N.
\]
The proposition follows at once.

9. GAP PRINCIPLES

Let \( a \) and \( b \) be positive integers with \( M = \max\{a, b\} \).

**Lemma 9.1.** For any real \( Z \geq 1 \) there are at most eight integral solutions
\((x, y, z)\) of (1.1) with
\[
Z \leq |z| < \sqrt{M \cdot Z}.
\]

**Proof.** Every solution of (1.1) with \( z \neq 0 \) comes in a block of eight, each
block containing exactly one solution with all coordinates positive. So if
the lemma is false, there would be at least 16 solutions, and so we could
find two different solutions \((x, y, z)\) and \((x', y', z')\), each with all coor-
dinates positive, and
\[
Z \leq z, z' < \sqrt{M \cdot Z}.
\]  \hspace{1cm} (9.1)
We must have \( z \neq z' \). We can assume for the moment \( M = b \). Now consider
the determinant \( \Delta \) defined by
\[
\begin{vmatrix}
  y & z \\
  y' & z'
\end{vmatrix} = \begin{vmatrix}
  y - z \sqrt{\bar{b}} & z \\
  y' - z' \sqrt{\bar{b}} & z'
\end{vmatrix}.
\]
We have
\[
0 < y - z \sqrt{\bar{b}} = (y + z \sqrt{\bar{b}})^{-1} < (2z \sqrt{b})^{-1} \leq (2 \sqrt{M \cdot Z})^{-1}, \hspace{1cm} (9.2)
\]
and similarly for \( y' - z' \sqrt{\bar{b}} \). Using these and (9.1) we find that
\[
|\Delta| < 2(2 \sqrt{M \cdot Z})^{-1} \sqrt{M \cdot Z} = 1.
\]
Since \( \Delta \) is a rational integer, it follows that \( \Delta = 0 \). But this is not possible,
because
\[
(y/z)^2 = b + z^{-2} \neq b + z'^{-2} = (y'/z')^2.
\]
Such a contradiction proves the lemma.
This “gap” was comparatively small. To widen it we will now assume that $a$ and $b$ are distinct.

**Lemma 9.2.** For any real $Z \geq 1$ there are at most 16 integral solutions $(x, y, z)$ of (1.1) with

$$Z \leq |z| < \sqrt{M \cdot Z^2}.$$ 

**Proof.** Every solution of (1.1) with $z \neq 0$ comes in a block of 8, each block containing exactly two solutions with all coordinates the same sign. So if the lemma is false, there would be at least 24 solutions, and we could find 6 different solutions each with all coordinates the same sign. Let $(x, y, z), (x', y', z'), (x'', y'', z'')$ be any three of these. Then

$$Z \leq |z|, |z'|, |z''| < \sqrt{M \cdot Z^2}. \quad (9.3)$$

Again assume $M = b$. Applying (9.2) to $(x, y, z)$, we see that $|y - z / \sqrt{b}| < (2 \sqrt{M \cdot Z})^{-1}$, and similarly for $y' - z' / \sqrt{b}, y'' - z'' / \sqrt{b}$. If $a = 1$ the only solutions to (1.1) are $(x, y, z) = (\pm 1, \pm 1, 0)$, so the lemma is trivial. Thus we can assume $a \geq 2$. Now the analogue of (9.2) for $x, z$ gives $|x - z / \sqrt{a}| < (2 \sqrt{Z})^{-1}$ and similarly for $x' - z' / \sqrt{a}, x'' - z'' / \sqrt{a}$. Consider the determinant $A$ defined by

$$\begin{vmatrix} x & y & z \\ x' & y' & z' \\ x'' & y'' & z'' \end{vmatrix} = \begin{vmatrix} x - z / \sqrt{a} & y - z / \sqrt{b} & z \\ x' - z' / \sqrt{a} & y' - z' / \sqrt{b} & z' \\ x'' - z'' / \sqrt{a} & y'' - z'' / \sqrt{b} & z'' \end{vmatrix}.$$ 

Recalling (9.3), we find that the Euclidean lengths of the column vectors are at most

$$\sqrt{3} \cdot (2 \sqrt{Z})^{-1}, \quad \sqrt{3} \cdot (2 \sqrt{M \cdot Z})^{-1}, \quad \sqrt{3} \cdot \sqrt{M \cdot Z^2}$$

respectively. So Hadamard’s inequality gives

$$|A| \leq \sqrt{27} / (4 \sqrt{2}) < 1.$$ 

Therefore $A = 0$, and this means that our three solutions lie in a proper subspace of the real vector space $\mathbb{R}^3$.

So we have shown that any three out of our 6 solutions above lie in a proper subspace. This implies that they all lie in a proper subspace. But now the Bezout Lemma 2.1 gives a contradiction, which establishes the present lemma.
10. PROOF OF THEOREM

We can assume \( a \) and \( b \) are positive, and also that \( M = \max\{a, b\} \geq 3 \). We divide the integral solutions of (1.1) into three classes: the "trivial" ones with \( z = 0 \), the "small" ones with \( 1 \leq |z| < M^{3/2} \), and the "large" ones with \( |z| \geq M^{3/2} \). We shall prove that the respective cardinalities are bounded by 4, 64, and 64, giving 132 in all.

The trivial solutions are indeed trivially counted.

We count the small solutions by means of two applications of Lemma 9.1 with \( Z = 1, \sqrt{M} \), giving at most 16 with \( 1 \leq |z| < M^{3/2} \). Then we apply Lemma 9.2 three times with \( Z = M, M^{3/2}, M^{11/2} \) to give at most 48 with \( M \leq |z| < M^{33/2} \). So there are indeed at most 64 small solutions.

There probably do not exist large solutions. But if there do, let \((x_0, y_0, z_0)\) be one with \( |z_0| \) minimal and all coordinates positive, so that

\[ z_0 \geq M^{31/2}. \tag{10.1} \]

We shall prove that all solutions \((x, y, z)\) of (1.1) satisfy

\[ |z| \leq 200^{10/3} M^{28} |z_0|^{17/3}. \tag{10.2} \]

For this we can assume that \( x, y, z \) are positive. Define

\[ a_2 = a, \quad N = abz_0^2, \quad q = abz_0 z, \quad p_2 = ay_0 y. \]

With \( \theta_2 = \sqrt{1 + a_2/N} \) we find

\[ \theta_2 - p_2/q = (y_0/az_0)(\sqrt{b} - y/z). \]

Using \( y_0^2 \leq 2bz_0^2 \) and (9.2) we find

\[ |\theta_2 - p_2/q| \leq z^{-2}. \]

Similarly, with \( a_1 = b, p_1 = bx_0, x, \) and \( \theta_1 = \sqrt{1 + a_1/N} \) we get

\[ |\theta_1 - p_1/q| \leq z^{-2}. \]

Also,

\[ N = abz_0^2 \geq Mz_0^2 \geq M^{24} \]

by (10.1). So our proposition applies, to give \( z^{-2} \geq (200M^3N)^{-1} q^{-17/10} \). After a short calculation we get (10.2) as desired, using \( ab \leq M^2 \).

Now we can apply Lemma 9.2 four times with \( Z = z_0, \sqrt{M \cdot z_0^2}, M^{3/2}z_0^4, M^{11/2}z_0^8 \) to deduce that there are at most 64 solutions with \( z_0 \leq |z| < M^{31/2}z_0 \). Any solution with \( |z| < z_0 \) is small, by the minimality of \( |z_0| \).
and has therefore already been counted. By (10.2) we now need only to observe that \(200^{10/3}M^{28/3} < M^{15/2} \pi^p\), but this follows from (10.1) with quite a lot to spare. The proof of the theorem is thereby complete.

REFERENCES


