MATHEMATICS OF COMPUTATION
Volume 67, Number 222, April 1998, Pages 833–842
S 0025-5718(98)00918-1

SOLVING CONSTRAINED PELL EQUATIONS

KIRAN S. KEDLAYA

ABSTRACT. Consider the system of Diophantine equations $x^2 - ay^2 = b$, $P(x, y) = z^2$, where P is a given integer polynomial. Historically, such systems have been analyzed by using Baker's method to produce an upper bound on the integer solutions. We present a general elementary approach, based on an idea of Cohn and the theory of the Pell equation, that solves many such systems. We apply the approach to the cases $P(x, y) = cy^2 + d$ and $P(x, y) = cx + d$, which arise when looking for integer points on an elliptic curve with a rational 2-torsion point.

1. INTRODUCTION

In this paper, we describe an elementary method for solving certain systems of Diophantine equations of the form

$$x^2 - ay^2 = b, \qquad P(x, y) = z^2, \tag{1}$$

where a is a positive integer that is not a perfect square, b is a nonzero integer, and $P(x, y)$ is a polynomial with integer coefficients. Such systems arise, in particular, when looking for integer points on elliptic curves with rational 2-torsion (i.e. curves of the form $y^2 = Q(x)$, where Q is a reducible cubic polynomial). These curves appear in various contexts, such as the square pyramid problem of Lucas, and in the study of P_t-sets (see Section 6).

Much of the study of systems of the form (1) has involved using Baker's results on linear forms in logarithms of algebraic numbers [2] to give an upper bound on the size of the solutions. (The finiteness of the number of solutions is guaranteed, in general, by the work of Thue [17] and Siegel [16], but their methods do not yield effectively computable bounds.) Using Baker's bound, plus additional techniques of Diophantine approximation and lengthy computations to close the gap, Baker and Davenport [3] showed that the system $x^2 - 3y^2 = -2, z^2 - 8y^2 = -7$ has no solutions in nonnegative integers other than $(x, y, z) = (1, 1, 1)$ or $(19, 11, 31)$. Grinstead [7] developed a more efficient technique to close the gap; his method was used by Brown [4] to handle the equations $y^2 - 2t^2 = 1, u^2 - 5t^2 = 1$, which have no solution other than $(y, t, u) = (1, 0, 1)$. Pinch [15] applied the same approach to systems of two Pell equations where two unknowns are not equal, but rather differ by a constant.

Received by the editor January 11, 1995 and, in revised form, November 4, 1996.
1991 *Mathematics Subject Classification.* Primary 11Y50; Secondary 11D09, 11D25.
Key words and phrases. Pell equations, integer points on elliptic curves, computer solution of Diophantine equations.
This work was done during a summer internship at the Supercomputing Research Center (now Center for Computing Studies), Bowie, MD, in the summer of 1992.

On the other hand, several authors have given elementary solutions to systems of the form (1), starting with Cohn [6], who considered the case where P is a linear polynomial. Cohn's approach uses congruence arguments to eliminate some cases, and a clever invocation of quadratic reciprocity to handle the remaining cases. (If no solutions exist, congruence arguments usually suffice, but they fail in the presence of a solution.) Using similar techniques together with the theory of the Pell equation, Kangasabapathy and Ponnudurai [10], reestablished the result of Baker and Davenport. The method was adapted by Mohanty and Ramasamy [13] to the equations $x^2 - 5y^2 = -20, z^2 - 2y^2 = 1$, which have only the solution $(x, y, z) = (0, 2, 3)$. (In passing, we note that yet another approach, involving elliptic curves, has been taken by Ono [14].)

We present a systematic yet general procedure, using the methods of Cohn and the theory of the Pell equation, that solves many such systems. (Note that while the aforementioned elementary proofs all treat systems with $b = 1$, this restriction is easily lifted.) In this form, the procedure can be easily automated; in so doing, we have re-established several known results and obtained some new ones. It must be noted, however, that in some cases our procedure fails to solve a system completely; hence we cannot call it an "algorithm" as defined in [8]. Moreover, the procedure is not inherently suitable for proving results about more than one system at a time.

The structure of the paper is as follows. In Section 2, we summarize the relevant properties of the Pell equation. In Section 3, we describe the procedure and prove that its completion, given an initial list of solutions, ensures that no other solutions exist. In Section 4, we modify the procedure to overcome an obstacle arising when P is an even polynomial in both variables (which occurs when solving simultaneous Pell equations). In Section 5, we make explicit the connection between (1) and integer points on elliptic curves. In Section 6, we describe specific results that we have proved using an automated version of the procedure; certification of these results appears in the Appendix.

2. Theory of the Pell equation

We now summarize the properties of the Pell equation

$$x^2 - ay^2 = b,$$

where a is not a perfect square. We first consider the related equation

$$u^2 - av^2 = 1.$$

Proposition 1. *The Pell equation $u^2 - av^2 = 1$, where a is not a perfect square, has infinitely many solutions. Furthermore, all solutions with $u > 0$ are given by*

$$(u_k + v_k\sqrt{a}) = (u_1 + v_1\sqrt{a})^k,$$

where (u_1, v_1) is the smallest solution in positive integers, and k is any integer.

Notice that

$$(u_1 + v_1\sqrt{a})^{-k} = (u_k + v_k\sqrt{a})^{-1} = (u_k - v_k\sqrt{a})$$

so that $u_{-k} = u_k$ and $v_{-k} = -v_k$.

We now return to the original equation.

Proposition 2. *There exists a finite set T of solutions of the equation $x^2 - ay^2 = b$ such that for any solution (x, y),*

$$(x \pm y\sqrt{a}) = (x_0 \pm y_0\sqrt{a})(u \pm v\sqrt{a})$$

for some $(x_0, y_0) \in T$ and some (u, v) with $u^2 - av^2 = 1$.

We call (u_1, v_1) the *fundamental solution*, and the elements of T *base solutions*. (Note that (x_0, y_0) and $(-x_0, y_0)$ are distinct base solutions.) Hua [9, §11.5] gives an algorithm, using continued fractions, for producing the fundamental and base solutions. See [5] for results on the existence and number of base solutions.

Now fix $(x_0, y_0) \in T$, and define $x_n = u_n x_0 + a v_n y_0, y_n = u_n y_0 + v_n x_0$, so that

$$(x_n \pm y_n\sqrt{a}) = (x_0 \pm y_0\sqrt{a})(u_n \pm v_n\sqrt{a}).$$

From the identity

$$(x_{n+r} \pm y_{n+r}\sqrt{a}) = (x_n \pm y_n\sqrt{a})(u_1 \pm v_1\sqrt{a})^r = (x_n \pm y_n\sqrt{a})(u_r \pm v_r\sqrt{a}),$$

we deduce the relations $x_{n+r} = x_n u_r + a y_n v_r$ and $y_{n+r} = y_n u_r + x_n v_r$. Using the fact that $u_{-k} = u_k$ and $v_{-k} = -v_k$, we have the identities

$$\begin{aligned} x_{n+r} + x_{n-r} &= 2x_n u_r, \\ x_{n+r} - x_{n-r} &= 2a y_n v_r, \\ y_{n+r} + y_{n-r} &= 2y_n u_r, \\ y_{n+r} - y_{n-r} &= 2a x_n v_r. \end{aligned}$$

In case $b = 1$ and $(x_0, y_0) = (1, 0)$, we have $(x_n, y_n) = (u_n, v_n)$. Hence the same identities hold with u and v in place of x and y.

Proposition 3. *For all n, k, r, we have $y_{n+2kr} \equiv (-1)^k y_n \pmod{u_r}$ and $y_{n+2kr} \equiv y_n \pmod{v_r}$.*

Proof. The identities above imply that $y_{n+2r} \equiv -y_n \pmod{u_r}$ and $y_{n+2r} \equiv y_n \pmod{v_r}$. Applying these k times gives the desired result. □

Of course, the same result holds for u_n, v_n, or x_n as well.

Proposition 4. *For all k, n, we have $v_n | v_{kn}$; if k is odd, we also have $u_n | u_{kn}$.*

Proof. From the remarks following Proposition 3, we have that

$$u_{n+2\frac{k-1}{2}n} \equiv (-1)^{\frac{k-1}{2}} u_n \equiv 0 \pmod{u_n}.$$

We similarly have that $v_{kn} \equiv v_n$ or $v_0 \pmod{v_n}$, but $v_0 = 0$, so $v_n | v_{kn}$ in either case. □

Proposition 5. *Let $\{t_n\}$ be a sequence satisfying the recurrence relation*

$$t_{n+1} = 2t_n u_1 - t_{n-1}.$$

(In particular, we could have $t_n = u_n$, v_n, x_n or y_n.) Then $\{t_n \pmod m\}$ is completely periodic for any positive integer m.

Proof. Since the number of pairs of residue classes modulo m is finite, there must exist $n, k > 0$ such that $(t_n, t_{n+1}) \equiv (t_{n+k}, t_{n+k+1}) \pmod m$. However, since $t_{n-1} = 2t_n u_1 - t_{n+1}$, we also have $t_{n-1} \equiv t_{n+k-1} \pmod m$, and so on down to $t_0 \equiv t_k \pmod m$. Hence $\{t_n \pmod m\}$ is completely periodic. □

A more precise result, useful in computations, is due to Lehmer [12]; we note here only that for $m = p^k$ where p is an odd prime not dividing a, the period divides $p^{k-1}(p^2 - 1)$.

3. The procedure

We now present our procedure for checking that a given list of solutions to a system of the form (1) is complete. We first describe the calculations, then show how their successful completion implies the completeness of the list, using the propositions of Section 2, some congruence arguments, and quadratic reciprocity.

Let (u_n, v_n) denote the nth solution of the Pell equation $u^2 - av^2 = 1$. For each base solution (x_0, y_0) of the equation $x^2 - ay^2 = b$, let S be the set of integers m such that (x_m, y_m) is in the given list of solutions; we wish to prove that $P(x_m, y_m)$ is a perfect square if and only if $m \in S$.

For each $m \in S$, let $\alpha = P(-x_m, -y_m)$. If $|\alpha|$ is a perfect square, we give up; otherwise, let β be the product of all primes that divide α an odd number of times. Let l be the period of $\{u_n \pmod{\beta}\}$ (guaranteed to exist by Proposition 5). Let r be the largest odd divisor of l, and let q be the largest integer such that $2^q | l$, unless 4 does not divide l, in which case let $q = 2$. Let s be the order of 2 in the group $(\mathbb{Z}/r\mathbb{Z})^\times$.

Define the set

$$U = \left\{ t \in \{0, \dots, r-1\} : \left(\frac{u_{2^q t}}{\beta}\right) = -1 \right\}.$$

If U is empty, we give up; otherwise, find an odd number j such that for each of $k = q, \dots, q+s-1$, there exist $g|j$ and $t \in U$ such that $2^{k-q} g \equiv t \pmod{\beta}$. Let $\gamma_m = 2^q j$.

Let γ be twice the least common multiple of γ_m over all $m \in S$, assuming all of these can be computed without having to give up. Now find an integer δ with the following property: for every $n \in \{0, \dots, \delta\gamma - 1\}$, either $n \equiv m \pmod{2\gamma_m}$ for some $m \in S$; or there exists a prime p such that $\{x_i \pmod p\}$ and $\{y_i \pmod p\}$ have periods dividing $\delta\gamma$, and $P(x_n, y_n)$ is a nonresidue $\pmod p$. (By Propositions 3 and 4, the period condition can be ensured by having $p | v_\eta$ for some η such that $2\eta | \gamma\delta$.)

Theorem 1. *Let notation be as above. If δ can be found satisfying the specified properties, then $P(x_m, y_m)$ is a perfect square if and only if $m \in S$.*

Proof. Suppose $P(x_n, y_n)$ is a perfect square for some $n \notin S$. By the construction of δ, there must exist m such that $n \equiv m \pmod{2\gamma_m}$, or else there would be a prime p such that $P(x_n, y_n)$ is not a quadratic residue mod p. However, $n \neq m$ since $n \notin S$, and so $n = m + 2^{k+1} jh$ for some h, k with h odd and $k \geq q$. Now

$$x_n = x_{m + hj2^{k+1}} = x_{m + 2h(2^k j)} \equiv -x_m \pmod{u_{j2^k}}$$

and similarly $y_n \equiv -y_m \pmod{u_{j2^k}}$. Therefore

$$P(x_n, y_n) \equiv P(-x_m, -y_m) = \alpha \pmod{u_{j2^k}}.$$

The construction ensures that for some $t \in U$ and some $g|j$, $2^{k-q} g \equiv t \pmod{\beta}$. Since $k \geq q \geq 2$ and $\{u_n \pmod 8\}$ has period dividing 4 (easily verified), the Jacobi symbols $\left(\frac{-1}{u_{g2^k}}\right)$ and $\left(\frac{2}{u_{g2^k}}\right)$ both equal 1. Now since $|\alpha|/\beta$ is a perfect square and

$u_{2^k g} | u_{2^k j}$ by Proposition 4, we have by quadratic reciprocity

$$\left(\frac{P(x_n, y_n)}{u_{2^k g}}\right) = \left(\frac{\alpha}{u_{2^k g}}\right) = \left(\frac{\beta}{u_{2^k g}}\right) = \left(\frac{u_{2^k g}}{\beta}\right) = \left(\frac{u_{2^q t}}{\beta}\right) = -1,$$

contradicting the assumption that $P(x_n, y_n)$ is a perfect square. □

Note that after the calculation has been performed, the values of $\alpha, \gamma_m, \delta, p$ can be given as a "certificate" from which the other values can be reconstructed and the calculation easily verified.

4. A variation on the procedure

Notice that the procedure fails if $P(x_m, y_m)$ and $P(-x_m, -y_m)$ are both perfect squares for some m. In particular, if $P(x, y) = Q(x^2, y^2)$ for some polynomial Q (which occurs when solving simultaneous Pell equations, for instance), the procedure will fail if there are any solutions at all.

Fortunately, a simple modification to the procedure skirts this difficulty: take $\alpha = Q(-a^2 y_m^2, -x_m^2)$ instead of $\alpha = P(-x_m, -y_m)$. Now instead of arguing that $x_n \equiv x_m \pmod{u_{j2^k}}$ and similarly for y_n, we put $i = (h-1)/2$, write $n = m + j2^k + 2i \cdot j2^k$ and note that

$$x_n \equiv (-1)^d x_{m+j2^k} \pmod{u_{j2^k}}$$

and similarly for y_n. Now

$$x_n \equiv (-1)^i (x_m u_{j2^k} + a y_m v_{j2^k}) \equiv (-1)^i a y_m v_{j2^k} \pmod{u_{j2^k}}$$

and similarly $y_n \equiv (-1)^h x_m v_{j2^k} \pmod{u_{j2^k}}$. Since $v_{j2^k}^2 \equiv -1 \pmod{u_{j2^k}}$, we discover that

$$\begin{aligned} x_n^2 &\equiv -a^2 y_m^2 \pmod{u_{j2^k}}, \\ y_n^2 &\equiv -x_m^2 \pmod{u_{j2^k}}, \end{aligned}$$

and so

$$P(x_n, y_n) = Q(x_n^2, y_n^2) \equiv Q(-a^2 y_m^2, -x_m^2) = \alpha \pmod{u_{j2^k}}.$$

From this point, the argument proceeds as before.

It should be noted that this modification was used in [13]. Note that the same obstruction remains if $P(x, y) = \pm P(-x, -y)$, but P is not an even polynomial in both variables, e.g. $P(x, y) = xy$ or x^3. However, we expect that other modifications are possible; for one example, see [10].

5. Integer points on elliptic curves

Our principal application of the procedure is the location of integer points on elliptic curves with at least one rational 2-torsion point, i.e. curves of the form

$$y^2 = (ax + b)(cx^2 + dx + e),$$

where a, b, c, d, e are integers. If (x, y) is such a point, then we must have $ax + b = km^2$, $cx^2 + dx + e = kn^2$ for some k, and k must divide the constant

$$a^2(cx^2 + dx + e) - (acx + ad - bc)(ax + b) = a^2 e - abd + b^2 c.$$

Thus the problem reduces to a finite set of systems of the form

$$ax + b = km^2,$$
$$cx^2 + dx + e = kn^2.$$

A linear change of variables turns the second equation into a Pell equation, putting the system in the form (1).

In case the curve factors completely, and hence has the form

$$y^2 = (ax + b)(cx + d)(ex + f),$$

we have an additional recourse if the previous approach fails to yield results. We can write $ax + b = gl^2, cx + d = hm^2, ex + f = kn^2$, where again g, h, k are constrained to divide some constants. By eliminating x using two of the three equations at a time, we can write down three Pell equations, i.e. $(cgl)^2 - (cgah)m^2 = (bc - ad)cg$. Any two of these three equations yield a system whose solutions give integer points of the curve.

Such flexibility makes this case especially convenient. If we treat it as a partially factoring curve, we can write down three factorizations and apply the method to each one in hopes of finding a solution. On the other hand, we can take the second approach and write down systems of two Pell equations. But since each system is actually comprised of three Pell equations, any two of which give the same answers, we have three choices in each of these cases. We can also decide which of the two equations serves as the constraining polynomial. Thus in this case we have many options to try before admitting failure.

6. Applications and results

We now present several problems to which our procedure can be applied. All are variations on the problem of finding integer points on elliptic curves. Certificates for the claimed results appear in the Appendix.

Mordell asked for proof that the only solutions in integers to

$$y^2 = \binom{x}{0} + \binom{x}{1} + \binom{x}{2} + \binom{x}{3}$$

or equivalently

$$6y^2 = (x + 1)(x^2 - x + 6)$$

are $x = -1, 0, 2, 7, 15, 74$. It is easily shown that $x^2 - x + 6 = kz^2$ for $k \in \{1, 2, 3, 6\}$. The case $k = 1$ is trivial, and our procedure completely solves the case $k = 3$. Unfortunately, it cannot complete the other two cases, so a complete elementary proof of the result remains elusive.

Lucas' square pyramid problem is to show that the only solutions in positive integers to the equation

$$6q^2 = r(r + 1)(2r + 1)$$

are $(q, r) = (1, 1), (49, 24)$. By modular considerations, one shows that either r is 6 times a square, or $r + 1$ is twice a square and $2r + 1$ is three times a square. These give rise to the two systems

$$6x^2 - y^2 = -1, \quad z^2 - 2y^2 = -1, \tag{2}$$

$$x^2 - 2y^2 = -1, \quad 3z^2 - 2y^2 = -1. \tag{3}$$

Lucas gave an elementary solution for the first system, but was unable to solve the second. The first elementary solution of the second system was given by Ma [11], with improvements by Anglin [1]. Our method solves the second system (though not the first), thus providing a new elementary solution of Lucas' problem.

Another application of the method arises in the study of P_t-sets. For a nonzero integer t, a *P_t-set* is a set of 3 or more nonzero integers, the product of any two of whose elements, plus t, is a perfect square. The integer $x \notin S$ is said to *extend* the P_t-set S if $S \cup \{x\}$ is also a P_t-set. For example, 120 extends the P_1-set {1, 3, 8}.

Finding integers d that extend a given P_t-set $\{a, b, c\}$ reduces immediately to finding integer points on the elliptic curve $y^2 = (ax + t)(bx + t)(cx + t)$. More precisely, one seeks solutions of the system

$$bx^2 - ay^2 = t(b - a), \quad bz^2 - cy^2 = t(b - c).$$

In this language, Baker and Davenport proved that the P_1-set {1, 3, 8} can be extended only by 120 (the other solution of the system gives 0). Mohanty and Ramasamy proved the P_{-1}-set {1, 5, 10} has no extension (though 1 is a solution), and Brown proved the same for {1, 2, 5}.

Using our procedure, we were quite successful reproducing the known extension results and proving several new ones. The procedure produces an elementary proof (differing slightly from the proof in [10]) of Baker and Davenport's result, it reproduces the result of [13], and it gives an elementary proof of Brown's result (which has also been done by Walsh [18]). It also produced new results about other P_t-sets, summarized in the following table. Each P_t-set is given with the corresponding value of t and a list of all integers that satisfy the ensuing system of Pell equations. These include certain integers that are not considered extensions: 0 when t is a perfect square, or x already in the set such that $x^2 + t$ is a square. (For brevity, a certificate has only been included in the Appendix for the first P_t-set.)

P_t-set	t	Extensions
{1, 3, 120}	1	0, 8, 1680
{1, 8, 120}	1	0, 3, 4095
{1, 8, 15}	1	0, 528
{1, 15, 24}	1	0, 1520
{1, 24, 35}	1	0, 3480
{2, 12, 24}	1	0, 2380
{1, 5, 12}	4	0, 96
{1, 5, 96}	4	0, 12, 672
{1, 18, 29}	7	93
{2, 7, 19}	11	35

P_t-set	t	Extensions
{1, 2, 145}	-1	1
{1, 2, 4901}	-1	1
{1, 5, 65}	-1	1
{1, 5, 20737}	-1	1
{1, 10, 17}	-1	1
{1, 26, 37}	-1	1
{1, 5, 6}	-5	21
{1, 12, 17}	-8	57
{2, 6, 10}	-11	6, 30
{2, 10, 30}	-11	6, 18

Appendix: Certification of results

In this appendix we give the output produced by an implementation of our procedure on the problems described in Section 6; this output can be used to verify that the procedure can be completed in these cases, without repeating all of the calculations. The *Mathematica* code of the author's implementation can be obtained on the WWW at the following location:

`http://www.math.princeton.edu/~kkedlaya.`

The output for each system appears in a separate paragraph, and consists of the following:

- A description of the system being solved.
- The fundamental solution of the Pell equation.
- Each base solution, followed by the values of γ_m and α for each $m \in S$, or the message "No solutions in this family" if S is empty.
- A summary of the distinct values of α and their corresponding values of γ_m.
- A list of the primes p required in the definition of δ.
- A list of all solutions of the system.

We first present the output on the case $x+1 = 2m^2$, $x^2-x+6 = 3n^2$ of Mordell's equation, which has the single solution $x = 7$. Recall that this reduces to a system of type (1) as follows: the discriminant of $x^2 - x + 6 - 3n^2$ is $12n^2 - 23$, so there exists k such that $k^2 - 12n^2 = -23$ and $x = (1 + k)/2$, implying $k + 3 = 4m^2$.

```
Solving n^2 - 12x^2 = -23, n = 4y^2 - 3
Fundamental solution: {7, 2}
Base solution of this family: {5, 2}
No solutions in this family.
Mod 3 (period 3) excludes: {0, 1, 2}
Base solution of this family: {13, 4}
Solution {13, 4, 8} gamma_m 4 alpha -40
Alpha -40 period (1) 12 order 2 gamma_m 4
Mod 7 (period 4) excludes: {3}
Mod 97 (period 8) excludes: {5, 6}
Mod 607 (period 16) excludes: {1, 2, 10}
Mod 708158977 (period 32) excludes: {9, 25}
Possible values of n: {13}
```

Next is the output for Lucas' problem (using the second form of the procedure). Our implementation solves systems of the form $an + b = cx^2$, $dn + e = fy^2$, $gn + h = iz^2$ by rewriting them in the form (1) as follows:

$$afy^2 - cdx^2 = ae - bd,$$
$$aiz^2 - cgx^2 = ah - bg,$$

where x is now the shared variable. As noted earlier, it is sometimes necessary to change the order of the original equations to get a system that can be solved.

```
Solving n + 1 = 2x^2, 2n + 1 = 3y^2, n = z^2
Fundamental solution: {7, 2}
Base solution of this family: {1, 1}
Solution {-1, 1, 1} gamma_m 4 alpha -40
Solution {1, 1, 1} gamma_m 4 alpha -40
Alpha -40 period (1) 12 order 2 gamma_m 4
Mod 5 (period 3) excludes: {1}
Mod 193 (period 12) excludes: {2, 9}
Mod 97 (period 8) excludes: {1, 2, 5, 6}
Possible values of n: {1}
```

Here we give the output of the program on the P_t-sets whose extensions were previously established (the P_1-set $\{1, 3, 8\}$, and the P_{-1}-sets $\{1, 2, 5\}$ and $\{1, 5,$

10}), as well as the set $\{1, 3, 120\}$, which had not been previously investigated. The reduction to (1) proceeds as for Lucas' problem.

```
Solving n + 1 = x^2, 3n + 1 = y^2, 8n + 1 = z^2
Fundamental solution: {2, 1}
Base solution of this family: {1, 1}
Solution {-19, 11, 31} gamma_m 60 alpha -8727
Solution {-1, 1, 1} gamma_m 12 alpha -87
Solution {1, 1, 1} gamma_m 12 alpha -87
Solution {19, 11, 31} gamma_m 60 alpha -8727
Alpha -8727 period (l) 5820 order 48 gamma_m 60
Alpha -87 period (l) 60 order 4 gamma_m 12
Mod 3 (period 6) excludes: {1, 4}
Mod 11 (period 10) excludes: {1, 3, 6, 8}
Mod 29 (period 15) excludes: {5, 9}
Mod 61 (period 60) excludes: {14, 15, 44, 45}
Mod 193 (period 24) excludes: {5, 6, 17, 18}
Mod 37441 (period 40) excludes: {7, 12, 27, 32}
Possible values of n: {0, 120}

Solving 2n - 1 = x^2, 5n - 1 = y^2, n - 1 = z^2
Fundamental solution: {19, 6}
Base solution of this family: {2, 1}
Solution {2, 1, 0} gamma_m 4 alpha -130
Alpha -130 period (l) 60 order 4 gamma_m 4
Mod 19 (period 4) excludes: {1, 3}
Mod 7 (period 8) excludes: {2, 6}
Possible values of n: {1}

Solving 5n - 1 = x^2, 10n - 1 = y^2, n - 1 = z^2
Fundamental solution: {3, 2}
Base solution of this family: {1, 0}
Solution {3, -2, 0} gamma_m 4 alpha -170
Solution {3, 2, 0} gamma_m 4 alpha -170
Alpha -170 period (l) 24 order 2 gamma_m 4
Mod 11 (period 12) excludes: {0, 2, 4, 6, 8, 10}
Possible values of n: {1}

Solving n + 1 = x^2, 3n + 1 = y^2, 120n + 1 = z^2
Fundamental solution: {2, 1}
Base solution of this family: {1, 1}
Solution {-71, 41, 449} gamma_m 420 alpha -1815831
Solution {-5, 3, 31} gamma_m 12 alpha -10071
Solution {-1, 1, 1} gamma_m 12 alpha -1431
Solution {1, 1, 1} gamma_m 12 alpha -1431
Solution {5, 3, 31} gamma_m 12 alpha -10071
Solution {71, 41, 449} gamma_m 420 alpha -1815831
Alpha -1815831 period (l) 11124 order 306 gamma_m 420
Alpha -10071 period (l) 3348 order 90 gamma_m 12
Alpha -1431 period (l) 108 order 18 gamma_m 12
```

```
Mod 11 (period 10) excludes: {2, 7}
Mod 29 (period 15) excludes: {4, 5, 6, 8, 9, 10}
Mod 61 (period 60) excludes: {14, 15, 16, 18, 41, 43, 44, 45}
Mod 71 (period 7) excludes: {2, 4}
Mod 139 (period 70) excludes: {6, 8, 19, 26, 28, 41, 43, 50, 61, 63}
Mod 757 (period 84) excludes: {6, 77}
Mod 2017 (period 21) excludes: {8, 10, 12}
Mod 2521 (period 28) excludes: {7, 20}
Mod 10333 (period 84) excludes: {14, 27, 56, 69}
Mod 193 (period 24) excludes: {2, 4, 5, 6, 7, 9, 14, 16, 17, 18,
                                                        19, 21}
Possible values of n: {0, 8, 1680}
```

Acknowledgments

I would like to thank Dr. M. L. Robinson for numerous helpful conversations and the Supercomputing Research Center for the use of its computer facilities.

References

1. W. Anglin, *The square pyramid puzzle*, American Mathematical Monthly **97** (1990), 120–123. MR **91e:**11026
2. A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika **15** (1968), 204–216. MR **41:**3402
3. 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. MR **40:**1333
4. Ezra Brown, *Sets in which* $xy+k$ *is always a square*, Mathematics of Computation **45** (1985), 613–620. MR **86k:**11019
5. Duncan Buell, *Binary Quadratic Forms: Classic Theory and Modern Computations*, Springer-Verlag, New York, 1989. MR **92b:**11021
6. J. H. E. Cohn, *Lucas and Fibonacci numbers and some diophantine equations*, Proc. Glasgow Math. Assoc. **7** (1965), 24–28. MR **31:**2202
7. C. M. Grinstead, *On a method of solving a class of Diophantine equations*, Mathematics of Computation **32** (1978), 936–940. MR **58:**10724
8. J. E. Hopcroft and J.D. Ullman, *Formal Languages and Their Relation to Automata*, Addison-Wesley, Reading, 1969. MR **38:**5533
9. Loo-Keng Hua, *Introduction to Number Theory*, Springer-Verlag, Berlin, 1982. MR **83f:**10001
10. P. Kangasabapathy and T. Ponnudurai, *The simultaneous Diophantine equations* $y^2 - 3x^2 = -2$ *and* $z^2 - 8x^2 = -7$, Quart. J. Math. Oxford (3) **26** (1975), 275–278. MR **52:**8027
11. De Gang Ma, *An elementary proof of the solution to the Diophantine equation* $6y^2 = x(x+1)(2x+1)$, Sichuan Daxue Xuebao **4** (1985), 107–116. MR **87e:**11039
12. D. McCarthy (ed.), *Selected Papers of D. H. Lehmer*, Charles Babbage Research Centre, Winnipeg, 1981.
13. S. P. Mohanty and A. M. S. Ramasamy, *The simultaneous diophantine equations* $5y^2 - 20 = x^2$ *and* $2y^2 + 1 = z^2$, Journal of Number Theory **18** (1984), 356–359. MR **85h:**11013
14. K. Ono, *Euler's concordant forms*, Acta Arith. **78** (1996), 101–123. CMP 97:05
15. R. G. E. Pinch, *Simultaneous Pellian equations*, Math. Proc. Camb. Phil. Soc. **103** (1988), 35–46. MR **89a:**11029
16. C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. (1929), 1.
17. A. Thue, *Über Annäherungenswerte algebraischen Zahlen*, J. reine angew. Math. **135** (1909), 284–305.
18. P. G. Walsh, *Elementary methods for solving simultaneous Pell equations*, preprint.

Department of Mathematics, Princeton University, Princeton, New Jersey 08544
E-mail address: kkedlaya@math.princeton.edu