PELL'S EQUATION, II

KEITH CONRAD

1. Introduction

In Part I we met Pell's equation $x^2 - dy^2 = 1$ for nonsquare positive integers d. We stated Lagrange's theorem that every Pell equation has a nontrivial solution (an integral solution besides $(\pm 1, 0)$) and saw what all solutions to Pell's equation look like if there's a nontrivial solution. As in Part I, "solution" means integral solution. Here we will prove Lagrange's theorem in Section 2 and show in Section 3 how to find all the solutions of a generalized Pell equation $x^2 - dy^2 = n$. Examples are in Section 4.

2. Pell's Equation has a Nontrivial Solution

Our proof that $x^2 - dy^2 = 1$ has a nontrivial solution will be nonconstructive. The starting point is the following lemma about integral multiples of $\sqrt{d}$ that are close to integers.

Lemma 2.1. *For each nonsquare positive integer d, there are infinitely many positive integers x and y such that $|x - y\sqrt{d}| < 1/y$.*

The point here is not just that there are integral multiples of $\sqrt{d}$ close to integers, but the distance can be controlled by the multiplier on $\sqrt{d}$ (infinitely often).

Proof. We use the pigeonhole principle. For any integer $m \geq 2$ consider the $m+1$ numbers

$$0,\ \sqrt{d},\ 2\sqrt{d},\ \ldots,\ m\sqrt{d}. \tag{2.1}$$

These numbers have fractional parts in $[0, 1)$. View $[0, 1)$ as m half-open intervals $[0, 1/m)$, $[1/m, 2/m)$, $\ldots$, $[(m-1)/m, 1)$. By the pigeonhole principle, two of the $m+1$ numbers in (2.1), say $a\sqrt{d}$ and $b\sqrt{d}$ with $a < b$, have fractional parts in the same interval, so

$$a\sqrt{d} = A + \varepsilon, \quad b\sqrt{d} = B + \delta, \tag{2.2}$$

where $A, B \in \mathbf{Z}$ and ε and δ lie in a common interval $[i/m, (i+1)/m)$. Thus

$$|\varepsilon - \delta| < \frac{1}{m}.$$

This inequality is strict since we are using half-open intervals. Using (2.2),

$$|\varepsilon - \delta| < \frac{1}{m} \Longrightarrow \left|(a\sqrt{d} - A) - (b\sqrt{d} - B)\right| < \frac{1}{m} \Longrightarrow \left|(B - A) - (b - a)\sqrt{d}\right| < \frac{1}{m}.$$

Set $x = B - A$ and $y = b - a$, so x and y are integers with $0 < y \leq m$. Thus

$$|x - y\sqrt{d}| < \frac{1}{m} \leq \frac{1}{y}. \tag{2.3}$$

Since x is within 1 of $y\sqrt{d}$, we have $x > y\sqrt{d} - 1 \geq \sqrt{d} - 1 > 0$, so $x \geq 1$.

Having found a pair of positive integers (x, y) such that $|x - y\sqrt{d}| < 1/y$, to get a second pair with this property choose a positive integer m' such that $1/m' < |x - y\sqrt{d}|$. (There is

such an m' because $x - y\sqrt{d} \neq 0$, as $\sqrt{d}$ is irrational.) Run through the argument above with m' in place of m to find x' and y' in $\mathbf{Z}^+$ satisfying $|x' - y'\sqrt{d}| < 1/m'$ with $y' \leq m'$, so $|x' - y'\sqrt{d}| < 1/y'$. From the inequalities

$$|x' - y'\sqrt{d}| < \frac{1}{m'} < |x - y\sqrt{d}|, \tag{2.4}$$

the pair (x, y) is obviously not the same as the pair (x', y'). By repeating this argument again to get a smaller $|x'' - y''\sqrt{d}|$, and so on, we are done. □

Example 2.2. Let $d = 7$. We will give two solutions to $|x - y\sqrt{7}| < 1/y$. Taking $m = 10$, among the fractional parts of $k\sqrt{7}$ for $0 \leq k \leq 10$ (given to two decimal places in the table below) there are three pairs of integers (a, b) where $a\sqrt{7}$ and $b\sqrt{7}$ have the same first decimal digit and thus differ by less than $1/10$: $(a, b) = (2, 5)$, $(4, 7)$, and $(6, 9)$.

k	0	1	2	3	4	5	6	7	8	9	10
Fractional part of $k\sqrt{7}$	0	.64	.29	.93	.58	.22	.87	.52	.16	.81	.45

Using $a = 2$ and $b = 5$, we have

$$2\sqrt{7} = 5.29\ldots, 5\sqrt{7} = 13.22\cdots \Longrightarrow |(2\sqrt{7} - 5) - (5\sqrt{7} - 13)| < \frac{1}{10} \Longrightarrow |8 - 3\sqrt{7}| < \frac{1}{10} < \frac{1}{3}$$

so we can use $(x, y) = (8, 3)$. The other two choices for (a, b) lead to the same values for x and y.

To get a second pair of integers (x', y') such that $|x' - y'\sqrt{7}| < 1/y'$, since $|8 - 3\sqrt{7}| \approx .0627 > 1/20$, we look at the fractional parts of $k\sqrt{7}$ for $0 \leq k \leq 20$ and seek two fractional parts in some interval $[i/20, (i + 1)/20)$. This happens when k is 1 and 15:

$$\sqrt{7} = 2.645\ldots, \quad 15\sqrt{7} = 39.686\ldots,$$

so

$$|(\sqrt{7} - 2) - (15\sqrt{7} - 39)| \approx .04 < \frac{1}{20} \Longrightarrow |37 - 14\sqrt{7}| < \frac{1}{20} < \frac{1}{14}$$

and we can use $(x', y') = (37, 14)$.

The only properties we needed of $\sqrt{d}$ in Lemma 2.1 are that it is irrational and greater than 1. A similar argument shows that for any real irrational α, the inequality $|x - y\alpha| < 1/y$ holds for infinitely many pairs of integers (x, y) with $y > 0$ (we have to give up on insisting that $x > 0$ too if α is negative).

Theorem 2.3 (Lagrange)**.** *For every positive integer d that is not a square, the equation $x^2 - dy^2 = 1$ has a nontrivial solution.*

Proof. We will start by showing there's some nonzero integer M such that the equation $x^2 - dy^2 = M$ is satisfied for infinitely many x and y in $\mathbf{Z}^+$. Then we'll combine this with modular arithmetic to show $x^2 - dy^2 = 1$ has a positive solution.

From Lemma 2.1, $|x - y\sqrt{d}| < 1/y$ for infinitely many x and y in $\mathbf{Z}^+$. For such x and y we will show

$$|x^2 - dy^2| < 1 + 2\sqrt{d},$$

where the main point is that this upper bound does not involve x or y.

First we will bound x from above in terms of y:

$$x = x - y\sqrt{d} + y\sqrt{d} \leq |x - y\sqrt{d}| + y\sqrt{d} < \frac{1}{y} + y\sqrt{d} \leq 1 + y\sqrt{d}.$$

Then

$$|x^2 - dy^2| = (x + y\sqrt{d})|x - y\sqrt{d}| < (1 + y\sqrt{d} + y\sqrt{d})\frac{1}{y} = \frac{1}{y} + 2\sqrt{d} \leq 1 + 2\sqrt{d}.$$

Thus $|x^2 - dy^2| < 1 + 2\sqrt{d}$ for infinitely many pairs of positive integers (x, y). By the pigeonhole principle, there is an $M \in \mathbf{Z}$ with $|M| < 1 + 2\sqrt{d}$ such that

$$x^2 - dy^2 = M \tag{2.5}$$

for infinitely many pairs of positive integers (x, y), and $M \neq 0$ since $\sqrt{d}$ is irrational.

For positive integers x and y satisfying (2.5), reduce x and y modulo $|M|$. The infinitely many pairs (x mod $|M|, y$ mod $|M|$) must have a repetition infinitely often, since there are only finitely many pairs of integers mod M. So there are positive integral solutions (x_1, y_1) and (x_2, y_2) to (2.5) such that $x_1 \equiv x_2 \bmod |M|$, $y_1 \equiv y_2 \bmod |M|$, and $(x_1, y_1) \neq (x_2, y_2)$.

Write $x_1 = x_2 + Mk$ and $y_1 = y_2 + M\ell$, where k and ℓ are in $\mathbf{Z}$. Then

$$\begin{aligned} x_1 + y_1\sqrt{d} &= x_2 + y_2\sqrt{d} + M(k + \ell\sqrt{d}), \\ x_1 - y_1\sqrt{d} &= x_2 - y_2\sqrt{d} + M(k - \ell\sqrt{d}). \end{aligned}$$

Since $M = x_2^2 - dy_2^2 = (x_2 + y_2\sqrt{d})(x_2 - y_2\sqrt{d})$, substituting this into the two equations above gives

$$x_1 + y_1\sqrt{d} = (x_2 + y_2\sqrt{d})(1 + (x_2 - y_2\sqrt{d})(k + \ell\sqrt{d})) \tag{2.6}$$

$$x_1 - y_1\sqrt{d} = (x_2 - y_2\sqrt{d})(1 + (x_2 + y_2\sqrt{d})(k - \ell\sqrt{d})). \tag{2.7}$$

Combine like terms in the second factor on the right side of (2.6) to write it as $x + y\sqrt{d}$ with $x, y \in \mathbf{Z}$. The second factor on the right side of (2.7) is $x - y\sqrt{d}$, so we have

$$\begin{aligned} x_1 + y_1\sqrt{d} &= (x_2 + y_2\sqrt{d})(x + y\sqrt{d}) \\ x_1 - y_1\sqrt{d} &= (x_2 - y_2\sqrt{d})(x - y\sqrt{d}). \end{aligned}$$

Multiplying these last two equations together, we get $M = M(x^2 - dy^2)$. Thus $x^2 - dy^2 = 1$. To show $(x, y) \neq (\pm 1, 0)$, assume otherwise. If $(x, y) = (1, 0)$ then $x_1 = x_2$ and $y_1 = y_2$, but this contradicts the fact that the pairs (x_1, x_2) and (x_2, y_2) are different. If $(x, y) = (-1, 0)$ then $x_1 = -x_2$, but this contradicts the fact that x_1 and x_2 are positive. □

3. Solving the Generalized Pell Equation

We saw in the previous section that Pell's equation has a nontrivial solution. Using a nontrivial solution of Pell's equation we will describe a method to write down all the solutions of a generalized Pell equation $x^2 - dy^2 = n$, where n is any nonzero integer. In particular, if such an equation has no solutions then the method will tell us that.

The key algebraic idea is that solutions to $x^2 - dy^2 = n$ remain solutions when multiplied by solutions of $x^2 - dy^2 = 1$: if $a^2 - db^2 = 1$ and $x^2 - dy^2 = n$ then the coefficients of the product $x' + y'\sqrt{d} := (a + b\sqrt{d})(x + y\sqrt{d})$ satisfy $x'^2 - dy'^2 = n$, which you can check.

Example 3.1. A solution of $x^2 - 7y^2 = 29$ is $(6, 1)$ and a solution of $x^2 - 7y^2 = 1$ is $(8, 3)$. From

$$(6 + \sqrt{7})(8 + 3\sqrt{7}) = 69 + 26\sqrt{7},$$

another solution of $x^2 - 7y^2 = 29$ is $(69, 26)$.

In words, we have shown a *Pell multiple* of a solution of $x^2 - dy^2 = n$ is again a solution, where "solution" means either the pair (x, y) or the number $x + y\sqrt{d}$ and "Pell multiple" means either the coefficients $(ax + dby, ay + bx)$ of the number $(a + b\sqrt{d})(x + y\sqrt{d})$ where $a^2 - db^2 = 1$ or the number itself. The special case $n = 1$ is a result we saw in Part I: the product of two Pell solutions is again a Pell solution (for the same d, of course).

Being a Pell multiple is a symmetric relation: if $x' + y'\sqrt{d} = (x + y\sqrt{d})(a + b\sqrt{d})$ where $a^2 - db^2 = 1$ then $x + y\sqrt{d} = (x' + y'\sqrt{d})(a - b\sqrt{d})$ and $a^2 - d(-b)^2 = 1$. To check if two numbers $x + y\sqrt{d}$ and $x' + y'\sqrt{d}$ are Pell multiples, form their ratio and rationalize the denominator to check the coefficients are integers that satisfy Pell's equation. For example, $1 + \sqrt{3}$ is a Pell multiple of $1 - \sqrt{3}$ since their ratio is $-2 - \sqrt{3}$, which is a solution of $x^2 - 3y^2 = 1$, while $4 + \sqrt{3}$ and $4 - \sqrt{3}$ are not Pell multiples since their ratio $(19 + 8\sqrt{3})/13$ does not even have integer coefficients.

Our goal is to show there is a finite list of solutions to $x^2 - dy^2 = n$ such that every other solution is a Pell multiple of one of them. That is, up to allowing multiplication by Pell solutions to generate new solutions there are only finitely many essentially different solutions of a generalized Pell equation.

Example 3.2. We'll see later that every solution of $x^2 - 6y^2 = 3$ is $\pm(3 + \sqrt{6})(5 + 2\sqrt{7})^k$ for some $k \in \mathbf{Z}$, where $5^2 - 7 \cdot 2^2 = 1$, so each solution is a Pell multiple of $3 + \sqrt{6}$ or $-3 - \sqrt{6}$.

Theorem 3.3. *Fix $u = a + b\sqrt{d}$ where $a^2 - db^2 = 1$ with $a > 0$ and $b > 0$. For each $n \in \mathbf{Z} - \{0\}$, every solution of $x^2 - dy^2 = n$ is a Pell multiple of a solution (x, y) where $|x| \leq \sqrt{|n|u}$ and $|y| \leq \sqrt{|n|u}/\sqrt{d}$.*

Proof. We will use absolute values and logarithms. For $(x, y) \in \mathbf{Z}^2 - \{(0, 0)\}$ define

$$L(x + y\sqrt{d}) = (\log|x + y\sqrt{d}|, \log|x - y\sqrt{d}|) \in \mathbf{R}^2.$$

The crucial algebraic property is $L(\alpha\beta) = L(\alpha) + L(\beta)$ for all α and β. Check this. In particular, $L(\alpha^k) = kL(\alpha)$ for $k \in \mathbf{Z}$.

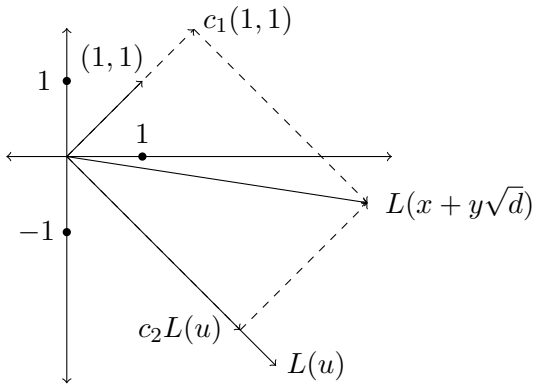
Since $a^2 - db^2 = 1$ we have $1/u = a - b\sqrt{d}$, so $a - b\sqrt{d} > 0$ and therefore

$$L(u) = (\log u, \log(1/u)) = (\log u, -\log u) = (\log u)(1, -1).$$

This vector is linearly independent of $(1, 1)$, so $\{(1, 1), L(u)\}$ is a basis of $\mathbf{R}^2$. Therefore when $x^2 - dy^2 = n$ we have

$$L(x + y\sqrt{d}) = c_1(1, 1) + c_2 L(u) \tag{3.1}$$

for some real numbers c_1 and c_2. See the figure below.



Writing out the coordinates on both sides of (3.1),

$$(\log|x+y\sqrt{d}|, \log|x-y\sqrt{d}|) = (c_1 + c_2\log u, c_1 - c_2\log u).$$

Adding the coordinates we can solve for c_1:

$$c_1 = \frac{\log|x+y\sqrt{d}| + \log|x-y\sqrt{d}|}{2} = \frac{\log|(x+y\sqrt{d})(x-y\sqrt{d})|}{2} = \frac{\log|n|}{2}.$$

Thus when $x^2 - dy^2 = n$,

$$L(x+y\sqrt{d}) = \frac{\log|n|}{2}(1,1) + c_2L(u). \tag{3.2}$$

Let k be the closest integer to c_2, so the difference $\delta = c_2 - k$ satisfies $|\delta| \le \frac{1}{2}$. Then (3.2) becomes

$$\begin{aligned} L(x+y\sqrt{d}) &= \frac{\log|n|}{2}(1,1) + (k+\delta)L(u) \\ &= \frac{\log|n|}{2}(1,1) + kL(u) + \delta L(u). \end{aligned}$$

Since $kL(u) = L(u^k)$, we have

$$L((x+y\sqrt{d})u^{-k}) = L(x+y\sqrt{d}) - kL(u) = \frac{\log|n|}{2}(1,1) + \delta L(u).$$

Set $x' + y'\sqrt{d} = (x+y\sqrt{d})u^{-k} = (x+y\sqrt{d})(a-b\sqrt{d})^k$. Then (x',y') is a Pell multiple of (x,y) and the bound $|\delta| \le \frac{1}{2}$ gives us bounds on the coordinates of $L(x'+y'\sqrt{d})$:

$$\log|x'+y'\sqrt{d}| = \frac{\log|n|}{2} + \delta\log u \le \frac{\log|n|}{2} + \frac{1}{2}\log u \Longrightarrow |x'+y'\sqrt{d}| \le \sqrt{|n|u}$$

and

$$\log|x'-y'\sqrt{d}| = \frac{\log|n|}{2} - \delta\log u \le \frac{\log|n|}{2} + \frac{1}{2}\log u \Longrightarrow |x'-y'\sqrt{d}| \le \sqrt{|n|u}.$$

Thus

$$|x'| = \left|\frac{(x'+y'\sqrt{d}) + (x'-y'\sqrt{d})}{2}\right| \le \sqrt{|n|u}$$

and

$$|y'| = \left|\frac{(x'+y'\sqrt{d}) - (x'-y'\sqrt{d})}{2\sqrt{d}}\right| \le \frac{\sqrt{|n|u}}{\sqrt{d}}.$$

Since $(x+y\sqrt{d})u^{-k} = x'+y'\sqrt{d}$ we can write $x+y\sqrt{d} = (x'+y'\sqrt{d})u^k$, so every solution of $x^2-dy^2 = n$ is a Pell multiple of a solution having the bounds indicated in the theorem. □

Corollary 3.4. *For any generalized Pell equation $x^2 - dy^2 = n$ with $n \neq 0$ there is a finite set of solutions such that every solution is a Pell multiple of one of these solutions.*

Proof. We will give two proofs.

First proof: Theorem 3.3 tells us every solution is a Pell multiple of a solution with $|x| \leq \sqrt{|n|u}$ and $|y| \leq \sqrt{|n|u}/\sqrt{d}$. There are only finitely many such x and y.

Second proof: At the end of the proof of Theorem 2.3 we showed that if $x_1^2 - dy_1^2 = M$ and $x_2^2 - dy_2^2 = M$ with $x_1 \equiv x_2 \bmod M$ and $y_1 \equiv y_2 \bmod M$ then we can write $x_2+y_2\sqrt{d} = (x_1+y_1\sqrt{d})(x+y\sqrt{d})$ where $x^2-dy^2 = 1$. Thus $x_1+y_1\sqrt{d}$ and $x_2+y_2\sqrt{d}$ are Pell multiples. Replacing M with n, any two solutions of $x^2 - dy^2 = n$ having the same reduction mod n are Pell multiples of each other, so there are at most n^2 different solutions of $x^2 - dy^2 = n$ up to Pell multiples since there are at most n^2 pairs of integers mod n. □

The second proof of Corollary 3.4 is not as practical as the first because it is not computationally effective. It doesn't give a bounded range of x and y values to seek solutions of $x^2 - dy^2 = n$ up to Pell multiples. In particular, the second proof can't be used to show such an equation has no solutions while the first proof can, as we'll see in an Example 4.4.

4. Examples of Theorem 3.3

We now apply Theorem 3.3 in several examples to see how it works in practice. Since the upper bound on $|y|$ in the theorem is smaller than the upper bound on $|x|$, we will run through the possible values of y fitting its bound and see when there are corresponding x for which $x^2 - dy^2 = n$ instead of the other way around.

Example 4.1. We will describe all the solutions of $x^2 - 6y^2 = 3$ in integers. An obvious solution is $(3, 1)$ and we'll show every solution is a Pell multiple of $(3, 1)$ or $(-3, -1)$.

For a positive solution of $a^2 - 6b^2 = 1$ we take $(a, b) = (5, 2)$, so set $u = 5 + 2\sqrt{6}$. From Theorem 3.3, the bound $|y| \leq \sqrt{|n|u}/\sqrt{d} = \sqrt{3u}/\sqrt{6} \approx 1.25$ forces y to be $1, 0$, or -1. Solutions to $x^2 - 6y^2 = 3$ with such y-values are $(\pm 3, 1)$ and $(\pm 3, -1)$. Therefore Theorem 3.3 tells us that every solution of $x^2 - 6y^2 = 3$ in integers has the form

$$x + y\sqrt{6} = (\pm 3 + \sqrt{6})(5 + 2\sqrt{6})^k \quad \text{or} \quad (\pm 3 - \sqrt{6})(5 + 2\sqrt{6})^k$$

where $k \in \mathbf{Z}$. Up to a Pell multiple there are four possible solutions:

$$3 + \sqrt{6}, \quad -3 + \sqrt{6}, \quad 3 - \sqrt{6}, \quad -3 - \sqrt{6}.$$

The solutions $3 + \sqrt{6}$ and $3 - \sqrt{6}$ are Pell multiples: $3 + \sqrt{6} = (3 - \sqrt{6})u$. Likewise $-3 - \sqrt{6} = (-3 + \sqrt{6})u$. Therefore every solution of $x^2 - 6y^2 = 3$ in integers is a Pell multiple of $\pm(3 + \sqrt{6})$. Thus every solution has the form $\pm(3 + \sqrt{6})(5 + 2\sqrt{6})^k$ with $k \in \mathbf{Z}$ and we can't simplify this further since $\pm(3 + \sqrt{6})$ are not Pell multiples of each other.

Taking $k = 0, 1, 2$, the values of $(3+\sqrt{6})(5+2\sqrt{6})^k$ are $3+\sqrt{6}$, $27+11\sqrt{6}$, and $267+109\sqrt{6}$, so the first three solutions of $x^2 - 6y^2 = 3$ in positive integers are $(3, 1)$, $(27, 11)$, and $(267, 109)$.

Example 4.2. We will completely solve $x^2 - 7y^2 = 57$ in integers.

One nontrivial solution of $a^2 - 7b^2 = 1$ is $(8, 3)$, so set $u = 8 + 3\sqrt{7}$. The y-bound in Theorem 3.3 is $|y| \leq \sqrt{57u}/\sqrt{7} \approx 11.39$. The solutions to $x^2 - 7y^2 = 57$ for such y are $(x, y) = (\pm 8, \pm 1)$, $(\pm 13, \pm 4)$, and $(\pm 20, \pm 7)$.

Every solution of $x^2 - 7y^2 = 57$ is therefore one of

$$\pm(8 \pm \sqrt{7})u^k, \quad \pm(13 \pm 4\sqrt{7})u^k, \quad \text{or} \quad \pm(20 \pm 7\sqrt{7})u^k$$

with $k \in \mathbf{Z}$, but this list has redundancies. Since $20 + 7\sqrt{7} = (13 - 4\sqrt{7})u$ and $20 - 7\sqrt{7} = (13 + 4\sqrt{7})/u$, we can drop the third set of solutions since it is part of the second set of solutions.

Example 4.3. We will completely solve $x^2 - 19y^2 = 36$ in integers. Obvious solutions are $(\pm 6, 0)$, and thus also Pell multiples of these, but there are further solutions.

A nontrivial solution of $a^2 - 19b^2 = 1$ is $(170, 39)$ (this is the solution with the smallest positive b), so we let $u = 170 + 39\sqrt{19}$. Solutions to $x^2 - 19y^2 = 36$ when $|y| \leq \sqrt{36u}/\sqrt{19} \approx 25.3$ are $(x, y) = (\pm 6, 0)$, $(\pm 44, \pm 10)$, and $(\pm 70, \pm 16)$. The third solution pair is a Pell multiple of the second solution pair since $70 + 16\sqrt{19} = (44 - 10\sqrt{19})u$ and $70 - 16\sqrt{19} = (44 + 10\sqrt{17})/u$. Therefore every solution to $x^2 - 19y^2 = 36$ has the form

$$\pm 6u^k \quad \text{or} \quad \pm(44 \pm 10\sqrt{7})u^k$$

with $k \in \mathbf{Z}$.

Example 4.4. We will completely solve $x^2 - 37y^2 = 11$ in integers.

A solution of $a^2 - 37b^2 = 1$ is $(73, 12)$. Using $u = 73 + 12\sqrt{37}$, the y-bound in Theorem 3.3 is $|y| \leq \sqrt{11u}/\sqrt{37} \approx 6.58$. For no y in this range does $x^2 - 37y^2 = 11$ for an $x \in \mathbf{Z}$, so the equation $x^2 - 37y^2 = 11$ has no solutions.

Although Theorem 3.3 provides a general method to show $x^2 - dy^2 = n$ has no solutions, the lack of solutions can often be proved more simply using congruences, as we saw in Part I. For instance, $x^2 - 5y^2 = 2$ has no solution since $x^2 \equiv 2 \bmod 5$ has no solution. But congruence methods do not always suffice to prove there are no solutions! The equation $x^2 - 37y^2 = 11$ is an example. We saw it has no solutions in $\mathbf{Z}$ in Example 4.4, but it does have rational solutions such as $(9/2, 1/2)$ and $(24/7, 1/7)$, and using these rational solutions it can be shown that for every $m \geq 2$ the congruence $x^2 - 37y^2 \equiv 11 \bmod m$ is solvable.

5. Using Continued Fractions

In this final section we will explain how Pell equations and generalized Pell equations can be solved using continued fractions. We will assume the reader is already familiar with the basic theory of continued fractions.

The connection between continued fractions and generalized Pell equations comes from the following theorem.

Theorem 5.1. *If positive integers x and y satisfy $x^2 - dy^2 = n$ with $|n| < \sqrt{d}$ then x/y is a convergent to the continued fraction of $\sqrt{d}$.*

Proof. Our argument is taken from [1, p. 204]. A basic theorem about continued fractions is that for a real number α, if x and y are integers with $y \neq 0$ and $|x/y - \alpha| < 1/(2y^2)$ then $x/y = p/q$ for some convergent p/q to α. (We can't say $x = p$ and $y = q$ unless we know $\gcd(x, y) = 1$ and $y > 0$, and we're not assured $\gcd(x, y) = 1$ in general unless n is squarefree.) Taking $\alpha = \sqrt{d}$, if $x^2 - dy^2 = n$ with $|n| < \sqrt{d}$ and $x, y > 0$ then

$$\left|\frac{x}{y} - \sqrt{d}\right| = \frac{|n|}{y^2(x/y + \sqrt{d})} < \frac{\sqrt{d}}{y^2(x/y + \sqrt{d})} = \frac{1}{y^2(x/(y\sqrt{d}) + 1)},$$

so to show $|x/y - \sqrt{d}| < 1/(2y^2)$, and hence x/y is a convergent to $\sqrt{d}$, it suffices to prove $x/(y\sqrt{d}) > 1$, or equivalently $x > y\sqrt{d}$. If $n > 0$ then $x^2 - dy^2 = n > 0 \Longrightarrow x^2 > dy^2$, so $x > y\sqrt{d}$ since x and y are positive.

If $n < 0$ then $x^2 - dy^2 < 0 \Longrightarrow x < y\sqrt{d}$ and our argument breaks down. Instead of looking at x/y as an approximation to $\sqrt{d}$, look at y/x as an approximation to $1/\sqrt{d}$:

$$\left|\frac{y}{x} - \frac{1}{\sqrt{d}}\right| = \frac{|n|}{\sqrt{d}x(y\sqrt{d} + x)} = \frac{|n|}{dx^2(y/x + 1/\sqrt{d})} < \frac{1}{x^2(\sqrt{d}y/x + 1)}.$$

This is less than $1/(2x^2)$ if $\sqrt{d}y/x > 1$, or equivalently $x < y\sqrt{d}$, which is true, so y/x is a convergent to $1/\sqrt{d}$. If $\sqrt{d} = [a_1, a_2, a_3, \dots]$ then $a_1 \geq 1$ so $1/\sqrt{d} = [0, a_1, a_2, \dots]$,[1] which means the convergents to $\sqrt{d}$ are the reciprocals of the convergents to $1/\sqrt{d}$ after the initial convergent 0. Thus y/x being a convergent to $1/\sqrt{d}$ makes x/y a convergent to $\sqrt{d}$. □

Corollary 5.2. *For any positive solution to $x^2 - dy^2 = \pm 1$, there is a convergent p/q to $\sqrt{d}$ such that $x = p$ and $y = q$.*

Proof. Apply Theorem 5.1 with $n = \pm 1$. In this case $\gcd(x, y) = 1$ and $y > 0$, so x and y are the numerator and denominator of a convergent to $\sqrt{d}$. □

This corollary was the basis for Lagrange's proof that Pell's equation $x^2 - dy^2 = 1$ has a nontrivial solution. He proved $\sqrt{d}$ has a periodic continued fraction and explained where to find the positive solutions of $x^2 - dy^2 = 1$ among the convergents to $\sqrt{d}$.

Example 5.3. The continued fraction of $\sqrt{6}$ is $[2, \overline{2, 4}]$, and the table of convergents below suggests (and it is true) that every other convergent provides a solution to $x^2 - 6y^2 = 1$.

		2	2	4	2	4	2	4	2	4	2	4
0	1	2	5	22	49	218	485	2158	4801	21362	47525	211462
1	0	1	2	9	20	89	198	881	1960	8721	19402	86329
$x^2 - 6y^2$		-2	1	-2	1	-2	1	-2	1	-2	1	-2

Not only is the continued fraction of $\sqrt{d}$ periodic, but also $x^2 - dy^2$ when x/y runs through the convergents to $\sqrt{d}$ is periodic. All possible values of $x^2 - dy^2$ when x/y is a convergent to $\sqrt{d}$ occur before the last term in the second period of the continued fraction. This and Theorem 5.1 let us determine all nonzero n with $|n| < \sqrt{d}$ for which $x^2 - dy^2 = n$ has a solution. For instance, $\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$ so we compute $x^2 - 13y^2$ in the table below where x/y runs through convergents just before the second 6.

		3	1	1	1	1	6	1	1	1	1
0	1	3	4	7	11	18	119	137	256	393	649
1	0	1	1	2	3	5	33	38	71	109	180
$x^2 - 13y^2$		-4	3	-3	4	-1	4	-3	3	-4	1

Since $\sqrt{13} \approx 3.6$, the only n with $|n| < \sqrt{13}$ for which $x^2 - 13y^2 = n$ is solvable in $\mathbf{Z}$ are ± 1 and ± 3.

[1] A continued fraction with $a_1 < 0$ has a much more complicated continued fraction for its reciprocal than when $a_1 \geq 0$.

If $|n| > \sqrt{d}$ then solvability of $x^2 - dy^2 = n$ can be connected to solvability of $x^2 - dy^2 = n'$ for some nonzero integer n' where $|n'| < |n|$. Iterating this, eventually the case $|n| < \sqrt{d}$ is reached and we already explained how that can be settled using the continued fraction of $\sqrt{d}$. This reduction process is discussed in general in [1, pp. 210–213], and we now illustrate it with examples that were treated earlier by other methods.

Example 5.4. Consider $x^2 - 6y^2 = 3$ with $x, y \in \mathbf{Z}$. Note $3 > \sqrt{6}$. Reducing the equation mod 3, we get $x^2 \equiv 0 \bmod 3$, so $x \equiv 0 \bmod 3$. This is equivalent to $x = 3z$ for $z \in \mathbf{Z}$, so

$$\begin{aligned} x^2 - 6y^2 = 3 &\iff 9z^2 - 6y^2 = 3 \\ &\iff 3z^2 - 2y^2 = 1 \\ &\iff -2y^2 + (3z^2 - 1) = 0. \end{aligned}$$

Viewing the left side of the last equation as a quadratic polynomial in the integer y, its discriminant

$$0^2 - 4 \cdot (-2) \cdot (3z^2 - 1) = 4(6z^2 - 2)$$

has to be a perfect square, so $6z^2 - 2 = t^2$ for some $t \in \mathbf{Z}$, or equivalently $t^2 - 6z^2 = -2$. From this equation t is even. Conversely, if t and z are integers fitting that last equation then $x = 3z$ and $y = \pm\sqrt{4t^2}/(2(-2)) = \pm t/2$ are integers that satisfy $x^2 - 6y^2 = 3$.

Solving $x^2 - 6y^2 = 3$ is thus equivalent to solving $t^2 - 6z^2 = -2$. Since $|-2| < \sqrt{6}$, the ratio t/z (taking $t, z > 0$) must be a convergent to $\sqrt{6}$. From the table in Example 5.3 the first three positive solutions of $t^2 - 6z^2 = -2$ are $(t, z) = (2, 1)$, $(22, 9)$, and $(218, 89)$, leading to $(x, y) = (3z, t/2) = (3, 1)$, $(27, 11)$, and $(267, 109)$.

Example 5.5. If $x^2 - 37y^2 = 11$ for some $x, y \in \mathbf{Z}$ then $x^2 \equiv 37y^2 \equiv (2y)^2 \bmod 11$, so $x \equiv \pm 2y \bmod 11$. Write $x = \pm 2y + 11z$ with $z \in \mathbf{Z}$. Then

$$\begin{aligned} x^2 - 37y^2 = 11 &\iff (\pm 2y + 11z)^2 - 37y^2 = 11 \\ &\iff -33y^2 \pm 44yz + (121z^2 - 11) = 0 \\ &\iff -3y^2 \pm 4yz + (11z^2 - 1) = 0. \end{aligned}$$

For the quadratic polynomial in y to be solvable in $\mathbf{Z}$, its discriminant

$$(4z)^2 - 4 \cdot (-3) \cdot (11z^2 - 1) = 4(37z^2 - 3)$$

must be a perfect square, so $37z^2 - 3 = t^2$ for some $t \in \mathbf{Z}$, or equivalently $t^2 - 37z^2 = -3$. All our steps are reversible, so if $t^2 - 37z^2 = -3$ and y is a root of $-3y^2 \pm 4yz + (11z^2 - 1) = 0$ in $\mathbf{Z}$ then $(x, y) = (\pm 2y + 11z, y)$ satisfies $x^2 - 37y^2 = 11$.

We have reduced solvability of $x^2 - 37y^2 = 11$ to solvability of $t^2 - 37z^2 = -3$. Since $|-3| < \sqrt{37}$, t/z has to be a convergent to $\sqrt{37}$ if we take $t > 0$ and $z > 0$. Testing the convergents p/q of the first two periods of the continued fraction for $\sqrt{37}$, which is $[6, 12, 12, 12, \dots]$, the only possible values of $p^2 - 37q^2$ are ± 1. We don't get -3 as a value, so $t^2 - 37z^2 = -3$ has no solution and therefore $x^2 - 37y^2 = 11$ has no solution.

References

[1] J. E. Shockley, "Introduction to Number Theory," Holt, Rinehart and Winston, New York, 1967.