

PELL'S EQUATION, II

KEITH CONRAD

1. INTRODUCTION

In Part I we met Pell's equation $x^2 - dy^2 = 1$ for nonsquare d in \mathbf{Z}^+ .¹ 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 $x^2 - dy^2 = 1$ are 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 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 each integer $m \geq 2$ consider the $m + 1$ numbers

$$(2.1) \quad 0, \sqrt{d}, 2\sqrt{d}, \dots, m\sqrt{d}.$$

The fractional part of every real number is in $[0, 1)$. View $[0, 1)$ as m half-open intervals $[0, 1/m)$, $[1/m, 2/m)$, \dots , $[(m-1)/m, 1)$. 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

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

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

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

This inequality is strict since $[i/m, (i+1)/m)$ is a half-open interval. Using (2.2),

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

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

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

This implies x is positive: since $|x - y\sqrt{d}| < 1$, $x > y\sqrt{d} - 1 \geq \sqrt{d} - 1 > 0$.

¹See <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn1.pdf>.

Having found a pair (x, y) in \mathbf{Z}^+ such that $|x - y\sqrt{d}| < 1/y$, to get a second such pair choose $m' \in \mathbf{Z}^+$ where $1/m' < |x - y\sqrt{d}|$. (Such an m' exists since $x - y\sqrt{d} \neq 0$, as \sqrt{d} is *irrational*.) Run through the argument above with m' in place of m to find x' and y' in \mathbf{Z}^+ such that $|x' - y'\sqrt{d}| < 1/m'$ with $y' \leq m'$, so $|x' - y'\sqrt{d}| < 1/y'$. Since

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

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

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) are three pairs of integers (a, b) where $a\sqrt{7}$ and $b\sqrt{7}$ lie in a common interval $[i/10, (i+1)/10)$, so the fractional parts differ by less than $1/10$: $(a, b) = (2, 5)$, $(4, 7)$, and $(6, 9)$. For all three pairs, $b - a = 3$.

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

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

so we can use $(x, y) = (8, 3)$. The choices $(a, b) = (4, 7)$ and $(6, 9)$ also lead to $(x, y) = (8, 3)$.

To get another pair (x', y') in \mathbf{Z}^+ where $|x' - y'\sqrt{7}| < 1/y'$, since $|8 - 3\sqrt{7}| \approx .0627 > 1/20$ look at the fractional parts of $k\sqrt{7}$ for $0 \leq k \leq 20$ and find two fractional parts in the same interval $[i/20, (i+1)/20)$ so they differ by less than $1/20$. This happens when k is 0 and 14:

$$0\sqrt{7} = 0, \quad 14\sqrt{7} = 37.0405\dots,$$

so

$$|(0\sqrt{7} - 0) - (14\sqrt{7} - 37)| \approx .04 < \frac{1}{20} \implies |37 - 14\sqrt{7}| < \frac{1}{20} < \frac{1}{14}$$

and we can use $(x', y') = (37, 14)$. This also happens when k is 2 and 19:

$$2\sqrt{7} = 5.2915\dots, \quad 19\sqrt{7} = 50.2692\dots,$$

so

$$|(2\sqrt{7} - 5) - (19\sqrt{7} - 50)| \approx .02 < \frac{1}{20} \implies |45 - 17\sqrt{7}| < \frac{1}{20} < \frac{1}{14},$$

which means we can use $(x', y') = (45, 17)$.

What we used about \sqrt{d} in Lemma 2.1 is that it is irrational and greater than 1. A similar argument shows that for irrational $\alpha \in \mathbf{R}$, $|x - y\alpha| < 1/y$ for infinitely many pairs of integers (x, y) with $y > 0$ (give up on requiring $x > 0$ if $\alpha < 0$).

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. Lagrange's proof [7, pp. 669–731] used continued fractions. In the proof here, we will start by showing there's a nonzero integer M such that $x^2 - dy^2 = M$ has infinitely many solutions x and y in \mathbf{Z}^+ . Then we'll combine this with modular arithmetic to show $x^2 - dy^2 = 1$ has a solution in \mathbf{Z}^+ . The pigeonhole principle will be used twice.

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

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

for all such x and y . What matters here is that the upper bound does not involve x or y ; that it happens specifically to be $1 + 2\sqrt{d}$ is not crucial.

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

$$(2.5) \quad x^2 - dy^2 = M$$

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

For x and y in \mathbf{Z}^+ satisfying (2.5), reduce them mod $|M|$. By the pigeonhole principle, the infinitely many pairs $(x \bmod |M|, y \bmod |M|)$ have a repetition infinitely often since there are finitely many pairs mod $|M|$. (Here we use $M \neq 0$.) So there are (x_1, y_1) and (x_2, y_2) in \mathbf{Z}^+ fitting (2.5) such that $x_1 \equiv x_2 \pmod{|M|}$, $y_1 \equiv y_2 \pmod{|M|}$, and $(x_1, y_1) \neq (x_2, y_2)$.

Since $x_1 \equiv x_2 \pmod{|M|}$ and $y_1 \equiv y_2 \pmod{|M|}$, we have $x_1 = x_2 + Mk$ and $y_1 = y_2 + M\ell$ for some k and ℓ in \mathbf{Z} . Then

$$x_1 + y_1\sqrt{d} = x_2 + y_2\sqrt{d} + M(k + \ell\sqrt{d}),$$

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

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

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

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

Combine like terms in the second factor on the right in (2.6) to make it $x + y\sqrt{d}$ with $x, y \in \mathbf{Z}$ (we *don't* know they're positive). The second factor on the right in (2.7) is $x - y\sqrt{d}$, so

$$x_1 + y_1\sqrt{d} = (x_2 + y_2\sqrt{d})(x + y\sqrt{d})$$

$$x_1 - y_1\sqrt{d} = (x_2 - y_2\sqrt{d})(x - y\sqrt{d}).$$

Multiplying these last two equations together, we get $M = M(x^2 - dy^2)$. Thus $x^2 - dy^2 = 1$. We have $x \neq 0$ since $d > 0$. If $y = 0$ then $x = \pm 1$. If $(x, y) = (1, 0)$ then $x_1 = x_2$ and $y_1 = y_2$, but this contradicts the fact that (x_1, y_1) 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*. Thus $y \neq 0$.

Since $x \neq 0$ and $y \neq 0$, by changing signs on x and y in case either is negative we get a solution to $x^2 - dy^2 = 1$ with x and y in \mathbf{Z}^+ . \square

Remark 2.4. Without the congruences mod $|M|$ in the proof, from just $x_1^2 - dy_1^2 = M$ and $x_2^2 - dy_2^2 = M$ we can't say $x_1 + y_1\sqrt{d} = (x_2 + y_2\sqrt{d})(x + y\sqrt{d})$ where $x, y \in \mathbf{Z}$ (and $x^2 - dy^2 = 1$). For example, $5^2 - 2 \cdot 3^2 = 7$, $3^2 - 2 \cdot 1^2 = 7$, and $5 + 3\sqrt{2} = (3 + \sqrt{2})(\frac{9}{7} + \frac{4}{7}\sqrt{2})$ where $(9/7, 4/7)$ is a solution to $x^2 - 2y^2 = 1$, but it is not an *integral* solution.

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 a 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 $(6 + \sqrt{7})(8 + 3\sqrt{7}) = 69 + 26\sqrt{7}$, a second 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 a “solution” means either the pair (x, y) or the number $x + y\sqrt{d}$ and a “Pell multiple” of it means either the coefficients $(ax + dby, ay + bx)$ of the product $(a + b\sqrt{d})(x + y\sqrt{d})$ where $a^2 - db^2 = 1$ or the product 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 in Example 4.1 that the integral solutions of $x^2 - 6y^2 = 3$ occur as $x + y\sqrt{6} = \pm(3 + \sqrt{6})(5 + 2\sqrt{6})^k$ for some $k \in \mathbf{Z}$, where $5^2 - 6 \cdot 2^2 = 1$, so each solution $x + y\sqrt{6}$ is a Pell multiple of $3 + \sqrt{6}$.

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

$$(3.1) \quad |x'| \leq \frac{\sqrt{|n|}(\sqrt{u} + 1/\sqrt{u})}{2} \quad \text{and} \quad |y'| \leq \frac{\sqrt{|n|}(\sqrt{u} + 1/\sqrt{u})}{2\sqrt{d}}.$$

If $n > 0$ then we can take $|y'| \leq \sqrt{n}(\sqrt{u} - 1/\sqrt{u})/(2\sqrt{d}) < \sqrt{nu}/(2\sqrt{d})$.

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 in $\mathbf{Z}[\sqrt{d}] - \{0\}$. Check this. In particular, $L(\alpha^k) = kL(\alpha)$ for $k \in \mathbf{Z}$.

Since $(a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 = \pm 1$, we have $|a - b\sqrt{d}| = 1/u > 0$, so

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

This vector is linearly independent of $(1, 1)$ since $\log u > 0$ (we have $u > 1$ since $u = a + b\sqrt{d}$ with a and b in \mathbf{Z}^+), so $\{(1, 1), L(u)\}$ is a basis of \mathbf{R}^2 . Thus when $x^2 - dy^2 = n$ we have

$$(3.2) \quad L(x + y\sqrt{d}) = c_1(1, 1) + c_2L(u)$$

for some real numbers c_1 and c_2 . See Figure 1.

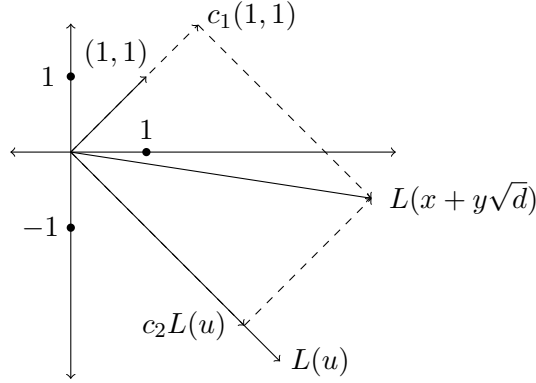


FIGURE 1. $L(x + y\sqrt{d})$ as a linear combination of $L(1)$ and $L(u)$.

Writing out the coordinates on both sides of (3.2),

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

Adding the coordinates lets us 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 $x^2 - dy^2 = n$, (3.2) becomes

$$(3.3) \quad L(x + y\sqrt{d}) = \frac{\log |n|}{2}(1, 1) + c_2L(u).$$

Let $k \in \mathbf{Z}$ minimize $|c_2 - k|$ so $\delta := c_2 - k$ has $|\delta| \leq \frac{1}{2}$. Then (3.3) says

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

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

$$(3.4) \quad L((x + y\sqrt{d})u^{-k}) = L(x + y\sqrt{d}) - kL(u) = \frac{\log |n|}{2}(1, 1) + \delta L(u).$$

Set $x' + y'\sqrt{d} = (x + y\sqrt{d})u^{-k}$, which has integer coefficients since u and u^{-1} have integer coefficients, so $x + y\sqrt{d} = (x' + y'\sqrt{d})u^k$ where $x'^2 - dy'^2 = n$ (since $a^2 - db^2 = 1$) and

$$(3.5) \quad (\log |x' + y'\sqrt{d}|, \log |x' - y'\sqrt{d}|) = \left(\frac{\log |n|}{2} + \delta \log u, \frac{\log |n|}{2} - \delta \log u \right).$$

One of $\pm\delta$ is ≤ 0 and the other is ≥ 0 . Since $|\delta| \leq \frac{1}{2}$ and $\log u > 0$, the coordinate in (3.5) where $\pm\delta \geq 0$ is at most $(\log |n|)/2 + (\log u)/2 = \log \sqrt{|n|u}$ and the coordinate where $\pm\delta \leq 0$ is at most $(\log |n|)/2 = \log \sqrt{|n|}$. Therefore one of $|x' + y'\sqrt{d}|$ or $|x' - y'\sqrt{d}|$ is at most $\sqrt{|n|u}$ and the other is at most $\sqrt{|n|}$.

To bound $|x'|$ and $|y'|$ from bounds on $|x' + y'\sqrt{d}|$ and $|x' - y'\sqrt{d}|$, we will use

$$(3.6) \quad |x'| = \frac{|(x' + y'\sqrt{d}) + (x' - y'\sqrt{d})|}{2}, \quad |y'| = \frac{|(x' + y'\sqrt{d}) - (x' - y'\sqrt{d})|}{2\sqrt{d}}.$$

Set $s := \max(|x' + y'\sqrt{d}|, |x' - y'\sqrt{d}|)$. The two numbers $|x' + y'\sqrt{d}|$ and $|x' - y'\sqrt{d}|$ have product $|x'^2 - dy'^2| = |n|$, so these two numbers are s and $|n|/s$ in some order. Thus

$$|x'| = \frac{|(x' + y'\sqrt{d}) + (x' - y'\sqrt{d})|}{2} \leq \frac{|x' + y'\sqrt{d}| + |x' - y'\sqrt{d}|}{2} = \frac{1}{2} \left(s + \frac{|n|}{s} \right).$$

We saw one of s or $|n|/s$ is at most $\sqrt{|n|}$, so the other is at least $\sqrt{|n|}$. Since s is a maximum, $\sqrt{|n|} \leq s \leq \sqrt{|n|u}$. By calculus, $t + |n|/t$ is increasing for $t \geq \sqrt{|n|}$, so

$$|x'| \leq \frac{1}{2} \left(s + \frac{|n|}{s} \right) \leq \frac{1}{2} \left(\sqrt{|n|u} + \frac{|n|}{\sqrt{|n|u}} \right) = \frac{\sqrt{|n|}(\sqrt{u} + 1/\sqrt{u})}{2}$$

and

$$|y'| \leq \frac{|x' + y'\sqrt{d}| + |x' - y'\sqrt{d}|}{2\sqrt{d}} = \frac{1}{2\sqrt{d}} \left(s + \frac{|n|}{s} \right) \leq \frac{\sqrt{|n|}(\sqrt{u} + 1/\sqrt{u})}{2\sqrt{d}}.$$

When $n > 0$, we can sharpen the bound on $|y'|$. The equation $x'^2 - dy'^2 = n$ implies $x' + y'\sqrt{d}$ and $x' - y'\sqrt{d}$ have the same sign (their product is positive). Since $|x' + y'\sqrt{d}|$ and $|x' - y'\sqrt{d}|$ are s and n/s in some order, $x' + y'\sqrt{d}$ and $x' - y'\sqrt{d}$ are either s and n/s in some order or $-s$ and $-n/s$ in some order. Either way,

$$|y'| = \frac{|(x' + y'\sqrt{d}) - (x' - y'\sqrt{d})|}{2\sqrt{d}} = \frac{|s - n/s|}{2\sqrt{d}}.$$

Since $\sqrt{n} \leq s \leq \sqrt{nu}$, we have $\sqrt{n/u} \leq n/s \leq \sqrt{n}$, so s and n/s lie in the interval $[\sqrt{n/u}, \sqrt{nu}]$. Therefore $|s - n/s|$ is at most the length of that interval, which tells us

$$|y'| = \frac{|s - n/s|}{2\sqrt{d}} \leq \frac{\sqrt{nu} - \sqrt{n/u}}{2\sqrt{d}} = \frac{\sqrt{n}}{2\sqrt{d}} \left(\sqrt{u} - \frac{1}{\sqrt{u}} \right). \quad \square$$

The bounds on $|x'|$ and $|y'|$ in Theorem 3.3 when $n > 0$ satisfy the generalized Pell equation: if $x' = \sqrt{n}(\sqrt{u} + 1/\sqrt{u})/2$ and $y' = \sqrt{n}(\sqrt{u} - 1/\sqrt{u})/(2\sqrt{d})$, then $x'^2 - dy'^2 = n$ (it's not important what number u is). These bounds on $|x'|$ and $|y'|$ may not be in \mathbf{Z} , but we'll see in Examples 4.1 and 4.4 that the bounds sometimes are in \mathbf{Z} . In the appendix, infinitely many examples are given where the bounds in (3.1) are in \mathbf{Z} and are the smallest solution of $x'^2 - dy'^2 = n$ in \mathbf{Z}^+ .

Remark 3.4. The first bounds I learned for $|x'|$ and $|y'|$ were $|x'| \leq (|n| + u)/2$ and $|y'| \leq (|n| + u)/(2\sqrt{d})$, which is in [1, p. 244]. A careful reading of the derivation of those bounds in [1] shows that $|x'| \leq \sqrt{|n|u}$ and $|y'| \leq \sqrt{|n|u/d}$, which is sharper since $\sqrt{ab} \leq (a + b)/2$ (the arithmetic-geometric mean inequality), and that was what I originally wrote in Theorem 3.3. That those bounds on $|x'|$ and $|y'|$ can be cut down by essentially

a factor of 2, as in (3.1), was shown to me by Yosei Lii, who also explained the drop by a factor of 2 just from the triangle inequality in (3.6) without any calculus:

$$|x' + y'\sqrt{d}| + |x' - y'\sqrt{d}| \leq \sqrt{|n|u} + \sqrt{|n|} = \sqrt{|n|}(\sqrt{u} + 1),$$

so

$$(3.7) \quad |x'| = \left| \frac{(x' + y'\sqrt{d}) + (x' - y'\sqrt{d})}{2} \right| \leq \frac{|x' + y'\sqrt{d}| + |x' - y'\sqrt{d}|}{2} \leq \frac{\sqrt{|n|}(\sqrt{u} + 1)}{2}$$

and

$$(3.8) \quad |y'| = \left| \frac{(x' + y'\sqrt{d}) - (x' - y'\sqrt{d})}{2\sqrt{d}} \right| \leq \frac{|x' + y'\sqrt{d}| + |x' - y'\sqrt{d}|}{2\sqrt{d}} \leq \frac{\sqrt{|n|}(\sqrt{u} + 1)}{2\sqrt{d}}.$$

The bounds (3.7) and (3.8) are weaker than the bounds in (3.1) since $0 < 1/\sqrt{u} < 1$, but the distinction between these two bounds on $|x'|$ and $|y'|$ is negligible in practice. I later learned that the bounds in Theorem 3.3 were found by Chebyshev in 1851 [2, pp. 260, 262]. A generalization of the bound on $|y'|$ in (3.1) is in [5, Theorem 4.5].

When $n = 1$, there is no guarantee that an integral solution (x', y') to $x'^2 - dy'^2 = 1$ fitting the bounds on $|x'|$ and $|y'|$ in (3.1) is not the trivial solution $(1, 0)$. More generally, when n is a perfect square, an integral solution to $x'^2 - dy'^2 = n$ fitting (3.1) might have $y' = 0$. Of course Theorem 3.3 is useless when $n = 1$ since the bounds in this theorem depend on already knowing a number $u = a + b\sqrt{d}$ with $a, b \in \mathbf{Z}^+$ where $a^2 - db^2 = 1$. When n is not a perfect square, integral solutions (x', y') to $x'^2 - dy'^2 = n$ must have $y' \neq 0$. For example, the bounds in Theorem 3.3 can be used for $n = -1$ to determine whether the so-called negative Pell equation $x^2 - dy^2 = -1$ has an integral solution once we know a nontrivial solution to $a^2 - db^2 = 1$.

Corollary 3.5. *For a 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 may assume there is a solution. To prove the conclusion, here are two proofs.

Proof #1: Each solution is a Pell multiple of a solution with $|x| \leq \sqrt{|n|}(\sqrt{u} + 1/\sqrt{u})/2$ and $|y| \leq \sqrt{|n|}(\sqrt{u} + 1/\sqrt{u})/(2\sqrt{d})$ by Theorem 3.3, so x and y have finitely many choices.

Proof #2: By the end of the proof of Theorem 2.3, if $x_1^2 - dy_1^2 = M$ and $x_2^2 - dy_2^2 = M$ with $x_1 \equiv x_2 \pmod{|M|}$ and $y_1 \equiv y_2 \pmod{|M|}$ 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 , all integral solutions of $x^2 - dy^2 = n$ with 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 $|n|$. \square

The second proof of Corollary 3.5, unlike the first, is not practical because it is not computationally effective: it doesn't give a bounded range of x and y values that contain the solutions of $x^2 - dy^2 = n$ up to a Pell multiple. In particular, the second proof can't show $x^2 - dy^2 = n$ has no solutions while the first proof can, as we'll see in Example 4.5.

Remark 3.6. For the negative Pell equation $x^2 - dy^2 = -1$, with squarefree d , the existence of a solution in \mathbf{Z} requires no prime factor of d to be 3 mod 4. Among squarefree $d > 0$ with no prime factor that is 3 mod 4, the proportion for which $x^2 - dy^2 = -1$ has a solution in \mathbf{Z} is $1 - \prod_{\text{odd } j \geq 1} (1 - 1/2^j)$ ($\approx 58\%$) by a theorem of Koymans and Pagano [6].

4. EXAMPLES OF THEOREM 3.3

We now apply Theorem 3.3 in several examples to see how it works in practice. In all cases but the last one we'll have $n > 0$, so we'll use the bound on $|y'|$ at the end of the theorem rather than the bound on $|y'|$ in (3.1).

Example 4.1. We will describe all the solutions of $x^2 - 6y^2 = 3$ in integers. An obvious solution is $(3, 1)$ and its sign changes in coordinates $(3, -1)$, $(-3, 1)$, and $(-3, -1)$. What are all the integral solutions?

As a positive solution of $a^2 - 6b^2 = 1$ we will take $(a, b) = (5, 2)$, so set $u = 5 + 2\sqrt{6}$. By the end of Theorem 3.3, $|y'| \leq \sqrt{|n|}(\sqrt{u} - 1/\sqrt{u})/(2\sqrt{d}) = \sqrt{3}(\sqrt{u} - 1/\sqrt{u})/(2\sqrt{6}) = 1$, which forces y' to be 1, 0, or -1 . Solutions to $x'^2 - 6y'^2 = 3$ with such y' -values are $(\pm 3, 1)$ and $(\pm 3, -1)$. (In particular, the bound on $|y'|$ at the end of Theorem 3.3 is optimal in this case.) Thus the integral solutions of $x^2 - 6y^2 = 3$ have the form

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

where $k \in \mathbf{Z}$. Up to multiplication by powers of u , there are four solutions:

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

These four solutions are related in pairs by powers of u : $3 - \sqrt{6} = (3 + \sqrt{6})u^{-1}$, and $-3 + \sqrt{6} = (-3 - \sqrt{6})u^{-1}$. Therefore every solution of $x^2 - 6y^2 = 3$ in integers has the form

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

for some $k \in \mathbf{Z}$ and this list has no repetitions.

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 \mathbf{Z}^+ 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 $u = 8 + 3\sqrt{7}$. By the end of Theorem 3.3, $|y'| \leq \sqrt{57}(\sqrt{u} - 1/\sqrt{u})/(2\sqrt{7}) \approx 5.33$. The integral solutions to $x'^2 - 7y'^2 = 57$ for such y' are $(x', y') = (\pm 8, \pm 1)$ and $(\pm 13, \pm 4)$.

The integral solutions of $x^2 - 7y^2 = 57$ therefore have the form

$$(4.1) \quad x + y\sqrt{7} = \pm(8 \pm \sqrt{7})u^k \quad \text{or} \quad \pm(13 \pm 4\sqrt{7})u^k$$

with $k \in \mathbf{Z}$. No pair of numbers among $13 \pm 4\sqrt{7}$ and $8 \pm \sqrt{7}$ has a ratio that is a power of u (in fact, no pair has a ratio of the form $m + n\sqrt{7}$ with $m, n \in \mathbf{Z}$). Therefore (4.1) has no repetitions.

The solution $(x, y) = (20, 7)$ appears in (4.1) as $20 + 7\sqrt{7} = (13 - 4\sqrt{7})u$.

Example 4.3. We will completely solve $x^2 - 19y^2 = 36$ in integers. An obvious pair of solutions is $(\pm 6, 0)$. What are the rest?

A nontrivial solution of $a^2 - 19b^2 = 1$ in positive integers is $(170, 39)$ (this solution has the smallest positive b), so let $u = 170 + 39\sqrt{19}$. By the end of Theorem 3.3, $|y'| \leq \sqrt{36}(\sqrt{u} - 1/\sqrt{u})/(2\sqrt{19}) \approx 12.65$, so $(x', y') = (\pm 6, 0)$ and $(\pm 44, \pm 10)$. Therefore the integral solutions to $x^2 - 19y^2 = 36$ have the form

$$x + y\sqrt{19} = \pm 6u^k \quad \text{or} \quad \pm(44 \pm 10\sqrt{19})u^k$$

with $k \in \mathbf{Z}$. These solutions have no repetitions since no pair among 6 , -6 , $44 + 10\sqrt{19}$, and $44 - 10\sqrt{19}$ has a ratio that is a power of u .

The solution $(x, y) = (70, 16)$ appears as $70 + 16\sqrt{19} = (44 - 10\sqrt{19})u$.

Example 4.4. We will completely solve $x^2 - 103y^2 = 2$ in integers.

A solution of $a^2 - 103b^2 = 1$ in positive integers is $(227528, 22419)$ (this solution has the smallest positive b), so let $u = 227528 + 22419\sqrt{103}$. By the end of Theorem 3.3, $|y'| \leq \sqrt{2}(\sqrt{u}-1/\sqrt{u})/(2\sqrt{103}) = 47$. The only nonnegative y' in this range where $x'^2 - 103y'^2 = 2$ for some $x' \in \mathbf{Z}$ is $y' = 47$, for which $x' = \pm 477$. (As in Example 4.1, the bound on $|y'|$ this time is optimal.) Therefore the integral solutions to $x^2 - 103y^2 = 2$ have the form

$$x + y\sqrt{103} = \pm(477 \pm 47\sqrt{103})u^k$$

with $k \in \mathbf{Z}$. These solutions have repetitions since $477 - 47\sqrt{103} = (477 + 47\sqrt{103})/u$,² so the integral solutions to $x^2 - 103y^2 = 2$ without repetitions are

$$x + y\sqrt{103} = \pm(477 + 47\sqrt{103})u^k.$$

Example 4.5. We will show $x^2 - 37y^2 = 11$ has no integral solution.

A solution of $a^2 - 37b^2 = 1$ is $(73, 12)$, so let $u = 73 + 12\sqrt{37}$. By the end of Theorem 3.3, $|y'| \leq \sqrt{11}(\sqrt{u}-1/\sqrt{u})/(2\sqrt{37}) \approx 3.27$. For no y' in this range is $x'^2 - 37y'^2 = 11$ for an $x' \in \mathbf{Z}$, so the equation $x^2 - 37y^2 = 11$ has no solution in \mathbf{Z} .

Example 4.6. We will show $x^2 - 194y^2 = -1$ has no integral solution.

A solution of $a^2 - 194b^2 = 1$ is $(195, 14)$. Using $u = 195 + 14\sqrt{194}$ in (3.1), since $n = -1 < 0$, $|y'| \leq \sqrt{1}(\sqrt{u}+1)/(2\sqrt{194}) \approx 0.71 < 1$. The only choice is $y' = 0$, for which $x'^2 - 194y'^2 = -1$ has no integral solution x' . Thus $x^2 - 194y^2 = -1$ has no solution in \mathbf{Z} .

Example 4.7. We will show $x^2 - 733y^2 = 383$ has no integral solution.

A solution of $a^2 - 733b^2 = 1$ is $(195307849, 7213860)$,³ so let $u = 195307849 + 7213860\sqrt{733}$. Since $\sqrt{383}(\sqrt{u}-1/\sqrt{u})/(2\sqrt{733}) \approx 7143.19$, we use a computer to search through all y' from 0 to 7143 and in no case is $733y'^2 + 383$ a perfect square. Therefore $x^2 - 733y^2 = 383$ has no solution in \mathbf{Z} .

At the end of Remark 3.4 it was mentioned that the bounds $|y'| \leq \sqrt{|n|}(\sqrt{u}+1/\sqrt{u})/(2\sqrt{d})$ (for all n) and $|y'| \leq \sqrt{n}(\sqrt{u}-1/\sqrt{u})/(2\sqrt{d})$ (for $n > 0$) are not in practice substantially better than the bound $|y'| \leq \sqrt{|n|}(\sqrt{u}+1)/(2\sqrt{d})$. The table below illustrates this by comparing such bounds for most of the examples in this section (those where $n > 0$).

Example	$x^2 - dy^2 = n$	$\sqrt{n}(\sqrt{u}-1/\sqrt{u})/(2\sqrt{d})$	$\sqrt{ n }(\sqrt{u}+1)/(2\sqrt{d})$
4.1	$x^2 - 6y^2 = 3$	1	1.46
4.2	$x^2 - 7y^2 = 57$	5.33	7.12
4.3	$x^2 - 19y^2 = 36$	12.65	13.37
4.4	$x^2 - 103y^2 = 2$	47	47.06
4.5	$x^2 - 37y^2 = 11$	3.27	3.56
4.7	$x^2 - 733y^2 = 383$	7143.19	7143.55

The website <https://www.alpertron.com.ar/QUAD.HTM> will give you all the solutions to $x^2 - dy^2 = n$ as a recursive sequence (x_n, y_n) or tell you there are no integral 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 seen in Part I.

²If $x^2 - dy^2 = \pm 2$, then the ratio $(x + y\sqrt{d})/(x - y\sqrt{d})$ is a unit in $\mathbf{Z}[\sqrt{d}]$.

³Yes, this is the smallest solution in positive integers a and b .

Example 4.8. There is no solution to $x^2 - 37y^2 = 2$ in \mathbf{Z} since $x^2 - 37y^2 \equiv 2 \pmod{4}$ has no solution: the congruence is $x^2 - y^2 \equiv 2 \pmod{4}$ and the squares mod 4 are 0 and 1, which don't differ by 2.

Congruence methods do not always suffice to prove there are no solutions in \mathbf{Z} . The equations $x^2 - 37y^2 = 11$ and $x^2 - 194y^2 = -1$, which we met in Examples 4.5 and 4.6, are instances of this. They have no \mathbf{Z} -solutions but they have rational solutions: $x^2 - 37y^2 = 11$ has solutions $(9/2, 1/2)$ and $(32/3, 5/3)$, and $x^2 - 194y^2 = -1$ has solutions $(13/5, 1/5)$ and $(5/13, 1/13)$. From these pairs of rational solutions it can be shown that $x^2 - 37y^2 \equiv 11 \pmod{m}$ and $x^2 - 194y^2 \equiv -1 \pmod{m}$ are each solvable for all $m \geq 2$.

Exercise. Use the method of Example 4.5 to show $x^2 - 37y^2 = n$ has no solution in \mathbf{Z} for $n = 3, 5, 6, 7, 8, 10$.

For $n = 5, 6, 8$, and 10 the lack of \mathbf{Z} -solutions to $x^2 - 37y^2 = n$ can also be proved in a more elementary way, as with $n = 2$, by showing there is no solution to either $x^2 - 37y^2 \equiv n \pmod{4}$ or $x^2 \equiv n \pmod{37}$. This doesn't work for $n = 3$ or $n = 7$, just as we saw it doesn't for $n = 11$: for all $m \geq 2$ there is a solution to $x^2 - 37y^2 \equiv 3 \pmod{m}$ and $x^2 - 37y^2 \equiv 7 \pmod{m}$.

5. USING CONTINUED FRACTIONS

In this section, for those who know about continued fractions, we will explain how Pell and generalized Pell equations can be solved with continued fractions. The link between continued fractions and generalized Pell equations is due to the next theorem of Lagrange [4, Art. 38].

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 [9, 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 $x^2 - dy^2 = n > 0 \implies x^2 > dy^2$, so $x > y\sqrt{d}$ since x and y are positive.

If $n < 0$ then $x^2 - dy^2 < 0 \implies x < y\sqrt{d}$ 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 $1/\sqrt{d} = [0, a_1, a_2, \dots]$,⁴ which

⁴A continued fraction $[a_1, a_2, a_3, \dots]$ with $a_1 < 0$ has a much more complicated rule for the continued fraction of its reciprocal than when $a_1 \geq 0$: see <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/contfrac-neg-invert.pdf>. Fortunately we're not dealing with $a_1 < 0$ here.

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} . \square

Corollary 5.2. *For each 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} . \square

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 so is $x^2 - dy^2$ when x/y runs through the convergents to \sqrt{d} . All distinct 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 n with $0 < |n| < \sqrt{d}$ such that $x^2 - dy^2 = n$ has a solution.

Example 5.4. Since $\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$, we compute $x^2 - 13y^2$ in the table below where x/y runs through convergents just before the second 6. Since $\sqrt{13} \approx 3.6$, the table tells us the only n with $0 < |n| < \sqrt{13}$ for which $x^2 - 13y^2 = n$ is solvable in \mathbf{Z} are ± 1 and ± 3 . (Although ± 4 appears in the bottom row of the table, $|\pm 4| > \sqrt{13}$.)

		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

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} . Such a reduction process goes back to Lagrange [8, pp. 422–426], and more recent references are [3, pp. 454–457] and [9, pp. 210–213]. We'll illustrate this with two examples that were treated in the previous section using Theorem 3.3.

Example 5.5. Consider $x^2 - 6y^2 = 3$ with $x, y \in \mathbf{Z}$. Note $3 > \sqrt{6}$. Reducing the equation mod 3, we get $x^2 \equiv 0 \pmod{3}$, so $x \equiv 0 \pmod{3}$. 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 y , its discriminant

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

is a perfect square, so $6z^2 - 2 = t^2$ for some $t \in \mathbf{Z}$. Write this as $t^2 - 6z^2 = -2$ and note t is even. Conversely, if integers t and z fit $t^2 - 6z^2 = -2$ then $x = 3z$ and $y = \pm\sqrt{4t^2}/(2(-2)) = \pm t/2$ are integers that satisfy $x^2 - 6y^2 = 3$.

If $t, z \in \mathbf{Z}^+$ satisfy $t^2 - 6z^2 = -2$ then t/z is a convergent to $\sqrt{6}$ since $|-2| < \sqrt{6}$. By the table in Example 5.3 the first three solutions of $t^2 - 6z^2 = -2$ in \mathbf{Z}^+ 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 5.6. Consider $x^2 - 37y^2 = 11$ with $x, y \in \mathbf{Z}$. Note $11 > \sqrt{37}$. We have $x^2 \equiv 37y^2 \equiv (2y)^2 \pmod{11}$, so $x \equiv \pm 2y \pmod{11}$. 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

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

is a perfect square, so $37z^2 - 3 = t^2$ for some $t \in \mathbf{Z}$. Write this as $t^2 - 37z^2 = -3$. All steps are reversible, so if $t^2 - 37z^2 = -3$ and y in \mathbf{Z} fits $-3y^2 \pm 4yz + (11z^2 - 1) = 0$ then $(x, y) = (\pm 2y + 11z, y)$ satisfies $x^2 - 37y^2 = 11$.

If $t, z \in \mathbf{Z}^+$ satisfy $t^2 - 37z^2 = -3$ then t/z is a convergent to $\sqrt{37}$ since $|-3| < \sqrt{37}$. Testing the convergents p/q of the first two periods of the continued fraction for $\sqrt{37}$, which is $[6, 12, 12, \dots]$, the only values of $p^2 - 37q^2$ are ± 1 . Since -3 isn't a value of $p^2 - 37q^2$, $t^2 - 37z^2 = -3$ has no solution in \mathbf{Z} and thus $x^2 - 37y^2 = 11$ has no solution in \mathbf{Z} , which we found by another method in Example 4.5.

Exercise. Use the method of Example 5.6 to show $x^2 - 37y^2 = 7$ has no solution in \mathbf{Z} by relating it to $t^2 - 37z^2 = -4$.

APPENDIX A. OPTIMALITY OF THE BOUNDS IN THEOREM 3.3

In Examples 4.1 and 4.4, the bound on $|x'|$ in (3.1) and the bound on $|y'|$ at the end of Theorem 3.3 if $n > 0$ are the *only* solution in \mathbf{Z}^+ within the range of those bounds:

- the first solution to $x^2 - 6y^2 = 3$ in \mathbf{Z}^+ is $(x, y) = (3, 1)$, and in Example 4.1 with $u = 5 + 2\sqrt{6}$, $\sqrt{n}(\sqrt{u} + 1/\sqrt{u})/2 = 3$ and $\sqrt{n}(\sqrt{u} - 1/\sqrt{u})/(2\sqrt{d}) = 1$,
- the first solution to $x^2 - 103y^2 = 2$ in \mathbf{Z}^+ is $(x, y) = (477, 47)$ and in Example 4.4 with $u = 227528 + 22419\sqrt{103}$, $\sqrt{n}(\sqrt{u} + 1/\sqrt{u})/2 = 477$ and $\sqrt{n}(\sqrt{u} - 1/\sqrt{u})/(2\sqrt{d}) = 47$.

A third example is $x^2 - 23y^2 = 2$. The least unit greater than 1 in $\mathbf{Z}[\sqrt{23}]$ is $u = 24 + 5\sqrt{23}$, with norm 1. Theorem 3.3 says integral solutions of $x^2 - 23y^2 = 2$ are powers of u times solutions where $|x| \leq \sqrt{2}(\sqrt{u} + 1/\sqrt{u})/2 = 5$ and $|y| \leq \sqrt{2}(\sqrt{u} - 1/\sqrt{u})/(2\sqrt{23}) = 1$. The only solution in that range in positive integers is $(x, y) = (5, 1)$.

This naturally raises the question: are there infinitely many equations $x^2 - dy^2 = n$ where the bounds on $|x'|$ and $|y'|$ from Theorem 3.3 for $n > 0$ are optimal? Yes!

Theorem A.1. *For an integer $m \geq 2$, let $d = m^2 - 2$. The bounds on $|x'|$ and $|y'|$ in Theorem 3.3 for the equation $x^2 - dy^2 = 2$ are $|x'| \leq m$ and $|y'| \leq 1$, and the only solution in positive integers within those bounds is $(x', y') = (m, 1)$.*

The family of equations $x^2 - (m^2 - 2)y^2 = 2$ has $x^2 - 23y^2 = 2$ as the special case $m = 5$.

Proof. The equation $x^2 - (m^2 - 2)y^2 = 2$ has no integral solution when $y = 0$, and when $y = 1$ we have $x = m$.

For $m \geq 2$, the smallest solution of $a^2 - (m^2 - 2)b^2 = 1$ in positive integers is $(a, b) = (m^2 - 1, m)$. Equivalently, the least unit of norm 1 that's greater than 1 in $\mathbf{Z}[\sqrt{m^2 - 2}]$ is $m^2 - 1 + m\sqrt{m^2 - 2}$: when $m = 2$, the fundamental unit of $\mathbf{Z}[\sqrt{2}]$ is $1 + \sqrt{2}$, with norm -1 , and $(1 + \sqrt{2})^2 = 3 + 2\sqrt{2} = m^2 - 1 + m\sqrt{m^2 - 2}$, while when $m \geq 3$, the fundamental unit of $\mathbf{Z}[\sqrt{m^2 - 2}]$ is $m^2 - 1 + m\sqrt{m^2 - 2}$ and it has norm 1. In Theorem 3.3, we can set $u = m^2 - 1 + m\sqrt{m^2 - 2}$,

We will show the bounds from Theorem 3.3 for integral solutions of $x^2 - (m^2 - 2)y^2 = 2$ are $|x'| \leq m$ and $|y'| \leq 1$. That makes the bounds from Theorem 3.3 optimal since (i) $(x', y') = (m, 1)$ is a solution, (ii) there's no solution when $y' = 0$, and (iii) when $x'^2 - (m^2 - 2)y'^2 = 2$ and $y' > 1$, we have $x'^2 \geq 4(m^2 - 2) + 2 > m^2$, so $x' > m$.

To show the bounds on $|x'|$ and $|y'|$ from Theorem 3.3 are m and 1 means

$$\frac{\sqrt{2}(\sqrt{u} + 1/\sqrt{u})}{2} = m, \quad \frac{\sqrt{2}(\sqrt{u} - 1/\sqrt{u})}{2\sqrt{m^2 - 2}} = 1.$$

Since $u > 1$, these equations are true if the squares of both sides are true, so we will check

$$\frac{u + 2 + 1/u}{2} = m^2, \quad \frac{u - 2 + 1/u}{2(m^2 - 2)} = 1.$$

Both equations are equivalent to $u^2 - 2(m^2 - 1)u + 1 = 0$, and u is a root of $t^2 - 2(m^2 - 1)t + 1$ by the quadratic formula. \square

Theorem A.2. *For an integer $m \geq 1$, let $d = 4m^2 + 2$. The bounds on $|x'|$ and $|y'|$ in Theorem 3.3 for the equation $x^2 - dy^2 = 2m^2 + 1$ are $|x'| \leq 2m^2 + 1$ and $|y'| \leq m$, and $(x, y) = (2m^2 + 1, m)$ is a solution.*

The equation $x^2 - (4m^2 + 2)y^2 = 2m^2 + 1$ becomes $x^2 - 6y^2 = 3$ when $m = 1$.

In contrast to Theorem A.1, the smallest solution to $x^2 - (4m^2 + 2)y^2 = 2m^2 + 1$ in positive integers might not be $(x, y) = (2m^2 + 1, m)$, but it does appear to be most of the time. For $1 \leq m \leq 100$, there is no solution in positive integers where $y \leq m - 1$ with three exceptions: $m = 11$ $((x, y) = (27, 1))$, $m = 12$ $((x, y) = (51, 2))$, and $m = 70$ $((x, y) = (297, 2)$ and a second solution $(1683, 12))$. It would be nice to have a proof that for infinitely many m there is no solution in positive integers where $y \leq m - 1$.

Proof. It is easy to check that $(x, y) = (2m^2 + 1, m)$ is a solution of $x^2 - (4m^2 + 2)y^2 = 2m^2 + 1$.

View $4m^2 + 2$ as $M^2 + 2$ for the even value $M = 2m$. For $M \geq 1$, the fundamental unit of $\mathbf{Z}[\sqrt{M^2 + 2}]$ is $M^2 + 1 + M\sqrt{M^2 + 2}$ and it has norm 1, so the smallest solution of $a^2 - (M^2 + 2)b^2 = 1$ in positive integers is $(a, b) = (M^2 + 1, M)$. Letting $M = 2m$, in Theorem 3.3 with $d = M^2 + 2 = 4m^2 + 2$, we can set $u = (2m)^2 + 1 + 2m\sqrt{(2m)^2 + 2} = 4m^2 + 1 + 2m\sqrt{4m^2 + 2}$. In Theorem 3.3 we'll show the bounds on $|x'|$ and $|y'|$ using u as above are $|x'| \leq 2m^2 + 1$ and $|y'| \leq m$:

$$\frac{\sqrt{2m^2 + 1}(\sqrt{u} + 1/\sqrt{u})}{2} = 2m^2 + 1, \quad \frac{\sqrt{2m^2 + 1}(\sqrt{u} - 1/\sqrt{u})}{2\sqrt{4m^2 + 2}} = m.$$

Since $u > 1$, these equations are true if the squares of both sides are true, so we will check

$$u + 2 + \frac{1}{u} = 4(2m^2 + 1), \quad u - 2 + \frac{1}{u} = 8m^2.$$

Both equations are equivalent to $u^2 - (8m^2 + 2)u + 1 = 0$, and u is a root of $t^2 - (8m^2 + 2)t + 1$ by the quadratic formula. \square

Is there an infinite family of generalized Pell equations, including $x^2 - 103y^2 = 2$ as a special case, where the bounds on $|x'|$ and $|y'|$ in Theorem 3.3 are (infinitely) often the first solution in positive integers? Here is my only attempt at answering this. Let's think of 103 as $m^2 + 3$ for $m = 10$. In terms of this m , the minimal solution $(x, y) = (477, 47)$ has the form $(4m^2 + 7m + 7, 4m + 7)$, and it's straightforward to check

$$(4m^2 + 7m + 7)^2 - (m^2 + 3)(4m + 7)^2 = 8m^2 - 70m - 98,$$

so we can view $x^2 - 103y^2 = 2$ as the special case of $x^2 - (m^2 + 3)y^2 = 8m^2 - 70m - 98$ for $m = 10$. Check $8m^2 - 70m - 98 > 0$ if $m \geq 10$ ($8t^2 - 70t - 98$ has larger root 9.97...).

For $m = 10$ we are in Example 4.4, where the bounds on $|x'|$ and $|y'|$ in Theorem 3.3 for $x^2 - 103y^2 = 2$ are its first solution $(477, 47)$.

For $m = 11$, we have $m^2 + 3 = 124$, $8m^2 - 70m - 98 = 100$, and the fundamental unit of $\mathbf{Z}[\sqrt{124}]$ is $4620799 + 414960\sqrt{124}$, with norm 1. Using this unit as u , the bounds on $|x'|$ and $|y'|$ for $x^2 - 124y^2 = 100$ in Theorem 3.3 are $|x'| \leq 15200$ and $|y'| \leq 1365$, but $(15200, 1365)$ is not the smallest solution in positive integers: two smaller solutions are $(134, 12)$ and $(568, 51)$, with $(4m^2 + 7m + 7, 4m + 7) = (568, 51)$ when $m = 11$. (Of course there is also the solution $(x', y') = (10, 0)$.)

For $m = 12$, we have $m^2 + 3 = 147$, $8m^2 - 70m - 98 = 214$, and the fundamental unit of $\mathbf{Z}[\sqrt{147}] = \mathbf{Z}[7\sqrt{3}]$ is $97 + 8\sqrt{147}$, with norm 1. Using this unit as u , the bounds on $|x'|$ and $|y'|$ for $x^2 - 147y^2 = 214$ in Theorem 3.3 are $|x'| \leq 102.401\dots$ and $|y'| \leq 8.359\dots$ (not integers). The only positive integer solution of $x^2 - 147y^2 = 214$ in that range is $(x', y') = (19, 1)$, and the solution $(x', y') = (4m^2 + 7m + 7, 4m + 7) = (667, 55)$ is outside that range. So in short, this attempt at fitting $x^2 - 103y^2 = 2$ into a nice infinite family where the bounds in Theorem 3.3 are optimal appears to be a failure.

REFERENCES

- [1] W. W. Adams, L. J. Goldstein, "Introduction to Number Theory," Prentice-Hall, Englewood Cliffs, NJ, 1976.
- [2] P. L. Chebyshev, *Sur les formes quadratiques*, J. Math. Pures Appl. **16** (1851), 257–282. URL <https://eudml.org/doc/234874>.
- [3] G. Chrystal, "Algebra, an Elementary Text-Book, Part II" Adam and Charles Black, Edinburgh, 1889. URL <https://archive.org/details/algebraelemen08chrygoog/page/n7/mode/2up>.
- [4] L. Euler, "Elements of Algebra," Longman, Hurst, Rees, Orme and Co., London 1822. URL <https://archive.org/details/elementsalgebra00lagrgoog/mode/2up>.
- [5] D. Flath, "Introduction to Number Theory," Wiley-Interscience, New York, 1989.
- [6] P. Koymans and C. Pagano, *On Steinhilber's conjecture*, <https://arxiv.org/abs/2201.13424>.
- [7] J. L. Lagrange, *Solution d'un problème d'arithmétique*, Oeuvres de Lagrange, Tome I, Gauthier-Villars, Paris, 1867, 669–731. URL <https://archive.org/details/oeuvresdelagrang01lagr/page/668/mode/2up>.
- [8] J. L. Lagrange, *Sur la solution des problèmes indéterminés du second degré*, Oeuvres de Lagrange, Tome II, Gauthier-Villars, Paris, 1868, 377–535. URL <https://archive.org/details/uvresdelagrang09natiigoog/page/n389/mode/2up>.
- [9] J. E. Shockley, "Introduction to Number Theory," Holt, Rinehart and Winston, New York, 1967.