

PELL'S EQUATION, I

KEITH CONRAD

1. INTRODUCTION

For a positive integer d that is not a square, an equation of the form

$$x^2 - dy^2 = 1$$

is called *Pell's equation*. We are interested in x and y that are both integers, and the term “solution” will always mean an integral solution. The obvious solutions $(x, y) = (\pm 1, 0)$, are called the *trivial solutions*. They are the only solutions where $x = \pm 1$ or $y = 0$ (separately). Solutions where $x > 0$ and $y > 0$ will be called *positive solutions*. Every nontrivial solution can be made into a positive solution by changing the sign of x or y .

We don't consider the case when d is a square, since if $d = c^2$ with $c \in \mathbf{Z}$ then $x^2 - dy^2 = x^2 - (cy)^2$ and the only squares that differ by 1 are 0 and 1, so $x^2 - (cy)^2 = 1 \implies x = \pm 1$ and $y = 0$. Thus Pell's equation for square d only has trivial solutions.

In Section 2 we'll show how solutions to Pell's equation can be found. In Section 3 we'll discuss an elementary problem about polygonal numbers that is equivalent to a specific Pell equation. Section 4 describes how to create new solutions of Pell's equation if we know one nontrivial solution and in Section 5 we will see how all solutions can be generated from a minimal nontrivial solution. In the final Section 6 a generalized Pell equation is introduced, where the right side is not 1.

2. EXAMPLES OF SOLUTIONS

To find a nontrivial solution of $x^2 - dy^2 = 1$ by elementary methods, rewrite the equation as $x^2 = dy^2 + 1$ and then set $y = 1, 2, 3, \dots$ until you reach a value where $dy^2 + 1$ is a perfect square. Call that value x^2 and then we have a solution (x, y) .

Example 2.1. Two positive solutions of $x^2 - 2y^2 = 1$ are $(3, 2)$ and $(17, 12)$, since $2y^2 + 1$ is a square when $y = 2$ and 12, where it has values $9 = 3^2$ and $289 = 17^2$. See below.

| y | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|------------|---|---|----|----|----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|
| $2y^2 + 1$ | 3 | 9 | 19 | 33 | 51 | 73 | 99 | 129 | 163 | 201 | 243 | 289 | 339 | 393 | 451 |
| Square? | X | ✓ | X | X | X | X | X | X | X | X | X | ✓ | X | X | X |

Example 2.2. Three positive solutions of $x^2 - 3y^2 = 1$ are $(2, 1)$ and $(7, 4)$, and $(26, 15)$, as shown by the table below.

| y | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|------------|---|----|----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| $3y^2 + 1$ | 4 | 13 | 28 | 49 | 76 | 109 | 148 | 193 | 244 | 301 | 364 | 433 | 508 | 589 | 676 |
| Square? | ✓ | X | X | ✓ | X | X | X | X | X | X | X | X | X | X | ✓ |

The table below gives a positive solution to $x^2 - dy^2 = 1$ for nonsquare d from 2 to 24 where x and y are as small as possible.

| | | | | | | | | | | | | | | | | | | | | |
|-----|---|---|---|---|---|---|----|----|----|-----|----|----|----|----|-----|----|----|-----|----|----|
| d | 2 | 3 | 5 | 6 | 7 | 8 | 10 | 11 | 12 | 13 | 14 | 15 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| x | 3 | 2 | 9 | 5 | 8 | 3 | 19 | 10 | 7 | 649 | 15 | 4 | 33 | 17 | 170 | 9 | 55 | 197 | 24 | 5 |
| y | 2 | 1 | 4 | 2 | 3 | 1 | 6 | 3 | 2 | 180 | 4 | 1 | 8 | 4 | 39 | 2 | 12 | 42 | 5 | 1 |

The theorem suggested by such data is a hard result of Lagrange.

Theorem 2.3 (Lagrange, 1768). *For any positive integer d that is not a square, the equation $x^2 - dy^2 = 1$ has a nontrivial solution.*

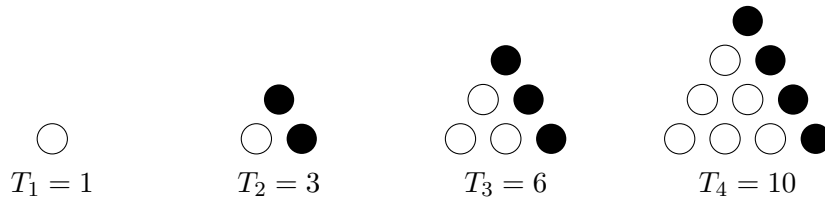
This theorem, which will be proved in Part II, is our hunting license to search for solutions by tabulating $dy^2 + 1$ until it takes a square value. We are guaranteed this search will eventually terminate, but we are not assured how long it will take. In fact, the smallest positive solution of $x^2 - dy^2 = 1$ can be unusually large compared to the size of d . The table above illustrates this if we compare the smallest positive solutions when $d = 12, 13,$ and 14 . As more extreme examples, see the smallest positive solutions below when $d = 61$ or 109 compared with nearby values of d .

| | | | | | | |
|-----|----|------------|----|------|-----------------|-----|
| d | 60 | 61 | 62 | 108 | 109 | 110 |
| x | 31 | 1766319049 | 63 | 1351 | 158070671986249 | 21 |
| y | 4 | 226153980 | 8 | 130 | 15140424455100 | 2 |

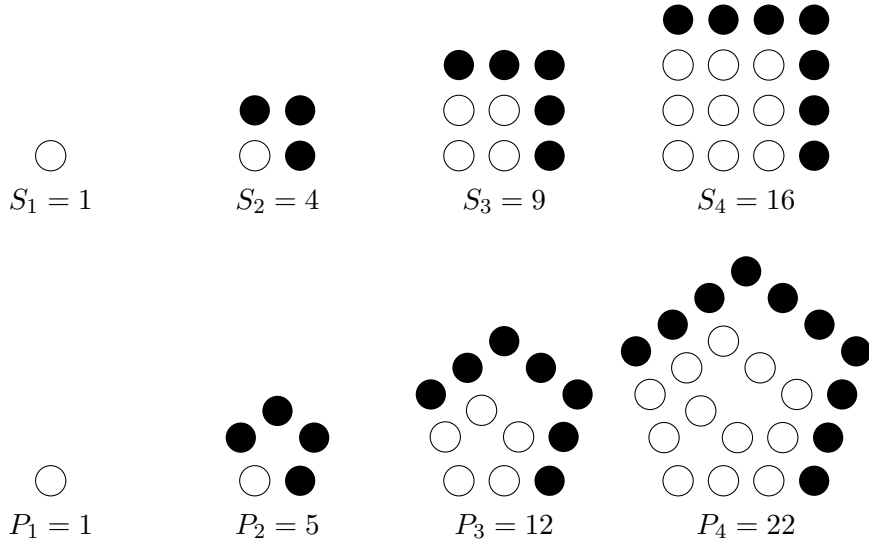
While Lagrange was the first person to give a proof that Pell's equation for general (nonsquare) d has a nontrivial solution, 100 years earlier Fermat claimed to have a proof and challenged other mathematicians in Europe to prove it. In one letter he wrote that anyone failing this task should at least try to find solutions to $x^2 - 61y^2 = 1$ and $x^2 - 109y^2 = 1$, where he said he chose small coefficients "pour ne vous donner pas trop de peine" (so you don't have too much work). He clearly was being mischievous. If Fermat had posed his challenge to mathematicians in India then he may have gotten a positive response: a nontrivial solution to $x^2 - 61y^2 = 1$ had already been known there for 500 years.

3. TRIANGULAR-SQUARE NUMBERS

A positive integer n is called *triangular* if n dots can be arranged to look like an equilateral triangle. The first four triangular numbers are 1 (a degenerate case), 3, 6, and 10. In the pictures below, the shading shows how each triangular number is built from the previous one by adding a new side.



For any $k \geq 3$, a *k-gonal number* is a positive integer n for which n dots can be arranged to look like a regular k -gon. The first four square and pentagonal numbers, corresponding to $k = 4$ and $k = 5$, are shown below. Both sequences start with 1 as a degenerate case.



A formula for the n th square number S_n is obvious: $S_n = n^2$. To get a formula for the n th triangular and pentagonal numbers, T_n and P_n , the first few values suggest how to write them as a sum of terms in an arithmetic progression (which are their real definitions):

$$T_n = 1 + 2 + \dots + n = \sum_{k=1}^n k, \quad P_n = 1 + 4 + \dots + (3n - 2) = \sum_{k=1}^n (3k - 2).$$

This works for square numbers too: $S_n = 1 + 3 + \dots + (2n - 1) = \sum_{k=1}^n (2k - 1)$ is n^2 . Using the formula for the sum of terms in an arithmetic progression,

$$T_n = \frac{n(n + 1)}{2} \quad \text{and} \quad P_n = \frac{n(3n - 1)}{2}.$$

With these formulas we fill in the table below of the first 10 triangular, square, and pentagonal numbers.

| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|-------|---|---|----|----|----|----|----|----|-----|-----|
| T_n | 1 | 3 | 6 | 10 | 15 | 21 | 28 | 36 | 45 | 55 |
| S_n | 1 | 4 | 9 | 16 | 25 | 36 | 49 | 64 | 81 | 100 |
| P_n | 1 | 5 | 12 | 22 | 35 | 51 | 70 | 92 | 117 | 145 |

Besides the common value 1, we see 36 is both triangular and square: $36 = T_8 = S_6$. Call a positive integer a *triangular-square number* if it is both T_m for some m and S_n for some n . Finding these numbers is the same as solving a particular Pell equation.

Theorem 3.1. *Triangular-square numbers correspond to solutions of $x^2 - 2y^2 = 1$ in positive integers x and y .*

Proof. Using the formulas for T_m and S_n ,

$$\begin{aligned} T_m = S_n &\iff \frac{m(m+1)}{2} = n^2 \\ &\iff m^2 + m = 2n^2 \\ &\iff \left(m + \frac{1}{2}\right)^2 - \frac{1}{4} = 2n^2 \\ &\iff (2m+1)^2 - 1 = 2(2n)^2 \\ &\iff (2m+1)^2 - 2(2n)^2 = 1. \end{aligned}$$

Because every step is reversible, finding triangular–square numbers is equivalent to solving $x^2 - 2y^2 = 1$ in positive integers x and y where $x = 2m + 1$ is odd and $y = 2n$ is even: $T_{(x-1)/2} = S_{y/2}$. (While we want $x = 2m + 1$ with $m \geq 1$, we can say $x > 0$ instead of $x \geq 3$ because the only solution of $x^2 - 2y^2 = 1$ with $x = 1$ has $y = 0$, which is not positive.)

Including the constraints that x is odd and y is even in the correspondence between triangular–square numbers and positive solutions of $x^2 - 2y^2 = 1$ is unnecessary because they are *forced* by the equation $x^2 - 2y^2 = 1$. Indeed, writing the equation as $x^2 = 2y^2 + 1$ shows x^2 is odd, so x is odd. Then $x = 2m + 1$ for some integer m , and feeding that into the Pell equation makes $4m^2 + 4m + 1 - 2y^2 = 1$, so $y^2 = 2m^2 + 2m$. Thus y^2 is even, so y is even. \square

Example 3.2. From the solutions $(x, y) = (3, 2)$ and $(17, 12)$ of $x^2 - 2y^2 = 1$ we get the triangular–square numbers $T_1 = S_1 = 1$ and $T_8 = S_6 = 36$ by writing $x = 2m + 1$ and $y = 2n$ in each case to find m and n .

As practice with the ideas in the proof of Theorem 3.1, show that finding square–pentagonal numbers, which are numbers of the form S_m and P_n for some positive integers m and n , is the same as solving $x^2 - 6y^2 = 1$ in positive integers where x is one less than a multiple of 6. The first three positive solutions of $x^2 - 6y^2 = 1$ are $(5, 2)$, $(49, 20)$, $(485, 198)$, and only the first and third have x one less than a multiple of 6; they lead to the square–pentagonal numbers $1 = S_1 = P_1$ and $9801 = S_{99} = P_{81}$ if you work out the details.

4. NEW SOLUTIONS FROM OLD SOLUTIONS

We found in Section 2, by making a table, that two solutions of $x^2 - 2y^2 = 1$ are $(3, 2)$ and $(17, 12)$. They are closely related when we convert the pair (x, y) into the number $x + y\sqrt{2}$:

$$(4.1) \quad 17 + 12\sqrt{2} = (3 + 2\sqrt{2})^2.$$

Let's raise $3 + 2\sqrt{2}$ to a few powers beyond the second:

$$(4.2) \quad (3 + 2\sqrt{2})^3 = 99 + 70\sqrt{2}, \quad (3 + 2\sqrt{2})^4 = 577 + 408\sqrt{2}, \quad (3 + 2\sqrt{2})^5 = 3363 + 2378\sqrt{2}.$$

The coefficient pairs $(99, 70)$, $(577, 408)$, and $(3363, 2378)$ are all solutions to $x^2 - 2y^2 = 1$.

Similarly, we previously found three solutions of $x^2 - 3y^2 = 1$: $(2, 1)$, $(7, 4)$, and $(26, 15)$. When we convert the pair (x, y) into the number $x + y\sqrt{3}$ we have

$$(4.3) \quad 7 + 4\sqrt{3} = (2 + \sqrt{3})^2 \quad \text{and} \quad 26 + 15\sqrt{3} = (2 + \sqrt{3})^3.$$

The key to solving $x^2 - dy^2 = 1$ in \mathbf{Z} is to study numbers of the form $x + y\sqrt{d}$ where $x, y \in \mathbf{Z}$. Such numbers are *closed under multiplication*:

$$(4.4) \quad (x + y\sqrt{d})(x' + y'\sqrt{d}) = (xx' + dy'y') + (xy' + yx')\sqrt{d}$$

and $xx' + dyy'$ and $xy' + yx'$ are both integers.¹ This formula is similar to the rule for multiplying complex numbers: $(x + yi)(x' + y'i) = (xx' - yy') + (xy' + yx')i$, which is the case $d = -1$ (for Pell's equation we are taking $d > 0$).

Just as a complex number $x + yi$ has a real part x and an imaginary part y , a number $x + y\sqrt{d}$ with $x, y \in \mathbf{Z}$ has coefficients x and y . The coefficients of such a number are unique: if $x + y\sqrt{d} = x' + y'\sqrt{d}$ with $x, y, x', y' \in \mathbf{Z}$ then $x = x'$ and $y = y'$. Indeed, if $y \neq y'$ then $\sqrt{d} = (x - x')/(y' - y)$ is rational, which is a contradiction (nonsquare integers have irrational square roots). Thus $y = y'$, so $x + y\sqrt{d} = x' + y\sqrt{d}$, which implies $x = x'$.

Theorem 4.1. *If $X^2 - dY^2 = 1$ has solutions (x, y) and (x', y') then the coefficients of $(x + y\sqrt{d})(x' + y'\sqrt{d})$ are also a solution.*

Proof. Using the coefficients from (4.4) we compute

$$\begin{aligned} (xx + dyy')^2 - d(xy' + yx')^2 &= (x^2x'^2 + 2dxx'y'y' + d^2y^2y'^2) - d(x^2y'^2 + 2xx'y'y' + y^2x'^2) \\ &= x^2x'^2 + d^2y^2y'^2 - dx^2y'^2 - dy^2x'^2 \\ &= x^2(x'^2 - dy'^2) - dy^2(x'^2 - dy'^2) \\ &= x^2 - dy^2 \\ &= 1. \end{aligned}$$

□

Corollary 4.2. *If $X^2 - dY^2 = 1$ has a solution (x, y) then the coefficients of $(x + y\sqrt{d})^n$ are also a solution for all $n \in \mathbf{Z}$. In particular, this Pell equation has infinitely many solutions if it has a nontrivial solution.*

Proof. The coefficients of $(x + y\sqrt{d})^n$ are solutions for $n \geq 1$ by repeated multiplication using Theorem 4.1. If $(x, y) \neq (\pm 1, 0)$ then $x + y\sqrt{d} \neq \pm 1$, so the powers $(x + y\sqrt{d})^n$ for $n \geq 1$ are distinct and give us infinitely many solutions of $X^2 - dY^2 = 1$.

To show the coefficients of $(x + y\sqrt{d})^n$ are solutions for $n < 0$, write $n = -N$ and set $(x + y\sqrt{d})^N = x_N + y_N\sqrt{d}$ with $x_N, y_N \in \mathbf{Z}$. Then $x_N^2 - dy_N^2 = 1$, so

$$\begin{aligned} (x + y\sqrt{d})^{-N} &= \frac{1}{(x + y\sqrt{d})^N} \\ &= \frac{1}{x_N + y_N\sqrt{d}} \\ &= \frac{x_N - y_N\sqrt{d}}{(x_N + y_N\sqrt{d})(x_N - y_N\sqrt{d})} \\ &= \frac{x_N - y_N\sqrt{d}}{x_N^2 - dy_N^2} \\ &= x_N - y_N\sqrt{d} \end{aligned}$$

and $(x_N, -y_N)$ is a solution. Finally, the coefficients of $(x + y\sqrt{d})^0$ are $(1, 0)$. □

Example 4.3. Since $(3 + 2\sqrt{2})^4 = 577 + 408\sqrt{2}$, we have $(3 + 2\sqrt{2})^{-4} = 577 - 408\sqrt{2}$.

If we were not dealing with solutions of Pell's equation, negative powers would not have integer coefficients. *e.g.*, $(5 + 2\sqrt{2})^{-1} = 5/17 - (2/17)\sqrt{2}$.

¹If we use a cube root instead of a square root, such sums would not be closed under multiplication, *e.g.*, $(1 + \sqrt[3]{2})(1 - \sqrt[3]{2}) = 1 - \sqrt[3]{4} \neq x + y\sqrt[3]{2}$ for any x and y in \mathbf{Z} .

5. ALL SOLUTIONS TO A PELL EQUATION

We will describe all solutions to $x^2 - dy^2 = 1$ using inequalities on numbers $x + y\sqrt{d}$. Comparing the size of such numbers is not generally the same as comparing coefficients: $x + y\sqrt{d} < x' + y'\sqrt{d}$ is not the same as $x < x'$ and $y < y'$. Consider $1 + 2\sqrt{2} < 7 - \sqrt{2}$. But for Pell solutions, under a mild condition it is the same!

Lemma 5.1. *If $x^2 - dy^2 = 1$ and $x + y\sqrt{d} > 1$ then $x > 1$ and $y > 0$.*

Proof. The crucial point is that $1/(x + y\sqrt{d}) = x - y\sqrt{d}$ when $x^2 - dy^2 = 1$. Therefore

$$x + y\sqrt{d} > 1 > x - y\sqrt{d} > 0.$$

From $x + y\sqrt{d} > x - y\sqrt{d}$ we get $2y\sqrt{d} > 0$, so $y > 0$. Then $y \geq 1$ since y is an integer, so $x > y\sqrt{d} \geq \sqrt{d} > 1$. \square

Without the hypothesis $x^2 - dy^2 = 1$ in Lemma 5.1 its conclusion does not follow. For instance, $5 - \sqrt{2} > 1$ and $-2 + 3\sqrt{2} > 1$.

Lemma 5.2. *Suppose $x^2 - dy^2 = 1$ and $a^2 - db^2 = 1$ where $a, b \geq 0$. Then*

$$a + b\sqrt{d} < x + y\sqrt{d} \iff a < x \text{ and } b < y.$$

Proof. The implication (\Leftarrow) is obvious. To prove (\Rightarrow) , we have $a \geq 1$ since no Pell solution has $a = 0$, so $x + y\sqrt{d} > 1$ and therefore x and y are positive by Lemma 5.1. Reciprocating the inequality

$$a + b\sqrt{d} < x + y\sqrt{d}$$

we get

$$x - y\sqrt{d} < a - b\sqrt{d}$$

and adding these gives

$$(a + x) + (b - y)\sqrt{d} < (a + x) + (y - b)\sqrt{d}.$$

Therefore $b - y < y - b$, so $b < y$. Then $a^2 = 1 + db^2 < 1 + dy^2 = x^2$, so $a < x$ from positivity. \square

Theorem 5.3. *Let (x_1, y_1) be the positive solution to $x^2 - dy^2 = 1$ with y_1 as small as possible. The solutions to $x^2 - dy^2 = 1$, up to sign, are all generated from (x_1, y_1) by taking powers of $x_1 + y_1\sqrt{d}$:*

$$x + y\sqrt{d} = \pm(x_1 + y_1\sqrt{d})^n$$

for some $n \in \mathbf{Z}$ and some sign.

Proof. By Corollary 4.2 the coefficients of $(x_1 + y_1\sqrt{d})^n$ satisfy $x^2 - dy^2 = 1$ for every $n \in \mathbf{Z}$, and clearly this is also true for coefficients of $-(x_1 + y_1\sqrt{d})^n$.

Conversely, suppose $x^2 - dy^2 = 1$. If x and y are positive integers we'll show $x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ for some $n \geq 1$. Since $x + y\sqrt{d} > 1$ and the numbers $(x_1 + y_1\sqrt{d})^n$ for $n = 0, 1, 2, \dots$ form an increasing sequence that starts at 1 and tends to ∞ , $x + y\sqrt{d}$ lies between two of these powers:

$$(5.1) \quad (x_1 + y_1\sqrt{d})^n \leq x + y\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}$$

for some $n \geq 0$. Dividing through (5.1) by $(x_1 + y_1\sqrt{d})^n$,

$$1 \leq (x + y\sqrt{d})(x_1 + y_1\sqrt{d})^{-n} < x_1 + y_1\sqrt{d}.$$

The number in the middle is $(x + y\sqrt{d})(x_1 - y_1\sqrt{d})^n$, which is a Pell solution since Pell solutions are closed under multiplication (Theorem 4.1). Write it as $a + b\sqrt{d}$, so

$$(5.2) \quad 1 \leq a + b\sqrt{d} < x_1 + y_1\sqrt{d}.$$

If $1 < a + b\sqrt{d}$ then a and b are positive by Lemma 5.1, so $b < y_1$ by Lemma 5.2. This contradicts the minimality of y_1 among positive solutions, so $1 = a + b\sqrt{d}$, which implies $x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^n$. Since (x, y) is nontrivial n is not 0, so $n \geq 1$.

If (x, y) is a nontrivial solution to Pell's equation and x and y are not both positive then one of the three numbers

$$-x - y\sqrt{d} = -(x + y\sqrt{d}), \quad x - y\sqrt{d} = \frac{1}{x + y\sqrt{d}}, \quad -x + y\sqrt{d} = \frac{-1}{x + y\sqrt{d}}.$$

has both coefficients positive, so $\pm(x + y\sqrt{d})^{\pm 1} = (x_1 + y_1\sqrt{d})^N$ for $N \geq 1$ and some choices of signs on the left side. Therefore $x + y\sqrt{d} = \pm(x_1 + y_1\sqrt{d})^{\pm N}$. The trivial solutions also arise in this way using $N = 0$. □

Remark 5.4. The geometric meaning of the sign changes on x and y at the end of the proof is to replace a number $\alpha = x + y\sqrt{d}$ with one of $-\alpha, 1/\alpha$, or $-1/\alpha$. When $\alpha \neq \pm 1$ exactly one of $\alpha, -\alpha, 1/\alpha$, or $-1/\alpha$ will be greater than 1, and we're selecting the choice that's greater than 1 so its coefficients are a positive Pell solution.

Example 5.5. The positive solution of $x^2 - 2y^2 = 1$ with least y -value is $(3, 2)$, so every positive solution comes from coefficients of $(3 + 2\sqrt{2})^n$ for $n \geq 1$.

Example 5.6. The positive solution of $x^2 - 3y^2 = 1$ with least y -value is $(2, 1)$, so the positive solutions are the coefficients of $(2 + \sqrt{3})^n$ for $n \geq 1$.

Example 5.7. The positive solution of $x^2 - 5y^2 = 1$ with least y -value is $(9, 4)$, so every positive solution comes from coefficients of $(9 + 4\sqrt{5})^n$ for $n \geq 1$.

6. GENERALIZED PELL EQUATIONS

The equation $x^2 - dy^2 = n$ where n is a nonzero integer is a *generalized Pell equation*. The special case $x^2 - dy^2 = -1$ is called a *negative Pell equation*. To find a solution (in \mathbf{Z}) rewrite the equation as $x^2 = dy^2 + n$ and compute the right side for $y = 1, 2, \dots$ until it's a square.

In the tables below we try to solve $x^2 - 2y^2 = -1$ and $x^2 - 3y^2 = -1$. For $1 \leq y \leq 15$ two solutions are found for the first equation, $(1, 1)$ and $(7, 5)$, and none for the second.

| | | | | | | | | | | | | | | | |
|------------|---|---|----|----|----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|
| y | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| $2y^2 - 1$ | 1 | 7 | 17 | 31 | 49 | 71 | 97 | 127 | 161 | 199 | 241 | 287 | 337 | 391 | 449 |
| Square? | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

| | | | | | | | | | | | | | | | |
|------------|---|----|----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| y | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| $3y^2 - 1$ | 2 | 11 | 26 | 47 | 74 | 107 | 146 | 191 | 242 | 299 | 362 | 431 | 506 | 587 | 674 |
| Square? | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

A longer search in the second case would be fruitless: $x^2 - 3y^2 = -1$ has no integral solutions. To prove some generalized Pell equation like $x^2 - 3y^2 = -1$ has no solution, an argument by contradiction using modular arithmetic often works.

Example 6.1. If integers x and y satisfy $x^2 - 3y^2 = -1$ then reduce both sides mod 3 to get $x^2 \equiv -1 \pmod{3}$. This congruence has no solution: the only squares mod 3 are 0 and 1. Thus $x^2 - 3y^2 = -1$ has no solution (in \mathbf{Z}).

Example 6.2. The equation $x^2 - 5y^2 = 2$ has no integral solution because reducing the equation mod 5 makes it $x^2 \equiv 2 \pmod{5}$, which has no solution. By the same idea, the generalized Pell equations $x^2 - 5y^2 = 3$ and $x^2 - 5y^2 = 7$ have no solutions.

Example 6.3. The equation $x^2 - 5y^2 = 6$ has no solution, but we can't prove this by reducing both sides mod 5 to get $x^2 \equiv 6 \pmod{5}$, since that congruence *has* a solution so there is no contradiction. Reduce mod 3 instead: the equation becomes $x^2 - 5y^2 \equiv 0 \pmod{3}$, or $x^2 \equiv 5y^2 \equiv 2y^2 \pmod{3}$. This too has a solution, namely $(0, 0)$, so it doesn't seem like progress has been made. But this is progress because $(0, 0)$ is the *only* solution mod 3, since the squares mod 3 are 0 and 1, and the only way one of these is twice the other mod 3 is when they're both 0. Therefore if $x^2 - 5y^2 = 6$ in \mathbf{Z} then x and y are both multiples of 3. That makes the left side a multiple of 9, which contradicts the right side being 6.

We used modular arithmetic here (reducing mod 3), but in a more subtle way than in the previous two examples.

Here is a problem about sums of squares whose solution is equivalent to solving a particular generalized Pell equation.

Theorem 6.4. *Finding positive integers a and b satisfying*

$$(6.1) \quad a^2 + (a + 1)^2 = b^2 + (b + 1)^2 + (b + 2)^2$$

is the same as solving $x^2 - 6y^2 = 3$ in positive integers x and y other than $(3, 1)$.

Proof. Expanding the squares and combining like terms,

$$\begin{aligned} a^2 + (a + 1)^2 = b^2 + (b + 1)^2 + (b + 2)^2 &\iff 2a^2 + 2a + 1 = 3b^2 + 6b + 5 \\ &\iff 2(a^2 + a) = 3(b^2 + 2b) + 4 \\ &\iff 2 \left(\left(a + \frac{1}{2} \right)^2 - \frac{1}{4} \right) = 3((b + 1)^2 - 1) + 4 \\ &\iff ((2a + 1)^2 - 1) = 6((b + 1)^2 - 1) + 8 \\ &\iff (2a + 1)^2 - 6(b + 1)^2 = 3. \end{aligned}$$

All steps are reversible, so solving the original equation with $a, b \geq 1$ is equivalent to solving $x^2 - 6y^2 = 3$ with odd $x \geq 3$ and any $y \geq 2$. Requiring x to be odd can be dropped since it is forced by the equation $x^2 - 6y^2 = 3$: the number $x^2 = 6y^2 + 3$ must be odd, so x must be odd. \square

For a Pell equation $x^2 - dy^2 = 1$, multiplying two known solutions as numbers $x + y\sqrt{d}$ leads to a third solution (Theorem 4.1). For a generalized Pell equation $x^2 - dy^2 = n$, multiplying a known solution *with a solution of the Pell equation $x^2 - dy^2 = 1$* leads to a new solution of $x^2 - dy^2 = n$. The proof is like that of Theorem 4.1. Details are left to the reader.

Example 6.5. One solution of $x^2 - 6y^2 = 3$ is $(3, 1)$. A nontrivial solution of $x^2 - 6y^2 = 1$ is $(5, 2)$. Therefore a second solution of $x^2 - 6y^2 = 3$ comes from the coefficients of

$$(3 + \sqrt{6})(5 + 2\sqrt{6}) = 27 + 11\sqrt{6}.$$

Check $27^2 - 6 \cdot 11^2 = 3$. In the context of Theorem 6.4 the solution $(27, 11)$ of $x^2 - 6y^2 = 3$ leads to a solution of (6.1): $2a + 1 = 27 \Rightarrow a = 13$ and $b + 1 = 11 \Rightarrow b = 10$, so $13^2 + 14^2 = 10^2 + 11^2 + 12^2$. This is more attractive if we swap the two sides: $10^2 + 11^2 + 12^2 = 13^2 + 14^2$.

As an application of math to art, consider the painting in Figure 1 by Bogdanov-Belsky, where the children have to calculate $(10^2 + 11^2 + 12^2 + 13^2 + 14^2)/365$ in their heads. If they knew $10^2 + 11^2 + 12^2 = 13^2 + 14^2$, they could find the numerator as $2(13^2 + 14^2)$, so only two squares would have to be computed instead of five. Since $2(13^2 + 14^2) = 2(169 + 196) = 2(365)$, dividing by 365 shows the fraction is 2.



FIGURE 1. Bogdanov-Belsky's *Mental Calculation* (1895)

The bold artistic details on the blackboard and knowledge of the period when the painting was produced help us find the deeper meaning of this work of art: it is advocating for the inclusion of generalized Pell equations in the math curriculum of 19th century peasants.