Pell's Equation

M.Xu mi KS

1 Introduction

In 1657, Pierre de Fermat challenged English mathematicians to find whole-number solutions to equations such as $x^2 - 61y^2 = 1$. The smallest solution turns out to be $x = 1766319049$ and $y = 226153980$, which the Indian mathematician Bhāskara II had already found in the 12th century. Equations like this are named after the English mathematician John Pell, but only because Leonhard Euler mistakenly credited Pell with a solution found by William Brouncker.

The standard Pell's equation is any Diophantine equation generally written in the form:

$$x^2 - ny^2 = 1, \tag{1}$$

where n is a positive non-square integer, and we are interested in pairs of integer solutions (x, y). We can also generalise the standard equation (1) by replacing 1 on the right-hand side with any other integer $t \neq 1$, i.e.,

$$x^2 - ny^2 = t. \tag{2}$$

The obvious solutions to equation (1) are $(x, y) = (\pm 1, 0)$, and these are called the trivial solutions. In this article we will show that, given one non-trivial solution, a standard Pell's equation (1) has infinitely many different solutions, and illustrate the method to find all its solutions; we then discuss some interesting properties of those solutions.

2 Why n Must Be Non-Square

As stated previously, n must be non-square. If n is a non-zero square number, e.g., $n = m^2 > 0$ with $m \in \mathbb{Z}^+$, then $x^2 - ny^2 = x^2 - (my)^2$, and the only pair of squares which differ by 1 are 0 and 1, so $x^2 - (my)^2 = 1 \implies x = \pm 1$ and $y = 0$, yielding only the trivial solutions.

Since only x^2 and y^2 appear in Pell's equations, changing the sign of x, of y, or of both does not affect the equation. Therefore every integer solution (x, y) has three corresponding solutions $(x, -y)$, $(-x, y)$ and $(-x, -y)$, and our study can be focused on solutions where x and y are both positive integers, which are called non-trivial solutions.

3 New Solutions from Old

Given the example equation $x^2 - 2y^2 = 1$, two positive solutions are $(3, 2)$ and $(17, 12)$, since $2y^2 + 1$ is a square when $y = 2$ and $y = 12$, where $2y^2 + 1 = 9 = 3^2$ and $2y^2 + 1 = 289 = 17^2$.

y	1	2	3	4	5	6	7	8	9	10	11	12
$2y^2 + 1$	3	9	19	33	51	73	99	129	163	201	243	289
Square?	×	✓	×	×	×	×	×	×	×	×	×	✓

As another example, the equation $x^2 - 3y^2 = 1$ has positive solutions $(2, 1)$, $(7, 4)$, $(26, 15)$, etc.

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?	✓	×	×	✓	×	×	×	×	×	×	×	×	×	×	✓

Joseph Louis Lagrange proved that, as long as n is not a perfect square, the standard Pell's equation (1) has infinitely many distinct integer solutions. Searching by trial, as above, quickly becomes impractical, but there is a much better way to find new solutions.

Let (a, b) and (c, d) be two, not necessarily different, non-trivial solutions to a standard Pell's equation, that is, $a^2 - nb^2 = c^2 - nd^2 = 1$. We multiply them, and obtain

$$\begin{aligned} 1 &= (a^2 - nb^2)(c^2 - nd^2) \\ &= a^2c^2 + n^2b^2d^2 - na^2d^2 - nb^2c^2 \\ &= [(ac + nbd)^2 - 2nabcd] - [n(ad + bc)^2 - 2nabcd] \\ &= (ac + nbd)^2 - n(ad + bc)^2. \end{aligned}$$

This identity was first discovered by the Indian mathematician Brahmagupta around 628 AD. It gives us a new solution $(ac+nbd,\ ad+bc)$, since, as $a, b, c, d \in \mathbb{Z}^+$, we have $ac+nbd > a$, $ad+bc > b$, $ac+nbd > c$ and $ad+bc > d$. Notice that if either of the two solutions is the trivial solution instead, say $(a, b) = (1, 0)$, then $(ac + nbd,\ ad + bc) = (c, d)$, so we do not obtain a new solution. Repeating this process allows us to keep finding new solutions from existing old solutions. So, given just one non-trivial solution, we can generate infinitely many other distinct non-trivial solutions.

4 The Fundamental Solution

The fundamental solution is the minimal solution among all non-trivial solutions to a standard Pell's equation (1), meaning the solution with the smallest positive y (or, equivalently, the smallest positive x). A rigorous proof of the existence of the fundamental solution to any standard Pell's equation is not in the scope of this article. We can demonstrate some examples here, however.

The table below shows fundamental solutions to (1) for non-square n from 2 to 15:

n	2	3	5	6	7	8	10	11	12	13	14	15
x	3	2	9	5	8	3	19	10	7	649	15	4
y	2	1	4	2	3	1	6	3	2	180	4	1

The fundamental solutions to standard Pell's equations may appear random. Sometimes they may be quite large even for a small n, as in some of the examples in the table below:

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

5 Finding All Solutions

We can obtain **all** solutions to (1) from the fundamental solution. A rigorous proof that **all** solutions can be found this way relies on the minimality of the fundamental solution, and is beyond the scope of this article. Here we shall demonstrate how we obtain all solutions from the fundamental solution.

5.1 Iterative Formulas

If (u, v) is the fundamental solution, i.e., (u, v) is the minimal positive integer pair satisfying $u^2 - nv^2 = 1$, then

$$\begin{cases} x = u^2 + nv^2 \\ y = 2uv \end{cases} \rightarrow \begin{cases} x' = ux + nvy \\ y' = vx + uy \end{cases} \rightarrow \begin{cases} x'' = ux' + nvy' \\ y'' = vx' + uy' \end{cases}, \ \ldots$$

will give us all pairs of ever-increasing solutions (u, v), (x, y), (x', y'), (x'', y''), ... For example, for $x^2 - 2y^2 = 1$ with fundamental solution $(u, v) = (3, 2)$, the first step gives $(x, y) = (9+8,\ 12) = (17, 12)$, and the next gives $(x', y') = (3 \cdot 17 + 2 \cdot 2 \cdot 12,\ 2 \cdot 17 + 3 \cdot 12) = (99, 70)$, matching the solutions found by trial in Section 3.

In fact all non-trivial solutions can be obtained in this iterative way. We shall rewrite the simultaneous recurrence formulas as:

$$x_{k+1} = ux_k + nvy_k, \tag{3}$$

$$y_{k+1} = vx_k + uy_k, \tag{4}$$

where $k \in \mathbb{Z}^+$ and $(x_1, y_1) = (u, v)$. Sometimes we may extend the subscript k down to 0 to include the trivial solution $(x_0, y_0) = (1, 0)$.

The two simultaneous first-order linear recurrence formulas above can be rewritten as two separate second-order linear recurrence relations, in the sense that the sequences $\{x_k\}$ and $\{y_k\}$ appear decoupled. For $\{x_k\}$:

$$\begin{aligned} x_{k+2} &= ux_{k+1} + nvy_{k+1} \\ &= ux_{k+1} + nv(vx_k + uy_k) \\ &= ux_{k+1} + nv(vx_k + u(x_{k+1} - ux_k)/(nv)) \\ &= 2ux_{k+1} - (u^2 - nv^2)x_k \\ &= 2ux_{k+1} - x_k. \end{aligned}$$

Similarly, for $\{y_k\}$, substituting $x_k = (y_{k+1} - uy_k)/v$ from (4) gives $y_{k+2} = 2uy_{k+1} - y_k$. These formulas may be useful in situations where our interest is solely in one of the two sequences.

5.2 Closed-Form Formulas

In some other situations it may be more convenient to calculate solutions in closed form instead of using the iterative formulas above. This can be derived either from the two separate second-order recurrence formulas above, or from the simultaneous first-order recurrence relation. Here we show a quick way from the latter.

Adding $\sqrt{n}$ times (4) to (3):

$$\begin{aligned} x_{k+1} + \sqrt{n}y_{k+1} &= ux_k + nvy_k + \sqrt{n}vx_k + \sqrt{n}uy_k \\ &= (u + \sqrt{n}v)x_k + (\sqrt{n}u + nv)y_k \\ &= (u + \sqrt{n}v)(x_k + \sqrt{n}y_k). \end{aligned}$$

If we treat $x_k + \sqrt{n}y_k$ as a new sequence (of real numbers rather than only integers), then it is a geometric sequence with ratio $u + \sqrt{n}v$ and first term $u + \sqrt{n}v$. Therefore,

$$x_k + \sqrt{n}y_k = (u + \sqrt{n}v)^k. \tag{5}$$

Subtracting $\sqrt{n}$ times (4) from (3):

$$\begin{aligned} x_{k+1} - \sqrt{n}y_{k+1} &= ux_k + nvy_k - \sqrt{n}vx_k - \sqrt{n}uy_k \\ &= (u - \sqrt{n}v)(x_k - \sqrt{n}y_k). \end{aligned}$$

Again, we have another geometric sequence $x_k - \sqrt{n}y_k$ with ratio $u - \sqrt{n}v$ and first term $u - \sqrt{n}v$. So,

$$x_k - \sqrt{n}y_k = (u - \sqrt{n}v)^k. \tag{6}$$

The closed-form formulas for x_k and y_k can be obtained by adding and subtracting (5) and (6), then dividing by 2 and by $2\sqrt{n}$ respectively:

$$x_k = \frac{(u + \sqrt{n}v)^k + (u - \sqrt{n}v)^k}{2}, \tag{7}$$

$$y_k = \frac{(u + \sqrt{n}v)^k - (u - \sqrt{n}v)^k}{2\sqrt{n}}. \tag{8}$$

5.3 Properties of the Closed-Form Formulas

Note that although there is an irrational number $\sqrt{n}$ in the closed-form formulas (7) and (8), it can be proved through mathematical induction that (x_k, y_k) is always a pair of positive integers. In addition, we start with $k \in \mathbb{Z}^+$, but we can obtain the trivial solution $(x_0, y_0) = (1, 0)$ by setting $k = 0$. It can be seen that $(x_1, y_1) = (u, v)$ is the fundamental solution. If k is a negative integer instead, it can be seen that $x_{-k} = x_k$ and $y_{-k} = -y_k$, which is still a pair of integers satisfying the standard Pell's equation (1), only with a negative y value. Combined with the sign changes from Section 2, these formulas actually give **all** the solutions to a standard Pell's equation: every solution is $\pm(x_k, y_k)$ for some $k \in \mathbb{Z}$.

The term $u + \sqrt{n}v > 1$ as $u, v \in \mathbb{Z}^+$, and this also implies that $0 < u - \sqrt{n}v < 1$, because $u^2 - nv^2 = 1 \iff (u + \sqrt{n}v)(u - \sqrt{n}v) = 1$. Therefore, as k increases, both elements of the solution pair (x_k, y_k) grow exponentially. That is, for sufficiently large k:

$$x_k \approx \frac{(u + \sqrt{n}v)^k}{2} \qquad \text{and} \qquad y_k \approx \frac{(u + \sqrt{n}v)^k}{2\sqrt{n}}.$$

6 Approximating $\sqrt{n}$

From (7) and (8) we can also derive a method to approximate the irrational number $\sqrt{n}$ with rational numbers. In fact, we can approximate it with the sequences $\{x_k\}$ and $\{y_k\}$ to any precision required. Dividing (7) by (8):

$$\begin{aligned}\sqrt{n} \approx \frac{x_k}{y_k} &= \sqrt{n} \times \frac{(u+\sqrt{n}v)^k + (u-\sqrt{n}v)^k}{(u+\sqrt{n}v)^k - (u-\sqrt{n}v)^k} \\ &= \sqrt{n} \times \frac{((u+\sqrt{n}v)^k + (u-\sqrt{n}v)^k) \times (u-\sqrt{n}v)^k}{((u+\sqrt{n}v)^k - (u-\sqrt{n}v)^k) \times (u-\sqrt{n}v)^k} \\ &= \sqrt{n} \times \frac{1 + (u-\sqrt{n}v)^{2k}}{1 - (u-\sqrt{n}v)^{2k}}.\end{aligned}$$

Clearly, $(u-\sqrt{n}v)^{2k} \to 0$ as $k \to +\infty$. That means $\sqrt{n} = \lim_{k\to+\infty} x_k/y_k$. Here is an example of using solutions to the standard Pell's equation $x^2 - 2y^2 = 1$ to approximate $\sqrt{2}$:

k	(x_k, y_k)	x_k/y_k	Decimal	Error
1	$(3, 2)$	$3/2$	1.500000000	8.58×10^{-2}
2	$(17, 12)$	$17/12$	1.416666667	2.45×10^{-3}
3	$(99, 70)$	$99/70$	1.414285714	7.22×10^{-5}
4	$(577, 408)$	$577/408$	1.414215686	2.12×10^{-6}
5	$(3363, 2378)$	$3363/2378$	1.414213625	6.25×10^{-8}

In fact, the fractions x_k/y_k are among the best possible rational approximations to $\sqrt{n}$: they appear among the convergents of the continued fraction of $\sqrt{n}$, which is also how fundamental solutions are usually found in practice.

7 Conclusion

Although this article has explored methods for finding all integer solutions to Pell's equation, and their interesting properties, there remains much more to investigate. For example, a generalised Pell's equation (2) may have no integer solutions at all, or it may have several distinct families of solutions, each combining a particular solution to (2) with the infinitely many solutions to its corresponding standard Pell's equation (1). Why, and how? For another example, Lagrange's proof that every standard Pell's equation has a minimal non-trivial solution (in other words, the existence of the fundamental solution), alongside the use of continued fractions to find these fundamental solutions, offers further fascinating insights into the mathematics behind these equations.

References

Bradley, C. J. *Introduction to Number Theory.* United Kingdom Mathematics Trust, 2010.

Conrad, Keith. "Pell's Equation, I." *University of Connecticut.* `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn1.pdf`.

"Pell's Equation." *Wikipedia*, Wikimedia Foundation. `https://en.wikipedia.org/wiki/Pell%27s_equation`.

"Pell's Equation and Its Importance." *Mathematics Stack Exchange.* `https://math.stackexchange.com/questions/583055/pells-equation-and-its-importance`.