Solving Pell's equations

Dave Neary

May 2021

1 Pell's equations

Pell's equations are equations with integer solutions of the form:

$$a^2 - mb^2 = 1$$

Surprisingly, solutions to this equation are closed under multiplication:

$$\begin{aligned}
(a^2 - mb^2)(c^2 - md^2) &= 1 && \text{\# 1 times 1 is 1} \\
a^2c^2 - mb^2c^2 - ma^2d^2 + m^2b^2d^2 &= 1 && \text{\# Expand product} \\
(a^2c^2 + m^2b^2d^2) - m(b^2c^2 + a^2d^2) &= 1 && \text{\# Regrouping terms} \\
(a^2c^2 + 2mabcd + m^2b^2d^2) - m(b^2c^2 + 2abcd + a^2d^2) &= 1 && \text{\# Add/subtract } 2mabcd \\
(ac + mbd)^2 - m(bc + ad)^2 &= 1 && \text{\# Rewriting terms as squares}
\end{aligned}$$

So given any integer solution to the equation, we can multiply that solution by itself to give another solution of the same form. If we have at least one solution, these equations **always** have an infinite number of solutions for $m \in \mathbb{N}$.

It is easy to see that if $m = k^2$ then any solution gives $a^2 - (kb)^2 = (a - kb)(a + kb) = 1$ which has only one solution in integers, $a = 1, b = 0$, since the difference between two distinct squares is always bigger than 1 otherwise.

For example, with $m = 3$:

$$\begin{aligned}
2^2 - 3 \cdot 1^2 &= 1 && \text{\# Base solution} \\
(2^2 - 3 \cdot 1^2)^2 = 7^2 - 3 \cdot 4^2 &= 1 && \text{\# Second solution} \\
(2^2 - 3 \cdot 1^2)^3 &= (7^2 - 3 \cdot 4^2)(2^2 - 3 \cdot 1^2) \\
&= 26^2 - 3 \cdot 15^2 = 1 && \text{\# Third solution}
\end{aligned}$$

And we can continue this to generate as many solutions as we like!

If we look at the ratio between a and b, something interesting emerges:

$$\begin{aligned}
a^2 - 3b^2 &= 1 \\
a^2 &= 3b^2 + 1 \\
\left(\frac{a}{b}\right)^2 &= 3 + \frac{1}{b^2}
\end{aligned}$$

So as the values of a, b get bigger, the ratio $\frac{a}{b}$ gets closer and closer to $\sqrt{3}$! And indeed, our third solution $\frac{26}{15} = 1.7333\cdots$, is just one part in 1000 away from the actual square root of 3.

2 Introduction

Pell's equations are of the form:

$$a^2 - mb^2 = \pm 1$$

for positive integers m. Lagrange proved that if m is not a perfect square, the equation has infinite solutions $(a, b) \in \mathbb{Z}^2$!

for some values of m, it is easy to identify a solution - for example, for $m = 3$, $(2, 1)$ is a solution to:

$$a^2 - 3b^2 = 1$$

then, by factoring this expression as a difference of squares $\sum_{i=2}^{n} \lfloor \sqrt[i]{n} \rfloor = \sum_{i=2}^{n} \lfloor \log_i(n) \rfloor$

$$(a - \sqrt{3}b)(a + \sqrt{3}b) = 1$$

we get two expressions in the extension of integers $\mathbb{Z}[\sqrt{3}]$ which we can then raise to any power n using the binomial theorem. $(a + \sqrt{3}b)^n = A + \sqrt{3}B$, and $(a - \sqrt{3}b)^n = A - \sqrt{3}B$ which generates an infinity of solutions.

For example, $(a + \sqrt{3}b)^2 = (a^2 + 3b^2) + (2ab)\sqrt{3}, (a - \sqrt{3}b)^2 = (a^2 + 3b^2) - (2ab)\sqrt{3}$ so from the base solution $(2, 1)$, we can generate another solution $(2^2 + 3 \cdot 1^2, 2 \cdot 2 \cdot 1) = (7, 4)$ and we can check that $7^2 - 3 \cdot 4^2 = 1$ - and we can do the same thing for any integer power of $2 + \sqrt{3}$! That's kind of neat.

3 General method for finding base solution

For $m = 3$, finding a solution is easy, but how about $m = 10$? Or $m = 19$? For some values of m finding a base solution to generate others from takes some work.

One general method for finding a base case is to find increasingly accurate rational approximations of $\frac{a}{b} \approx \sqrt{m}$ - at some point, the approximation will be close enough that the difference $a^2 - mb^2 = 1$. One of the most efficient ways to do that is to calculate the continued fraction for $\sqrt{m}$.

for example, for $m = 10$:

$$\begin{aligned}\sqrt{10} &= 3 + \sqrt{10} - 3 \\ &= 3 + \frac{(\sqrt{10} - 3)(\sqrt{10} + 3)}{\sqrt{10} + 3} \\ &= 3 + \frac{1}{6 + \sqrt{10} - 3}\end{aligned}$$

and we have a repetition. the continued fraction for $\sqrt{10} = [3; 6, 6, 6, \cdots]$ and the first few convergents are 3, $\frac{19}{6}$, $\frac{117}{37}$, $\frac{721}{228}$ - and these alternate between $a^2 - 10b^2 = \pm 1$.

This method of finding continued fractions for square roots works in general, but for some values of m it takes a long time to repeat, and a long time to converge to a "near-miss" value of 1.

For $\sqrt{19}$ for example:

$$\begin{aligned}
\sqrt{19} &= 4 + \sqrt{19} - 4 \\
&= 4 + \frac{(\sqrt{19} - 4)(\sqrt{19} + 4)}{\sqrt{19} + 4} \\
&= 4 + \frac{1}{\frac{1}{3}(\sqrt{19} + 4)} \\
&= 4 + \frac{1}{2 + \frac{1}{3}(\sqrt{19} - 2)} \\
&= 4 + \frac{1}{2 + \frac{1}{\frac{1}{5}(\sqrt{19}+2)}}
\end{aligned}$$

Repeating this process until repetition, we find that:

$$\sqrt{19} = [4; 2, 1, 3, 1, 2, 8, \cdots]$$

By investigating the convergents of the continued fraction, we find that they are:

$$4, \frac{9}{2}, \frac{13}{3}, \frac{48}{11}, \cdots$$

by finding repeatedly accurate convergents, and looking at every second convergent (the ones bigger than $\sqrt{19}$) we eventually find our base solution for $m = 19$, which is ...