Pell's Equation

To solve the so-called Pell's Equation

$$x^2 - Dy^2 = 1$$

in integers one uses the continued fraction expansion for $\sqrt{D}$. We assume that $D \geq 2$ is not a square. The expansion

$$\sqrt{D} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

turns out to be periodic. Indeed, it is of the form

$$\sqrt{D} = [a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}]$$

where the period $a_1, a_2, \ldots, a_2, a_1, 2a_0$ is of length m.

For example

$$\begin{array}{rcl} \sqrt{53} & = & [7, \overline{3, 1, 1, 3, 14}], \quad m = 5 \\ \sqrt{54} & = & [7; \overline{2, 1, 6, 1, 2, 14}], \quad m = 6 \end{array}$$

where $a_0 = 7$, $2a_0 = 14$ and $3, 1, 1, 3$ is a palindrome (ABBA, REGNINGER).

We only need to know that it is periodic, which property we do not prove now.

Then we form the sequence

$$\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$$

of *convergents*, where

$$\frac{p_0}{q_0} = a_0, \quad \frac{p_1}{q_1} = a_0 + \frac{1}{a_1}, \quad \frac{p_2}{q_2} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}, \quad \ldots.$$

The fundamental formulas

$$\begin{cases} p_{k+1} & = & a_{k+1} p_k + p_{k-1} \\ q_{k+1} & = & a_{k+1} q_k + q_{k-1} \end{cases}$$

are expedient for the calculation.

Teorem 1. *If $x = p$, $y = q$ solves Pell's equation, then p/q is one of the convergents in the expansion of $\sqrt{D}$.*

Bevis. The idea is that p/q approximates $\sqrt{D}$ so accurately that only a convergent is capable of that. Indeed, we estimate

$$\begin{array}{rcl} (p - \sqrt{D}q)(p + \sqrt{D}q) & = & 1 \\ 0 < \dfrac{p}{q} - \sqrt{D} & = & \dfrac{1}{q(p + \sqrt{D}q)} < \dfrac{1}{2q^2} \end{array}$$

because $p \geq \sqrt{D}q > q$, so that $p + \sqrt{D}q > 2q$.

Now the theorem follows from the following lemma, which we do not prove here.

Lemma 1. *If the (irrational) number $x > 0$ satisfies*

$$\left| x - \frac{a}{b} \right| < \frac{1}{2b^2}, \quad \textit{(a,b natural numbers)},$$

then a/b must be one of the convergents in the expansion of x in a continued fraction.

□

The next problem is to figure out which convergents yield an answer. Since $p/q > \sqrt{D}$, they must be of odd orders. In terms of the period length m, *the answer is the following*:

$$\begin{array}{lll} x = p_{m-1}, & y = q_{m-1}, & \text{if m is even} \\ x = p_{2m-1}, & y = q_{2m-1}, & \text{if m is odd.} \end{array}$$

This yields the smallest solution, say x_1,y_1. The formula

$$x_n + \sqrt{D}y_n = (x_1 + \sqrt{D}y_1)^n, \quad n = 1, 2, \ldots$$

then generates all solutions.

Thus, for example,

$$x_2 + \sqrt{D}y_2 = x_1^2 + Dy_1^2 + \sqrt{D} \cdot 2x_1y_1,$$

so that

$$x_2 = x_1^2 + Dy_1^2, \quad y_2 = 2x_1y_1.$$

The proof that we have selected the right convergents and that we obtain *all* positive solutions is omitted. That the formula generates solutions, if one starts from a solution, follows from

$$\begin{aligned} x_n^2 - Dy_n^2 &= (x_n - \sqrt{D}y_n)(x_n + \sqrt{D}y_n) \\ &= (x_1 - \sqrt{D}y_1)^n (x_1 + \sqrt{D}y_1)^n \\ &= (x_1^2 - Dy_1^2)^n = 1^n = 1, \end{aligned}$$

where also the property that

$$x_n - \sqrt{D}y_n = (x_1 - \sqrt{D}y_1)^n$$

is needed.

There is also a formula due to Brahmagupta (598-670) that produces solutions from solutions:

$$(x^2 - Dy^2)(u^2 - Dv^2) = (xu + Dyv)^2 - D(xv + yu)^2.$$

In particular,

$$(x^2 - Dy^2)^2 = (x^2 + Dy^2)^2 - D(2xy)^2.$$

We turn to another example.

Solve the equation $x^2 - 41y^2 = 1$. In accordance with the procedure outlined above, we find that

$$\sqrt{41} = [6; \overline{2, 2, 12}], \quad m = 3; \quad 2m - 1 = 5.$$

k	0	1	2	3	4	5	6
a_k	6	2	2	12	2	2	12
$\frac{p_k}{q_k}$	$\frac{6}{1}$	$\frac{13}{2}$	$\frac{32}{5}$	$\frac{397}{62}$	$\frac{826}{129}$	$\frac{\mathbf{2049}}{\mathbf{320}}$	$\frac{25414}{3969}$.

Since $p_5/q_5 = 2049/320$, the solution is given by $x = 2049$, $y = 320$.

(In passing, we seize the opportunity to mention that

$$0 < \frac{2049}{320} - \sqrt{41} < \frac{1}{320 \cdot 3969} < \frac{1}{2 \cdot 320^2}.)$$

All solutions come from

$$x_n + \sqrt{41} y_n = (2049 + \sqrt{41} \cdot 320)^n, \quad n \geq 1.$$

We have $x_2 = 8396801$, $y_2 = 1311360$.

For *the expansion of the square root* the procedure is

$$\begin{aligned}
\sqrt{41} &= 6 + \sqrt{41} - 6 = 6 + \cfrac{1}{\cfrac{1}{\sqrt{41} - 6}} \\
\frac{1}{\sqrt{41} - 6} &= \frac{\mathbf{\sqrt{41} + 6}}{\mathbf{5}} = \frac{10 + \sqrt{41} - 4}{5} = 2 + \frac{\sqrt{41} - 4}{5} \\
&= 2 + \frac{25}{5(\sqrt{41} + 4)} = 2 + \cfrac{1}{\cfrac{\sqrt{41} + 4}{5}} \\
\frac{\sqrt{41} + 4}{5} &= \frac{10 + \sqrt{41} - 6}{5} = 2 + \frac{\sqrt{41} - 6}{5} = 2 + \frac{5}{5(\sqrt{41} + 6)} \\
&= 2 + \frac{1}{\sqrt{41} + 6} \\
\sqrt{41} + 6 &= 12 + \sqrt{41} - 6 = 12 + \frac{1}{\frac{\mathbf{\sqrt{41}+6}}{\mathbf{5}}}.
\end{aligned}$$

Now the pattern repeats itself. We have

$$\sqrt{41} = 6 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{12 + \cfrac{1}{\frac{\sqrt{41}+6}{5}}}}}$$

from which we easily finish.