Pell's equation and continued fractions
Two mathematical gems

Torbjörn Tambour

Department of Mathematics, Stockholm University

Linnæus University
March 12, 2014

Pell's equation

Pell's equation is the Diophantine equation

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

where d is an integer ≥ 2.

If d is a square, then the only solutions are $(\pm 1, 0)$. Hence we assume that d is not a square.

Pell's equation

Why is Pell's equation interesting?

1. Because of its connection with the group of units in the ring of algebraic integers in the quadratic number field $\mathbf{Q}(\sqrt{d})$.
2. Because of its connection with approximation of real numbers with rationals. If $x^2 - dy^2 = 1$, then

$$\left|\sqrt{d} - \frac{x}{y}\right| < \frac{1}{Cy^2}$$

for some constant $C \geq 2$ independent of x and y.

The equation is named after the English mathematician John Pell (1610-1685), who had nothing to do with it. It was Euler who by mistake attributed a solution method to Pell. The equation has a long and rich history.

Pell's equation

One solution to $x^2 - 2y^2 = 1$ is $(x, y) = (3, 2)$. Define x_n, y_n by

$$(3 + 2\sqrt{2})^n = x_n + y_n\sqrt{2}.$$

Then $(\pm x_n, \pm y_n)$ are also solutions and in fact they are *all* solutions to the equation.

Pell's equation

Define an automorhism

$$\begin{array}{rcl} \mathbf{Q}(\sqrt{d}) & \to & \mathbf{Q}(\sqrt{d}) \\ \xi = a + b\sqrt{d} & \mapsto & \xi' = a - b\sqrt{d}. \end{array}$$

and put $N(\xi) = \xi\xi'$ (cf. complex conjugation and absolute value). Then $(\xi\eta)' = \xi'\eta'$ and $N(\xi\eta) = N(\xi)N(\eta)$. If $\xi = a + b\sqrt{d}$, then

$$N(\xi) = \xi\xi' = a^2 - db^2.$$

The map N is called the *norm*.

The solutions to Pell's equation correspond to the elements of $\mathbf{Z}[\sqrt{d}]$ with norm 1.

Pell's equation

Let us say that the number $a + b\sqrt{d}$ is a solution to $x^2 - dy^2 = 1$ if $a^2 - db^2 = 1$. From $N(\xi\eta) = N(\xi)N(\eta)$ follows

Theorem

The solutions to Pell's equation $x^2 - dy^2 = 1$ form a group P_d under multiplication.

Since $(\pm 1, 0)$ are solutions (the trivial ones), P_d is not empty. But does it always contain non-trivial elements? And in that case, what is its structure?

Theorem (Lagrange 1768)

Pell's equation always has non-trivial solutions. There is a smallest solution $a + b\sqrt{d} > 1$ such that all solutions can be written $\pm(a + b\sqrt{d})^n$ for $n \in \mathbf{Z}$. Hence P_d is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}$.

The second part of the theorem is easy to prove. One can give a short but non-constructive proof of the existence of non-trivial solutions using the pidgeon hole principle, but we will later use continued fractions to prove this.

The smallest solution $a + b\sqrt{d} > 1$ is called the *fundamental solution* to $x^2 - dy^2 = 1$.

Pell's equation

d	Fundamental solution
2	$3 + 2\sqrt{2}$
3	$2 + \sqrt{3}$
5	$9 + 4\sqrt{5}$
6	$5 + 2\sqrt{6}$
7	$8 + 3\sqrt{7}$
10	$19 + 6\sqrt{10}$
11	$10 + 3\sqrt{11}$
13	$649 + 180\sqrt{13}$

Pell's equation

Now things get considerably more interesting:

d	Fundamental solution
29	$9801 + 1820\sqrt{29}$
61	$226153980 + 1766319049\sqrt{61}$
94	$2143295 + 221064\sqrt{94}$

The obvious question is:

How do we find the fundamental solution?

The not so obvious answer is:

By using continued fractions.

Continued fractions

Using the division algorithm repeatedly gives

$$\frac{87}{38} = 2+\frac{11}{38} = 2+\frac{1}{38/11} = 2+\frac{1}{3+5/11} = 2+\cfrac{1}{3+\cfrac{1}{11/5}} = 2+\cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{5}}}$$

(cf. Euclid's algorithm). The last expression is the *continued fraction expansion of* $87/38$. We denote it by $[2,3,2,5]$.

Continued fractions

Another example:

$$
\begin{aligned}
\frac{137}{44} &= 3+\frac{5}{44} = 3+\frac{1}{44/5} = 3+\frac{1}{8+4/5} \\
&= 3+\cfrac{1}{8+\cfrac{1}{5/4}} = 3+\cfrac{1}{8+\cfrac{1}{1+\cfrac{1}{4}}} \\
&= [3,8,1,4]
\end{aligned}
$$

And yet another:

$$
\begin{aligned}
[2, 10, 5, 7, 6] &= \left[2, 10, 5, 7 + \frac{1}{6}\right] = \left[2, 10, 5, \frac{43}{6}\right] \\
&= \left[2, 10, 5 + \frac{6}{43}\right] = \left[2, 10, \frac{221}{43}\right] \\
&= \left[2, 10 + \frac{43}{221}\right] = \left[2, \frac{2253}{221}\right] = 2 + \frac{221}{2253} \\
&= \frac{4727}{2253}
\end{aligned}
$$

Continued fractions

The continued fraction expansion of an irrational number:

$$\begin{aligned}
\sqrt{2}+1 &= 2+\left(\sqrt{2}-1\right) = 2+\frac{1}{\sqrt{2}+1} \\
&= 2+\cfrac{1}{2+\cfrac{1}{\sqrt{2}+1}} \\
&= 2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{\sqrt{2}+1}}}
\end{aligned}$$

We would like to write $\sqrt{2}+1=[2,2,2,\ldots]$, but what does this mean?

Continued fractions

Clearly the continued fraction expansion of a (positive real) number terminates if and only if the number is rational.

For an arbitrary (irrational) number A define the positive integers a_i (a_0 might be 0) and the real numbers $\xi_i > 1$ by

$$
\begin{aligned}
A &= a_0 + \frac{1}{\xi_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\xi_2}} \\
&= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\xi_3}}} = \dots
\end{aligned}
$$

Continued fractions

Hence we have

$$A = [a_0, a_1, \ldots a_n, \xi_{n+1}].$$

Terminology:

$$A_n = [a_0, a_1, \ldots a_n] \text{ are called } \textit{convergents}$$

$$\xi_n \text{ are called } \textit{complete quotients}$$

in the continued fraction expansion of A.

Theorem

We have

$$\lim_{n\to\infty} A_n = A$$

and

$$A_{2k} < A, \quad A_{2k+1} > A \quad \text{for all } k.$$

If $A_n = p_n/q_n$, *where* p_n *and* q_n *are coprime integers, then*

$$|A - A_n| < \frac{1}{a_{n+1} q_n^2} \quad \text{for all } n.$$

We write

$$A = [a_0, a_1, a_2, \ldots]$$

and call this the continued fraction expansion of A.

Continued fractions

On the other hand:

Theorem

Let $A > 0$ be an irrational number and p and q coprime integers such that

$$\left| A - \frac{p}{q} \right| < \frac{1}{2q^2}.$$

Then p/q is a convergent in the continued fraction expansion of A.

Continued fractions

We saw earlier that

$$\sqrt{2} + 1 = [2, 2, 2, \ldots] = [\overline{2}].$$

Let

$$\alpha = [1, 1, 1, \ldots] = [\overline{1}].$$

Then

$$\alpha = [1, \alpha] = 1 + \frac{1}{\alpha},$$

which gives

$$\alpha = \frac{\sqrt{5} + 1}{2}.$$

Continued fractions

Let

$$\beta = [3, 1, 3, 1, 3, 1, \ldots] = [\overline{3, 1}].$$

Then

$$\begin{aligned} \beta &= [3, 1, \beta] = \left[3, 1 + \frac{1}{\beta}\right] = \left[3, \frac{\beta + 1}{\beta}\right] \\ &= 3 + \frac{\beta}{\beta + 1} = \frac{4\beta + 3}{\beta + 1}, \end{aligned}$$

which gives

$$\beta = \frac{\sqrt{21} + 3}{2}.$$

Continued fractions

Theorem

The number α has a continued fraction expansion of the form

$$\alpha = [b_0, b_1, \ldots, b_m, \overline{a_0, a_1, \ldots, a_n}]$$

if and only if it is a quadratic irrationality, i.e. a root of an irreducible equation of the form $Ax^2 + Bx + C = 0$.

An expansion of this form is said to be *ultimately periodic*.

Let $[\alpha]$ denote the integer part of α.

Theorem

The continued fraction expansion of a quadratic irrationality of the form

$$A = \sqrt{d} + [\sqrt{d}]$$

is purely periodic, i.e.

$$A = [\overline{a_0, a_1, \ldots, a_n}].$$

Continued fractions

$$\begin{aligned}
\sqrt{7}+2 &= 4+(\sqrt{7}-2) = \left[4, \frac{1}{\sqrt{7}-2}\right] = \left[4, \frac{\sqrt{7}+2}{3}\right] \\
&= \left[4, 1+\frac{\sqrt{7}-1}{3}\right] = \left[4, 1, \frac{3}{\sqrt{7}-1}\right] = \left[4, 1, \frac{\sqrt{7}+1}{2}\right] \\
&= \left[4, 1, 1+\frac{\sqrt{7}-1}{2}\right] = \left[4, 1, 1, \frac{2}{\sqrt{7}-1}\right] \\
&= \left[4, 1, 1, \frac{\sqrt{7}+1}{3}\right] = \left[4, 1, 1, 1+\frac{\sqrt{7}-2}{3}\right] \\
&= \left[4, 1, 1, 1, \frac{3}{\sqrt{7}-2}\right] = \left[4, 1, 1, 1, \sqrt{7}+2\right]
\end{aligned}$$

Let $D = [\sqrt{d}]$ and assume that $A = D + \sqrt{d} = [\overline{a_0, a_1, \ldots, a_n}]$. Then $a_0 = 2D$ and we write

$$A = [D, \overline{a_1, a_2, \ldots, a_n, 2D}].$$

Define p_k, q_k by

$$\begin{aligned} A_1 &= [D, a_1, a_2, \ldots, a_n] = \frac{p_1}{q_1} \\ A_2 &= [D, a_1, a_2, \ldots, a_n, 2D, a_1, a_2, \ldots, a_n] = \frac{p_2}{q_2} \end{aligned}$$

and so on. Then it can be shown that

$$p_k^2 - dq_k^2 = (-1)^{k(n+1)}.$$

The proof is elementary, but a bit too long to discuss here. We see the connection to Pell's equation.

We get the solutions to Pell's equation $x^2 - dy^2 = 1$ as follows.

n odd, $n+1$ even: $p_1 + q_1\sqrt{d}$ is the fundamental solution

n even, $n+1$ odd: $p_2 + q_2\sqrt{d}$ is the fundamental solution and p_1, q_1 is a solution to $x^2 - dy^2 = -1$

$$\underline{x^2 - 2y^2 = 1}$$

$$\sqrt{2} + 1 = [\overline{2}], \quad \sqrt{2} = [1, \overline{2}], \quad n = 0$$

$$\frac{p_1}{q_1} = [1] = 1, \quad p_1 = q_1 = 1$$

so $1 + \sqrt{2}$ is a solution to $x^2 - 2y^2 = -1$

$$\frac{p_2}{q_2} = [1, 2] = \frac{3}{2}, \quad p_2 = 3, q_2 = 2$$

so the fundamental solution to $x^2 - 2y^2 = 1$ is $3 + 2\sqrt{2}$

$$\underline{x^2 - 7y^2 = 1}$$

$$\sqrt{7} + 2 = [\overline{4, 1, 1, 1}], \quad \sqrt{7} = [2, \overline{1, 1, 1, 4}], \quad n = 3$$

$$\frac{p_1}{q_1} = [2, 1, 1, 1] = \frac{8}{3}$$

so the fundamental solution to $x^2 - 7y^2 = 1$ is $8 + 3\sqrt{7}$

$$\underline{x^2 - 13y^2 = 1}$$

$$\sqrt{13} + 3 = [\overline{6, 1, 1, 1, 1}], \quad \sqrt{13} = [3, \overline{1, 1, 1, 1, 6}], \quad n = 4$$

$$\frac{p_1}{q_1} = [3, 1, 1, 1, 1] = \frac{18}{5}$$

so $18 + 5\sqrt{13}$ is a solution to $x^2 - 13y^2 = -1$

The fundamental solution to $x^2 - 13y^2 = 1$

is $(18 + 5\sqrt{13})^2 = 649 + 180\sqrt{13}$.

Pell's equation and continued fractions

$$\underline{x^2 - 94y^2 = 1}$$

$$\sqrt{94} + 9 = [\overline{18, 1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1}], \quad n = 15$$

$$\frac{p_1}{q_1} = [9, 1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1] = \frac{2143295}{221064}$$

so the fundamental solution to $x^2 - 94y^2 = 1$ is

$$2143295 + 221064\sqrt{94}$$

Archimedes' cattle problem

In 1773 Lessing published a manuscript from the Wolfenbüttel library containing a problem that is nowadays attributed to Archimedes. The problem asks for the number of white, black, dappled and brown bulls and cows belonging to the Sun god Helios. An analysis of the problem reveals that it is necessary to solve the Pell equation $x^2 - dy^2 = 1$ for

$$d = 410\,286\,423\,278\,424.$$

A solution was given by the German mathematician A. Amthor in 1880, but he didn't directly apply the continued fraction method. It has been shown that the period in the expansion of $\sqrt{d}$ has length 203 254 and that the fundamental solution has 206 545 digits.

Historical remarks

Brahmagupta, 7th century: With the help of one solution one can generate infinitely many new ones.

Javadena, Bhaskara, 11th century: Method to find one solution, probably involving continued fractions.

Fermat: The first European mathematician to study Pell's equation. For special values of d (e.g. $d = 61$) he gave it as a challenge to colleagues.

Euler: Systematic analysis of Pell's equation using continued fractions.

Historical remarks

$$e - 1 = [1, 1, 2, 1, 1, 4, 1, 1, 6, \ldots]$$

$$\pi =$$

$$[3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1, 84, 2, 1, 1, 15, 3, 13, \ldots$$

Some convergents in the expansion of π:

$$A_0 = 3,\ A_1 = \frac{22}{7},\ A_2 = \frac{333}{106},\ A_3 = \frac{355}{113},\ A_4 = \frac{103993}{33102}$$