11. Pell Equation

We now turn to the problem of finding integral solutions to quadratic equations in two variables. This is an order of magnitude harder than finding integral solutions to a homogeneous quadratic equation in three variables, equivalently to finding rational solutions to quadratic equations in two variables.

As before, one can transform a general quadratic to a conic which is a line, a parabola, an ellipse or a hyperbola. The line and the parabola are easy to handle (they correspond to the case when the dependence on at least one variable is linear). Hence we are left with an ellipse or a hyperbola. With some work, as before we reduce to an equation of the form

$$Ax^2 + By^2 + C = 0.$$

It is convenient to multiply through by A and relabel so that we get the equation

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

where d, $k \in \mathbb{Z}$ and d is square-free. This equation is quite famous and is called Pell's equation.

If $d < 0$ and $k > 0$ then we get an ellipse. In this case just try every integer y such that

$$|y| \leq \sqrt{\frac{-k}{d}},$$

and see when $k + dy^2$ is a square. If $d < 0$ and $k < 0$ there are no real solutions and so no integer solutions. If $d = 1$ then the equation reduces to

$$(x - y)(x + y) = k,$$

and solutions correspond to factorisations of k. The only really interesting case is when $d > 1$ and d is square-free.

Note that

$$x^2 - dy^2 = (x - \sqrt{d}y)(x + \sqrt{d}y).$$

The factors $x - \sqrt{d}y$ and $x + \sqrt{d}y \in \mathbb{Z}[\sqrt{d}]$. Note that $\mathbb{Z}[\sqrt{d}]$ is an integral domain (indeed it is a subring of the real numbers).

Definition-Lemma 11.1. *Suppose that $\alpha = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. x and y are called the **components** of α.*

$$\bar{\alpha} = x - y\sqrt{d}$$

*is called the **conjugate** of α and*

$$\begin{aligned} N(\alpha) &= \alpha\bar{\alpha} \\ &= x^2 - dy^2, \end{aligned}$$

is called the ***norm*** *of* α.

The norm is totally multiplicative.

Proof. Suppose that α and $\beta \in \mathbb{Z}[\sqrt{d}]$. We have

$$\begin{aligned} N(\alpha\beta) &= \alpha\beta\overline{(\alpha\beta)} \\ &= \alpha\beta\bar{\alpha}\bar{\beta} \\ &= \alpha\bar{\alpha}\beta\bar{\beta} \\ &= N(\alpha)N(\beta). \end{aligned}$$

□

Observe that a solution to Pell's equation corresponds to $\alpha = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ such that $N(\alpha) = k$. Note also that since $\sqrt{d}$ is irrational,

$$x_1 + y_1\sqrt{d} = x_2 + y_2\sqrt{d} \qquad \text{if and only if} \qquad x_1 = x_2, y_1 = y_2.$$

Pick an integer m and consider what happens if we reduce modulo m, meaning we reduce the components modulo m. It is straightforward to check that we get an equivalence relation this way. There are m choices for the residue class of x and m choices for the residue class of y, making m^2 choices in total, so that there are m^2 equivalence classes. This equivalence relation respects addition and multiplication.

Consider solutions to Pell's equation with x and y positive. If we have a solution then

$$x - y\sqrt{d} = \frac{k}{x + y\sqrt{d}}.$$

Suppose that there are infinitely many such solutions. Then x and y are going to infinity and the expression above is going to zero.

It follows that the ratio x/y gets closer to $\sqrt{d}$ and we get better and better approximations of $\sqrt{d}$. In fact if

$$\frac{x}{y} \approx \sqrt{d} \qquad \text{then} \qquad x + y\sqrt{d} \approx 2y\sqrt{d}$$

and so if we have a solution to Pell's equation then

$$\left|\sqrt{d} - \frac{x}{y}\right| \approx \frac{|k|}{y^2(2\sqrt{d})}.$$

This is quite striking and it is not at all clear that such close approximations actually exist.

In fact we have the following general result:

Theorem 11.2. *If* ξ *is a real number and* t *is a natural number then there are integers* x *and* y *such that*

$$|y\xi - x| < \frac{1}{t} \qquad \textit{where} \qquad 1 \leq y \leq t.$$

Proof. Consider the fractional parts of the multiples of ξ,

$$0, \qquad \{\,\xi\,\}, \qquad \{\,2\cdot\xi\,\}, \qquad \ldots, \qquad \{\,t\cdot\xi\,\}.$$

There are $t+1$ such numbers and they belong to the interval $[0,1)$. Divide this interval into t equal parts in the obvious way,

$$[0,1/t), \qquad [1/t,2/t), \qquad \ldots, \qquad [(t-1)/t,1).$$

By the pigeonhole principle two of the fractional parts must land in the same interval. Therefore

$$|\{\,j\cdot\xi\,\}-\{\,i\cdot\xi\,\}|<\frac{1}{t},$$

where $0\le i<j\le t$. But

$$i\cdot\xi=\llcorner i\cdot\xi\lrcorner+\{\,i\cdot\xi\,\},$$

so that

$$\begin{aligned} y\xi-x&=(j-i)\xi-x\\ &=(\llcorner j\cdot\xi\lrcorner-\llcorner i\cdot\xi\lrcorner)-x+\{\,j\cdot\xi\,\}-\{\,i\cdot\xi\,\}\\ &=\{\,j\cdot\xi\,\}-\{\,i\cdot\xi\,\}, \end{aligned}$$

where

$$y=j-i>0 \qquad \text{and} \qquad x=\llcorner j\cdot\xi\lrcorner-\llcorner i\cdot\xi\lrcorner\in\mathbb{Z}. \qquad \square$$

Corollary 11.3. *If ξ is irrational then the inequality*

$$|x-y\xi|<\frac{1}{y}$$

has infinitely many solutions.

Proof. Suppose we have finitely many solutions, (x_i,y_i), $1\le i\le k$, where $y_i>0$. We may assume that they are ordered worse to best, in the sense that

$$|x_i-y_i\xi|>|x_j-y_j\xi| \qquad \text{if and only if} \qquad i<j.$$

As ξ is irrational

$$|x_k-y_k\xi|>0.$$

Therefore we may find $t\in\mathbb{N}$ such that

$$|x_k-y_k\xi|>\frac{1}{t}.$$

By (11.2) we may find (x,y)

$$|x-y\xi|<\frac{1}{t} \qquad \text{where} \qquad 1\le y\le t.$$

It follows that $(x, y) \neq (x_k, y_k)$. On the other hand as $y \leq t$

$$|x - y\xi| < \frac{1}{y}. \qquad \square$$

Theorem 11.4. *There is an integer k, with*

$$|k| < 1 + 2\sqrt{d},$$

such that Pell's equation has infinitely many solutions.

Proof. Pick a solution (x, y) to

$$|x - y\sqrt{d}| < \frac{1}{y}.$$

We have

$$\begin{aligned} |x + y\sqrt{d}| &= |x - y\sqrt{d} + 2y\sqrt{d}| \\ &\leq |x - y\sqrt{d}| + 2y\sqrt{d} \\ &< \frac{1}{y} + 2y\sqrt{d} \\ &\leq (1 + 2\sqrt{d})y. \end{aligned}$$

It follows that

$$\begin{aligned} |x^2 - y^2 d| &= |x - y\sqrt{d}| \cdot |x + y\sqrt{d}| \\ &< \frac{1}{y}(1 + 2\sqrt{d})y \\ &< 1 + 2\sqrt{d}. \end{aligned}$$

Now use the fact that there are infinitely many choices of (x, y) but only finitely many integers whose absolute value is less than $1 + 2\sqrt{d}$. $\square$

Theorem 11.5. *If $d > 1$ is square-free then there are integers x and $y \neq 0$ such that*

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

Proof. Pick a natural number k such that one of the equations

$$N(\alpha) = \pm k$$

has infinitely many solutions $\alpha \in \mathbb{Z}[\sqrt{d}]$. As there are only finitely many residue classes modulo k, we can find three solutions with the same residue class.

Therefore we can find α_1 and $\alpha_2 \in \mathbb{Z}[\sqrt{d}]$ with

$$N(\alpha_1) = N(\alpha_2) = \pm k, \qquad \alpha_1 \equiv \alpha_2 \mod k \qquad \text{but} \qquad \alpha_1 \neq \pm\alpha_2.$$

It follows that

$$\begin{aligned}\alpha_1\bar{\alpha}_2 &\equiv \alpha_2\bar{\alpha}_2 \\ &\equiv 0 \mod k,\end{aligned}$$

so that

$$\beta = \frac{\alpha_1\bar{\alpha}_2}{k} \in \mathbb{Z}[\sqrt{d}].$$

Observe that

$$\begin{aligned}N(\beta) &= \beta\bar{\beta} \\ &= \frac{\alpha_1\bar{\alpha}_2 \cdot \bar{\alpha}_1\alpha_2}{k^2} \\ &= \frac{\alpha_1\bar{\alpha}_1 \cdot \alpha_2\bar{\alpha}_2}{k^2} \\ &= \frac{N(\alpha_1)N(\alpha_2)}{k^2} \\ &= 1.\end{aligned}$$

If $\beta = x + y\sqrt{d}$ then we have

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

If $y = 0$ then $x \pm 1$ and so $\beta = \pm 1$. This would imply that

$$\alpha_1\bar{\alpha}_2 = \pm k = \pm\alpha_1\bar{\alpha}_1.$$

Cancelling the α_1 gives

$$\bar{\alpha}_2 = \bar{\alpha}_1 \qquad \text{so that} \qquad \alpha_1 = \pm\alpha_2,$$

a contradiction. □