Pell's Equation

Handout for MATHS 714

Let A be a positive integer which is not a perfect square. The equation

$$x^2 - Ay^2 = 1 \tag{1}$$

is called *Pell's equation*.

The requirement that A is not the square of a whole number is equivalent to the fact that the number $\sqrt{A}$ is irrational. It is very important! In this case the set of numbers $\mathbb{Q}(\sqrt{A})$ consisting of

$$p + q\sqrt{A}, \qquad p, q \in \mathbb{Q}, \tag{2}$$

are quadratic irrationalities with the following properties:

$$(p + q\sqrt{A}) + (r + s\sqrt{A}) = (p + r) + (q + s)\sqrt{A}, \tag{3}$$

$$(p + q\sqrt{A})(r + s\sqrt{A}) = (pr + qsA) + (ps + qr)\sqrt{A}, \tag{4}$$

$$(p + q\sqrt{A})^{-1} = \frac{1}{p^2 - q^2A}(p - q\sqrt{A}). \tag{5}$$

Note that if $p^2 - q^2A = 0$, then either $p = q = 0$ or $q \neq 0$. In the latter case $A = \frac{p^2}{q^2}$ or $\sqrt{A} = \frac{p}{q}$ which is a contradiction. Thus $p^2 - q^2A \neq 0$ unless $p + q\sqrt{A} = 0$ which is equivalent to $p = q = 0$, and the inverse (5) exists for every non-zero quadratic irrationality (2). This number deserves a special notation and for $u = p + q\sqrt{A}$ we denote $N(u) = p^2 - q^2A$.

In relation to the solutions of (1) we will be especially interested in quadratic irrationalities

$$z_1 + z_2\sqrt{A}, \qquad z_1, z_2 \in \mathbb{Z}.$$

This set of numbers we will denote $\mathbb{Z}(\sqrt{A})$.

Proposition 1. *Let $u, v \in \mathbb{Z}(\sqrt{A})$, then $u+v$, $uv \in \mathbb{Z}(\sqrt{A})$. If $u \in \mathbb{Z}(\sqrt{A})$ and $N(u) = 1$, then $u^{-1} \in \mathbb{Z}(\sqrt{A})$.*

Proof. Let us denote $\bar{u} = p - q\sqrt{A}$, then the formula (5) can be written as $u\bar{u} = N(u)$. Thus we have

$$u^{-1} = \frac{\bar{u}}{N(u)} = \bar{u} \in \mathbb{Z}(\sqrt{A}).$$

□

Inspecting (4) and replacing q by $-q$ and s by $-s$ we also get

$$\bar{u}\bar{v} = \overline{uv}. \tag{6}$$

(Note the analogy with the complex numbers!) Formulae (5) and (6) also imply a very important formula

$$N(uv) = N(u)N(v). \tag{7}$$

Indeed, we have $N(uv) = uv\overline{uv} = uv\bar{u}\bar{v} = u\bar{u}v\bar{v} = N(u)N(v)$.

It is time now to relate these properties of the new function $N(x)$ to the solutions of (1) and also to the solutions of the equation

$$x^2 - Ay^2 = k, \qquad k \in \mathbb{Z}. \tag{8}$$

Proposition 2. *A pair of integers (x, y) is a solution to Pell's equation (8) if and only if $N(u) = k$ for $u = x + y\sqrt{A}$. In particular, a pair of integers (x, y) is a solution to Pell's equation (1) if and only if $N(u) = 1$.*

Proof. As $N(u) = x^2 - Ay^2$ we see that the statement $N(u) = 1$ is simply a reformulation of the statement that the pair (x, y) is a solution to the equation (1). □

Theorem 1. *Suppose that a pair of integers (a, b) is a solution to Pell's equation (1) and (x, y) is an arbitrary solution to the Diophantine equation (8). Let us denote $u = x+y\sqrt{A}$, $v = a + b\sqrt{A}$, and*

$$uv = (xa + ybA) + (xb + ya)\sqrt{A} = x' + y'\sqrt{A}, \tag{9}$$

where $x' = xa + ybA$ and $y' = xb + ya$. Then this pair of integers (x', y') is also a solution to the equation (8).

Proof. This follows from the multiplicative property of the norm. Indeed, $N(uv) = N(u)N(v) = 1 \cdot k = k$. □

This theorem gives us a very important tool to obtain a number of solutions of (8) if we know at least one solution of (1) different from the trivial solution $(1, 0)$. We reformulate Theorem 1 now in terms of geometric transformations of the plane.

Theorem 2. *Suppose that a pair of integers (a, b) is a solution to Pell's equation (1). Let us consider a linear transformation of the plane $(x, y) \to (x', y')$, where*

$$\begin{aligned} x' &= ax + bAy, \\ y' &= bx + ay. \end{aligned}$$

Then this transformation maps the solutions of (8) again onto the solutions of (8).

It is clear now why the solution $(1, 0)$ of (1) is called trivial. It is because of the fact that the corresponding linear transformation for $a = 1$ and $b = 0$ is simply the identity transformation.

Example 1. *Let us consider the equation*

$$x^2 - 2y^2 = 1. \tag{10}$$

It has a nontrivial solution $(x, y) = (3, 2)$. Then the following linear transformation

$$\begin{aligned} x' &= 3x + 4y, \\ y' &= 2x + 3y \end{aligned}$$

will produce more solutions of

$$x^2 - 2y^2 = k.$$

if we know one. For example, we can get some more solutions of (10). Applying twice the linear transformation to the pair $(3, 2)$ we get two more solutions of (10):

$$(3, 2) \to (17, 12) \to (99, 70).$$

Or else the solution $(5, 3)$ to the equation

$$x^2 - 2y^2 = 7$$

gives us another solution of this equation, namely: $(5, 3) \to (27, 19)$.

It is clear now that it is important to prove that the equation (1) *always* has a nontrivial solution for every positive integer A which is not the square of a whole number. We shall start proving this with the following

Lemma 1. *Let α be an irrational number. Then for every positive integer t the inequality*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{tq}. \tag{11}$$

has an integer solution (p, q) such that $1 \leq q \leq t$.

Proof. Let $[\gamma]$ be the integer part and $\{\gamma\}$ be the fractional part of a real number γ, i.e., $[\gamma] \in \mathbb{Z}$ and $0 \le \{\gamma\} < 1$. (For example, $\left[\frac{3}{2}\right] = 1$, $\{\frac{3}{2}\} = \frac{1}{2}$, and $\left[\sqrt{5}\right] = 2$, $\{\sqrt{5}\} = \sqrt{5}-2$.) It is always true that $\gamma = [\gamma] + \{\gamma\}$.

Let us divide the unit interval $[0, 1)$ (where 0 is included and 1 is not) into t intervals

$$\left[0, \frac{1}{t}\right), \ \left[\frac{1}{t}, \frac{2}{t}\right), \ \dots \ , \left[\frac{t-1}{t}, 1\right) \tag{12}$$

of equal length $1/t$. Let us consider $t+1$ numbers $\{\alpha k\}$, $k = 1, 2, \dots, t+1$. By Pigeonhole Principle at least two of them, say $\{\alpha k_1\}$ and $\{\alpha k_2\}$, will be situated in the same interval of the partition (12) of the unit interval. Thus

$$|\{\alpha k_1\} - \{\alpha k_2\}| < \frac{1}{t}.$$

Replacing here $\{\alpha k_i\}$ by $\alpha k_i - [\alpha k_i]$ we get

$$|\alpha k_1 - [\alpha k_1] - (\alpha k_2 - [\alpha k_2])| < \frac{1}{t}.$$

or $|q\alpha - p| < \frac{1}{t}$, where $q = k_1 - k_2$ and $p = [\alpha k_1] - [\alpha k_2]$. Dividing by q we get (11). It is clear that $q \le (t+1) - 1 = t$. □

Corollary 1 (Dirichlet). *Let α be an irrational number. Then the inequality*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{13}$$

has infinitely many integer solutions (p, q).

Proof. As

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{tq} \le \frac{1}{q^2}$$

we see that every solution to (11) is also a solution to (13). It is also clear that as t grows more and more new solutions of (13) will emerge. □

Lemma 2. *For some integer k such that $|k| < 2\sqrt{A} + 1$ the equation*

$$x^2 - Ay^2 = k$$

has infinitely many integer solutions.

Proof. Let (p, q) be a solution to the inequality (13) with $\alpha = \sqrt{A}$. Then $\frac{p}{q} < \sqrt{A} + 1$ and

$$\left|p^2 - Aq^2\right| = q^2 \left|\sqrt{A} - \frac{p}{q}\right| \cdot \left|\sqrt{A} + \frac{p}{q}\right| < q^2 \cdot \frac{1}{q^2} \cdot \left|\sqrt{A} + \frac{p}{q}\right| < 2\sqrt{A} + 1.$$

Therefore $|p^2 - Aq^2|$ can take only finitely many integer values k satisfying

$$-(2\sqrt{A}+1) < k < 2\sqrt{A}+1.$$

As the inequality (13) has infinitely many solutions by Pigeonhole Principle for some k in this range the equation $x^2 - Ay^2 = k$ also has infinitely many integer solutions. □

Lemma 3. *There exist a nonzero integer k and two positive integers $0 \le a, b < |k|$ such that the equation (8) has infinitely many integer solutions (x, y) such that $x \equiv a \pmod{|k|}$ and $y \equiv b \pmod{|k|}$.*

Proof. Let k be such that the equation (8) has an infinite number of solutions. Such k exists according to Lemma 2. We assume that $k \neq -1$ and we consider this case later.

We need Pigeonhole Principle again. For an arbitrary solution (x, y) of (8) we have $x \equiv i \pmod{|k|}$ and $y \equiv j \pmod{|k|}$ for some $0 \le i, j \le |k|$. As we have k possibilities for i and k possibilities for j, in total, we have k^2 possibilities for the pair (i, j). Again we have a finite number of boxes and infinite number of solutions to (8) to go into them. Therefore there will be an infinite number of solutions at least in one of them. □

Theorem 3. *For every positive integer A which is not the square of a whole number Pell's equation (1) has a nontrivial integer solution $(a, b) \neq (1, 0)$.*

Proof. The idea of constructing a solution to Pell's equation is as follows. Let (x_1, y_1) and (x_2, y_2) be two distinct solutions to (8). This means that for $u_1 = x_1 + y_1\sqrt{A}$ and $u_2 = x_2 + y_2\sqrt{A}$ we have $N(u_1) = N(u_2) = k$. Since $N(u_1 u_2^{-1}) = N(u_1)N(u_2)^{-1} = 1$, the idea is to consider $v = u_1 u_2^{-1} = a + b\sqrt{A}$. Then $N(v) = 1$, hence (a, b) is a solution of (1). We now have to take care of two things: to secure that a and b are integers and to check that this solution is nontrivial. To deal with the first problem let us calculate a and b:

$$v = \left(x_1 + y_1\sqrt{A}\right)\frac{\left(x_2 - y_2\sqrt{A}\right)}{k} = \frac{(x_1x_2 - Ay_1y_2)}{k} + \frac{(x_1y_2 - x_2y_1)}{k}\sqrt{A},$$

whence

$$a = \frac{(x_1x_2 - Ay_1y_2)}{k}, \qquad b = \frac{(x_1y_2 - x_2y_1)}{k}. \tag{14}$$

Let (x_1, y_1) and (x_2, y_2) be two distinct solutions to (8) such that

$$x_1 \equiv x_2 \pmod{|k|} \qquad y_1 \equiv y_2 \pmod{|k|},$$

which existence is guaranteed by Lemma 3. Then

$$x_1x_2 - Ay_1y_2 \equiv x_1^2 - Ay_1^2 \equiv 0 \pmod{|k|},$$

and

$$x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{|k|}.$$

Therefore in (14) a and b are integers.

We need to prove now that the solution obtained is a nontrivial one. Suppose that $(a, b) = (1, 0)$. In this case $v = u_1u_2^{-1} = 1 + 0\sqrt{A} = 1$ and $u_1 = u_2$. This contradiction completes the proof. □

Exercise 1. *Let $k \neq 1$ be an integer and A be a positive integer which is not the square of a whole number. Suppose that the equation (8) has at least one solution. Then it has infinitely many solutions.*

We can say much more about the solutions to Pell's equation. We need the following comment.

Lemma 4. *Let (x, y) be an integer solution to Pell's equation (1) and $u = x + y\sqrt{A}$.*

1. *If $x > 0$ and $y > 0$, then $u > 1$;*
2. *If $x > 0$ and $y < 0$, then $0 < u < 1$;*
3. *If $x < 0$ and $y > 0$, then $-1 < u < 0$;*
4. *If $x < 0$ and $y < 0$, then $u < -1$;*

Proof. Suppose $x > 0$ and $y > 0$. Since $(x - y\sqrt{A})(x + y\sqrt{A}) = 1$, we have $x - y\sqrt{A} > 0$ and $x + y\sqrt{A} > x - y\sqrt{A}$. Hence $u > 1$ and $\bar{u} < 1$. This proves the first two statements. The third and the forth statements follow from the first two. □

Definition 1. *Let (a, b) be a nontrivial solution to Pell's equation (1) with positive integer components $a > 0, b > 0$. We say that this solution is* fundamental *if the number $u = a + b\sqrt{A}$ takes the minimal possible value.*

Note that the number u is uniquely determined since $a + b\sqrt{A} = a' + b'\sqrt{A}$ implies $(b - b')\sqrt{A} = a' - a$ and $\sqrt{A}$ is rational unless $b = b'$ and $a = a'$. Let us also note that $u > 1$ by Lemma 4.

Theorem 4. *Let (x_1, y_1) be the fundamental solution to Pell's equation (1) and $u = x_1 + y_1\sqrt{A}$. Let*

$$u^n = x_n + y_n\sqrt{A}, \qquad n = 0, 1, 2, \ldots \tag{15}$$

Then $(\pm x_n, \pm y_n)$, $n = 0, 1, 2, \ldots$, is the complete set of solutions to Pell's equation.

Proof. The trivial solution $(1, 0)$ is in this set and we get it for $n = 0$. Let (x, y) be an arbitrary nontrivial solution to Pell's equation. We may assume that $x > 0$. Since $(x + y\sqrt{A})^{-1} = x - y\sqrt{A}$, we may also assume that $y > 0$. All we need to show is that $v = x + y\sqrt{A}$ can be represented as u^n for some positive integer n. Let us assume the contrary. As $x > 0$ and $y > 0$, we know that $v > 1$. Since $u > 1$ the terms of the sequence 1, u, u^2, …, u^n, … get arbitrary large, thus there exists n such that $u^n < v < u^{n+1}$. Let us multilply this inequality by $(u^n)^{-1}$. We get

$$1 < v(u^n)^{-1} < u, \tag{16}$$

where $v(u^n)^{-1} = \bar{x} + \bar{y}\sqrt{A}$ for some $\bar{x}, \bar{y} \in \mathbb{Q}$. Let us make a number of observations. Firstly, $(u^n)^{-1} = (u^{-1})^n = (x_1 - y_1\sqrt{A})^n$. This means that $(u^n)^{-1} \in \mathbb{Z}(\sqrt{A})$ and hence $v(u^n)^{-1} \in \mathbb{Z}(\sqrt{A})$, i.e., $\bar{x}, \bar{y}$ are integers. Secondly, $N(v(u^n)^{-1}) = N(v)N(u)^{-n} = 1$ and $(\bar{x}, \bar{y})$ is a solution to Pell's equation. Thirdly, by Lemma 4 and (16) we get $\bar{x} > 0, \bar{y} > 0$ because of the inequality $1 < v(u^n)^{-1}$. Finally, this contradicts to (16), namely to $v(u^n)^{-1} < u$, since u was fundamental. The theorem is proved. □

Exercise 2. *Suppose that a pair of integers (x_1, y_1), $x_1 > 0, y_1 > 0$, is a solution to Pell's equation $x^2 - Ay^2 = 1$. Then this solution is fundamental if and only if y_1 is minimal among all integers solutions with positive components.*

This Exercise gives us an algorithm how to find the minimal solution. We have to try subsequently $y_1 = 1, 2, \ldots$ until a matching x_1 is found. This algorithm is not an efficient one. For example, for the equation $x^2 - 109y^2 = 1$ the minimal solution (x_1, y_1) will have $y_1 = 15140424455100$. A better algorithm is beyond the scope of this lecture.