# Lecture 1

## Pell's equation

These are equations of the form

$$x^2 - dy^2 = \pm 1$$

where $d \in \mathbb{Z}_{\neq 0}$ square free.

Goal: Solve for $(x, y) \in \mathbb{Z}^2$.

RMK: 1) $\forall (x, y)$ sol$^n$s $(\pm x, \pm y)$ are also sol$^n$s.

2) If $d$ is not square free then $d = e^2 f$ for $e \in \mathbb{N}$, $f$ square free then $x^2 - dy^2 = x^2 - f(ey)^2$.

Theorem 1: Let $d \in \mathbb{N}$ be not a square and $\exists\ (s, t)$ s.t. $s^2 - dt^2 = \pm 1$. Then $\frac{s}{t}$ is a convergent to $\sqrt{d}$.

Proof: If $s^2 - dt^2 = \pm 1$ $(s, t \geq 0)$

$$\Rightarrow (s + \sqrt{d}\,t)(s - \sqrt{d}\,t) = \pm 1$$

Hence, $\left| \sqrt{d} - \frac{s}{t} \right| = \frac{1}{t(s + t\sqrt{d})}$

$$= \frac{1}{t^2\left(\frac{s}{t} + \sqrt{d}\right)} = \frac{1}{t^2\left(\sqrt{d + 1/t^2} + \sqrt{d}\right)}$$

$$s^2 - dt^2 = \pm 1 \Rightarrow \frac{s^2}{t^2} = d \pm \frac{1}{t^2}$$

$$\frac{s}{t} = \sqrt{d \pm \frac{1}{t^2}}$$

Now $d \pm \frac{1}{t^2} \geq d - 1$

$$\sqrt{d \pm \frac{1}{t^2}} + \sqrt{d} \geq \sqrt{d-1} + \sqrt{d} > 2$$

$$\Rightarrow \left| \sqrt{d} - \frac{s}{t} \right| \leq \frac{1}{2t^2}$$

Lemma (week 8) implies that $\frac{s}{t}$ is a convergent to $\sqrt{d}$. $\boxtimes$

RMK: All solutions of $x^2 - dy^2 = \pm 1$

$\rightsquigarrow$ convergents to $\sqrt{d}$.

But converse may not be true.

Ex: $x^2 - 2y^2 = \pm 1$

$\sqrt{2} = [1; \overline{2}]$

$r_1 = \frac{3}{2}$, $r_2 = \frac{7}{5}$, $r_3 = \frac{17}{12}$, $r_4 = \frac{41}{29}$

We want to solve $x^2 - 2y^2 = \pm 1$

$$3^2 - 2 \times 2^2 = 1$$
$$7^2 - 2 \times 5^2 = -1$$
$$17^2 - 2 \times 12^2 = 1$$
$$41^2 - 2 \times 29^2 = -1 \quad \ldots\ldots$$

But it is not always the case.

Ex. $x^2 - 3y^2 = \pm 1$

$\sqrt{3} = [1; \overline{1, 2}]$

$r_1 = \frac{2}{1}$, $r_2 = \frac{5}{3}$, $r_3 = \frac{7}{4}$, $r_4 = \frac{19}{11}$

$2^2 - 3 \times 1^2 = 1$, $5^2 - 3 \times 3^2 = -2$

$7^2 - 3 \times 4^2 = 1$, $19^2 - 3 \times 11^2 = -2$

$\vdots$

May be $r_1, r_3, r_5, \ldots$ give solutions.

Theorem 2

Let $d \in \mathbb{N}$ not a square. Suppose we have $\sqrt{d} = [a; \overline{a_1, \ldots, a_\ell}]$.

Let $\frac{s_n}{t_n}$ be the $n$'th convergent of the continued fraction of $\sqrt{d}$. Then

$$s_n^2 - d\,t_n^2 = \pm 1$$

if & only if $n = N\ell - 1$, $N \in \mathbb{N}$

Moreover, $s_{N\ell-1}^2 - d\,t_{N\ell-1}^2 = (-1)^{N\ell}$

RMK: Thm 2 is the "Converse" of Thm 1.

Ex: $x^2 - 2y^2 = \pm 1$

$\sqrt{2} = [1; \overline{2}] \Rightarrow \ell = 1.$

Thus $s_{N-1}^2 - 2t_{N-1}^2 = (-1)^N \quad \forall N \in \mathbb{N}.$

Ex: $x^2 - 3y^2 = \pm 1$

$\sqrt{3} = [1; \overline{1, 2}] \Rightarrow \ell = 2$

Thus, $s_{2N-1}^2 - 3t_{2N-1}^2 = (-1)^{2N} = 1. \quad \forall N \in \mathbb{N}.$

## Exercise

Show that if $\sqrt{d} = [a; \overline{a_1, a_2, \ldots, a_\ell}]$ with $\ell$ even then $x^2 - dy^2 = -1$ has no solution.

## Fundamental Solution

Consider the set of non-negative solutions of $x^2 - dy^2 = \pm 1$, i.e.

$$\{ s^2 - dt^2 = \pm 1 \;;\; s, t \geq 0,\ (s,t) \in \mathbb{Z}^2 \}$$

and order them according to

$$s + \sqrt{d}\, t < s' + \sqrt{d}\, t'.$$

**Exercise**: Let $s^2 - td^2 = 1$. Show that the above implies $s < s'$ & $t < t'$.

We call $(s,t) \in \mathbb{Z}^2_{\geq 0}$ with minimum $s + \sqrt{d}\, t$ to be the fundamental solution.

**Ex**: $x^2 - 2y^2 = -1$. The solutions are $(1,1), (7,5), \ldots$ $(1,1)$ is the fundamental solution.

Similarly, for $x^2 - 2y^2 = 1$ the solutions are $(3,2)$, $(17,12)$, ...
The fundamental solution is $(3,2)$.

Thus for $x^2 - 2y^2 = \pm 1$ the fundamental solution is $(1,1)$.

**Ex:** $x^2 - 3y^2 = \pm 1$.
The solutions are $(2,1)$, $(7,4)$, $(26,15)$ ... The fundamental solution is $(2,1)$.

**Note:** $(v_n, w_n)$ are denoted as solutions.

$$v_{n+1}, w_{n+1} = (v_n + 2w_n, \; v_n + w_n)$$

For instance, check $(1,1)$, $(3,2)$, $(7,5)$, $(17,12)$, ...

In other words,

$$v_{n+1} + \sqrt{2}\, w_{n+1} = (v_n + \sqrt{2}\, w_n)(1+\sqrt{2})$$

Or, $v_n + w_n\sqrt{2} = (1+\sqrt{2})^n$

Similarly, for $x^2 - 3y^2 = \pm 1$

$$v_n + w_n\sqrt{3} = (2+\sqrt{3})^n$$

where $(2,3)$ is the fundamental solution of $x^2 - 3y^2 = \pm 1$.

<u>Lemma</u>: Let $(s,t) = (v_1, w_1)$ be the fundamental solution to the Pell's equation $x^2 - dy^2 = \pm 1$. Define $(v_n, w_n)$ by $v_n + \sqrt{d}\, w_n = (s+t\sqrt{d})^n$

Then
$$v_n = \frac{1}{2}\left((s+t\sqrt{d})^n + (s-t\sqrt{d})^n\right)$$
$$w_n = \frac{1}{2\sqrt{d}}\left((s+t\sqrt{d})^n - (s-t\sqrt{d})^n\right)$$

<u>RMK</u>: $(v_n, w_n)$ is different from the $(s_n, t_n)$ which gives rise to the convergent $\frac{s_n}{t_n}$.

<u>Proof</u>: Induction on $n$.

$n=1$ ✓. Let it be true for $n$

i.e.
$$v_n = \frac{1}{2}\left((s+t\sqrt{d})^n + (s-t\sqrt{d})^n\right)$$
$$w_n = \frac{1}{2\sqrt{d}}\left((s+t\sqrt{d})^n - (s-t\sqrt{d})^n\right)$$

Then $\quad v_{n+1} = v_n s + d t w_n$

Because $\quad v_{n+1} + \sqrt{d}\, w_{n+1} = (s + t\sqrt{d})^{n+1}$

$$= (v_n + \sqrt{d}\, w_n)(s + t\sqrt{d})$$

$$= (v_n s + d t w_n) + \sqrt{d}\,(w_n s + t v_n)$$

$$v_{n+1} = \frac{1}{2}\left(s(s+t\sqrt{d})^n + s(s-t\sqrt{d})^n\right)$$

$$+ \frac{1}{2}\sqrt{d}\left(t(s+t\sqrt{d})^n - t(s-t\sqrt{d})^n\right)$$

$$= \frac{1}{2}\left((s+t\sqrt{d})^{n+1} + (s-t\sqrt{d})^{n+1}\right) \quad \square$$

**Theorem 3:** Let $(s,t)$ be the fundamental solution to $x^2 - dy^2 = \pm 1$ and let $s^2 - dt^2 = \varepsilon \in \{+1, -1\}$. Also, as before $(v_n + w_n\sqrt{d}) := (s+t\sqrt{d})^n$. Then $v_n^2 - w_n^2 d = \varepsilon^n$

**Note:** The above implies $(v_n, w_n)$ solves the Pell's equation $x^2 - dy^2 = \pm 1$. Although, we don't know yet if these are the only solutions.

Proof: By the previous lemma

$$v_n - w_n\sqrt{d} = \frac{1}{2}\left((s+t\sqrt{d})^n + (s-t\sqrt{d})^n\right)$$
$$- \frac{\sqrt{d}}{2\sqrt{d}}\left((s+t\sqrt{d})^n - (s-t\sqrt{d})^n\right)$$
$$= (s-t\sqrt{d})^n$$

Thus $v_n^2 - d w_n^2 = (v_n + \sqrt{d}\, w_n)(v_n - \sqrt{d}\, w_n)$

$$= (s+\sqrt{d}\,t)^n (s-\sqrt{d}\,t)^n$$
$$= (s^2 - dt^2)^n = \varepsilon^n.$$

Theorem 4: Let $(v, w)$ be a solution of $x^2 - dy^2 = \pm 1$. Then $(v, w)$ must be of the form $(v_n, w_n)$ for some $n \geq 1$.

RMK: Thus $(v_n, w_n)$ are all possible solutions to $x^2 - dy^2 = \pm 1$ where $v_n + \sqrt{d}\, w_n = (s+\sqrt{d}\,t)^n$ & $(s, t)$ is the fundamental solution to $x^2 - dy^2 = \pm 1$.