# Math 4400
## Week 13 – Thursday
### Rational approximation and Pell's equations

Last time: once we have one solution $(x_1, y_1)$ to $x^2 - Dy^2 = 1$, D squarefree positive integer. can produce many more by

$$(x_1 + y_1\sqrt{D})^k = x_k + y_k\sqrt{D}$$
$$N(\_\_\_^k) = N(\_)^k = 1.$$

Fact: If $(x_1, y_1)$ is the smallest positive integer solution (i.e. $x_1$ smaller than x coordinate of any other or equivalently $y_1$ smaller than y coordinate of any other)

$x^2 = 1 + Dy^2$

then all positive integer solutions are as above.

Example: Last time, $D=2$, the smallest positive integer solution to
$$x^2-2y^2=1$$
was $(x_1,y_1)=(3,2)$

Taking $(x_1+\sqrt{2}\,y_1)^k$ gave all other solutions, thus all square-triangular #s.

To justify fact, we divide by $x_1+\sqrt{D}\,y_1$.

$$\underbrace{(x+y\sqrt{D})}_{x^2-Dy^2=1}\Big/\underbrace{(x_1+y_1\sqrt{D})}_{\text{smallest solution}} = (x+y\sqrt{D})(x_1-y_1\sqrt{D})$$
$$= \underline{xx_1-Dyy_1} + \underline{(x_1y-xy_1)}\sqrt{D}$$

Need to show these are positive — see Theorem 43 on p. 129.

Just keep dividing!

More interesting — to have a smallest solution, first need to know there is <u>at least one</u> positive integer solution!

to Pell's equation $x^2-y^2D=1$.

Key observation: If $x^2 - Dy^2 = 1$ w/ $x, y > 0$

$$(x+\sqrt{D}y)(x-\sqrt{D}y) = 1$$

$$x - \sqrt{D}y = \frac{1}{x+\sqrt{D}y} < \frac{1}{y}.$$

so

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

$\downarrow$ divide by $y$.

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

says $\frac{x}{y}$ is fraction that approximates $\sqrt{D}$ well.

Example: $99^2 - 2 \cdot 70^2 = 1$

$\frac{99}{70} = 1.4142\ldots$ $\sqrt{2} = 1.41421\ldots$

agree up to first 4 decimal places

Idea: Reverse this – use existence of good rational approximations to find a solution.

Pigeonhole principle: If I put $n+1$ pigeons into $n$ pigeonholes, then one pigeonhole holds at least 2 pigeons

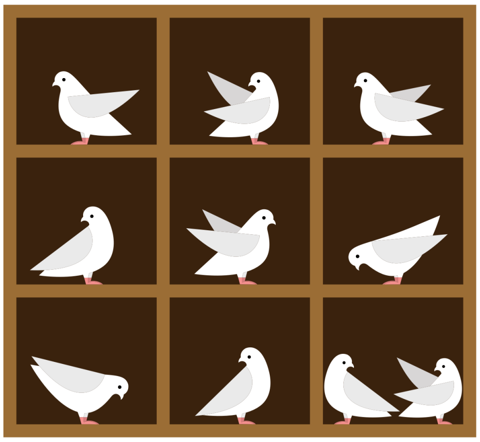

Image source: cantorsparadise.com

Also: If infinitely many pigeons in finitely many pigeonholes, then one pigeonhole holds infinitely many pigeons.

Dirichlet approximation principle: If $\alpha > 0$ is irrational, then there are infinitely many pairs $(x,y)$ of positive integers such that

$$\left| \frac{x}{y} - \alpha \right| < \frac{1}{y^2}.$$

$n=3$

$[\ )[\ )[\ )[\ )$ subdivide $[0,1)$ into intervals of length $\frac{1}{n}$.

Proof: Let $n > 0$.

$n$ Pigeonholes – $[0,\frac{1}{n}), [\frac{1}{n},\frac{2}{n}), [\frac{2}{n},\frac{3}{n}), \dots, [\frac{n-1}{n}, 1)$.

$n+1$ Pigeons – $\{0 \cdot \alpha\}$ $\{1 \cdot \alpha\}$ ..... $\{n\alpha\}$

$\{\beta\} = \beta - \lfloor \beta \rfloor$ is the fractional part.

Pigeonhole principle $\Rightarrow$ there is $0 \le k \le n-1$ and $0 \le i < j \le n$ s.t. $\{i\alpha\}$ and $\{j\alpha\}$ are both in $[\frac{k-1}{n}, \frac{k}{n})$.

so $(j-i)\alpha = j\alpha - i\alpha = \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor + \{j\alpha\} - \{i\alpha\}$

$$\alpha = \frac{\lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor}{j-i} + \frac{\{j\alpha\} - \{i\alpha\}}{j-i}$$

$$\alpha = \frac{x}{y} + \varepsilon \qquad y = j-i$$

$$|\varepsilon| = \frac{|\{j\alpha\} - \{i\alpha\}|}{j-i=y} < \frac{\frac{1}{n}}{y} = \frac{1}{ny} < \frac{1}{y^2}.$$

$n > j-i=y$

$\boxtimes$

Existence of solutions to Pell's equation:

For any $n$, positive integers $x \le n\sqrt{D}$ $y \le n$ s.t. $|x - y\sqrt{D}| < \frac{1}{n}$ (see proof of Dirichlet)

Then $N(x+y\sqrt{D}) = (x+y\sqrt{D})(x-y\sqrt{D}) < \frac{2n\sqrt{D}}{n} = 2\sqrt{D}$

Pigeonhole (again!) $\Rightarrow$ $\exists$ $m < 2\sqrt{D}$ s.t. $N(x+y\sqrt{D}) = m$ has infinitely many positive integer solutions $(x,y)$

For any two,

$$N\left(\frac{x_1+y_1\sqrt{D}}{x_2+y_2\sqrt{D}}\right) = \frac{N(x_1+y_1\sqrt{D})}{N(x_2+y_2\sqrt{D})} = \frac{m}{m} = 1.$$

$$\frac{x_1+y_1\sqrt{D}}{x_2+y_2\sqrt{D}} = \frac{(x_1+y_1\sqrt{D})(x_2-y_2\sqrt{D})}{m}$$

$$= \underbrace{\frac{x_1x_2 - y_1y_2D}{m}} + \underbrace{\frac{(y_1x_2 - x_1y_2)}{m}}\sqrt{D}$$

want integers.

Pigeonhole principle one more time:

Can assume $x_1 \equiv x_2 \bmod m$ and $y_1 \equiv y_2 \bmod m$.

(Pigeonholes — $(a,b)$ in $(\mathbb{Z}/m\mathbb{Z})^2$
$x \equiv a$, $y \equiv b$ ).

Then $x_1 x_2 - y_1 y_2 D \equiv x_1^2 - y_1^2 D \equiv m \equiv 0 \bmod m$

$y_1 x_2 - x_1 y_2 \equiv y_1 x_1 - x_1 y_1 \equiv 0 \bmod m.$