GR

Pell's Equation:

Solve $x^2 - ny^2 = N$ with $x, y \in \mathbb{Z}$.

This is an example of a Diophantine equation

Continued fractions can help us solve this:

WOLOG $x, y \geq 0$

If $n < 0$ then $N = x^2 - ny^2 \geq x^2 + y^2 \implies$ finitely many solutions

If n is a perfect square $n = p^2$

$N = x^2 - p^2y^2 = (x - py)(x + py) \implies$

$x - py = a$
$x + py = b$ with $ab = N$

(fin many choices $\implies$ fin many x, y.

$\implies 2x = a + b$
$2py = a - b$

But if $n>0$ is not a perfect square, then

$$\sqrt{n} = \langle \lfloor \sqrt{n} \rfloor, \overline{a_1, \ldots, a_{m-1}, 2\lfloor \sqrt{n} \rfloor} \rangle \quad \text{is irrational.}$$

Then note that, with $x, y \geq 0$

$$1 \leq N = x^2 - ny^2 = (x - \sqrt{n}y)(x + \sqrt{n}y) \quad \underline{\text{implies}}$$

$$\frac{N}{x+\sqrt{n}y} = x - \sqrt{n}y \quad \Rightarrow \quad \frac{|N|}{|x+\sqrt{n}y||y|} = \left| \sqrt{n} - \frac{x}{y} \right|$$

and $x - \sqrt{n}y > 0$ so $x > \sqrt{n}y$ so $\frac{x}{y\sqrt{n}} > 1$

so $\frac{x}{y\sqrt{n}} + 1 = \frac{x+y\sqrt{n}}{y\sqrt{n}} > 2$ so $x + y\sqrt{n} > 2y\sqrt{n}$

so $\left| \sqrt{n} - \frac{x}{y} \right| < \frac{|N|}{(2y\sqrt{n})(y)} = \frac{|N|}{\sqrt{n}} \frac{1}{2y^2}$

$\underline{\text{so}}$ if $N < n^2$ ($\sqrt{n}$?), then $x^2 - ny^2 = N \Longrightarrow$

$$\left| \sqrt{n} - \frac{x}{y} \right| < \frac{1}{2y^2} \Longrightarrow \frac{x}{y} \text{ is a } \underline{\text{convergent}} \text{ of } \sqrt{n}.$$

Focus on $N = \underline{1}$. So solutions to $x^2 - ny^2 = 1$

are $(x, y) = (h_r, k_r)$ for some r's.

$\underline{\text{Which ones}}$?

$\sqrt{n} = \langle a_0, \overline{a_1, \ldots, a_{m-1}, 2a_0} \rangle$ <u>means</u>

$$\sqrt{n} + a_0 = \langle \overline{2a_0, a_1, \ldots, a_{m-1}} \rangle = \langle 2a_0, a_1, \ldots, a_{m-1} + x_{m-1} \rangle$$
$$= \langle 2a_0, a_1, \ldots, a_{m-1}, \tfrac{1}{x_{m-1}} \rangle = \langle 2a_0, a_1, \ldots, a_{m-1}, \sqrt{n} + a_0 \rangle$$

<u>So</u> $\sqrt{n} = \langle a_0, \ldots, a_{m-1}, \sqrt{n} + a_0 \rangle$

<u>So</u> $\sqrt{n} = \dfrac{(\sqrt{n} + a_0) h_{m-1} + h_{m-2}}{(\sqrt{n} + a_0) k_{m-1} + k_{m-2}}$, <u>so</u>

$$\sqrt{n}\left((\sqrt{n} + a_0) k_{m-1} + k_{m-2}\right) = (\sqrt{n} + a_0) h_{m-1} + h_{m-2}$$

<u>So</u> $\sqrt{n}(a_0 k_{m-1} + k_{m-2} - h_{m-1}) = a_0 h_{m-1} + h_{m-2} - n k_{m-1}$

<u>So</u> $a_0 k_{m-1} + k_{m-2} - h_{m-1} = 0 \qquad a_0 h_{m-1} + h_{m-2} - n k_{m-1} = 0$

<u>So</u> $h_{m-1} = a_0 k_{m-1} + k_{m-2} \qquad n k_{m-1} = a_0 h_{m-1} + h_{m-2}$

<u>So</u> $h_{m-1}^2 - n k_{m-1}^2 = (a_0 k_{m-1} + k_{m-2}) h_{m-1} - (a_0 h_{m-1} + h_{m-2}) k_{m-1}$
$= k_{m-2} h_{m-1} - h_{m-2} k_{m-1} = (-1)^{m}$

If this is 1, we're <u>done</u>. If it is -1, then m is <u>odd</u>, so turn the crank <u>again</u>

$$\sqrt{n} = \langle a_0, \ldots, a_{m-1}, \underset{a_m}{2a_0}, \ldots, \underset{a_{2m-1}}{a_{m-1}}, \sqrt{n} + a_0 \rangle;$$

Same argument implies that

$$\sqrt{n} = \frac{(\sqrt{n}+a_0)h_{2m-1} + h_{2m-2}}{(\sqrt{n}+a_0)k_{2m-1} + k_{2m-2}} \quad \text{so}$$

$$h_{2m-1}^2 - nk_{2m-1}^2 = k_{2m-2}h_{2m-1} - h_{2m-2}k_{2m-1} = (-1)^{2m} = 1$$

In general, we get $h_{tm-1}^2 - nk_{tm-1}^2 = (-1)^{tm}$

In fact, wherever we stop,

$$\sqrt{n} = \langle a_0, \dots, a_s, \frac{\sqrt{n}+a}{b} \rangle, \text{ we get}$$

$$\sqrt{n} = \frac{\left(\frac{\sqrt{n}+a}{b}\right)h_s + h_{s-1}}{\left(\frac{\sqrt{n}+a}{b}\right)k_s + k_{s-1}} = \frac{(\sqrt{n}+a)h_s + bh_{s-1}}{(\sqrt{n}+a)k_s + bk_{s-1}}$$

$$\sqrt{n}\left((\sqrt{n}+a)k_s + bk_{s-1}\right) = (\sqrt{n}+a)h_s + bh_{s-1}$$

$$\sqrt{n}(ak_s + bk_{s-1} - h_s) = ah_s + bh_{s-1} - nk_s \quad \text{so}$$

$$h_s = ak_s + bk_{s-1}, \quad nk_s = ah_s + bh_{s-1} \quad \text{so}$$

$$h_s^2 - nk_s^2 = ak_sh_s + bh_sk_{s-1} - ah_sk_s - bh_{s-1}k_s$$

$$= b(h_sk_{s-1} - h_{s-1}k_s) = b(-1)^{s-1}$$

$n = 19$:

$x^2 - 19y^2 = 1 \qquad x^2 = 1 + 19y^2 \qquad \left(\frac{x}{y}\right)^2 - 19 = \frac{1}{y^2}$

$\sqrt{19}$

$a_0 = 4 \quad x_0 = \sqrt{19} - 4 \quad \frac{1}{\sqrt{19}-4} = \frac{\sqrt{19}+4}{3}$

$a_1 = 2 \quad x_1 = \frac{\sqrt{19}-2}{3} \quad \frac{3}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{5}$

$a_2 = 1 \quad x_2 = \frac{\sqrt{19}-3}{5} \quad \frac{5}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{2}$

$a_3 = 3 \quad x_3 = \frac{\sqrt{19}-3}{2} \quad \frac{2}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{5}$

$a_4 = 1 \quad x_4 = \frac{\sqrt{19}-2}{5} \quad \frac{5}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{3}$

$a_5 = 2 \quad x_5 = \frac{\sqrt{19}-4}{3} \quad \frac{3}{\sqrt{19}-4} = \sqrt{19}+4$

$a_6 = 8 \quad x_6 = \sqrt{19} - 4 = \underline{x_0}$.

$\sqrt{19} = \langle 4, \overline{2, 1, 3, 1, 2, 8} \rangle$

$h_0 = 4 \quad h_1 = 9 \quad h_2 = 13 \quad h_3 = 48 \quad h_4 = 61 \quad h_5 = 170 \quad h_6 = 1421$

$k_0 = 1 \quad k_1 = 2 \quad k_2 = 3 \quad k_3 = 11 \quad k_4 = 14 \quad k_5 = 39 \quad k_6 = 325$

$170^2 - 19(39)^2 =$

$28900 - 19 \cdot 1521 = 28900 - 28899 = \underline{1}$

$\begin{array}{r} 1521 \\ \times\ 19 \\ \hline 13689 \\ 1521 \\ \hline 28899 \end{array}$

$$= \langle a_0, a_1, \ldots, a_m, \underset{m+1}{2a_0}, a_1, \ldots, \underset{2m+1}{a_m}, \sqrt{n}+a_0 \rangle$$

$$\sqrt{n} = \langle a_0, \overline{a_1, \ldots, a_m, \underset{a_{m+1}}{2a_0}} \rangle$$

$$= \langle a_0, a_1, \ldots, a_m + x_m \rangle$$

$$= \langle a_0, a_1, \ldots, a_m, \frac{1}{x_m} \rangle = \langle a_0, a_1, \ldots, a_m, \sqrt{n}+a_0 \rangle$$

$$= \frac{(\sqrt{n}+a_0)h_m + h_{m-1}}{(\sqrt{n}+a_0)k_m + k_{m-1}}$$

8

$$\cancel{\sqrt{n} = \langle a_0, a_1} \quad \sqrt{n}\left((\sqrt{n}+a_0)k_m + k_{m-1}\right) = (\sqrt{n}+a_0)h_m + h_{m-1}$$

$$\sqrt{n}\left(a_0 k_m + k_{m-1} - h_m\right) = a_0 h_m + h_{m-1} - n k_m$$

$$\Rightarrow a_0 k_m + k_{m-1} - h_m = 0 = a_0 h_m + h_{m-1} - n k_m$$

$$\to h_m = a_0 k_m + k_{m-1} \qquad n k_m = a_0 h_m + h_{m-1}$$

$$\Rightarrow h_m^2 - n k_m^2 = h_m(a_0 k_m + k_{m-1}) - k_m(a_0 h_m + h_{m-1})$$

$$= h_m k_{m-1} - k_m h_{m-1} = (-1)^{m+1}$$