Let D be a fixed positive integer and it is not a square.

Pell's equation: $x^2 - Dy^2 = 1$.

Question: Find all positive integral solutions for Pell's equation.

Theorem (Pell's equation theorem) Let D is a positive integer that is not a perfect square. The Pell's equation

$$x^2 - Dy^2 = 1$$

always have infinitely many solutions in positive integers.

Moreover, let (x_1, y_1) be a solution with smallest x_1, then every solution (x_k, y_k) can be obtained by taking powers:

$$x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k \quad \text{for } k = 1, 2, 3, \ldots$$

Some facts: let D be a positive integers and it is not a square. Then

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$$

with
$$(a+b\sqrt{D}) + (c+d\sqrt{D}) = (a+c) + (b+d)\sqrt{D}$$
$$(a+b\sqrt{D}) \cdot (c+d\sqrt{D}) = (ac+bdD) + (ad+bc)\sqrt{D}$$

is a field.

For $\alpha = a + b\sqrt{D} \in \mathbb{Q}$, we can define its conjugate by:

$$\overline{\alpha} = a - b\sqrt{D}.$$

Then $\alpha \cdot \overline{\alpha} = a^2 - b^2 D$.

Check: $\underbrace{(a^2 - b^2 D)}_{\alpha \cdot \overline{\alpha}} \underbrace{(c^2 - d^2 D)}_{\beta \cdot \overline{\beta}} = \underbrace{(ac + bd\,D)^2 - (ad + bc)^2 \cdot D}_{(\alpha\beta) \cdot (\overline{\alpha}\,\overline{\beta})}$

Note: $\alpha = x + y\sqrt{D}$ and (x, y) is a solution for Pell's equation.

Then $\alpha \cdot \overline{\alpha} = 1$.

We will skip the proof of "Moreover" part.

Pigeonhole Principle: suppose that we have infinitely many pigeons but only finitely many pigeonholes. Then there exists a pigeonhole with infinitely many pegions.

Lemma: Let (x, y) be a pair of positive integers satisfying $|x - y\sqrt{D}| < \frac{1}{y}$, then:

$$|x^2 - y^2 D| < 3\sqrt{D}.$$

Proof: $|x^2-y^2D| = |x+y\sqrt{D}| \cdot |x-y\sqrt{D}|$

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

$$\Rightarrow \quad -\frac{1}{y}+y\sqrt{D} < x < y\sqrt{D}+\frac{1}{y}$$

$$-3y\sqrt{D} < -\frac{1}{y}+2y\sqrt{D} < x+y\sqrt{D} < 2y\sqrt{D}+\frac{1}{y} < 3y\sqrt{D}$$

$$\Rightarrow \quad |x+y\sqrt{D}| < 3y\sqrt{D}$$

$$\Rightarrow \quad |x^2-y^2\sqrt{D}| = |x+y\sqrt{D}|\,|x-y\sqrt{D}|$$

$$< 3y\sqrt{D} \cdot \frac{1}{y} = 3\sqrt{D}. \qquad \square$$

Next page for the proof of the theorem.

Proof of Theorem: Set $T = \lfloor 3\sqrt{D} \rfloor$

For $-T \leq n \leq T$, n an integer, we define:

$$\mathcal{A}(n) = \{ (x,y) : |x - y\sqrt{D}| < \frac{1}{y} \text{ and } x^2 - y^2 D = n \}$$

By Dirichele's Diophatine Approximation theorem, there are infinitely many pairs (x,y) satisfying $|x - y\sqrt{D}| < \frac{1}{y}$

(x,y) ---- pigeons --- infinitely many

By Lemma, if $|x - y\sqrt{D}| < \frac{1}{y}$, then $(x,y) \in \mathcal{A}(n)$ for some $n \in [-T, T]$

$\mathcal{A}(n)$ ---> pigeonhole --- finitely many $(2T+1)$

By Pigeonhole principle, there exists an $M \in [-T, T]$ and $\mathcal{A}(M)$ contains infinitely many pairs of (x,y)

Now $\mathcal{A}(M) = \{ (x,y) : |x - y\sqrt{D}| < \frac{1}{y}, \ x^2 - y^2\sqrt{D} = M \}$

has infinitely many solutions. ..

(x,y) --- pigeon --- infinitely many.

Next, for each $(x, y) \in \mathcal{A}(M)$, we consider

$$(x \pmod M,\ y \pmod M)$$

$$(a \pmod M,\ b \pmod M)_{\substack{0 \le a \le M-1 \\ 0 \le b \le M-1}}$$

... pigeon hole ... finitely many (at most M^2)

Then we can find $0 \le a, b \le M-1$ such that

$$\mathcal{A}(M; a, b) = \left\{ (x, y) : \begin{array}{l} |x - y\sqrt{D}| < \frac{1}{y},\ x^2 - Dy^2 = M \\ x \equiv a \pmod M \quad y \equiv b \pmod M \end{array} \right\}$$

contains ∞-many elements.

Take $(x_1, y_1) \neq (x_2, y_2) \in \mathcal{A}(M; a, b)$.

Then
$$x_1 \equiv x_2 \pmod M \qquad x_1^2 - y_1^2 D = M$$
$$y_1 \equiv y_2 \pmod M \qquad x_2^2 - y_2^2 D = M$$

Assume $x_1 > x_2 \ (>0)$ then $y_1 > y_2 > 0$

Set: $$x + y\sqrt{D} = \frac{x_1 - y_1\sqrt{D}}{x_2 - y_2\sqrt{D}} = \frac{(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D})}{x_2^2 - y_2^2 D}$$

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

$$= \frac{x_1x_2 - y_1y_2 D}{M} + \frac{x_1y_2 - x_2y_1}{M}\sqrt{D}$$

Claim: (x, y) is a solution for Pell's equation.

Proof of Claim: (We need to show:

① $(x, y) \neq (0,0)$

② $x^2 - y^2 D = 1$

③ x, y are integers.)

② : $$x^2 - y^2 D = \left(\frac{x_1x_2 - y_1y_2 D}{M}\right)^2 - \left(\frac{x_1y_2 - x_2y_1}{M}\right)^2 \cdot D$$

$$= \frac{(x_1^2 - y_1^2 D)(x_2^2 - y_2^2 D)}{M^2} = \frac{M^2}{M^2} = 1.$$

③ $x_1x_2 - y_1y_2 D \equiv x_1^2 - y_1^2 D \pmod{M} \equiv 0 \pmod{M}$

$\Rightarrow$ $x = \frac{x_1x_2 - y_1y_2 D}{M}$ is an integer.

$x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \pmod{M} \equiv 0 \pmod{M}$

$\Rightarrow$ $y = \frac{x_1y_2 - x_2y_1}{M}$ is an integer.

① : Both x, y are integers and $x^2 - Dy^2 = 1$

$\Rightarrow$ $x \neq 0$. We show: $y \neq 0$.

If $y = 0$, then $x_1y_2 = x_2y_1$

$$y_2^2 \cdot M = y_2^2(x_1^2 - y_1^2 D) = y_2^2 x_1^2 - y_1^2 y_2^2 D$$
$$= x_2^2 y_1^2 - y_1^2 y_2^2 D = y_1^2(x_2^2 - y_2^2 D)$$
$$= y_1^2 M$$

This forces: $y_1^2 = y_2^2 \Longrightarrow y_1 = y_2$ ($y_1, y_2 > 0$)

A contradiction ($(x_1, y_1) \neq (x_2, y_2)$)

This process also shows: every time we have

$(x_1, y_1) \neq (x_2, y_2) \in \mathcal{A}(M; a, b)$, we can get a

solution for $x^2 - Dy^2 = 1$.

$\mathcal{A}(M; a, b)$ contains infinitely many solutions and

hence there are infinitely many solutions for

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

$\square$