Higher Diophantine equations

Question (Diophantine equations)

Given a multivariable integer polynomial P, find integer (or rational) solutions $\mathbf{x} = (x_i)_i$ of the equation

$$P(\mathbf{x}) = 0.$$

Question (Diophantine equations)

Given a multivariable integer polynomial P, find integer (or rational) solutions $\mathbf{x} = (x_i)_i$ of the equation

$$P(\mathbf{x}) = 0.$$

Example 3.8.1 (Pythagorean Triples)

Find all triples of integers (a, b, c) such that

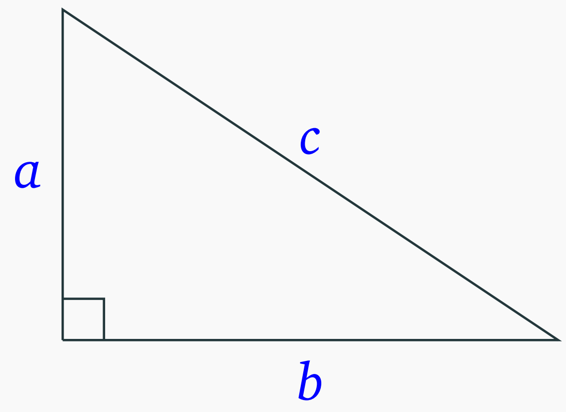
$$a^2 + b^2 = c^2.$$

Example 3.8.1 (Pythagorean Triples)

Find all triples of integers (a, b, c) such that

$$a^2 + b^2 = c^2.$$

The terminology comes from the *Pythagorean theorem*:



To figure out all solutions of 3.8.1, we first note that

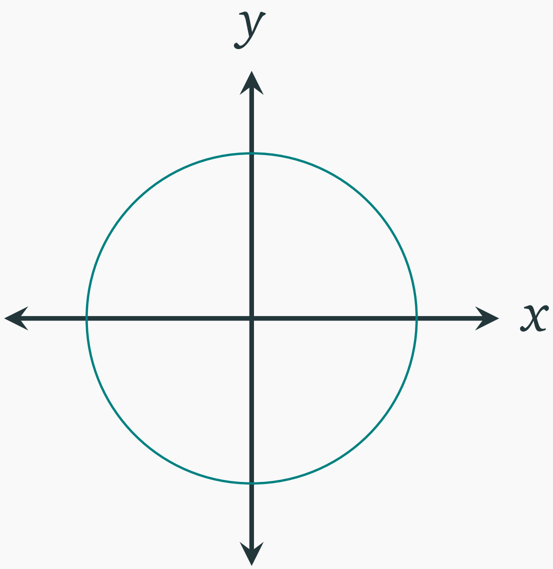
- $(0,0,0)$ is a solution (the *trivial solution*) of the equation

$$a^2 + b^2 = c^2.$$

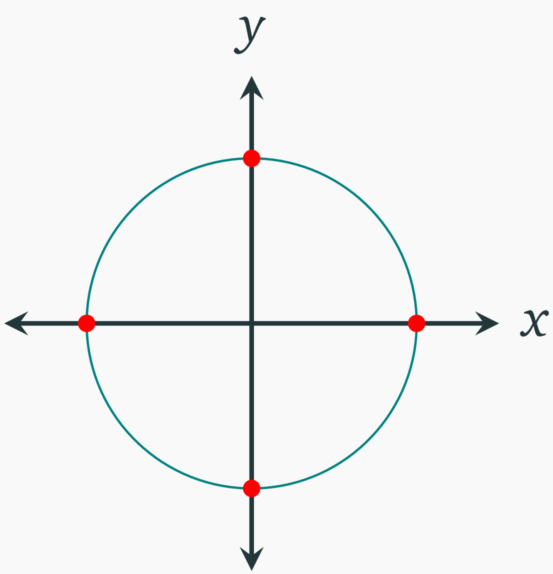
- Any *nontrivial* solution (a,b,c) gives a *rational* solution $(\frac{a}{c}, \frac{b}{c})$ of the equation

$$X^2 + Y^2 = 1.$$

Recall that the equation $X^2 + Y^2 = 1$ defines the unit circle.

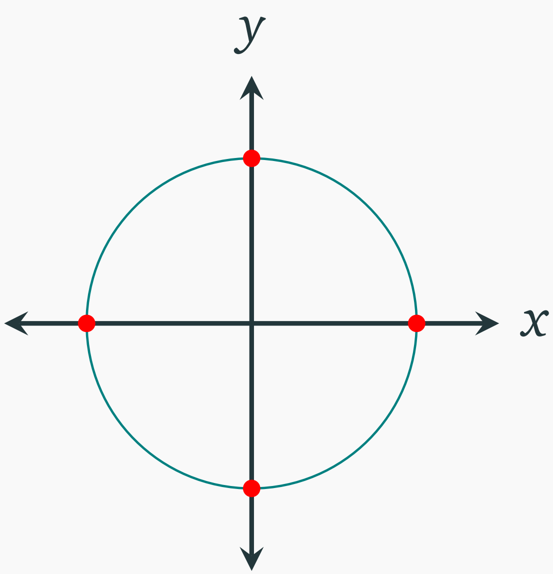


Recall that the equation $X^2 + Y^2 = 1$ defines the unit circle.



The *rational* solutions of the equation correspond to the *rational points* on the unit circle. For instance, $(1, 0)$, $(0, 1)$, $(-1, 0)$, and $(0, -1)$ are four obvious rational points on the unit circle.

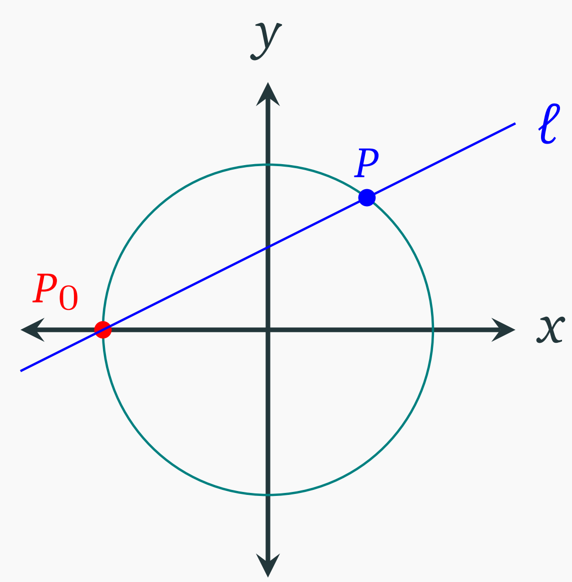
Recall that the equation $X^2 + Y^2 = 1$ defines the unit circle.



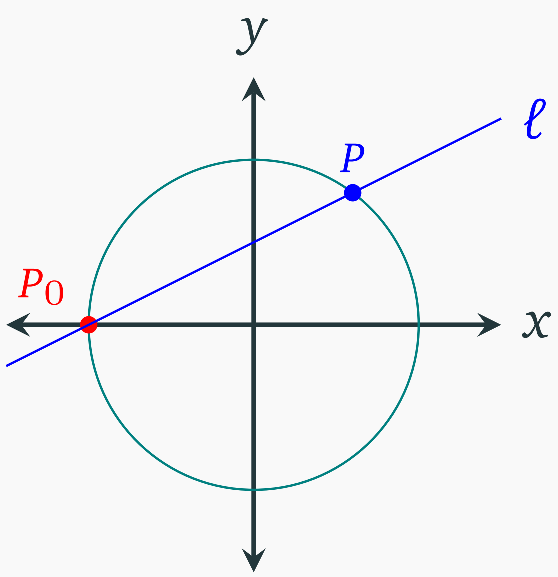
The *rational* solutions of the equation correspond to the *rational points* on the unit circle. For instance, $(1, 0)$, $(0, 1)$, $(-1, 0)$, and $(0, -1)$ are four obvious rational points on the unit circle.

The question is: what are all the rational points on the unit circle?

We start with a specific rational point, saying $P_0 = (-1, 0)$. Draw a (non-vertical) line ℓ through P_0, then it intersects with the unit circle by a point $P = (x, y)$.



We start with a specific rational point, saying $P_0 = (-1, 0)$. Draw a (non-vertical) line ℓ through P_0, then it intersects with the unit circle by a point $P = (x, y)$.



If P is a rational point, then the *slope* of ℓ is

$$\frac{y - 0}{x - (-1)} = \frac{y}{x + 1},$$

which is a rational number.

Conversely, suppose the *slope* of ℓ is a rational number t. Then the intersection point $P = (x, y)$ satisfies the system of equations:

$$\begin{cases} y = t(x+1), \\ x^2 + y^2 = 1. \end{cases}$$

Conversely, suppose the *slope* of ℓ is a rational number t. Then the intersection point $P = (x, y)$ satisfies the system of equations:

$$\begin{cases} y = t(x+1), \\ x^2 + y^2 = 1. \end{cases}$$

Solving it, we get:

$$x^2 + t^2(x+1)^2 = 1$$

Conversely, suppose the *slope* of ℓ is a rational number t. Then the intersection point $P = (x, y)$ satisfies the system of equations:

$$\begin{cases} y = t(x+1), \\ x^2 + y^2 = 1. \end{cases}$$

Solving it, we get:

$$\begin{aligned} & x^2 + t^2(x+1)^2 = 1 \\ \iff & x^2 - 1 + t^2(x+1)^2 = 0 \end{aligned}$$

Conversely, suppose the *slope* of ℓ is a rational number t. Then the intersection point $P = (x, y)$ satisfies the system of equations:

$$\begin{cases} y = t(x+1), \\ x^2 + y^2 = 1. \end{cases}$$

Solving it, we get:

$$\begin{aligned} & x^2 + t^2(x+1)^2 = 1 \\ \iff\ & x^2 - 1 + t^2(x+1)^2 = 0 \\ \iff\ & x - 1 + t^2(x+1) = 0 \end{aligned}$$

Conversely, suppose the *slope* of ℓ is a rational number t. Then the intersection point $P = (x, y)$ satisfies the system of equations:

$$\begin{cases} y = t(x+1), \\ x^2 + y^2 = 1. \end{cases}$$

Solving it, we get:

$$\begin{aligned} & x^2 + t^2(x+1)^2 = 1 \\ \iff & x^2 - 1 + t^2(x+1)^2 = 0 \\ \iff & x - 1 + t^2(x+1) = 0 \\ \iff & x = \frac{1-t^2}{1+t^2}. \end{aligned}$$

Conversely, suppose the *slope* of ℓ is a rational number t. Then the intersection point $P = (x, y)$ satisfies the system of equations:

$$\begin{cases} y = t(x+1), \\ x^2 + y^2 = 1. \end{cases}$$

Solving it, we get:

$$\begin{aligned} & x^2 + t^2(x+1)^2 = 1 \\ \iff & x^2 - 1 + t^2(x+1)^2 = 0 \\ \iff & x - 1 + t^2(x+1) = 0 \\ \iff & x = \frac{1-t^2}{1+t^2}. \end{aligned}$$

Hence, $P = (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ is a rational point.

We thus proved the following.

Lemma 3.8.2

Fix a rational point $P_0 = (-1, 0)$ on the unit circle. Then the rational points on the unit circle other than P_0 are one-one corresponding to lines through P_0 with slope $t \in \mathbb{Q}$.

We thus proved the following.

Lemma 3.8.2

Fix a rational point $P_0 = (-1, 0)$ on the unit circle. Then the rational points on the unit circle other than P_0 are one-one corresponding to lines through P_0 with slope $t \in \mathbb{Q}$.

This lemma allows we to parameterize the solution set

$$\left\{(x, y) \in \mathbb{Q}^2 \,\middle|\, x^2 + y^2 = 1\right\}$$

in $\mathbb{Q} \cup \{\infty\}$ (where P_0 corresponds to ∞).

Theorem 3.8.3 (Pythagorean Triples)

The Pythagorean triples are given by

$$
\begin{aligned}
\left\{(a, b, c) \in \mathbb{Z}^3 \,\middle|\, a^2 + b^2 = c^2\right\} \\
&= \mathbb{Z} \cdot \left\{(n^2 - m^2, 2mn, m^2 + n^2) \,\middle|\, (m, n) \in \mathbb{Z}^2\right\}
\end{aligned}
$$

Proof. Up to scales, the Pythagorean triples (a, b, c) correspond to rational points $(\frac{a}{c}, \frac{b}{c})$ and thus correspond to $\frac{m}{n} \in \mathbb{Q} \cup \{\infty\}$. □