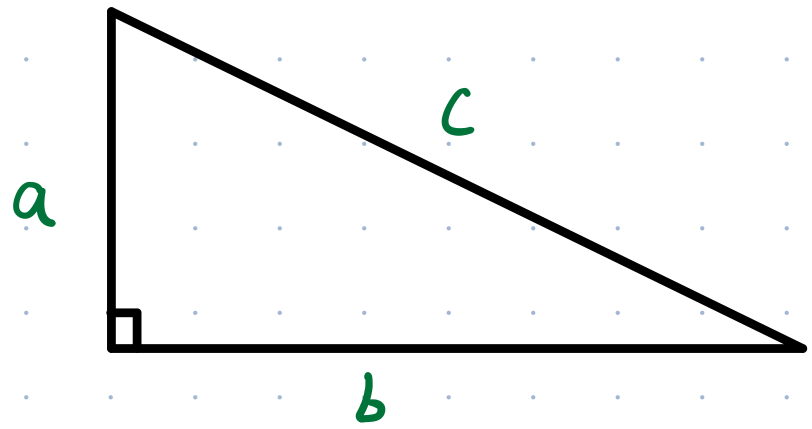
A Pythagroean triple (a, b, c)

consists of 3 positive integers s.t.

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



E.g.: $3^2+4^2=5^2$, $5^2+12^2=13^2$, ...

Q: What are all the Pythagroean triples?

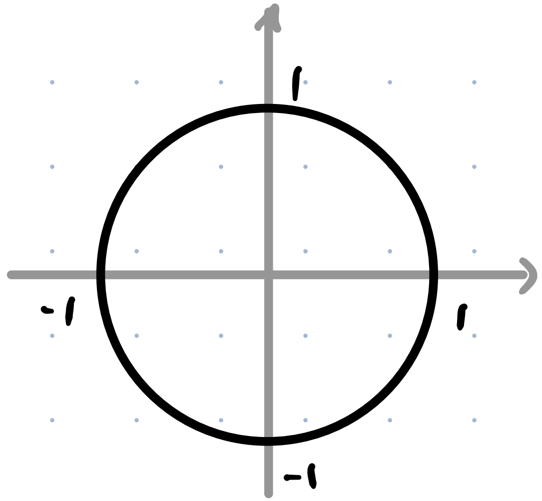
This is a Diophantine equation Problem:

$$S_1 := \{ \text{Solutions to } x^2+y^2=z^2 \text{ in } \mathbb{Z} \}$$

$S_2 := \{$ Solutions to $x^2 + y^2 = 1$ in $\mathbb{Q} \}$

Geometric interpretation: rational points on unit circle.

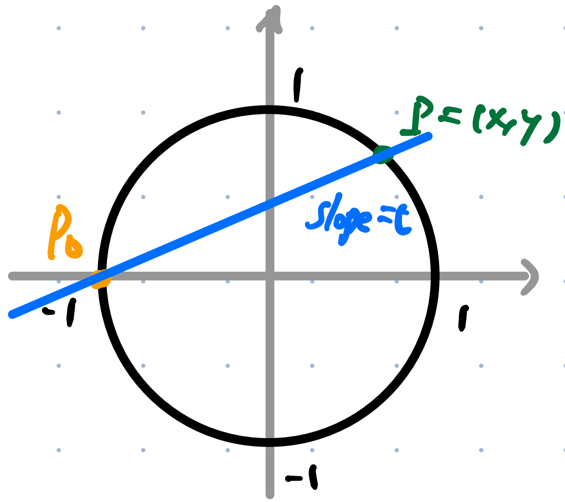
(coordinates are rational numbers)



Obvious ones:

$(1,0)$, $(0,1)$, $(-1,0)$, $(0,-1)$

Specific solutions.



Q: Can we construct general solutions from them?

Yes. from anyone of them.

Prop. Let $P_0 = (-1, 0)$. There is a bijection

$$\left\{ \begin{array}{l} P = (x,y) \in \mathbb{Q}^2 \\ \text{other than } P_0 \end{array} \,\middle|\, x^2 + y^2 = 1 \right\} \xleftrightarrow{\ \sim\ } \left\{ \begin{array}{l} \text{lines through } P_0 \\ \text{with slope } t \in \mathbb{Q} \end{array} \right\}$$

Proof: $f: P = (\overset{\neq -1}{x}, y) \longmapsto$ the line L through P_0 and P

Note that L has slope $\dfrac{y - 0}{x - (-1)} = \dfrac{y}{x+1}$ is rational since x and y are rational.

$g: L \longmapsto$ the other intersection point P of L and the unit circle

Note that L has defining equation:

$$y = t(x - (-1)) = t(x+1)$$

The equation of unit circle is $x^2 + y^2 = 1$.

Hence, the intersection point P is given by

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

which is equivalent to solve

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

$$\Longleftrightarrow \quad x^2 - 1 + t^2(x+1)^2 = 0$$

divided by $x+1$

$$\Longleftrightarrow \quad x - 1 + t^2(x+1) = 0$$

$$\Longleftrightarrow \quad x = \frac{1-t^2}{1+t^2}$$

Hence, $y = t(x+1) = \dfrac{2t}{1+t^2}$.

The point P is $\left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$. which is a rational point since t is rational.

You can verify $f \circ g = id$ & $g \circ f = id$ $\square$

Coro. (General solution of $x^2+y^2=z^2$)

$$\{(x,y,z)\in\mathbb{Z}^3 \mid x^2+y^2=z^2\}$$

$$= \mathbb{Z}\cdot\{(m^2-n^2,\ 2mn,\ m^2+n^2) \mid (m,n)\in\mathbb{Z}^2\}$$

Pf:

$$\underset{\text{other than }(0,0,0)}{\{(x,y,z)\in\mathbb{Z}^3 \mid x^2+y^2=z^2\}} \longrightarrow \{P=(x,y)\in\mathbb{Q}^2 \mid x^2+y^2=1\}$$

$$(x,y,z)\ (z\neq 0) \longmapsto \left(\frac{x}{z}, \frac{y}{z}\right)$$

$$??? \longmapsto \left(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2}\right) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

$k\cdot(m^2-n^2,\ 2mn,\ m^2+n^2)$

$$\frac{n}{m} = t$$

$\{$ lines through P_0 with slope $t\in\mathbb{Q}$ $\}$

Q: What are solutions of $x^2 + y^2 = N$ in $\mathbb{Q}$? ($N \neq 1$)

(Sum of squares)

- Note that:

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$$

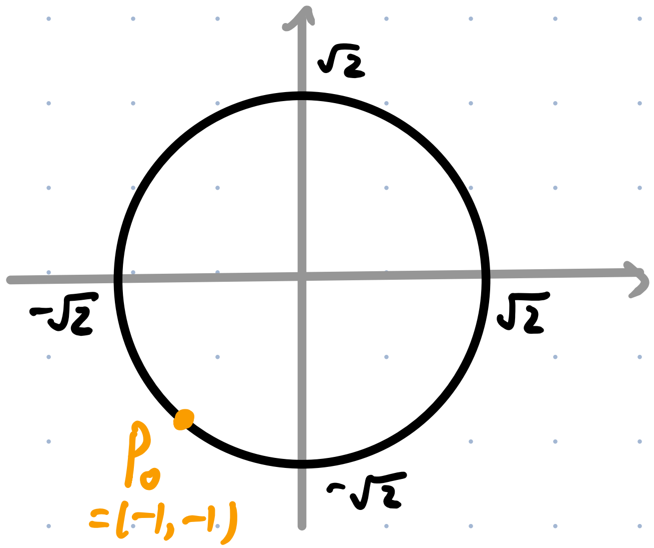
(how can one think of this?)

$$\underset{A}{\parallel} \cdot \underset{B}{\parallel} = N$$

So we only need to consider: N = prime case.

- $x^2 + y^2 = 2.$

obvious sol: $(\pm 1, \pm 1)$



Suppose $P = (x, y)$ is a sol other than P_0, then the line through them is has slope $\frac{y+1}{x+1} \in \mathbb{Q}$.

Conversely, any such a line with slope $t \in \mathbb{Q}$ intersects with the circle by P_0 and $\left(\frac{1+2t-t^2}{1+t^2}, \frac{t^2+2t-1}{1+t^2}\right)$

$$\begin{cases} y = t(x+1) - 1 \\ x^2 + y^2 = 2 \end{cases} \quad (x \neq -1)$$

$$\rightsquigarrow \quad x^2 + t^2(x+1)^2 - 2t(x+1) - 1 = 0$$

divided by $x+1$

$$\rightsquigarrow \quad x - 1 + t^2(x+1) - 2t = 0$$

$$\rightsquigarrow \quad x = \frac{1+2t-t^2}{1+t^2} \quad \rightsquigarrow \quad y = \frac{t^2+2t-1}{1+t^2}$$

Conclusion:

$$\{\underbrace{(x,y)\in\mathbb{Q}^2}_{\text{other than } P_0} \mid x^2+y^2=2\} = \left\{\left(\frac{1+2t-t^2}{1+t^2}, \frac{t^2+2t-1}{1+t^2}\right) \,\middle|\, t\in\mathbb{Q}\right\}$$

- $x^2+y^2=3$. any obvious one? Nope.

Indeed, it has no rational solution!

Proof: Need to show: $a^2+b^2=3c^2$ has no integer solution.

If (a,b,c) is such a solution. Then so does $\left(\frac{a}{g}, \frac{b}{g}, \frac{c}{g}\right)$, where $g=GCD(a,b,c)$.

Hence, we may assume $GCD(a,b,c)=1$.

- Could a, b being both even? No, this implies c is even.

- Could a, b being one odd one even?

$$\begin{cases} a = 2m \\ b = 2n+1 \end{cases} \rightarrow 3c^2 = (2m)^2 + (2n+1)^2$$

$$= 4m^2 + 4n^2 + 4n + 1 \quad ①$$

So c is odd.

But if $c = 2k+1$, we have

$$3c^2 = 3(2k+1)^2 = 12k^2 + 12k + 3 \quad ②$$

Compare ① & ②:

If we divide ① by 4, it has remindar 1

If we divide ② by 4, it has remindar 3

So they CANNOT EQUAL!

- Could a, b both odd?

$$\begin{cases} a = 2m+1 \\ b = 2n+1 \end{cases} \rightsquigarrow 3c^2 = (2m+1)^2 + (2n+1)^2$$

$$= 4m^2 + 4m + 4n^2 + 4n + \underline{2} \quad ③$$

So c has to be even.

But if $c = 2k$, then we have

$$3c^2 = 3(2k)^2 = 12k^2 \quad ④$$

Compare ③ & ④ :

If we divide ③ by 4, it has remindar 2

If we divide ④ by 4, it has remindar 0

So they CANNOT EQUAL !

Conclusion: IN ALL cases, $a^2 + b^2 = 3c^2$ has no integer solution.

(So $x^2 + y^2 = 3$ has no rational points)

Modular World

Defn.

Let m be a positive integer (called a **modulus**).

Say two integers a and b are **congruent modulo m**, written as

$$a \equiv b \mod m$$

if $m \mid a-b$

e.g. $7 \equiv 3 \mod 4$, $-1 \equiv 6 \mod 7$, $\cdots$

$\text{even}^2 \equiv 0 \mod 4$, $\text{odd}^2 \equiv 1 \mod 4$

Defn. Let x be an integer and m a modulus.
The natural representation of x modulo m is the remainder r left under the division algorithm

$$x = q \cdot m + r, \quad 0 \leq r < m.$$

Note that $x \equiv r \mod m$.

Prop. Two integers a and b are congruent modulo m if and only if they have the same natural representation modulo m.

Proof:

$$a = q_a \cdot m + r_a \qquad\qquad b = q_b \cdot m + r_b$$

$$a - b = (q_a - q_b) \cdot m + (\underbrace{r_a - r_b}) \rightsquigarrow -m < r_a - r_b < m$$

$$m \mid a - b \overset{\text{2-out-of-3}}{\iff} m \mid r_a - r_b \iff r_a = r_b$$

Prop. Let m be a modulus, and a, b, c, d are integers s.t.

$$a \equiv b \bmod m \quad \& \quad c \equiv d \bmod m$$

Then $a+c \equiv b+d \bmod m$ & $ac \equiv bd \bmod m$

Proof: (product)

$$a-b = m\cdot k_1, \quad c-d = m\cdot k_2 \qquad (k_1, k_2 \in \mathbb{Z})$$

then we have

$$a\cdot c = (b+mk_1)(d+mk_2)$$

$$= b\cdot d + \underbrace{m^2 k_1 k_2 + m(bk_2 + dk_1)}_{\text{divided by } m}$$

$$m \mid ac - b\cdot d \implies ac \equiv bd \bmod m \qquad \blacksquare$$

Application (Examples)

- Find the natural representation of $1234567 \cdot 20221018 \mod 10$

$$1234567 \equiv 7 \mod 10$$
$$20221018 \equiv 8 \mod 10$$

$$1234567 \cdot 20221018 \equiv 7 \cdot 8 = 56 \equiv 6 \mod 10.$$

- Find the natural representation of $24^5 \mod 13$

$$24 \equiv 11 \equiv -2 \mod 13$$

$$24^5 = (((24 \cdot 24) \cdot 24) \cdot 24) \cdot 24$$
$$\equiv (-2)^5 = -2^5 = -32 \mod 13 \qquad 39 - 32$$
$$\equiv 7 \mod 13$$

- Find the natural representation of $2^{10} \bmod 7$

- Please prepare the above quiz for next meeting.
- Please read pp. 127 – 139 for next lecture.