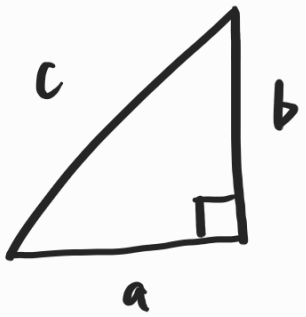
Lecture 2.1

Last time:

- $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$ are the set of natural numbers.

- There are infinitely many Pythagorean triples (a, b, c) in $\mathbb{N}$ satisfying

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



- A P triple (a, b, c) is primitive

if a, b, c share no common factors.

Q: Are there infinitely many primitive triples?

To explore this, let's rearrange the formula:

$$a^2 = c^2 - b^2 = (c-b)(c+b).$$

Ex $3^2 = 5^2 - 4^2 = (5-4)(5+4)$

$5^2 = 13^2 - 12^2 = (13-12)(13+12)$

$15^2 = 17^2 - 8^2 = (17-8)(17+8).$

Notice that when we let a be the odd number out of a, b and keep a^2 on the left, $c^2 - b^2$ factors as a product of squares, which appear not to share any factors.

Lemma If (a, b, c) is primitive and a is odd, then $c - b$ and $c + b$ are squares sharing no common factors.

Pf: Suppose d is a common factor of $c-b$ and $c+b$. Notice

$$(c+b) + (c-b) = 2c$$

and $$(c+b) - (c-b) = 2b$$

and d divides both expressions.

Since b and c share no common factors, $d = 1$ or 2. But

$$(c-b)(c+b) = a^2$$

is odd, so $d = 1$. That is,

$c-b$ and $c+b$ share no common factors. In order for

$$(c-b)(c+b) = a^2$$

to hold then, $c-b$ and $c+b$ must each be a square. □

Now let's give these squares names:

$$x^2 = c-b \quad \text{and} \quad y^2 = c+b.$$

for some $x, y \in \mathbb{N}$.

Then $a^2 = (c-b)(c+b) = x^2y^2$

so $a = xy$.

Also, $2b = (c-b) - (c+b) = x^2 - y^2$

$$\Rightarrow b = \frac{x^2-y^2}{2}$$

and $2c = (c-b) + (c+b) = x^2+y^2$

$$\Rightarrow c = \frac{x^2+y^2}{2}.$$

Theorem Every primitive triple (a,b,c) (a: odd) is of the form

$$a = xy, \quad b = \frac{x^2-y^2}{2}, \quad c = \frac{x^2+y^2}{2}$$

for some $x, y \in \mathbb{N}$ with $x > y$.

On the other hand, does every such $x, y \in \mathbb{N}$ determine a primitive triple?

That is, do xy, $\frac{x^2-y^2}{2}$ and $\frac{x^2+y^2}{2}$ ever share a common factor?

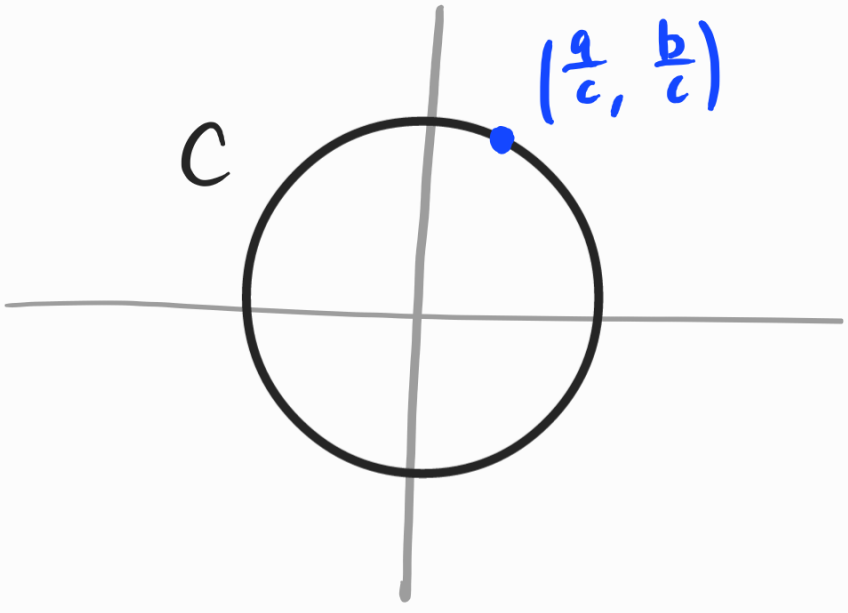
We will answer this after developing the language of divisibility further.

Pythagorean triples have another geometric interpretation.

Notice that dividing by c yields

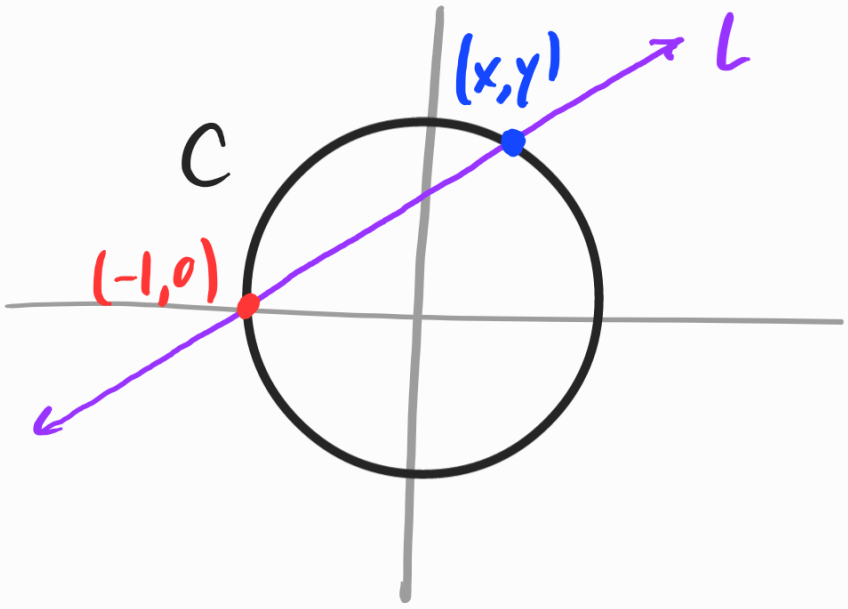
$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

That is, $x = \frac{a}{c}$ and $y = \frac{b}{c}$ are points on the unit circle



From both $\left(\frac{a}{c}, \frac{b}{c}\right)$ is

Even better, $\left(c, \frac{1}{c}\right)$ is a rational point on C and geometry can be used to find all rational pts on C:



Notice that $(-1,0)$ lies on C and for any other point (x,y) on C with rational coordinates, the line L through $(-1,0)$ and (x,y) has

an equation

$$y = m(x+1)$$

with m <u>rational</u>.

After a little algebra, we get

$$x = \frac{1-m^2}{1+m^2} \quad \text{and} \quad y = \frac{2m}{1+m^2}$$

and <u>every</u> choice of m yields a rational point.

Set $m = \frac{r}{s}$ for r, s integers.

Then $(x,y) = \left(\frac{s^2-r^2}{s^2+r^2} \quad \frac{2rs}{s^2+r^2} \right)$

$(r^2+s^2, \quad r^2+s^2)$

and this determines the Pythagorean triple

$$(a,b,c) = (s^2-r^2,\ 2rs,\ r^2+s^2).$$

Divisibility

It is useful to extend the natural numbers $\mathbb{N}$ to include 0 and negative numbers, together called the integers

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

These satisfy the following axioms, or mathematical rules that we take as facts.

Axioms of Arithmetic:

(1) Every $n \in \mathbb{N}$ has a successor $n+1$ and 1 is not the successor of any $n \in \mathbb{N}$. Moreover, if $m+1 = n+1$ then $m = n$, i.e. successors are unique.

(2) If $S \subseteq \mathbb{N}$ is a subset of

the natural numbers with the property that $1 \in S$ and for every $n \in S$, $n+1 \in S$ too, then $S = \mathbb{N}$.

(3) There is an addition operation

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(a, b) \longmapsto a+b$$

generalizing $(n, 1) \longmapsto n+1$ on $\mathbb{N}$

that satisfies:

(a) (Associativity) $(a+b)+c = a+(b+c)$.

(b) (Commutativity) $a+b = b+c$.

(c) (Identity) $a+0 = a$.

(d) (Inverses) $a + (-a) = 0$.

(4) There is a multiplication operation

$$\cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(a, b) \longmapsto ab$$

satisfying:

(a) (Associativity) $(ab)c = a(bc)$.

(b) (Commutativity) $ab = ba$.

(c) (Identity) $a \cdot 1 = a$.

(5) $+$ and $\cdot$ distribute:

$$a(b+c) = ab + ac.$$

Prop For any $a, b, c \in \mathbb{Z}$,

(a) If $a + c = b + c$ then $a = b$.

(b) $a \cdot 0 = 0$.

(c) $(-a) \cdot b = -(ab)$.

(d) $(-a) \cdot (-b) = ab$.

(e) If $ab = 0$ then $a = 0$ or $b = 0$.

(f) If $ac = bc$ and $c \neq 0$, then $a = b$.

Exercise 1: Use the Axioms of Arithmetic to prove the Proposition.

Def For $a, d \in \mathbb{Z}$, we say d **divides** a, or is a **divisor** of a, if $a = dn$ for some $n \in \mathbb{Z}$. We write $d|a$.

Further, $a, b \in \mathbb{Z}$ are **congruent modulo** d if $d|(a-b)$. This is written $a \equiv b \pmod{d}$.

Ex (1) $3|6$ because $6 = 3 \cdot 2$.

Likewise, $6 = 2 \cdot 3 \Rightarrow 2|6$.

(2) $7 \equiv 3 \pmod 2$ because

$$7 - 3 = 4 = 2 \cdot 2.$$

In fact, every odd number is congruent mod 2.

Exercise 2 Prove it!

(3) Every number $a \in \mathbb{Z}$ divides 0.
(why?!)

Here are some useful properties of divisibility and congruence.

Prop Let $a, b, c, d \in \mathbb{Z}$. Then

(a) If $a \mid b$ and $a \mid c$ then a also divides $b+c$, $b-c$ and bc.

(b) If $a \mid b$ and $a \mid c$ then $a^2 \mid bc$.

(c) $a \equiv a \pmod{d}$.

(d) If $a \equiv b \pmod{d}$ then $b \equiv a \pmod{d}$.

(e) If $a \equiv b \pmod{d}$ and $b \equiv c \pmod{d}$, then $a \equiv c \pmod{d}$.

Properties (c) – (e) say that $\equiv \pmod{d}$ is an equivalence relation.

Exercise 3 : Prove the Prop.

We'll talk about this more soon.

For now, we introduce the notion of a greatest common divisor.

Def The greatest common divisor of $a, b \in \mathbb{N}$ is the largest number $d \in \mathbb{N}$ such that $d \mid a$ and $d \mid b$, denoted $d = \gcd(a, b)$ or sometimes just $d = (a, b)$

When $\gcd(a,b) = 1$, we say a and b are relatively prime, or coprime.

Ex 4

$(12, 20) = 4$

$(18, 30) = 6$

$(36, 22) = 2$

$(45, 15) = 15$

$(15, 49) = 1$

$(120, 225) = 15$

$2^3 \cdot 3 \cdot 5$ $\qquad$ $3^2 \cdot 5^2$

In general, it is time-consuming to fully factor each number to compute a gcd.

Next time: an efficient algorithm for computing the gcd.