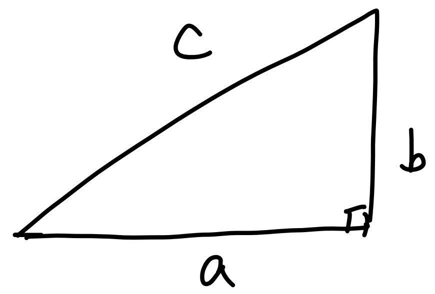
Suppose that we have a right triangle:



Pythagorean Theorem: $a^2+b^2=c^2$

Definition: A triple of positive integers (a,b,c) is called a Pythagorean triple if $a^2+b^2=c^2$

i.e, integers a, b, c will give the sides of a right triagle.

Example:

$$3^2+4^2=5^2$$
$$5^2+12^2=13^2$$
$$8^2+15^2=17^2$$
$$\cdots$$

In this class, our goal is to find all (primitive)? Pythagorean triples.

Observation: let (a,b,c) be a Pythagorean triple, then so will (da, db, dc) with d another integer.

This is because, $a^2+b^2=c^2 \Rightarrow (da)^2+(db)^2=(dc)^2$.

<u>Definition</u>: A <u>primitive Pythagoream triple</u> (PPT) is a triple of numbers (a,b,c) such that a,b,c have no common divisors and $a^2+b^2=c^2$.

Lemma: let (a,b,c) be a PPT, then we can assume that a odd and b even.

Proof: Here are 3 cases for the parity of a, b

Case I: Both of a,b are even

Case II: Both of a,b are odd

Caese III: One of of a,b is even and the other is odd.

↳ (and we can assume a is odd and b even)

Therefore, we need to <u>exclude</u> case I, II.

For case I: if a, b are even,

$a=2x, \quad b=2y.$ with x,y integers.

$$c^2=a^2+b^2=(2x)^2+(2y)^2=4(x^2+y^2)$$

$\Rightarrow 2|c. \Rightarrow 2|a,b,c \Rightarrow$ This is <u>not</u> primitive!

For case II: if a,b are odd, then

$a=2x+1 \quad b=2y+1$ with x,y integers

$$c^2=a^2+b^2=(2x+1)^2+(2y+1)^2$$
$$=4x^2+4x+1+4y^2+4y+1$$
$$=2(2x^2+2x+2y^2+2y+1)$$

On the one hand, $2|c^2 \Rightarrow 2|c \Rightarrow 4|c^2$

On the other hand, $2x^2+2x+2y^2+2y+1$ is odd

$$\Rightarrow 4\nmid 2(2x^2+2x+2y^2+2y+1)$$

A contradiction!

Therefore, only case III happens provided that

(a,b,c) is a PPT. $\square$

We can assume that a odd and b even

Theorem: Let (a,b,c) be a PPT with a odd an b even.

Then we can find odd integers $s>t\geq 1$ such that

(1) $\gcd(s,t)=1$

(2) $a=st \quad b=\frac{s^2-t^2}{2} \quad c=\frac{s^2+t^2}{2}$.

Furthermore, all PPT can be derived in this way.

Proof: (For "Furthermore" part, this will be a homework problem.)

Assume that (a,b,c) is a PPT with a odd and b even. This implies c odd.

$$a^2+b^2=c^2 \Rightarrow \quad a^2=c^2-b^2=(c-b)(c+b)$$

Claim: Both $c-b$ and $c+b$ are squares.

Proof of Claim: Notice that $a^2=(c+b)(c-b)$. it suffices to show that $\gcd(c+b,c-b)=1$.

Suppose not, let p be a prime and

$p \mid \gcd(c+b,c-b) \Rightarrow p \mid c+b$ and $p \mid c-b$

We also know that: b even and c odd.

$p \mid c+b \Rightarrow p$ is odd.

$$\Rightarrow p \mid c+b+c-b = 2c \Rightarrow p \mid c$$

$$p \mid c+b-(c-b) = 2b. \Rightarrow p \mid b$$

$a^2 = c^2 - b^2 \Rightarrow p \mid a \Rightarrow p \mid a, b, c.$

This contradicts that (a, b, c) is a PPT!

Therefore, we showed: both $c+b$, $c-b$ are squares.

Then we set $c+b = s^2$ $(c+b > c-b \Rightarrow s > t)$

$c-b = t^2$

$c+b$ odd $\Rightarrow s$ odd $c-b$ odd $\Rightarrow t$ odd.

By the proof of claim, $\gcd(c+b, c-b) = 1$

$$\Rightarrow \gcd(s, t) = 1. \quad (1) \checkmark$$

For (2), we have: $c+b = s^2$

$c-b = t^2$

$$\Rightarrow 2c = s^2 + t^2 \Rightarrow c = \frac{s^2+t^2}{2}$$

$$2b = s^2 - t^2 \Rightarrow b = \frac{s^2-t^2}{2}$$

$$a = \sqrt{(b+c)(b-c)} = \sqrt{s^2 \cdot t^2}$$

$$= st.$$

This means: $a = st$ $\quad b = \frac{s^2 - t^2}{2}$ $\quad c = \frac{s^2 + t^2}{2}$. $\square$

Theorem: A number c appears as the hypotenuse of a PPT (a, b, c) if and only if c is a product of primes each of which is $1 \pmod 4$.