Section 13.11

Recall: A Diophantine equ. is a polynomial equ. where the only coeffs. are integers.

Ex: $12x + 15y = 3$

↳ linear b/c max exponent is 1.

Ex: $ax + by = c$

↳ there are solns iff $(a, b) \mid c$

↳ Euclidean algorithm solves this equ.

Q (Hilbert's 10^{th} problem): Given a Diophantine equ. is there an algorithm to

1. classify when it has solns?
2. find the solns.?

A: No to both.

Ex: $x^2 - ny^2 = 1$

(1) We can classify for which n this solns.

(2) We can find the solns.

Ex: $a^2 + b^2 = c^2$

↳ there exist (integer) solns.

- $a = 3 \quad b = 4 \quad c = 5$
- $a = 5 \quad b = 12 \quad c = 13$
- $a = 6 \quad b = 8 \quad c = 10$

Def: A <u>Pythagorean triple</u> is a triple $(a, b, c) \in \mathbb{Z}^3$ so that $a^2 + b^2 = c^2$

Q: Can we classify Pythagorean triples?

Note: (a, b, c) sometimes means triple
sometimes means gcd.

Claim: There are infinitely many Pythagorean triples.

Pf: $(3^2 + 4^2 = 5^2)$

k^2

$\Rightarrow (3k)^2 + (4k)^2 = (5k)^2$

So $(3k, 4k, 5k)$ is a Pythagorean triple for any $k \in \mathbb{Z}_{>0}$

Def: A Pythagorean triple is <u>primitive</u> if $\gcd(a, b, c) = 1$

If (a, b, c) is primitive Pythagorean triple

$\rightarrow (ak, bk, ck)$ is an imprimitive Pythagorean triple

Other direction: Suppose (a, b, c) is a P.t. with $\gcd(a, b, c) = d$.

Then write $a = da'$, $b = db'$, $c = dc'$

for integers a', b', c'

So $\gcd(a', b', c') = 1$

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

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

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

and so (a', b', c') is a primitive P.t.

Q: Can we classify / count primitive P.t.s?

Thm: If m, n are relatively prime, pos. ints.

$m > n$, $m \not\equiv n \mod 2$, then

$$x = m^2 - n^2 \; ; \quad y = 2mn \; ; \quad z = m^2 + n^2$$

is a primitive Pythagorean triple.

Cor: Infinitely many Pythagorean triples.

Pf: $x^2 + y^2 = (m^2 - n^2)^2 + (2mn)^2$

$$= m^4 - 2m^2n^2 + n^4 + 4m^2n^2$$

$$= m^4 + 2m^2n^2 + n^4$$

$$= (m^2 + n^2)^2 = z^2$$

Claim: $\gcd(x, y, z) = 1$

If not, $\exists$ prime $p \mid x, y, z$

Since $m \not\equiv n \mod 2$

$$m^2 \not\equiv n^2 \mod 2$$

So $x = m^2 - n^2 \equiv 1 \mod 2$

So $p \neq 2$.

Since $p \mid x$ and $p \mid z$

$$p \mid x + z = (m^2 - n^2) + (m^2 + n^2) = 2m^2$$

$\hookrightarrow p \mid m$

$$p \mid z - x = 2n^2$$

$\hookrightarrow p \mid n$

This contradicts $\gcd(m, n) = 1$

So $\gcd(x, y, z) = 1$

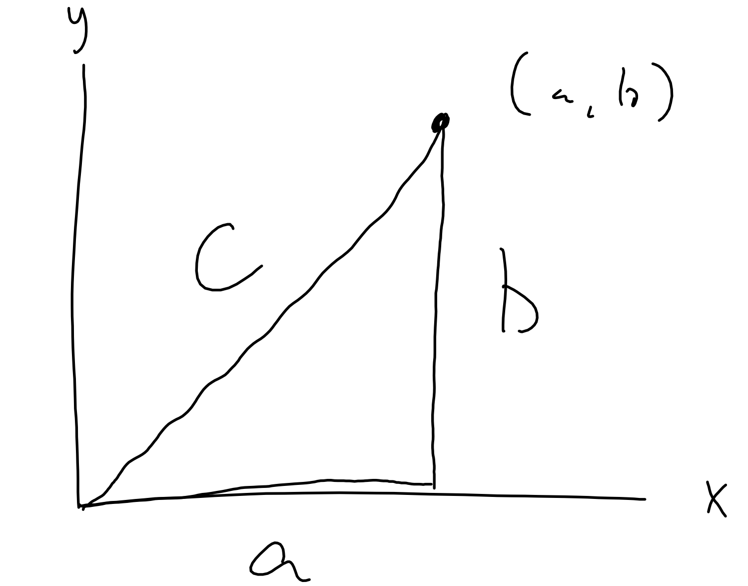
Claim: Every primitive P.t. has form $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$ for integers $m > n$, rel. prime, $m \not\equiv n \mod 2$.

Given: (x, y, z) prim. P.t.

Set $m = \sqrt{\frac{x+z}{2}}$

$n = \sqrt{\frac{z-x}{2}}$

Show $m, n \in \mathbb{Z}$ with desired properties.



Pyth. triples $\longleftrightarrow$ pts. (a, b) in quadrant I

$a, b \in \mathbb{Z}$ and distance from origin is an integer

Take (a, b), turn into a unit vector

$$(a, b) \rightsquigarrow \left(\frac{a}{c}, \frac{b}{c} \right)$$

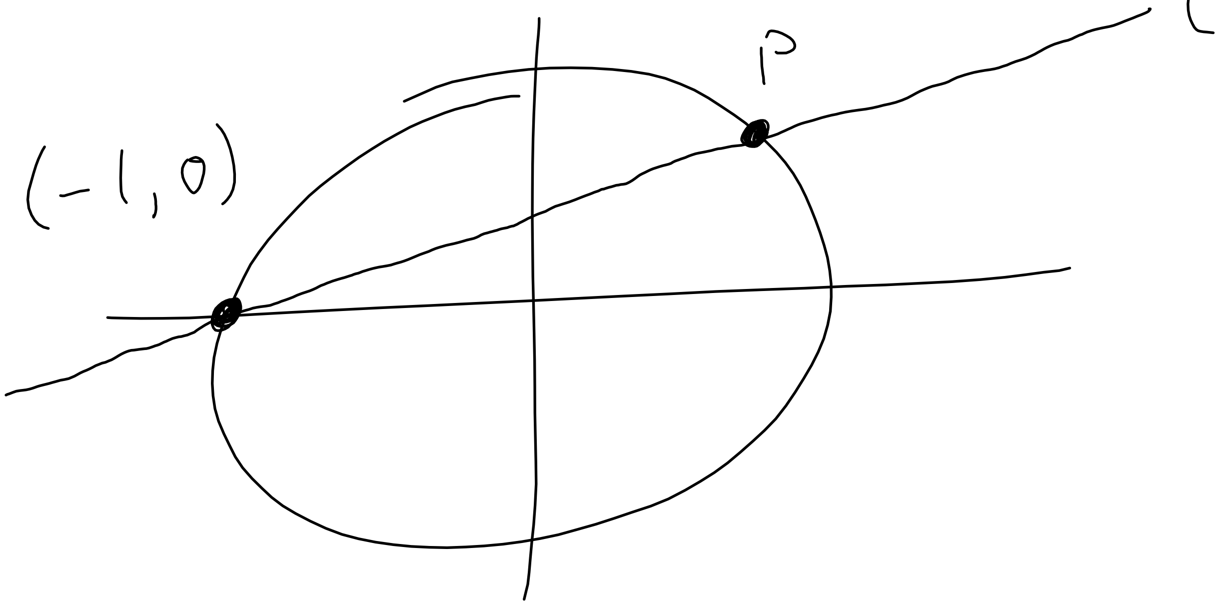
↳ rational pt.

unit vector $\longleftrightarrow$ on the unit circle

Pythagorean triples $\longrightarrow$ rational pt. on $x^2+y^2=1$

If $\left(\frac{p}{q}\right)^2 + \left(\frac{r}{s}\right)^2 = 1$ then

$$(ps)^2 + (rq)^2 = (qs)^2$$



Claim: if P is a rational pt. then slope of L is rational and if slope of L is rational, then P is a rational pt

"Pf:" $P = (x, y)$, suppose $x, y \in \mathbb{Q}$

Slope of $L = \dfrac{y}{x+1} \in \mathbb{Q}$

Now suppose slope of L (say, t) is rational

Equ. for L: $y = t(x+1)$

Also: $x^2 + y^2 = 1$

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

Solve for x in terms of t:

$$x = \frac{1-t^2}{1+t^2} \in \mathbb{Q}$$

$$y = t(x+1) = \frac{2t}{1+t^2} \in \mathbb{Q}$$

Lesson: Every rational pt. on the circle has the form

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

$43^2 = 40 \cdot 46 + 3^2$

b/c $43^2 - 3^2 = (43-3)(43+3)$

Ex: $t = \frac{11}{43}$

$$2t = \frac{22}{43}$$

$$1 - t^2 = 1 - \frac{121}{1849} = \frac{1728}{1849}$$

$$1 + t^2 = 1 + \frac{121}{1849} = \frac{1970}{1849}$$

$$(x, y) = \left(\frac{1728/1849}{1970/1849}, \frac{22/43}{1970/43^2} \right)$$

$$\left(\frac{1728}{1970}, \frac{22 \cdot 43}{1970} \right)$$

$$\rightarrow \quad 1728^2 + 946^2 = 1970^2$$

Ex: Teaching Calculus

Arc length of $y = f(x)$ on $[a, b]$

$$\int_a^b \sqrt{1 + f'(x)^2}\, dx$$

Goal: $1 + f'(x)^2 = g(x)^2$

$$\left(\frac{1-x^2}{1+x^2}\right)^2 + \left(\frac{2x}{1+x^2}\right)^2 = 1$$

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

$$\left(\frac{1-x^2}{2x}\right)^2 + 1 = \left(\frac{1+x^2}{2x}\right)^2$$

$$f'(x) = \frac{1-x^2}{2x} = \frac{1}{2x} - \frac{x}{2}$$

$$g(x) = \frac{1+x^2}{2x}$$

$$f(x) = \frac{1}{2} \log|x| - \frac{x^2}{4} + C$$