Day 9: Elliptic Curves

+ Crypto on your Computer

"Let G generate a group $\mathbb{G}$ of prime order"

What is a group?

- set objects
- a way to multiply
  - identity: 1
  - generator: G] special object
- associative $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, commutative $x \cdot y = y \cdot x$

Detour: Hobbies in antiquity → finding points on curves OR solving equations

Pythagoras: finding $a, b, c \in \mathbb{N}$ s.t

$$a^2 + b^2 = c^2 \qquad (3,4,5), \ (5,12,13)$$

Fermat: find $x, y, z \in \mathbb{Z}$ s.t. $x^3 + y^3 = z^3$

Fermat's last theorem: no such x, y, z

order 2 in y

order 3 in x

Diophantus: finding $x, y \in \mathbb{Q}$ s.t. $y^{2} = x^{3} - x + 9$

→ Diophantus wrote many books about solving eqns like this

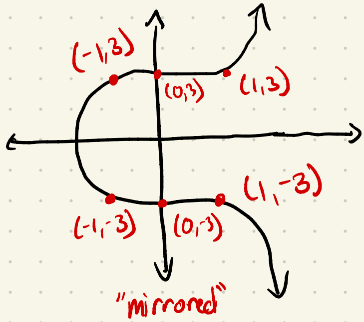
→ Fermat read one

→ That is where he wrote his last theorem

→ 1990s, Ander Wiles proves the thm... using elliptic curves.

Musical: Fermat's Last Tango

What does an elliptic curve look like?
What does Diophantus' curve look like



$y^2 = x^3 + Ax + B$

Find some rational points on $y^2 = x^3 - x + 9$ . . .

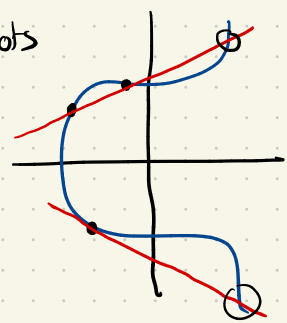
$x = 0,\ y = 3 \rightarrow$ on curve
$3^2 = 0^2 - 0 + 9$

$0 = x^3 - x + 9$
$x = 3 \rightarrow 27 - 3 + 9 > 0$
$x = 2 \rightarrow 8 - 2 + 9 > 0$
$x = -2 \rightarrow -8 + 2 + 9 > 0$
$x = -3 \rightarrow\ < 0$

$x = 2$
$y^2 = x^3 - x + 9$
$y^2 = 8 - 2 + 9$
$y^2 = 15$
$y = \pm\sqrt{15}$

How to find more rational points?

- → "flip": If (x, y) is on-curve, $(x, -y)$ is too.
- → "chord method": Pick two pts, draw a line, find the third intersection.
  - → Rational, b/c eqn is cubic in x → since irrational rts come in pairs $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$, 2 rational roots
    - → third pt is rational too.
- → "tangent method": Pick one pt, draw tangent, find other intersection.



Q: Chord $(P,Q) = R$

is this commutative? Chord $(P,Q) \stackrel{?}{=}$ Chord (Q,P) ✓

is this associative? Chord $(P,$ Chord $(Q,R)) \stackrel{?}{\neq}$ Chord (Chord (P,Q), $R)$

Flip (Chord (P,Q)) is associative

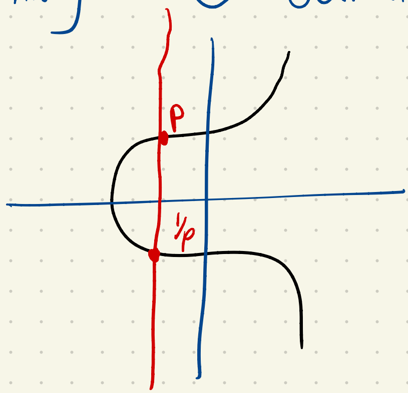
Okay, so, can "chord-then-flip" make a group?

- → to combine a pt with itself? → "tangent-then-flip"
- → need an identity.
  - → add "pt at infinity": $\mathcal{O}$: defined to be the identity

$\bullet\,\mathcal{O}$

$P \otimes 1/P = \mathcal{O}$

$P \otimes \mathcal{O} = P$



- → "flip": inverse.

We call this group $E(\mathbb{Q})$

↑ pts on curve w/ coordinates in $\mathbb{Q}$ + pt infinity.

- generator?
- bigger problem: rationals can get very big.

Idea: use modular arithmetic instead of rational arithmetic:

$E(\mathbb{Z}_p)$ ← points $x, y \in \mathbb{Z}_p$ s.t $y^2 = x^3 - x + 9 \pmod p$

+ pt at infinity.

we can also find a generator G, that produces a prime-order subgroup.

group abstraction	$E(\mathbb{Z}_p)$
$\mathbb{G}$	pts on the curve + pt at infinity
G	a particular pt on the curve
1	pt at infinity
$H \to 1/H$	flipping y coordinate
$H_1 \cdot H_2 \to H_3$	chord - then - flip
$H_1 \cdot H_1 \to H_2$	tangent - then - flip
H^n	repeated group operations

NIST curve P256 (aka secp256r1)

$E(\mathbb{Z}_p)$, with $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} + 1$

eqn: $x^3 - 3x + b$ (b is constant)

p is specially designed to make arithmetic mod p fast.

b was chosen by hashing a seed

Others: secq256r1, curve25519 ← $p = 2^{255} - 19$

Website:

cryptotool.py → Download to Desktop

python cryptotool.py keygen -k mykey

→ generate a random symmetric key
& save it to "my key"

python cryptotool.py enc -k mykey -m notes.pdf
-c myct