Elliptic Curve Cryptography

TODAY:
- Motivation
- Groups Review
- Elliptic Curves (ECs) over $\mathbb{R}$
- ECs over $\mathbb{F}$
- Efficient EC implementation
- Wrap-up

We've often said, "let $\mathbb{G}$ be a group of prime order p"

maybe for which discrete log (or later, DDH) is hard...

What groups do we actually use?

↖ and what is a group mathematically?

Groups (Review)

A group is a pair $(\mathbb{G}, \cdot)$, where $\mathbb{G}$ is a set, and $\cdot : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ is a binary operation, such that the following properties are satisfied:

(1) Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(2) Identity: $\exists e \in \mathbb{G}$ s.t. $\forall a \in \mathbb{G}$ $a \cdot e = e \cdot a = a$

(3) Inverse: $\forall a \in \mathbb{G}, \exists b \in \mathbb{G}$ s.t. $a \cdot b = b \cdot a = e$ ($b =$ "a^{-1}")

A group is <u>abelian</u> if $\cdot$ is commutative: $\forall a, b \in \mathbb{G}$, $a \cdot b = b \cdot a$

<u>cyclic</u> if $\exists$ $g \in \mathbb{G}$ (called the generator) s.t. $\forall a \in \mathbb{G}$ $\exists x \in \mathbb{N}$ s.t. $a = g^x$ (x times: $g \cdot g \cdot \ldots \cdot g$)

We often drop the operation when describing a group when it's clear.

Order. Order of a group $\mathbb{G}$ is the size of the set, $ord(\mathbb{G}) = |\mathbb{G}|$

Order of an element $h \in \mathbb{G}$

$$ord(h) = \text{smallest } k \in \mathbb{N} \text{ s.t. } h^k = e$$

how many times to apply the group operation before you get to the identity...

"Prime-order group" $ord(\mathbb{G})$ is prime.

Fact. Prime-order groups are <u>abelian</u> and <u>cyclic</u>.

Fact. $\mathbb{H} \leq \mathbb{G} \Rightarrow ord(\mathbb{H}) \mid ord(\mathbb{G})$

Subgroup. $(\mathbb{H}, \cdot)$ is a subgroup of $(\mathbb{G}, \cdot)$ if $\mathbb{H} \leq \mathbb{G}$. Denote as $(\mathbb{H}, \cdot) \leq (\mathbb{G}, \cdot)$.

note: it's the same operation $\cdot$ but restricted to $\mathbb{H}$,

$\cdot : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$.

Examples of prime-order groups.

- $(\mathbb{Z}_p, +)$: "additive" group of integers <u>modulo p</u>.

  group op is the usual + modulo p.

- prime-order sub-group of $(\mathbb{Z}_p^*, \cdot)$

  usually $p = 2q + 1$, where q is prime.

  Known as Sophie-Germain or "safe" primes

  p is prime $\Rightarrow ord(\mathbb{Z}_p^*) = p - 1 = 2q$.

  We use $\mathbb{H} \leq \mathbb{Z}_p^*$ where $ord(\mathbb{H}) = q$.

The Discrete Logarithm Problem (DLOG)

Let $\mathbb{G}$ be a cyclic group of order p with generator g.

$$\forall \text{PPT } \mathcal{A}, \quad \Pr\left[\mathcal{A}(\mathbb{G}, g, g^x) = x \;:\; x \xleftarrow{\$} \mathbb{Z}_p\right] \leq \text{negl}(\lambda)$$

DLOG is trivial in $(\mathbb{Z}_p, +)$

For $(\mathbb{Z}_p^*, \cdot)$, the best known algorithm is the General Number Field Sieve which runs in $2^{\tilde{O}((\log p)^{1/3})}$ (sub-exp. time)

- For $\lambda = 128$ bits of security, we need $|p| \approx 3072$ bits
- In 2019, record break for $|p| \approx 795$ bits

Group operations are expensive... Arithmetic modulo 3072-bit prime

Desire for crypto. 1. Efficient group operation (efficiency)

2. DLog (or other group-theoretic problems like CDH and DDH) are hard (security)

3. Additional structure : Pairings (Expressivity)

← next class

History of Elliptic Curves

Deep connections to number theory, geometry, and even complex analysis!

All started with Greek mathematician, Diophantus in 3rd century AD

Interested in integer and rational solutions to polynomial equations

main surviving work, *Arithmetica*: a collection of (solved) problems, such as

"find two numbers with sum 20, product 96"

"write given square number as sum of squares" ← famously, the problem Fermat annotated with "Fermat's Last Theorem" in the margins :)

↑ Andrew Wiles and Richard Taylor would later prove it, partly using EC theory (popular book about this written by Simon Singh)

and many more that amounted to finding rational points on curves

$$(x,y) \in \mathbb{Q}^2 \quad \text{s.t.} \quad f(x,y) = 0$$

for bi-variate poly, f.

E.g. in book 4 of Arithmetica,

exercise to find rational points satisfying

$$y^2 = x^3 - x + 9$$

Easy points: $(0, \pm 3)$, $(1, \pm 3)$, $(-1, \pm 3)$

Given these easy points,

can we derive other rational points?

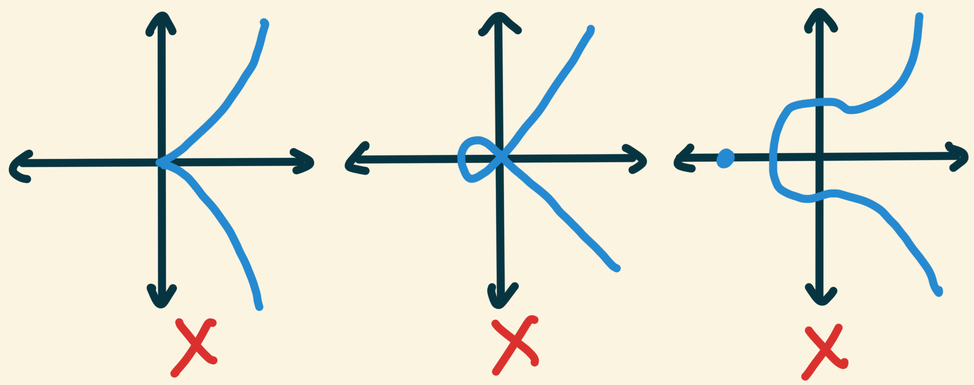
Elliptic Curves (ECs)

A smooth plane curve defined by

$$E : y^2 = x^3 + ax + b \quad \text{(Short Weierstrass form)}$$

for $a, b \in \mathbb{Q}$

A curve is smooth if it has no cusps, self-intersections or isolated points.



$$\iff \Delta := 4a^3 + 27b^2 \neq 0$$

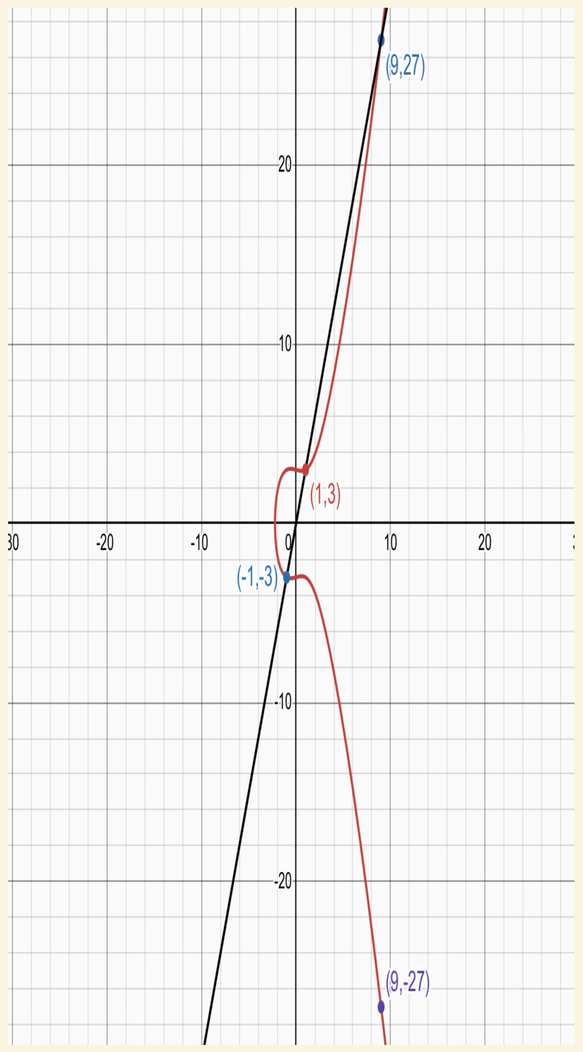
↑ discriminant of the curve

Why? Not smooth $\iff$ cubic x^3+ax+b has repeated roots $\iff$ shares root with derivative $3x^2+a$.

$3x^2+a=0$ when $x^2 = -a/3$. So, $x^3+ax+b=0 \iff x(x^2+a)+b=0$

$$\Rightarrow x\left(\frac{-a}{3}+a\right)+b=0 \iff x=\frac{-3b}{2a}. \Rightarrow \left(\frac{-3b}{2a}\right)^2 = -\frac{a}{3} \iff 4a^3+27b^2=0$$

e.g. $y^2 = x^3 - x + 9$



First Q.: Given some points on E, can we find other points in $\mathbb{Q}^2$?

(Diophantus)

↗ i.e., find solutions in $\mathbb{Q}$.

Key Observations

1. Symmetry: $(x,y) \in E \Rightarrow (x,-y) \in E$ (across x-axis)

2. Tangents at $y=0$ on E are vertical: Slope $\frac{dy}{dx} = \frac{3x^2+a}{2y} \xrightarrow{y \to 0} \infty$

3. Line that intersects $P_1=(x_1,y_1)$, $P_2=(x_2,y_2) \in C$ must intersect E at a third point $P_3=(x_3,y_3)$

   - Let $y=mx+d$ be the intersecting line.

   Then, $(mx+d)^2 = x^3-ax+b \Rightarrow f(x)=x^3-ax+b-(mx+d)^2$ has three roots $\alpha_1, \alpha_2, \alpha_3$. WLOG $\alpha_1=x_1$, $\alpha_2=x_2$.

   So, $f(x) = (x-x_1)(x-x_2)(x-\alpha_3) = \dots - (x_1+x_2+\alpha_3)x^2 \dots$

   $\Rightarrow \alpha_3 = m^2 - x_1 - x_2 \in \mathbb{Q}$

Procedure to Derive New Points

1. Draw a line between two points on E. ← use tangent if $P_1=P_2$
2. Obtain point of intersection (using (3))
3. Flip the point across x-axis to obtain new non-co-linear point (using (1))

"chord method" if $P_1 \neq P_2$
"tangent method" if $P_1=P_2$

Elliptic Curve Groups

We took two rational points on the curve and derived a third rational point on the curve.

Henri Poincaré (building on others) realized this actually has a group structure! That is, the chord and tangent method can be used to define a group operation on the set of rational points on an elliptic curve.

One subtlety. What about vertical lines? e.g. $y=0$ or a line through (x,y) and $(x,-y)$

We will add a distinguished element called the "point at infinity" or $\mathcal{O}$.

↖ an "artificial" point where all vertical lines intersect

For an elliptic curve $E/\mathbb{Q}$ ↖ just means defined over $\mathbb{Q}$: $y^2 = x^3+ax+b$,

define a group

$$E(\mathbb{Q}) := \{\mathcal{O}\} \cup \{(x,y)\in\mathbb{Q}^2 : y^2 = x^3+ax+b\}$$

formally handled using Projective or Jacobian coordinates...

with operation $\boxplus$ that satisfies the following:

(1) $\forall P \in E(\mathbb{Q})$, $P \boxplus \mathcal{O} = \mathcal{O} \boxplus P = P$ ($\mathcal{O}$ is the identity)

(2) $\forall P=(x,y)\in E(\mathbb{Q})\setminus\{\mathcal{O}\}$, define $-P := (x,-y)$, and $P \boxplus -P = -P \boxplus P = \mathcal{O}$ ↙ follows from chord method

↖ "additive" inverse And, $-\mathcal{O} := \mathcal{O}$

(3) $\forall P_1 = (x_1, y_1) \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, and $P_2 = (x_2, y_2) \in E(\mathbb{Q}) \setminus \{\mathcal{O}, -P_1\}$

define

$$s_c = \frac{y_2 - y_1}{x_2 - x_1}$$ slope of chord

$$s_t = \frac{3x_1^2 + a}{2y_1}$$ slope of tangent

← we know what happens with inverses ...

using chord

(i) if $P_1 \neq P_2$: $x_3 = s_c^2 - x_1 - x_2$

$y_3 = s_c(x_1 - x_3) - y_1$

← this corresponds to finding third point on line and flipping!

(ii) if $P_1 = P_2$ and $y_1 = 0$: vertical line, so $P_1 \boxplus P_2 = \mathcal{O}$

(iii) if $P_1 = P_2$ and $y_1 \neq 0$: $x_3 = s_t^2 - 2x_1$

$y_3 = s_t(x_1 - x_3) - y_1$ ← tangent to find third point then flip!

$P_1 \boxplus P_2 = (x_3, y_3)$ in (i) and (iii)

So, $\boxplus$ is well-defined, we defined an identity and inverses in $E(\mathbb{Q})$.

Turns out $\boxplus$ is also associative! ← manual algebra

Therefore, $(E(\mathbb{Q}), \boxplus)$ is a group.

So can we do cryptography with $E(\mathbb{Q})$?

Not quite!

Issues: - Rationals don't have finite representations.
Makes it difficult to implement securely since we don't handle infinite precision...
- hard to calculate order of the group

Can we obtain a finite group of prime order using the theory of Elliptic curves?

EC over Finite Fields

$\mathbb{F}_p$, finite field of order p, isomorphic to $\mathbb{Z}_p$: integers modulo p.

Let $p > 3$ be a prime.

An elliptic curve E defined over $\mathbb{F}_p$, $E/\mathbb{F}_p$,

$$E: y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$

Same as before!

We can define a group as before: $E(\mathbb{F}_p) = \{(x,y) \in \mathbb{F}^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$

⊞: like before Laws are proven with a lot of algebra...

Can calculate order of $E(\mathbb{F}_{p^e})$ in time $O(e \log(p))$ ← poly-time!

Example. $E/\mathbb{F}_5 : y^2 = x^3 + 2x + 1$

$$|E(\mathbb{F}_5)| = 7, \quad E(\mathbb{F}_5) = \{\mathcal{O}, (0,\pm 1), (1,\pm 2), (3,\pm 2)\}$$

↑ happens to be prime here, but not necessarily...

DLOG in EC Groups

Let $E/\mathbb{F}_p$ be an EC over $\mathbb{F}_p$ and $E(\mathbb{F}_p)$ be the group.

We want to work with a cyclic subgroup:

let $P \in E(\mathbb{F}_p)$ be of prime order q. ($|q| \approx |p|$ in bits)

Define $aP := \underbrace{P \boxplus P \boxplus \cdots \boxplus P}_{a \text{ times}}$

↑ additive notation

So, we have $qP = \mathcal{O}$ since $\text{ord}(P) = q$.

Theorem from group theory => P must generate a q-order subgroup of $(E(\mathbb{F}_p), \boxplus)$:

$$(\{\mathcal{O}, P, 2P, \ldots, (q-1)P\}, \boxplus)$$

DLog problem is given $P, \alpha P$ for $\alpha \xleftarrow{\$} \mathbb{Z}_q$, calculate α

For most ECs, the best DLog attacks are $\Omega(\sqrt{q})$. So for $\lambda = 128$, we need the group to be of size/order $\approx 2^{256}$. This is much better than $(\mathbb{Z}_p^*, \cdot)$ which requires larger groups for same security level!!

Exceptions where DLog is easy:

- $|E(\mathbb{F}_p)| = p$: "Anomalous" ECs ("SMART" attack)
- $|E(\mathbb{F}_p)|$ divides $p^B - 1$ for small B (MOV attack)

So in practice, we standardize ECs (e.g. P256, Curve 25519) to avoid common pitfalls

prime-order

we pick the prime-order subgroup

"twist-secure"

Efficient Implementation of EC Addition

Recall that the EC group operation required calculating the slope:

$$s_c = \frac{y_2 - y_1}{x_2 - x_1}$$

$$s_t = \frac{3x_1^2 + a}{2y_1}$$

← these are field inversions

much more expensive than addition or multiplication.

↳ can be computed using Fermat's Little Thm. and repeated squaring
or
Extended Euclidean Alg. & Bezout's Thm. ≈ 9 - 40 x field mult.!

Can we reduce field inversions??

Yes! By moving to a different coordinate system...

Jacobian Coordinates

Affine points : (x, y)

Substitute x with $\frac{X}{Z^2}$

y with $\frac{Y}{Z^3}$

Jacobian point : $(X : Y : Z)$ ← this is actually an equivalence class of points...

$(X : Y : Z) \sim (\lambda^2 X : \lambda^3 Y : \lambda Z)$ for any $\lambda \in \mathbb{F}_p^*$

Affine $\mapsto$ Jacobian : $(x, y) \mapsto (x : y : 1)$ or $(x^2 x, \lambda^3 y, \lambda)$ for any $\lambda \in \mathbb{F}_p^*$

Jacobian $\mapsto$ Affine : $(X : Y : Z) \mapsto \left(\frac{X}{Z^2}, \frac{Y}{Z^3}\right)$

e.g. $\mathcal{O} \mapsto (1 : 1 : 0)$ in Jacobian.

Why is this useful?

Let's say we want to compute $P \boxplus P = (x', y')$ ← doubling an EC point

$P = (x, y)$ in affine

Recall $x' = (s_t)^2 - 2x$, $y' = s_t(x - x') - y$, $s_t = \frac{3x^2 + a}{2y}$

In Jacobian coordinates:

we substitute $x \mapsto X/Z^2$, $y \mapsto Y/Z^3$

and obtain:

$$s_t = \frac{3\left(\frac{X}{Z^2}\right)^2 + a}{2\left(\frac{Y}{Z^3}\right)} = \frac{3X^2 + aZ^4}{2YZ}$$

$$x' = s_t^2 - 2\left(\frac{X}{Z^2}\right) = \frac{C}{4Y^2Z^2} \quad \text{and} \quad y' = s_t\left(\frac{X}{Z^2} - x'\right) - \frac{Y}{Z^3} = \frac{D}{8Y^3Z^3}$$

where C and D can be computed with a small number of adds and mults (try yourself)

Notice that $x' = \frac{C}{(2YZ)^2}$, $y' = \frac{D}{(2YZ)^3}$

So the Jacobian coordinate for $(x', y') = P \boxplus P$ is $(C : D : 2YZ)$

So, we can do all our EC additions in Jacobian coordinates, and at the end pay 1 inversion $1/Z$ to convert back to affine coordinates. $(X : Y : Z) \longmapsto \left(\frac{X}{Z^2} = X \cdot \left(\frac{1}{Z}\right)^2, \frac{Y}{Z^3} = Y\left(\frac{1}{Z}\right)^3\right)$

↖ required no inversions!

n Jacobian points $\longmapsto$ n Affine points

n inversions

can we do better?

Also yes! Montgomery's trick for batch inversions

Batch Inversion : Montgomery's Trick

We want to invert $z_1, \ldots, z_n$ ← n elements

Here's an algorithm:

$(p_i := \prod_{j \le i} z_j)$

(1) Compute partial products: z_1, $z_1 z_2$, $z_1 z_2 z_3$, ..., $z_1 z_2 \cdots z_n$ $(n-1)$ mults.

(2) Compute $I_{1,n} := (z_1 z_2 \cdots z_n)^{-1} = \frac{1}{z_1 \cdots z_n} = \frac{1}{p_n}$ (1 inversion)

(3) Compute $\frac{1}{z_n}$ as $I_{1,n} \cdot p_{n-1}$ (1 mult)

Observe $\frac{1}{z_n} = I_{1,n} \cdot p_{n-1}$

$= \frac{1}{z_1 \cdots z_n} \cdot z_1 \cdots z_{n-1} = \frac{1}{z_n}$

(4) Compute $I_{1,n-1} = I_{1,n} \cdot z_n = \frac{1}{z_1 \cdots z_{n-1}}$ (1 mult)

(5) Compute $\frac{1}{z_{n-1}}$ as $I_{1,n-1} \cdot p_{n-2}$ and so on...

In total inverting n elements requires $(n-1)$ mults + 1 inv. + $2 \times (n-1)$ mults

$= 3(n-1)$ mults + 1 inv.

so much cheaper!

Wrapping Up

- EC groups used widely in crypto
- Much more efficient in practice than using $\mathbb{Z}_p^*$ at similar security levels

  because $\mathbb{Z}_p^*$ has non-generic attacks that perform better!

- ECs have rich algebraic structure => cool crypto!

  We will see "Pairings" in the next lecture

  => (Identity-Based Encryption, Eff. signatures, ...)