Intro to Elliptic Curves

TOC

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

for which discrete log and DDH is hard.

What groups do cryptographers actually use?

Group Review

A group $(\mathbb{G}, \cdot)$ is a set $\mathbb{G}$ with a distinguished element 1 (called the identity) and a closed, associative binary operation $\cdot : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ such that

$\forall a \in \mathbb{G}, \exists b \in \mathbb{G}, \ a \cdot b = b \cdot a = 1$ (inverses)

$\forall a \in \mathbb{G}, \ a \cdot 1 = 1 \cdot a = a$ (identity)

Additionally, a group can be:

- abelian: if $\cdot$ is commutative, $\forall a, b \in \mathbb{G}, \ a \cdot b = b \cdot a$.
- cyclic: if $\exists g \in \mathbb{G}$ ("generator") s.t. $\mathbb{G} = \{g^0, g^1, \dots, g^{|\mathbb{G}|-1}\}$

MATH Fact: Prime order groups are abelian and cyclic!

<u>Subgroup</u>: a subset $\mathbb{H} \subseteq \mathbb{G}$ s.t. $(\mathbb{H}, \cdot)$ is also a group, where $\cdot$ is the natural restriction.

<u>Order</u>: the size of $|\mathbb{G}|$ or the least exponent $\in \mathbb{Z}$ s.t. $\underset{\in \mathbb{G}}{h}^{\mathrm{ord}(h)} = 1$.

Classic examples of prime order groups are:

- $(\mathbb{Z}_p, +)$: additive group of integers mod p
- a prime order subgroup of $(\mathbb{Z}_p^*, \cdot)$
  - often p is a Sophie-Germain prime (also called "safe") of the form $p = 2q + 1$

    q: prime

<u>Discrete Log $(\mathbb{G}, g)$</u>

$$\forall \text{ PPT } A, \quad \Pr\left[x = \hat{x} : \begin{array}{l} x \xleftarrow{\$} \mathbb{Z}_p, \\ \hat{x} \leftarrow A(\mathbb{G}, g, g^x) \end{array} \right] \leq \text{negl}(\lambda)$$

- DLog is ~~trivially easy~~ for $(\mathbb{Z}_p, +)$
- For $(\mathbb{Z}_p^*, \cdot)$, the best known algorithm is the General Number Field Sieve (faster than index calc) which runs in $2^{\tilde{O}((\log p)^{1/3})}$ (subexponential time).
  - For $\lambda = 128$ bits of ~~security~~, $|p| \approx 3072$ bits
  - In 2019, record was a $|p| \approx 795$ bits
  - Group operations are expensive: requires arithmetic mod a 3072 bit prime

<u>Desire</u>: we would like a group that
- has an efficient group operation
- DLog, CDH, or DDH is hard
- has additional structure pairings (next class) useful for cryptography

History of Elliptic Curves

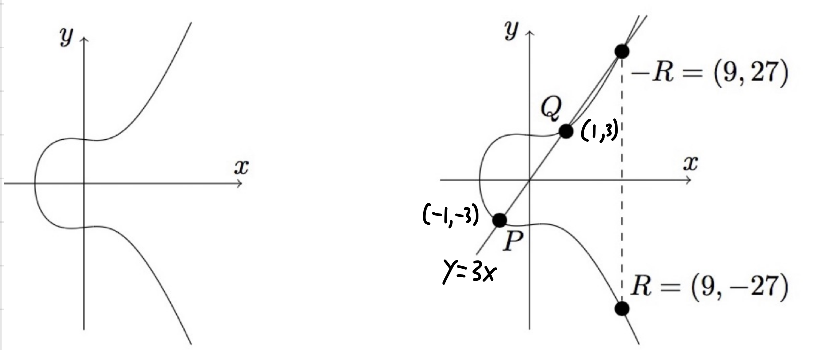
ECs are objects with deep connections to number theory and geometry. Diophantus, a greek mathematician in 3^{rd} century AD was interested in the set of rational points $\in \mathbb{Q} \times \mathbb{Q}$ such that $f(x,y)=0$, for bivariate poly f. In general, finding rational points on plane curves can be incredibly hard.

☆ Fermat wrote "Fermat's Last Thm" in the margins of Arithmetica (the series written by Diophantus on this subject)

☆ Andrew Wiles / Richard Taylor would later prove FLT using ECs – a popular book written about this by Simon Singh

In book 4 of Arithmetica, there was an excercise to find rational points satisfying $y^2 = x^3 - x + 9$.

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



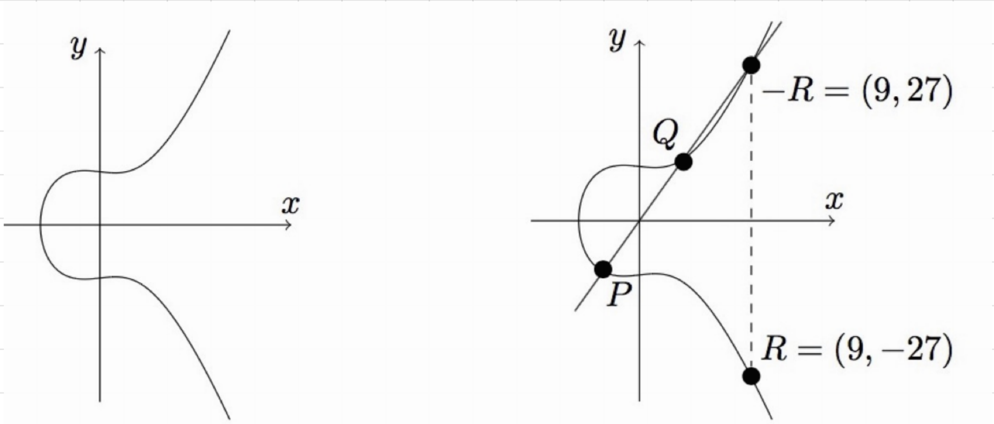
Given these easy points, can we derive other rational points?

Elliptic Curves

an elliptic curve is a smooth plane curve defined by an equation of the form

$$y^2 = x^3 + Ax + B \quad \text{(short Weierstrass form)}$$

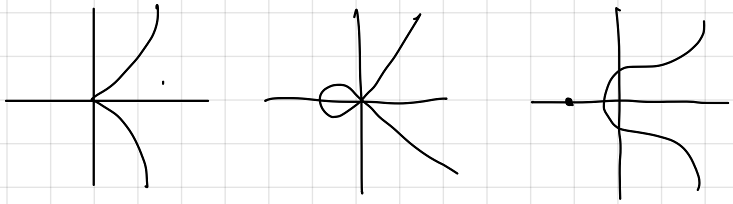
for $A, B \in \mathbb{Q}$.



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

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

Cannot be:

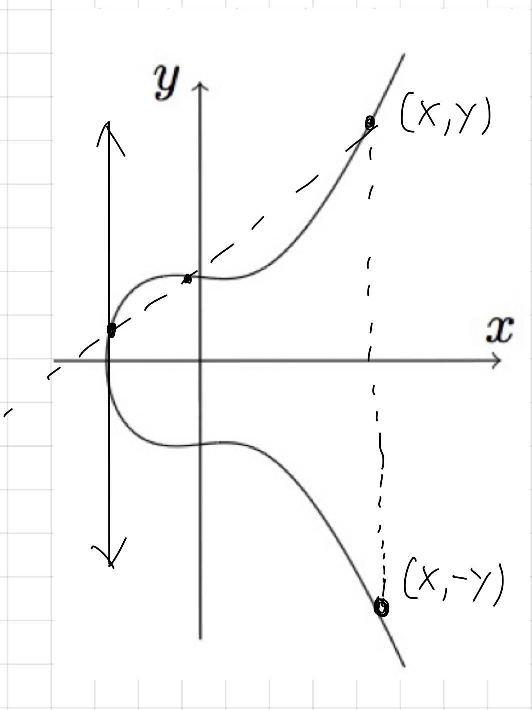


Thus, we restrict A and B such that the discriminat of the curve, $\Delta = -16(4a^3 + 27b^2) \neq 0$.

First goal: Given some points on the elliptic curve, can we enumerate other points? (Diophantus)

Key Observations

- An elliptic curve is symmetric: if a point (x, y) is on the curve so is $(x, -y)$.
- Lines tangent to the curve at the x-axis are vertical (slope $y' = \frac{3x^2+A}{2y}$ is ∞ when $y=0$)
- A line intersecting two points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ on the curve must intersect the curve at a third point $P_3 = (x_3, y_3)$ (ignoring vertical lines) [Chord Method]



— Suppose $y = mx+b$ goes through P_1, P_2. The equation $(mx+b)^2 = x^3 + Ax + B$ has three roots x_1, x_2, x_3 giving us the three points.

Procedure to derive new $\mathbb{Q}$ points

- Draw a line between two points on the curve
- Obtain the point of intersection
- flip the point across the x axis to obtain a new non-collinear point.

Sneak Peek gives us an associative operation $\longrightarrow$

Elliptic Curve Group

What we just saw is a procedure to take two points P1 and P2 on an elliptic curve and derive a new point P3 on the curve. If we denote this operation $\boxplus$, $P1 \boxplus P2 = P3$, is the operation a group operation with the set of points being the group?

Not Quite!

We didn't handle vertical lines nor adding points to themselves.

- Adding points to themselves can be handled by considering the line tangent to the curve at that point.
- Vertical lines requires a distinguished element called the point of infinity to be added to the group!

For an elliptic curve, $E: y^2 = x^3 + Ax + B$, we define a group $E(\mathbb{Q}) := \{\mathcal{O}\} \cup \{(x,y) \in \mathbb{Q} \mid y^2 = x^3 + Ax + B\}$ with $\boxplus$ defined as follows: (also define $-(x,y) = (x,-y)$)

Cases: $P1 \boxplus P2$

- If $P1 = \mathcal{O}$, then $P1 \boxplus P2 = P2$. Symmetrically, if $P2 = \mathcal{O}$.
- Else, if $P1 = -P2$ (the flip), $P1 \boxplus P2 = \mathcal{O}$.
- Else, define

$$\underset{\substack{\uparrow \\ \text{slope of} \\ \text{line}}}{\lambda} = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \quad \text{(chord method)} \\[2ex] \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \quad \text{(tangent method)} \end{cases}$$

If $P_1 \neq P_2$, $x_3 = \lambda^2 - x_1 - x_3$, $y_3 = \lambda(x_1 - x_3) - y_1$.

If $P_1 = P_2$, $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$.

$\uparrow$

often called doubling case.

Does this satisfy the properties of a group?

<u>Identity:</u> $\mathcal{O}$ ✓

<u>Inverses</u>: ✓ (the flip point)

<u>Associativity</u>: ✓ (a lot of manual algebra to prove)

Great! Can we do cryptography now?

Issues:

- Rationals don't have finite representations. This makes secure implementation hard since we don't handle infinite precision.
- hard to calculate exact order

How can we obtain a finite group of prime order using the theory of elliptic curves?

EC over Finite Fields

$\mathbb{F}_p \cong \mathbb{Z}_p$, we will refer to as a base field.

Let $p > 3$ be a prime. An elliptic curve E defined over a finite field $\mathbb{F}_p$ ($E/\mathbb{F}_p$) is an equation

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

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

this condition (the discriminant) avoids singularities

- $E(\mathbb{F}_p)$ is the set of points $(x,y) \in \mathbb{F}_p^2$ satisfying the equation and the special point at infinity $\mathcal{O}$.
- Schoof has alg running $O(\log(p^e))$ to get $|E(\mathbb{F}_{p^e})|$. ✓

Example: $E/\mathbb{F}_{11}: y^2 = x^3 + 4x + 4$, $|E(\mathbb{F}_{11})| = 11$

x	0	1	2	3	4	5	6	7	8	9	10
x^3+4x+4	4	9	9	10	7	6	2	1	9	10	10
y	±2	±3	±3	n/a	n/a	n/a	n/a	±1	±3	n/a	n/a

and so there are $\boxed{11}$ points modulo 11: $(0,\pm2)$, $(1,\pm3)$, $(2,\pm3)$, $(7,\pm1)$, $(8,\pm3)$, and ∞.

Here we have a prime order group!

Note: when moving from rationals to finite fields, the properties of the addition laws needs to be reproven. This is done with a lot of algebra.

DLog in EC Groups

Let $E/\mathbb{F}_p$ be an EC and $E(\mathbb{F}_p)$ be the group of points. Further, let P be a point in $E(\mathbb{F}_p)$ of prime order q ($|p| \approx |q|$ in bits)

$$q P := \underbrace{P \boxplus P \boxplus \ldots \boxplus P}_{q \text{ times}} = \mathcal{O}$$

P must generate a prime order subgroup $(\{\mathcal{O}, P, 2P, \ldots, (q-1)P\}, \boxplus)$ of $E(\mathbb{F}_p)$.

The DLog problem is given P, αP (for random $\alpha \in \mathbb{Z}_p$), calculate α.

- For most ECs, the best DLog attacks are $\Omega(\sqrt{q})$. This means for $\lambda = 128$ bits, the group needs to be size $\approx 2^{256}$. The group operation involves arithmetic modulo a 256-bit prime which is much faster than $(\mathbb{Z}_p^*, \cdot)$ with similar security levels. $p \neq |E(\mathbb{F}_p)| \approx p$
- There are exceptions in which DLog is easy:
  - when $|E(\mathbb{F}_p)| = p$, it is possible to map points to the additive group of $\mathbb{F}_p$ ("SMART" Attack)
  - when $|E(\mathbb{F}_p)|$ divides $p^B - 1$ for small B (MOV attack)
- In practice, we standardize ECs (P256, Curve25519, etc) to use that avoids common pitfalls.

  twist secure

  Drama about parameter selection

  - either we choose an EC whose group is already a prime or pick a prime order subgroup.

Efficient Implementation of EC operations

- Reviewing the elliptic curve group operation, the calculation of the slope requires a field inversion

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \\ \dfrac{3x_1^2 + A}{2y_1} \end{cases}$$

inversion

- A field inversion is much more expensive than a field addition or multiplication. Requires running a variant of the extended euclidean algo. $\approx$ 9 to 40 times a field mult (pratically)
- Can we avoid field inversions when adding points?

Jacobian Coordinates

Idea: We can "accumulate" our divisions by storing an additional element.

Let $(X : Y : Z)$ represent an affine point $\left(\frac{X}{Z^2}, \frac{Y}{Z^3}\right)$.

Affine $\mapsto$ Jacobian : $(X, Y) \mapsto (X : Y : 1)$,

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

Notice that when we convert to Jacobian coordinates we lose uniqueness. In particular, $\{(t^2X, t^3Y, t) \mid t \in \mathbb{F}\}$ all denote the same affine point (X, Y).

Simarly, $\mathcal{O} \mapsto \{(t^2 : t^3 : 0) \mid t \in \mathbb{F}\}$ (i.e. $Z = 0$)

Doubling Formula for Jacobian Coordinates

Doubling a Jacobian $(X:Y:Z)$

$$\lambda = \frac{3X_1^2 + A}{2Y} \qquad X_3 = \lambda^2 - 2X_1 \quad , \quad Y_3 = \lambda(X_1 - X_3) - Y_1$$

Substitute $\left(\frac{X}{Z^2}, \frac{Y}{Z^3}\right)$ into affine formulas,

$$\lambda = \frac{3\left(\frac{X}{Z^2}\right)^2 + A}{2\left(\frac{Y}{Z^3}\right)} = \frac{3X^2 + AZ^4}{2YZ}$$

$$\left.\begin{aligned} X_3 &= \lambda^2 - 2\left(\frac{X}{Z^2}\right) = \frac{C}{4Y^2Z^2} \\ Y_3 &= \lambda\left(\frac{X}{Z^2} - X_3\right) - \frac{Y}{Z^3} = \frac{D}{8Y^3Z^3} \end{aligned}\right\} \text{affine coords}$$

Notice $4Y^2Z^2 = (2YZ)^2$, $8Y^3Z^3 = (2YZ)^3$.

Thus, the Jacobian coords of doubling $(X:Y:Z)$ is $(C, D, 2YZ)$.

- calculation of C, D require only a small number of field add / field mults

Batch Conversion

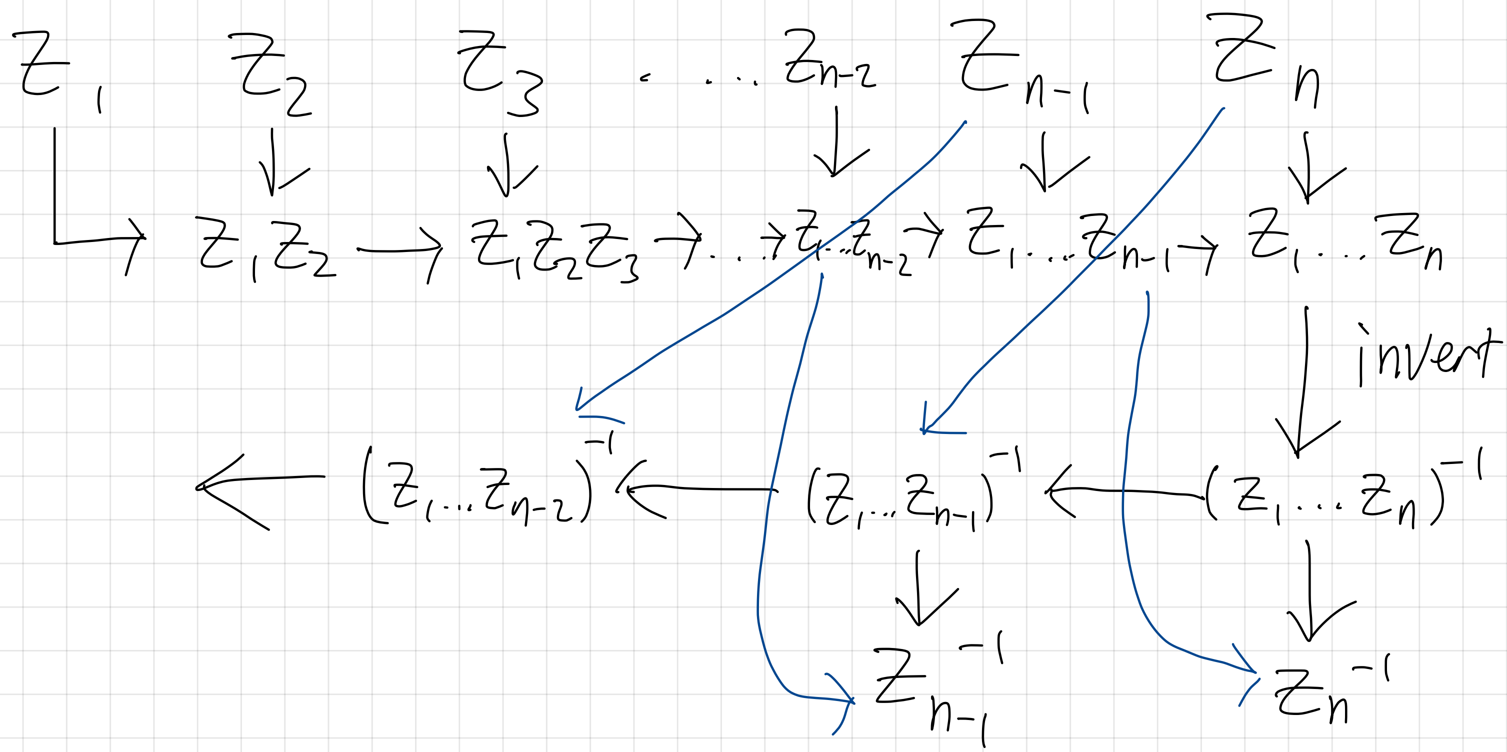
- To convert Jacobian coords to affine, we need to perform an inversion $(X:Y:Z) \mapsto \left(\frac{X}{Z^2}, \frac{X}{Z^3}\right)$, suffices to invert Z and then calc $\left(\frac{1}{Z}\right)^2, \left(\frac{1}{Z}\right)^3$.
- Naively, to convert n Jacobian points to n affine points, we require n inversions. However, we can batch inversions!

Batch Inversion

- We want to invert field elts, $z_1, \dots, z_n$.
- Alg
  - Compute table of partial products
    $$p := [z_1, z_1 z_2, \dots, z_1 z_2 \cdots z_n]$$
  - Invert $z_1 z_2 \cdots z_n$ as $I_{1,n} := \frac{1}{z_1 z_2 \cdots z_n} = \frac{1}{p_n}$
  - $\frac{1}{z_n} = I_{1,n} \cdot p_{n-1} = \frac{1}{z_1 \cdots z_n} \cdot z_1 \cdots z_{n-1}$
  - $I_{1,n-1} = I_{1,n} \cdot z_n = \frac{1}{z_1 z_2 \cdots z_{n-1}}$
  - $\frac{1}{z_{n-1}} = I_{1,n-1} \cdot p_{n-2}$ and so on

Inverting n elts requires 1 inversion, $O(n)$ mults

Diagram



Wrapping Up

- ECs used widely for PK crypto
- ECs are much more efficient in practice than using subgroups of $(\mathbb{Z}_p^*, \cdot)$ at similar security levels
- ECs have algebraic structure that enable many applications
  - pairings (identity based encryption, eff sigs, ..)
- most crypto libraries do not expose the group operations of ECs for safety