"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. $\mathbb{G} = \{g^0, g^1, \ldots, g^{|\mathbb{G}|-1}\}$

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. $h^{\mathrm{ord}(h)} = 1$. $\in \mathbb{G}$

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 $p = 2q+1$
    $\uparrow$ 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 $(\mathbb{Z}_p, +)$ "Integer division"
- For $(\mathbb{Z}_p^*, \cdot)$, the best known algorithm is the General Number Field Sieve which runs in $2^{\tilde{O}((\log p)^{1/3})}$ (subexponential time).
  - For $\lambda = 2^{128}$ 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, isogenies) 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 3rd 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.

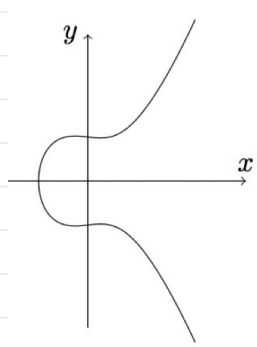
☆ Fermat wrote "Fermat's Last Thm" in the margins of Arithmetica (the series written by Diophantus on this subject)

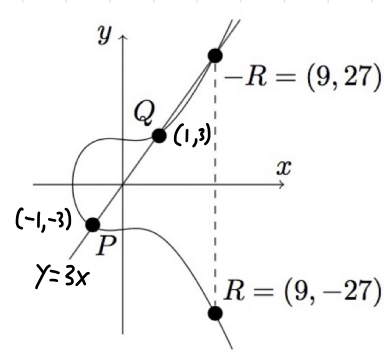
☆ Andrew Wiles / Richard Taylor would later prove FLT using ECs - a popular book written about this by Simon Singh

In book 4 of Arithmetica, find rational points satisfying

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

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



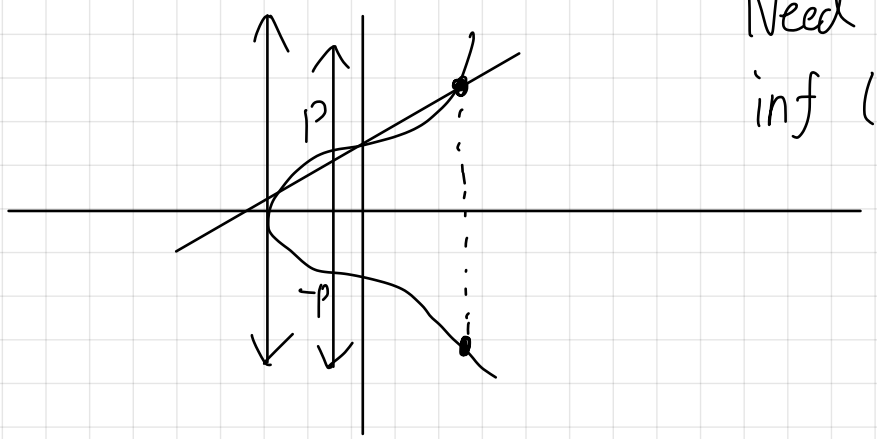


Let $-R$ denote the reflection of R across the x-axis.

<u>Chord Method:</u> for distinct rational points U, V s.t. $U \neq -V$, pass a line through U, V and find a third point W of intersection with the curve. (Poincare) "$U \boxplus V$"

<u>Tangent Method:</u> draw tangent line and consider second point of intersection. "$P \boxplus P$"

Almost a group operation, issues:



Need a point at inf (the identity)

Let $\tilde{E}(\mathbb{Q})$ be the set of rational points on a specific elliptic curve E. The group of an elliptic curve is defined as

$$\left(E(\mathbb{Q}) := \tilde{E}(\mathbb{Q}) \cup \{\mathcal{O}\}, \boxplus\right)$$

point at infinity

where $\boxplus : E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q})$ is "draw line, obtain intersection, reflect across x-axis", and $\mathcal{O}$ is the identity.

☆ can you convince yourself this is an abelian group

Rationals do not have concise representations, so we operate over finite fields.

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

$\mathbb{F}_{p^e}$ for $e \geq 2$ is an "extension" field of order p^e that contains a "copy" of $\mathbb{F}_p$ inside.

EC over Finite Fields

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 double roots

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

<u>Example</u>: $E/\mathbb{F}_{11} : y^2 = x^3 + 1$

$$E(\mathbb{F}_{11}) = \left\{\mathcal{O},\ (-1,0),\ (0,\pm 1),\ (2,\pm 3),\ (5,\pm 4),\ (7,\pm 5),\ (9,\pm 2)\right\}$$

$|E(\mathbb{F}_{11})| = 12$

EC Cryptography

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

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

P must generate a prime order subgroup $(\{\mathcal{O}, P, 2P, \dots, (q-1)P\}, \boxplus)$ of $E(\mathbb{F}_{p^e})$.

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.

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, ..)
  - isogenies (post quantum crypto, Delay encryption, ..)
  - more!
- most crypto libraries do not expose the group operations of ECs for safety