# Introduction to mathematical cryptography

## Lecture 3: Elliptic Curves

Sabrina Kunzweiler

Preliminary Arizona Winter School 2025

# What are elliptic curves

# Elliptic curves

Convention in this lecture: $K$ field, char$(p) \neq 2, 3$.

**Elliptic curve**

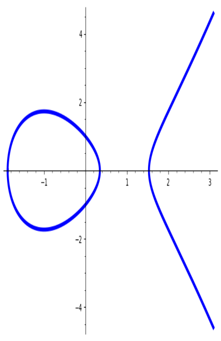
An **elliptic curve** $E$ defined over $K$ consists of a point at infinity $\infty$ and points $(x, y)$ in the plane satisfying an equation of the form

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

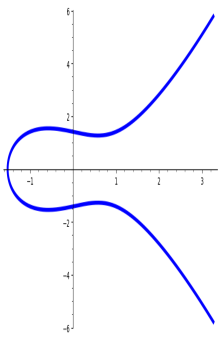
with $a, b \in K$ and $4a^3 + 27b^2 \neq 0$.

- Such an equation is called short Weierstrass equation.
- $4a^3 + 27b^2 \neq 0$ ensures smoothness
  $\Rightarrow \Delta = -16(4a^3 + 27b^2)$ is the discriminant of $E$.

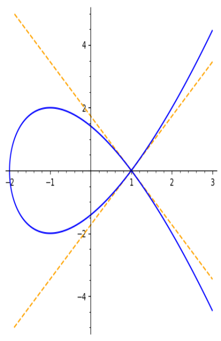
# Typical pictures of elliptic curves (over $\mathbb{R}$)




**(a)** $E_1/\mathbb{R}$ defined by $y^2 = x^3 - 3x + 1$.




**(b)** $E_2/\mathbb{R}$ defined by $y^2 = x^3 - x + 2$.




**(c)** $C/\mathbb{R}$ (not elliptic) $y^2 = x^3 - 3x + 2$

# Points on elliptic curves

# Rational points

**Points on elliptic curves**

Let $E : y^2 = x^3 + ax + b$ elliptic curve over $K$. For any field extension $L/K$, the set

$$E(L) = \underbrace{\{(u, v) \subset L^2 \mid v^2 = u^3 + au + b\}}_{\text{affine points}} \cup \{\infty\}$$

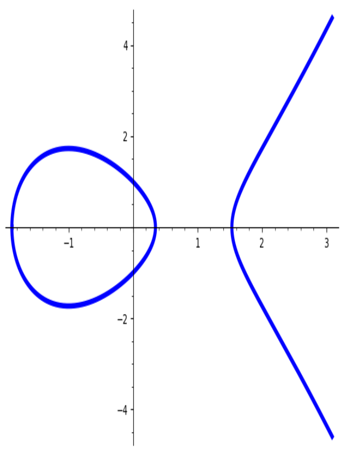
is called the set of $L$-rational points of $E$.

- Questions we discuss in this lecture:

  *What can we say about the order of an elliptic curve: $\#E(K)$ (over $\mathbb{R}$, over $\mathbb{Q}$, over $\mathbb{F}_q$)?*

  *What is the "structure" of the set $E(L)$?*

# Example $E : y^2 = x^3 - 3x + 1$




- $E/\mathbb{R}$: infinitely many points $\infty$, $P_1 = (0,1)$, $P_2 = (-1, \sqrt{3})$, $P_3 = (2, \sqrt{3})$, $P_4 = (3, \sqrt{19})$, ...
- $E/\mathbb{Q}$: infinitely many (here!) $\infty$, $P_1 = (0,1)$, $P_2 = (0,-1)$, $\left(\frac{9}{4}, \frac{19}{8}\right), \left(\frac{-152}{81}, \frac{107}{729}\right), \ldots,$
- $E/\mathbb{F}_{13}$: 19 points $\infty$, $(0,1)$, $(0,-1)$, $(1,5)$, $(1,-5)$, $(2,4)$, ...

# The point at infinity

An elliptic curve with short Weierstrass equation $y^2 = x^3 + ax + b$ should really be viewed as a planar projective curve.

- It lives in the projective plane $\mathbb{P}^2_K$
  - elements of $\mathbb{P}^2_K$:
    $(X, Y, Z) \in K^3 \setminus \{(0, 0, 0)\}$ modulo the equivalence relation
    $(X, Y, Z) \sim (\lambda X, \lambda Y, \lambda Z)$
  
  $\rightarrow$ notation: $(X : Y : Z) \in \mathbb{P}^2_K(K)$.
- It is defined by a homogeneous polynomial $F \in K[X, Y, Z]$ (all monomials have the same degree):

$$E : Y^2 Z = X^3 + aXZ^2 + bZ^3 \quad \text{in } \mathbb{P}^2.$$

Points on the projective curve:

- affine points: $(x : y : 1)$
- points at infinity $(x : y : 0) \Rightarrow$ here: only one $\infty = (0 : 1 : 0)$

# Elliptic curves in SageMath

```
# Example over QQ
sage: E1 = EllipticCurve([-3,1]); E1
Elliptic Curve defined by y^2 = x^3 - 3*x + 1 over Rational
    Field
sage: P1 = E1([0,1]); P1
(0 : 1 : 1)
sage: P2 = E1([9/4,19/8]); P2
(9/4 : 19/8 : 1)
sage: P2 == E1([18,19,8])
True
```

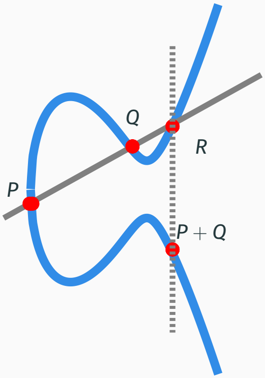
```
# Example over a finite field
sage: E2 = EllipticCurve(GF(13),[-3,1]); E2
Elliptic Curve defined by y^2 = x^3 + 10*x + 1 over Finite Field
     of size 13
sage: E2.points()
[(0 : 1 : 0), (0 : 1 : 1), (0 : 12 : 1), (1 : 5 : 1), (1 : 8 :
    1), (2 : 4 : 1), (2 : 9 : 1), (4 : 1 : 1), (4 : 12 : 1), (6
     : 2 : 1), (6 : 11 : 1), (9 : 1 : 1), (9 : 12 : 1), (10 : 3
     : 1), (10 : 10 : 1), (11 : 5 : 1), (11 : 8 : 1), (12 : 4 :
     1), (12 : 9 : 1)]
```

# The group law

# Geometric description

**Adding points $P, Q \in E$.**

- Line $L$ through $P$ and $Q$
- There is a third intersection point $R \in E \cap L$ (Bezout's Theorem)
- $P + Q$ is the reflection of $R$ across the $x$-axis



# Explicit formulas

## Group law

$E : y^2 = x^3 + ax + b$ elliptic curve over $K$,
$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\bar{K})$, then $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:

(a) If $x_1 \neq x_2$, then $(x_3, y_3) = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1)$ with $m = \frac{y_2 - y_1}{x_2 - x_1}$.

(b) If $x_1 = x_2$ and $y_1 = y_2 \neq 0$, then $(x_3, y_3) = (m^2 - 2x_1, m(x_1 - x_3) - y_1)$ with $m = \frac{3x_1^2 + a}{2y_1}$.

(c) If $x_1 = x_2$ and $y_1 \neq y_2$ or $y_1 = y_2 = 0$, then $P_1 + P_2 = \infty$.

Moreover, we define $P + \infty = P$ for all $P \in E(\bar{K})$.

Then $(E(\bar{K}), +)$ is an abelian group with identity element $\infty$.

# Relation with the geometric interpretation

Setup: $E : y^2 = x^3 + ax + b$ elliptic curve over $K$,
$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\bar{K})$, then $P_1 + P_2 = P_3 = (x_3, y_3)$:

(a) If $x_1 \neq x_2$, then $(x_3, y_3) = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1)$ with $m = \frac{y_2 - y_1}{x_2 - x_1}$.

*(handwritten notes)*

# Proving the group law

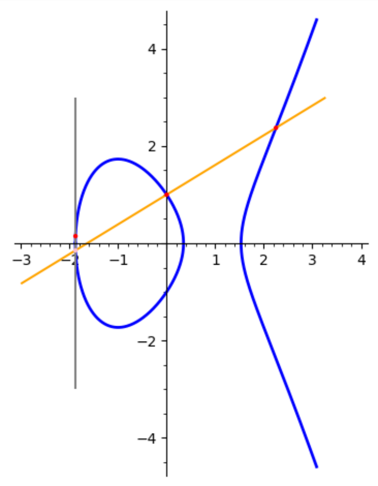
- **neutral element**: $P + \infty = P$ for $P$ (by definition)
  $\Rightarrow \mathcal{O}_E = \infty$ ✓
- **existence of inverses**: $P_1 = (x_1, y_1)$, then $-P_1 = (x_1, -y_1)$
  (case ($c$) of the group law). ✓
- **associativity**:
  - tedious computation with many case distinctions
    use computer algebra software (sage)
  - elegant proof using divisors (requires more algebraic geometry)

  (✓)

- **commutativity**: swap $P_1$ and $P_2$ everywhere - nothing changes ✓

# Example $E : y^2 = x^3 - 3x + 1$ over $\mathbb{Q}$ (doubling)

$$P_1 = (0, 1), \quad P_2 = \left(\frac{9}{4}, \frac{19}{8}\right) \in E(\mathbb{Q}).$$




- $x_1 = 0 \neq 9/4 = x_2$
  $\Rightarrow$ case (a)
- $m = \frac{\frac{19}{8} - 1}{\frac{9}{4} - 0} = \frac{11}{18}$
- $x_3 = \left(\frac{11}{18}\right)^2 - 0 - \frac{9}{4} = \frac{-152}{81}$
- $y_3 = \frac{11}{18}\left(0 - \frac{-152}{18}\right) - 1 = \frac{107}{729}$,

$$P_1 + P_2 = \left(\frac{-152}{81}, \frac{107}{729}\right).$$

# Scalar multiplication and torsion

# Scalar multiplication

**Notation**

Let $E$ be an elliptic curve over $K$, and $N \in \mathbb{Z}$ an integer.

$$[N] : E(K) \to E(K), \quad P \mapsto \underbrace{P + \cdots + P}_{N \text{ times}},$$

is the scalar multiplication by $N$.

**Spoiler**: Scalar multiplication is a *conjectural* cryptographic one-way function

- Evaluation is fast using a double-and-add strategy (Exercises)
  - Example: $[2^{10}]P = [2]([2] \cdots ([2]P)$
    $\to 10 = \log_2(2^{10})$ doublings
- Inversion is (conjecturally) hard: next lecture

# Torsion

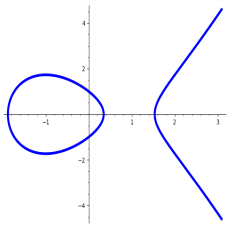
### $N$-torsion group

Let $E$ be an elliptic curve over $K$, $N \geq 1$ and integer. The group of points of order $N$ is denoted by

$$E[N] = \{P \in E(\bar{K}) \mid [N]P = \infty\}.$$

We say that $E[N]$ is the $N$-torsion group of $E$.

**Example 1:** $N = 2$




$E_1 : y^2 = x^3 - 3x + 1$ over $\mathbb{Q}$

- $x^3 - 3x + 1 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$
- $E[2] = \{(\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0), \infty\}$, but $E(\mathbb{Q})[2] = \{\infty\}$
- Note: $(\alpha_1, 0) + (\alpha_2, 0) = (\alpha_3, 0)$

$\Rightarrow$ $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

# Structure of the torsion group

**Structure of $E[N]$**

Let $E$ be an elliptic curve over $K$ and $N \geq 1$ an integer.

1. If $\text{char}(K) = 0$ or $\text{char}(K) = p$ with $p \nmid N$. Then

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

2. If $\text{char}(K) = p > 0$, then one of the following is true:
   (i) $E[p^k] \cong \{\infty\}$ for all $k \geq 1$.
   (ii) $E[p^k] \cong \mathbb{Z}/p^k\mathbb{Z}$ for all $k \geq 1$.

- Proof reference: Silverman Corollary III.6.4
- Main idea: study $[N]$, the multiplication by $N$ map, and find that it is of degree $N^2$ (requires more ingredients).

# Elliptic curves over finite fields

# Hasse's theorem

**What's the number of $\mathbb{F}_q$-rational points of an elliptic curve $E$?**

- Very rough bounds: $\infty \in E(\mathbb{F}_q)$ and $(x, y) \in E \setminus \{\infty\} \subset \mathbb{F}_q \times \mathbb{F}_q$

$$1 \leq \#E(\mathbb{F}_q) \leq 1 + q^2.$$

- Better upper bound: Let $x_0 \in \mathbb{F}_q$, then $y^2 = x_0^3 + ax_0 + b$ has at most two solutions $\pm y_0$.

$$1 \leq \#E(\mathbb{F}_q) \leq 1 + 2q.$$

**Theorem (Hasse, 1936)**

Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$. Then

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}.$$

# A concrete formula (special case)

**Lemma**

Let $p \equiv 2 \pmod 3$ be a prime , and consider the elliptic curve $E : y^2 = x^3 + 1$. Then $\#E(\mathbb{F}_p) = p + 1$.

Let $y_0 \in \mathbb{F}_p$. *How many solutions* $x_0 \in \mathbb{F}_p$ *with* $x_0^3 = y_0^2 - 1$ *are there?*

- Which elements in $\mathbb{F}_p$ are cubes?
  Since, $p \equiv 2 \pmod 3$, all elements are cubes!
    - $0 = 0^3$ is a cube
    - For $g \in \mathbb{F}_p^*$, we have $\sqrt[3]{g} = h = g^{(2p-1)/3} \in \mathbb{F}_{p^*}$.
- How many cube roots can exist?
  Exactly one, note that $\mathbb{F}_p$ does not contain primitive third roots of unity.

**Conclusion**: For every $y_0 \in \mathbb{F}_p$, there exists a unique $x_0 \in \mathbb{F}_p$ so that $(x_0, y_0) \in E(\mathbb{F}_p) \quad \Rightarrow \quad p$ affine points, and in total $\#E(\mathbb{F}_p) = p + 1$. $\square$

# Group structure of the rational points

**Proposition**

Let $E$ be an elliptic curve over $\mathbb{F}_q$. Then

$$E(\mathbb{F}_q) \cong \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z}$$

for some integers $N_1, N_2 \geq 1$ and $N_2 \mid N_1$.

**Proof**

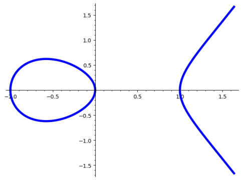
- Let $N = \#E(\mathbb{F}_q)$. Then $[N] \cdot P = \infty$ for every element $P \in E(\mathbb{F}_q)$ (finite group) $\Rightarrow E(\mathbb{F}_q) \subset E[N]$.
- $E(\mathbb{F}_q) \cong G \subset \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ (slide 15)
  $\Rightarrow G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z}$ with $N_1, N_2 \mid N$, and $N_2 \mid N_1$. □

**Question** What are the possible group structures for $E$:

1. $E : y^2 = x^3 - 3x + 1$ over $\mathbb{F}_{13}$, $\#E(\mathbb{F}_{13}) = 19$ (slide 4)
2. $E : y^2 = x^3 + x + 1$ over $\mathbb{F}_{13}$, $\#E(\mathbb{F}_{13}) = 18$.

# Example $E : y^2 = x^3 - x$ over $\mathbb{F}_5$

**Goal:** Determine the group structure of




$E : y^2 = x^3 - x$ over $\mathbb{F}_5$

1. Find a point $P_1 \in E(\mathbb{F}_5) \setminus \{\infty\}$ : $P_1 = (0, 0)$
2. Compute the order of $P_1$: $[2]P_1 = \infty$
   $\Rightarrow \mathbb{Z}/2\mathbb{Z} \cong \langle P_1 \rangle \subset E(\mathbb{F}_5)$
3. Find a point $P_2 \in E(\mathbb{F}_5) \setminus \langle P_1 \rangle$ : $P_2 = (1, 0)$
4. Compute the order of $P_2$: $[2]P_2 = \infty$
   $\Rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \langle P_1, P_2 \rangle \subset E(\mathbb{F}_5)$
5. Find a point $P_3 \in E(\mathbb{F}_5) \setminus \langle P_1, P_2 \rangle$ : $P_3 = (2, 1)$
6. Compute the order of $P_3$: $[2]P_3 = (0, 0) = P_1$
   $\Rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \langle P_3, P_2 \rangle \subset E(\mathbb{F}_5)$.

   We are done here! Why?

   - Hasse bound: $2 \leq \#E(\mathbb{F}_5) \leq 10$.
   - our computations: $8 \mid \#E(\mathbb{F}_5)$.

   $E(\mathbb{F}_5) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

# Summary of Lecture 3

Elliptic curves: geometric objects with a group structure

- Addition law $P + Q$ for $P, Q \in E(K)$
  - Explicit formulas
  - Geometric interpretation
- Scalar multiplication $[N] : E \to E$, and torsion points $E[N]$
- Elliptic curves over finite fields $\mathbb{F}_q$
  - Hasse bound: $1 + q - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq 1 + q + 2\sqrt{q}$
  - Group structure: $E(\mathbb{F}_q) \cong \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z}$.

**Next lecture Elliptic curves in cryptography**

- Why are elliptic curves better generic groups?
- Why are some elliptic curves worse generic groups?