Finding Maximal and Optimal Elliptic Curves

Alec Zabel-Mena

Universidad de Puerto Rico, Recinto de Rio Piedras

September 12, 2020

Groups

Definition

A nonempty set G with a binary operation $\cdot$ is called a **group** for for all $a, b, c \in G$

1. $a \cdot b \in G$.
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. $\exists e \in G$ such that $\forall a \in G$, $a \cdot e = e \cdot a = a$
4. $\forall a \in G\ \exists a^{-1} \in G$ such that, $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definition

A group G is **abelian** (or **commutative**) if for $a, b \in G$, $a \cdot b = b \cdot a$.

Examples of Groups

- The group of integers $\mathbb{Z}$.
- The group of integers modulo n, $\mathbb{Z}/n\mathbb{Z}$.
- The group of units of $\mathbb{Z}/n\mathbb{Z}$, $U(\mathbb{Z}/n\mathbb{Z})$.

Fields

Definition

A nonempty subset F, together with binary operations $+$ and $\cdot$, is called a **field** if it satisfies the following:

1. $(F, +)$ is an abelian group.
2. $(F, \cdot)$ is an abelian group.
3. For $a, b, c \in F$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Definition

For a field F, the **characteristic** of F is the smallest positive integer p such that $pa = 0$. We denote it by $\operatorname{char} F = p$

Examples of Fields

- The field of real numbers $\mathbb{R}$.
- The field of rational numbers$\mathbb{Q}$.
- The field of complex numbers$\mathbb{C}$.
- Finite fields, $\mathbb{F}_p$, where $\operatorname{char} \mathbb{F}_p = p$.

Definition

Definition

Let K be a field, and let $f(x) = x^3 + a_2x^2 + a_4x + a_6 \in K[x]$ a cubic polynomial with no multiple roots. The **elliptic curve** is the polynomial

$$y^2 + a_1xy + a_3y = f(x) \tag{1}$$

together with a **point at infinity** $\mathcal{O}$.

Examples.

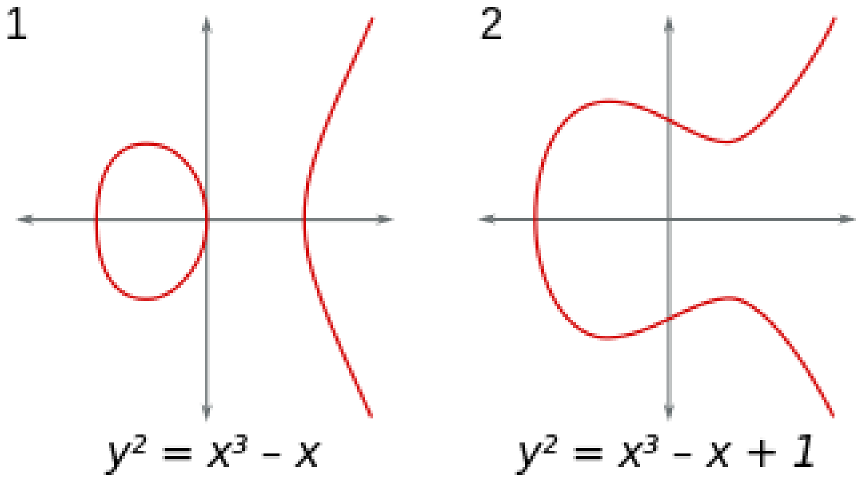

Figure 1:

The Addition Law on Elliptic Curves

Let $E(K)$ be an elliptic curve over a field K. We define the addition of points of $E(K)$ to be the binary operation $+$ such that $\forall P, Q, R \in E(K)$:

- If $P = \mathcal{O}$, Then $-P = \mathcal{O}$ and $P + Q = Q$.
- If $P = (x, y) \in E(K)$ then $-P = (x, -a_1x - a_3 - y) \in E(K)$.
- If $P \neq Q$, take the line $l = \overline{PQ}$ to be the line that cuts $E(K)$ at P, Q, and another point R. Then $P + Q = -R$.
- If $P = Q$, take the line $l = \overline{PQ}$ tangent at P cutting another point R. Then $P + Q = -R$.

The addition law

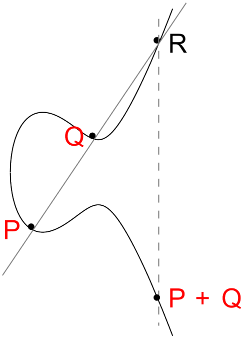

Figure 2:

The Zeta Function of an Elliptic Curve

- Consider the Elliptic Curve E defined over $\mathbb{F}_q$. Then E is defined over any extension field $\mathbb{F}_{q^r}$ for $r \in \mathbb{Z}^+$
- We denote $N_r = |E(\mathbb{F}_{q^r})|$ to be the number of $\mathbb{F}_{q^r}$ **rational points** on E.
- $N_1 = N = |E(\mathbb{F}_q)|$

The Zeta Function of an Elliptic Curve

Definition

We define the **Zeta function** of the elliptic curve E over $\mathbb{F}_q$ to be the formal power series over $\mathbb{Q}[[T]]$ defined by:

$$Z(E/\mathbb{F}_q) = \exp\left(\sum_r \frac{N_r T^r}{r}\right) \tag{2}$$

- The Weil conjectures give an explicit formula for the zeta fucntion of an elliptic curve

The Zeta Function of an Elliptic Curve

Theorem (The Weil Conjectures for an Elliptic Curve)

Let E be an elliptic curve over $\mathbb{F}_q$. The zeta function of E is the rational function of T of the form:

$$Z(E/\mathbb{F}_q, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)} \tag{3}$$

- Where $N_1 = q + 1 - a$.
- We can also find $a = \alpha + \beta$ where α and β is a complex conjugate pair such that $|\alpha| = |\beta| = \sqrt{q}$.
- By knowing N_1 and finding α and β one can find the number of $\mathbb{F}_{q^r}$ rational points by taking: $N_r = q^r + 1 - \alpha^r - \beta^r$

The Hasse Bound

Theorem (Hasse's Theorem)

Let N be the number of $\mathbb{F}_q$ rational points on an elliptic curve $E(\mathbb{F}_q)$. Then:

$$|N - (q+1)| \leq 2\sqrt{q} \tag{4}$$

- Hasse's theorem provides a good bound for testing whether certain elliptic curves are optimal optimal, or maximal.
- We find such curves.

q = 2 r = 2

for a6 in range(q): for a4 in range(q): for a3 in range(q):

for a2 in range(q): for a1 in range(q): b2=a1^2+4$*a2; b4 =$

$a1 * a3 + 2 * a4; b6 = a3^2 + 4 * a6; b8 = a1^2 * a6 - a1 * a3 * a4 +$

$a2 * a3^2 + 4 * a2 * a6 - a4^2$

References