Elliptic Curves over Finite Fields

Alexandra Sklyarova

May 2025

Adjusting Definitions

We can now extend our study of elliptic curves to the field $\mathbb{F}_p$
So let
$$C : y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{F}_p$$

Adjusting Definitions

We can now extend our study of elliptic curves to the field $\mathbb{F}_p$
So let

$$C : y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{F}_p$$

We will refer to the **rational points** of C as

$$C(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p,\ f(x, y) = 0\}$$

We refer to points that are not rational as those (x, y) where $x, y \in \mathbb{F}_q$ where $\mathbb{F}_q = \mathbb{F}_{p^e}$, some field extension of $\mathbb{F}_p$.

Non-Singular Curves

We will be looking exclusively at non-singular curves over finite fields.

Non-Singular Curves

We will be looking exclusively at non-singular curves over finite fields.
Recall, the discriminant is

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

In this case, a curve is non-singular if

$$p \neq 2$$

and the discriminant

$$D \not\equiv 0 \mod p$$

How big is $C(\mathbb{F}_p)$

We can first think about it conceptually.
Consider

$$y^2 = f(x) = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{F}_p, \text{ with } p \neq 2$$

In the group $\mathbb{F}_p^\times$, exactly half of the elements are **Quadratic Residues** while the other half are not.
Recall that quadratic residues are the set

$$\{a \in \mathbb{F}_p : a \equiv n^2 \mod p, \text{ for some } 0 < n < p\}$$

Now substitute each of $0, 1, ...p - 1$ into $y^2 = f(x)$.

How big is $C(\mathbb{F}_p)$

If $\mathbf{f}(\mathbf{x}) = \mathbf{0}$ then there is only one solution i.e. $y = 0$.

How big is $C(\mathbb{F}_p)$

If $\mathbf{f}(\mathbf{x}) = \mathbf{0}$ then there is only one solution i.e. $y = 0$.

If $\mathbf{f}(\mathbf{x}) \neq \mathbf{0}$ then there are two possibilities.

Either $f(x)$ is a quadratic residue, which means it would contribute two solutions for y. Or $f(x)$ is not a quadratic residue, which means it contributes 0 solutions.

How big is $C(\mathbb{F}_p)$

If $\mathbf{f}(\mathbf{x}) = \mathbf{0}$ then there is only one solution i.e. $y = 0$.

If $\mathbf{f}(\mathbf{x}) \neq \mathbf{0}$ then there are two possibilities.

Either $f(x)$ is a quadratic residue, which means it would contribute two solutions for y. Or $f(x)$ is not a quadratic residue, which means it contributes 0 solutions.

So each x either corresponds to 1 solution or it has a 50% chance of either contributing 2 solutions or 0 i.e.

$$|C(\mathbb{F}_p)| = p + 1 + \text{error term}$$

Hasse-Weil

We can actually compute the error term from the previous slide. Unfortunately, the proof of the theorem is far too complicated, but it is worth stating.

Hasse-Weil

We can actually compute the error term from the previous slide. Unfortunately, the proof of the theorem is far too complicated, but it is worth stating.

Hasse – Weil Theorem : If C is a non singular curve of genus g over $\mathbb{F}_p$, then the number of points on C with coordinates in $\mathbb{F}_p$ is

$$p + 1 + \epsilon, \quad \text{where } |\epsilon| \leq 2g\sqrt{p}$$

Here, elliptic curves have genus 1, so we see that

$$-2\sqrt{p} \leq |C(\mathbb{F}_p)| - p - 1 \leq 2\sqrt{p}$$

Reduction mod p Theorem

Theorem : Let

$$C : y^2 = x^3 + ax^2 + bx + c$$

be a non-singular cubic with $a, b, c \in \mathbb{Z}$ and discriminant $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$. Take $\Phi \subset C(\mathbb{Q})$ be a subgroup of points of finite order.

Then, for any prime p, let $P \to \tilde{P}$ be the reduction mod p map

$$\Phi \to \tilde{C}(\mathbb{F}_p), \quad P \mapsto \tilde{P} = \begin{cases} (\tilde{x}, \tilde{y}), & P = (x, y) \\ \tilde{\mathcal{O}}, & P = \mathcal{O} \end{cases}$$

Reduction mod p Theorem

Theorem : Let

$$C : y^2 = x^3 + ax^2 + bx + c$$

be a non-singular cubic with $a, b, c \in \mathbb{Z}$ and discriminant $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$. Take $\Phi \subset C(\mathbb{Q})$ be a subgroup of points of finite order.

Then, for any prime p, let $P \to \tilde{P}$ be the reduction mod p map

$$\Phi \to \tilde{C}(\mathbb{F}_p), \quad P \mapsto \tilde{P} = \begin{cases} (\tilde{x}, \tilde{y}), & P = (x, y) \\ \tilde{\mathcal{O}}, & P = \mathcal{O} \end{cases}$$

If $p \nmid 2D$, then it is an isomorphism of Φ into a subgroup of $\tilde{C}(\mathbb{F}_p)$.

A Theorem of Gauss

Theorem : Let p be a prime and M_p denote the number of projective solutions to

$$x^3 + y^3 + z^3 = 0, \quad x, y, z \in \mathbb{F}_p$$

If $p \not\equiv 1 \mod 3$ then $M_p = p + 1$.

If $p \equiv 1 \mod 3$ then there exists $A, B \in \mathbb{Z}$ s.t.

$$4p = A^2 + 27B^2$$

then $M_p = p + 1 + A$

Sato-Tate Conjecture

Recall, Hasse-Weil tells use the number of points in $C(\mathbb{F}_p)$ as $p + 1 + \epsilon$. We can encode this ϵ in terms of an angle as follows

$$\theta_p = \cos^{-1}\left(\frac{\epsilon}{2\sqrt{p}}\right), \quad 0 \leq \theta_p \leq \pi$$

Then we can visualize the distribution of M_p for all primes.

Sato-Tate Conjecture

Recall, Hasse-Weil tells use the number of points in $C(\mathbb{F}_p)$ as $p + 1 + \epsilon$. We can encode this ϵ in terms of an angle as follows

$$\theta_p = \cos^{-1}\left(\frac{\epsilon}{2\sqrt{p}}\right), \quad 0 \leq \theta_p \leq \pi$$

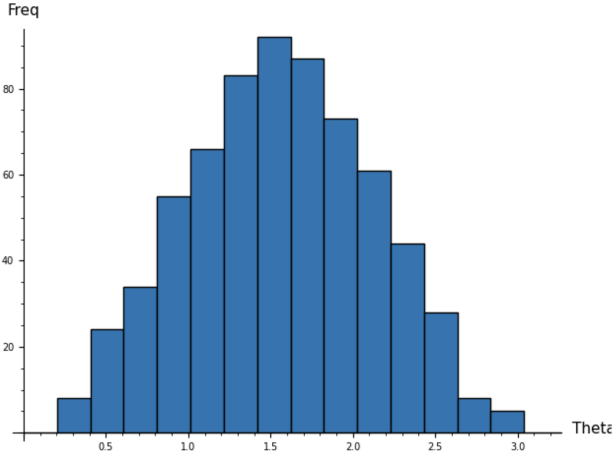
Then we can visualize the distribution of M_p for all primes.

Conjecture : Assume that the cubic curve does not have complex multiplication. For any fixed angles $0 \leq \alpha \leq \beta \leq \pi$ we have

$$\lim_{X \to \infty} \frac{|\{p \leq X : \alpha \leq \theta_p \leq \beta\}|}{\pi(X)} = \frac{2}{\pi} \int_\alpha^\beta \sin^2 t \, dt$$

Example 1

$$y^2 = x^3 + x^2 + x + 1$$



Example 2

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