The Number of Rational Points of Elliptic Curves Over Finite Fields

Speaker:Tao Qin
Advisor: Matt Papanikolas

June 2019

Table of Contents

Elliptic Curves

Definition

An elliptic curve is a pair (E, O), where E is a smooth curve of genus 1 in $\mathbb{P}^2$ and O is a point of E.

- We say E is defined over a field K if the following are satisfied:
  1. As a curve E is defined over K. This means the ideal of the curve is generated by some polynomials, whose coefficients are in K.
  2. O has coordinates in K.

- From this point, we will focus on the finite field F_p.

Weierstrass Equation

Definition

A Weierstrass equation defined over F_p is of the following form:
$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$
where $a_i \in F_p$ for all i.

- We can make a change of variables by using non-homogeneous coordinates: $x = X/Z$ and $y = Y/Z$. Then the Weierstrass equation will become: $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Weierstrass Equation

If p is neither 2 nor 3. We can continue to make a change of variables (omitted) and get a Weierstrass equation of the following form: $E : y^2 = x^3 + Ax + B$.

Definition

The discriminant of the above Weierstrass equation is defined to be $\triangle = -16(4A^3 + 27B^2)$.

Theorem

The curve defined by the above Weierstrass equation is smooth iff $\triangle$ is nonzero.

Relation between Elliptic Curves and Weierstrass Equations

Theorem

Let E be an elliptic curve defined over F_p.
(1) There exists functions $x, y \in F_p(E)$ such that the map $\phi : E \to \mathbb{P}^2$ where $\phi = [x, y, 1]$ gives an isomorphism of $E|F_p$ onto a curve given by a Weiestrass equation
$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ where $a_i \in F_p$ for all i. It satisfies that $\phi(O) = [0, 1, 0]$. Call x, y Weierstrass coordinates.
(2) Any two Weierstrass equations for E as in (1) are related by a linear change of variables of the form $X = u^2X' + r, Y = u^3Y' + su^2X' + t$ where u, r, s, t are in F_p and u is nonzero.
(3) Every smooth curve given by a Weierstrass equation as in (a) is an elliptic curve defined over F_p with base point $O = [0, 1, 0]$

Group Structure on Elliptic Curves

Bezout's Theorem (Simple Version)

Let L be a line in $\mathbb{P}^2$ and (E, O) an elliptic curve. Then L intersects with E in exactly 3 points, counted with multiplicity.

Group Law

Let P, Q be two points on E and L be the line passing P and Q. Then L will intersect E at the third point R. Now let L' denote the line passing through R and O. It will also intersect with E at a third point. We define this point to be the sum of P and Q, namely $P \oplus Q$. Under this definition of addition, we can check that the elliptic curve becomes an additive abelian group with identity element O.

Rational Points

Definition

We say a point P=[X,Y,Z] of an elliptic curve over F_p is a rational point(or F_p-rational point) if all the three coordinates are in F_p.

Theorem (Hasse 1930)

Let $E|F_p$ be an elliptic curve and let $E(F_p)$ be the set of rational points on E. Then we have the following estimate $|\#E(F_p) - p - 1| \leq 2\sqrt{p}$.

Distribution of the Number of Rational Points

Remark

We are focused on the ellptic curves of the form $E(a,b) : y^2 = x^3 - ax - b$.

Remark

For the elliptic curve $E(a,b)$, the number of rational points can be rewrritten by Legendre symbols:

$$\#E(a,b)(F_p) = p + 1 + \sum_{x=0}^{p-1} (x^3 - ax - b|p)$$

Definition

$$S_R(p) = \sum_{a,b=0}^{p-1} [\sum_{x=0}^{p-1} (x^3 - ax - b|p)]^{2R}$$

Distribution Formula 1 For Small R

Theorem (Birch 1968)

$S_R(p) \sim p^{R+2}\frac{(2R)!}{R!(R+1)!}$ *as* $R \to \infty$.

Theorem (Birch 1968)

For $p \geq 5$, $S_1(p) = p^2(p-1)$, $S_2(p) = p(p-1)(2p^2-3)$, $S_3(p) = p(p-1)(5p^3-9p-5)$, $S_4(p) = p(p-1)(14p^4-28p^2-20p-7)$, $S_5(p) = (p-1)(42p^6-90p^4-75p^3-35p^2-9p-\tau(p))$. *Here* τ *denotes the Ramanujan's* τ*-function.*

Remark

The Ramanujan's τ-function is a function from $\mathbb{N}$ to $\mathbb{Z}$ defined by :

$$\sum_{n\geq 1}\tau(n)q^n = q\prod_{n\geq 1}(1-q^n)^{24}.$$

Another Type of Weierstrass Equations

We can consider all the curves defined by the equations of the form $y^2 = x^3 - ax^2 - bx$. All the elliptic curves having a nontrivial point of order 2 are included in these equations.

Distribution Formula 2 For Small R

Conjecture

For $p \geq 5$, we have $S_1(p) = p(p-1)^2$, $S_2(p) = 2p(p-1)(p^2-p-3)$, $S_3(p) = (p-1)(5p^4 - 5p^3 - 18p^2 - 10p - b(p))$.

Remark

$b(p)$ is defined to be the coefficients of the following infinite product:

$$\sum_{n \geq 1} b(n) q^n = q \prod_{m \geq 1} (1-q^m)^8 (1-q^{2m})^8, \text{ where } q = e^{2\pi i z}.$$

Examples

Compute by using Distribution Formula 2

Take $R = 3, p = 11$. We know that $b(11) = 1092$. Then by our Distribution Formula 2
$S_3(11) = (11-1)(5*11^4 - 5*11^3 - 18*11^2 - 10*11 - 1092) = 631700$

Compute directly by using Legendre Symbols

$S_3(11) = \sum_{a,b=0}^{10} [\sum_{x=0}^{10} (x^3 - ax - b|11)]^6$. Use mathematica.