The Weil Conjectures for Elliptic Curves

Gaurish Korpal

The University of Arizona, Tucson

December 10, 2020

Outline

1. Elliptic curves
   - Definition
   - Group structure
2. Weil conjectures
   - Zeta function
   - Statement
3. Counting points over finite fields
   - Main lemma
   - An example

Elliptic curves

Definition

Since we won't be discussing any proofs in this seminar, it will be sufficient to restrict ourselves to the following definition of elliptic curves:

Elliptic curve

An elliptic curve over a field K is a nonsingular projective plane curve over K given by an affine equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with an extra point $O = [0 : 1 : 0]$ at infinity.

Therefore, in homegenous coordinates the equation will be:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

where $x = X/Z$ and $y = Y/Z$.

Examples and non-examples over $\mathbb{R}$

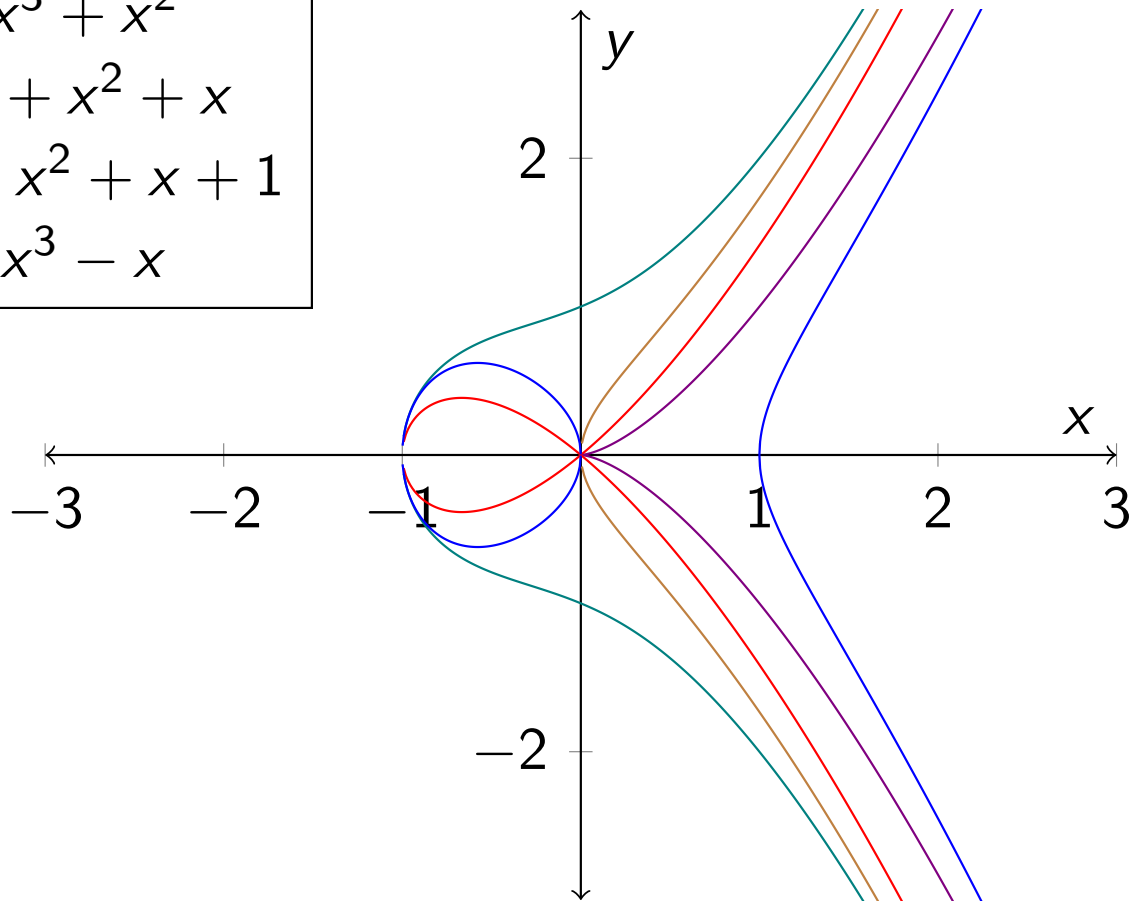
$y^2 = x^3$

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

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

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

$y^2 = x^3 - x$



Group structure

Since the equation of an elliptic curve $E \subset \mathbb{P}^2$ has degree three, any line $L \subset \mathbb{P}^2$ intersects E at exactly three points, counted with multiplicities (Bézout's theorem). Keeping this fact in mind, we define the following addition law on the points of E:

Addition law

Let $P, Q \in E$ be two points. Suppose L is the line through P and Q (if $P = Q$, then let L be the tangent line to E at P), and R is the third point of intersection of L with E. Then, let L' be the line through R and O which will intersect E at a third point. We denote that third point by $P + Q$.

Illustration over $\mathbb{R}$

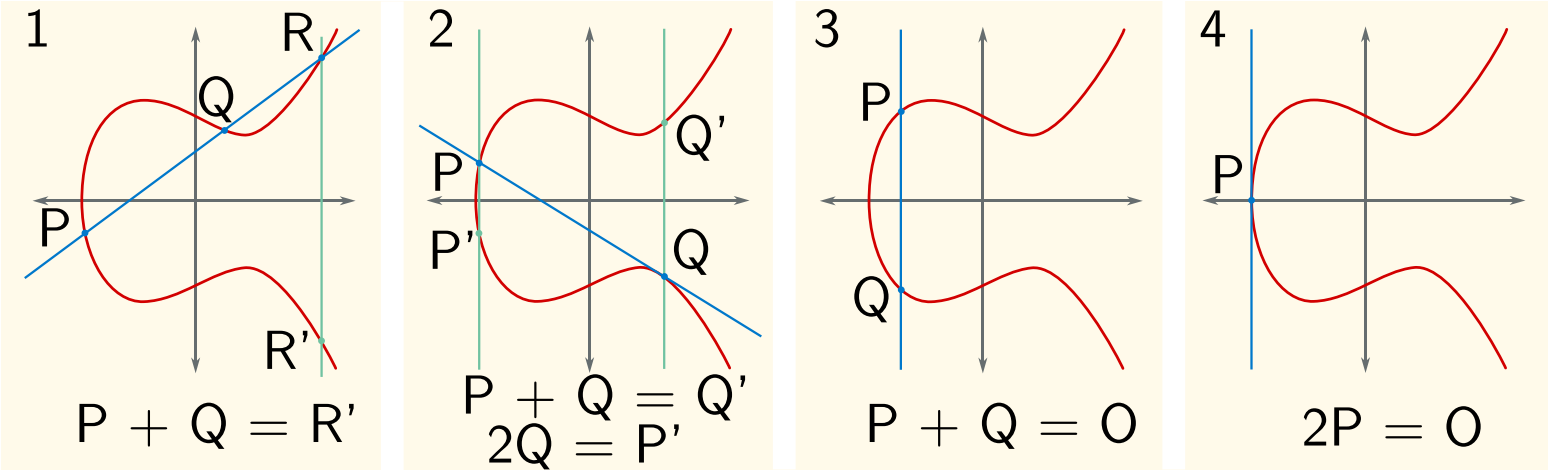


Figure: Addition of points on elliptic curve [SuperManu, CC BY-SA 3.0, via Wikimedia Commons, https://commons.wikimedia.org/wiki/File:ECClines-2.svg]

Key observation

The addition law makes E into an abelian group with identity element O.

Weil conjectures

Zeta function

$\mathbb{F}_q$ is a finite field with q elements, where q is a power of prime p.

$\mathbb{F}_{q^n}$ for each integer $n \geq 1$, is the extension of $\mathbb{F}_q$ of degree n, so $\#\mathbb{F}_{q^n} = q^n$.

$V/\mathbb{F}_q$ is a projective variety, such that V is the set of solutions to

$$f_1(x_0, \ldots, x_N) = \cdots = f_m(x_0, \ldots, x_N) = 0$$

where $f_1, \ldots, f_m$ are homogeneous polynomials with coefficients in $\mathbb{F}_q$.

$V(\mathbb{F}_{q^n})$ is the set of points of V with coordinates in $\mathbb{F}_{q^n}$

We encode the number of points in $V(\mathbb{F}_{q^n})$ for all $n \geq 1$ into the following generating function:

Zeta function

The zeta function of $V/\mathbb{F}_q$ is the power series

$$Z_{V/\mathbb{F}_q}(t) = \exp\left(\sum_{n=1}^{\infty}(\#V(\mathbb{F}_{q^n}))\frac{t^n}{n}\right)$$

Statement for elliptic curves

When the variety V is an elliptic curve E, the zeta function exhibits the following properties referred to as Weil conjectures:

Weil conjectures for elliptic curves

Let $E/\mathbb{F}_q$ be an elliptic curve. Then there is an $a \in \mathbb{Z}$ such that

$$Z_{E/\mathbb{F}_q}(t) = \frac{1 - at + qt^2}{(1-t)(1-qt)} \in \mathbb{Q}(t)$$

Further, over $\mathbb{C}$ we have

$$1 - at + qt^2 = (1 - \alpha t)(1 - \beta t)$$

with $|\alpha| = |\beta| = \sqrt{q}$.

The zeta function also satisfies the following functional equation:

$$Z_{E/\mathbb{F}_q}\left(\frac{1}{qt}\right) = Z_{E/\mathbb{F}_q}(t)$$

Counting points over finite fields

Main lemma

Following is the main lemma which enables us to simplify the zeta function and get the rational function stated above.

Lemma

Let $E/\mathbb{F}_q$ be an elliptic curve and $a = q + 1 - \#E(\mathbb{F}_q)$. If $\alpha, \beta \in \mathbb{C}$ are the roots of the polynomial $p(t) = t^2 - at + q$. Then α and β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$ and for every $n \geq 1$, we have

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$$

The quantity a is called the trace of Frobenius, because it is equal to the trace of the q-power Frobenius map considered as a linear transformation of the ℓ-adic Tate module of E.

An example over $\mathbb{F}_2$

Consider the following elliptic curve over $\mathbb{F}_2$:

$$E : y^2 - y = x^3 - x^2$$

Hence, E is a variety in $\mathbb{P}^2$ given by the homogeneous equation:

$$\bar{E} : Y^2Z - YZ^2 = X^3 - X^2Z$$

Since $\#\mathbb{F}_2 = 2$ is a small number, we can easily find that $[0:0:1], [1:0:1], [1:1:1], [0:1:1]$ and $O = [0:1:0]$ are the only points lying on E over $\mathbb{F}_2$. That is, $\boxed{\#E(\mathbb{F}_2) = 5}$.
Therefore, $a = 2 + 1 - 5 = -2$ and we can get α, β by finding the roots of $p(t) = t^2 + 2t + 2$. Hence, we have

$$\boxed{\#E(\mathbb{F}_{2^n}) = 2^n + 1 - (-1+i)^n - (-1-i)^n}$$

where $i = \sqrt{-1}$.

An example over $\mathbb{F}_2$ (contd.)

We can simplify the above formula to get:

$$\#E(\mathbb{F}_{2^n}) = 2^n + 1 - 2^{\frac{n}{2}+1}\cos\left(\frac{3n}{4}\pi\right)$$

$$= \begin{cases} 2^n + 1 - 2^{\frac{n}{2}+1} & \text{if } n \equiv 0 \pmod 8 \\ 2^n + 1 + 2^{\frac{n+1}{2}} & \text{if } n \equiv \pm 1 \pmod 8 \\ 2^n + 1 & \text{if } n \equiv \pm 2 \pmod 8 \\ 2^n + 1 - 2^{\frac{n+1}{2}} & \text{if } n \equiv \pm 3 \pmod 8 \\ 2^n + 1 + 2^{\frac{n}{2}+1} & \text{if } n \equiv 4 \pmod 8 \end{cases}$$

Observe that, $\#E(\mathbb{F}_2) = \#E(\mathbb{F}_4) = \#E(\mathbb{F}_8) = 5$, hence there are no new solutions even though we are going to a bigger field.
Using this formula, we can easily find that

$$\boxed{\#E(\mathbb{F}_{1024}) = 2^{10} + 1 = 1025}.$$

General estimate

Hasse's inequality

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

For example, for $q = 1021$, the prime nearest to $2^{10} = 1024$, $\#E(\mathbb{F}_{1021}) = 1000$ satisfying $|1021+1-1000| = 22 \leq 2\sqrt{1021} \approx 64$.

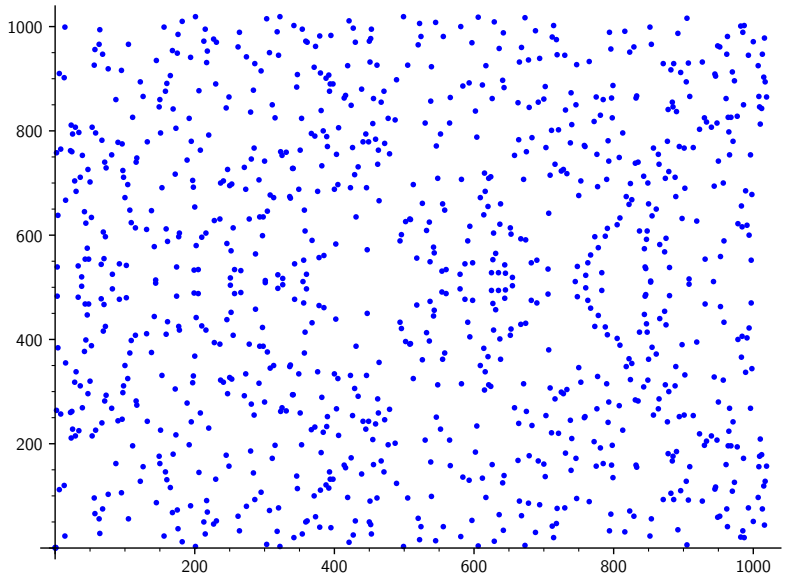


Figure: Plot of 999 affine points on $y^2 - y = x^3 - x$ over $\mathbb{F}_{1021}$. SageMathCell code:

```
E=EllipticCurve(GF(1021),[0,-1,-1,0,0]); A=E.plot(); A.save('v1.pgf')
```