Rational Points on elliptic curves

Real and Complex points on cubic curves

Ajay Prajapati
170063

Department of Mathematics and Statistics
Indian Institute of Technology, Kanpur

Mid-Semester Exam presentation

Story so far

1. How to solve general linear equations in two variables.
2. How to solve general quadratic equations in two variables.
3. Defined group law on points of general cubic equation in two variables as curves in Projective plane.
4. How to reduce the general cubic equation to Weierstrass Normal Form via Projective transformation. This transformation is group homomorphism and preserves rational points. Defined elliptic curves to be non-singular cubic curve.
5. Saw that singular cubic curves behave like quadratic curves which we know how to solve. This leaves the case to understand elliptic curves whose behaviour is very different from linear and quadratic case.
6. Algebraic formula for group law.
7. Looked at group of points of order 2 and 3 over different fields.

Elliptic over different fields

- Let $y^2 = x^3 + ax^2 + bx + c$ where a, b, c $\in \mathbb{Q}$ be equation of curve C.
- This defines several groups when considered over different fields.

$$C(\mathbb{Q}) = \{(x, y) \in C : x, y \in \mathbb{Q}\} \cup \{\mathcal{O}\} \tag{1}$$

$$C(\mathbb{R}) = \{(x, y) \in C : x, y \in \mathbb{R}\} \cup \{\mathcal{O}\} \tag{2}$$

$$C(\mathbb{C}) = \{(x, y) \in C : x, y \in \mathbb{C}\} \cup \{\mathcal{O}\} \tag{3}$$

- We have $\{\mathcal{O}\} \leq C(\mathbb{R}) \leq C(\mathbb{R}) \leq C(\mathbb{C})$ as subgroups.
- We could use methods of analysis to study $C(\mathbb{R})$ and $C(\mathbb{C})$.

Elliptic curves over $\mathbb{C}$

1. Non-singular cubic curves in two variables over $\mathbb{C}$ is called **Complex Elliptic Curve**. It can be written in Weierstrass Normal Form $y^2 = 4x^3 - g_2x - g_3$.

Elliptic curves over $\mathbb{C}$

1. Non-singular cubic curves in two variables over $\mathbb{C}$ is called **Complex Elliptic Curve**. It can be written in Weierstrass Normal Form $y^2 = 4x^3 - g_2 x - g_3$.
2. Complex elliptic curve is a object of study in itself. For now we forget the above definition of elliptic curve. We will arrive at above definition but our path will lead us to understanding elliptic curves more deeply. In particular, we will see why group law exists at all.

Lattices

Lattice(discrete additive subgroup)

Let ω_1 and ω_2 in $\mathbb{C}$ which are LI over $\mathbb{R}$.Then $\mathbb{Z}$ linear combination of them is called lattice in complex plane. $\Lambda = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$

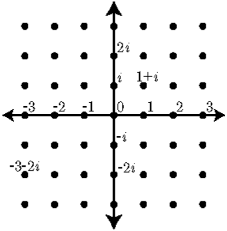

Figure: The ring of Gaussian integers ($Z[i]$)

Fundamental domain:

Definitions

Elliptic curve

Let Λ be a lattice in complex plane. Then $\mathbb{C}/\Lambda$ is called an **Elliptic curve** w.r.t Λ.

- Let Λ be a lattice in complex plane. Then a Λ periodic meromorphic function on $\mathbb{C}$ is called **Elliptic function**.

Weierstrass function

1. Weierstrass $\wp$ function defined below is an example of Elliptic function:

$$\wp(u) = \frac{1}{u^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right) \tag{4}$$

Weierstrass function

1. Weierstrass $\wp$ function defined below is an example of Elliptic function:

$$\wp(u) = \frac{1}{u^2} + \sum_{\omega\in\Lambda,\omega\neq 0} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right) \tag{4}$$

Theorem

The sum in (4) converges absolutely and uniformly for u in any compact subset of $\mathbb{C} - \Lambda$. So $\wp$(u) defines a holomorphic on $\mathbb{C} - \Lambda$.

2.

Weierstrass function

1. Weierstrass $\wp$ function defined below is an example of Elliptic function:

$$\wp(u) = \frac{1}{u^2} + \sum_{\omega\in\Lambda,\omega\neq 0} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right) \tag{4}$$

Theorem

The sum in (4) converges absolutely and uniformly for u in any compact subset of $\mathbb{C} - \Lambda$. So $\wp$(u) defines a holomorphic on $\mathbb{C} - \Lambda$.

2.

3. Given a lattice Λ, define Eisenstein series of Λ weight k (>2) by

$$G_k(\Lambda) = \sum_{\omega\in\Lambda,\omega\neq 0} \frac{1}{\omega^k} \tag{5}$$

Property of Weierstrass function

Theorem: Let $\wp$ be Weierstrass function w.r.t lattice Λ. Then

1. The functions $\wp$ and $\wp'$ satisfies the equation

$$(\wp(z)')^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda) \tag{6}$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$

Property of Weierstrass function

Theorem: Let $\wp$ be Weierstrass function w.r.t lattice Λ. Then

1. The functions $\wp$ and $\wp'$ satisfies the equation

$$(\wp(z)')^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda) \tag{6}$$

   where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$

2. Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ and $\omega_3 = \omega_1 + \omega_2$. Then the cubic satisfied by $\wp$ and $\wp'$ is

$$y^2 = 4(x - e_1)(x - e_2)(x - e_3) \text{ where } e_i = \wp(\omega_i/2) \tag{7}$$

   This equation is non-singular meaning right side has distinct roots.

Equivalence of two definitions

1. The differential equation (6) has very elegant and basic geometric interpretation. Suppose we take the function $P : \mathbb{C} \to \mathbb{P}^2_{\mathbb{C}}$ given by $P(u) = [\wp(u) : \wp'(u) : 1]$ if $u \notin \Lambda$ and $P(u) = [0 : 1 : 0]$.

Equivalence of two definitions

1. The differential equation (6) has very elegant and basic geometric interpretation. Suppose we take the function $P : \mathbb{C} \to \mathbb{P}^2_{\mathbb{C}}$ given by $P(u) = [\wp(u) : \wp'(u) : 1]$ if $u \notin \Lambda$ and $P(u) = [0 : 1 : 0]$.
2. The image of any non-lattice point is in xy-plane and coordinates satisfy the relation $y^2 = 4x^3 - g_2 x - g_3$ where cubic polynomial has distinct roots.

Equivalence of two definitions

1. The differential equation (6) has very elegant and basic geometric interpretation. Suppose we take the function $P : \mathbb{C} \to \mathbb{P}^2_{\mathbb{C}}$ given by $P(u) = [\wp(u) : \wp'(u) : 1]$ if $u \notin \Lambda$ and $P(u) = [0 : 1 : 0]$.
2. The image of any non-lattice point is in xy-plane and coordinates satisfy the relation $y^2 = 4x^3 - g_2 x - g_3$ where cubic polynomial has distinct roots.
3. So P defines map from complex plane to a curve E in $\mathbb{P}^2_{\mathbb{C}}$. This map can be shown to be surjective (uses argument principal).

Equivalence of two definitions

1. The differential equation (6) has very elegant and basic geometric interpretation. Suppose we take the function $P : \mathbb{C} \to \mathbb{P}^2_{\mathbb{C}}$ given by $P(u) = [\wp(u) : \wp'(u) : 1]$ if $u \notin \Lambda$ and $P(u) = [0 : 1 : 0]$.
2. The image of any non-lattice point is in xy-plane and coordinates satisfy the relation $y^2 = 4x^3 - g_2 x - g_3$ where cubic polynomial has distinct roots.
3. So P defines map from complex plane to a curve E in $\mathbb{P}^2_{\mathbb{C}}$. This map can be shown to be surjective (uses argument principal).
4. Since $\wp$ is Λ periodic, so we get a bijection from $\mathbb{C}/\Lambda$ to E (again injectivity uses agrument principal). So we established equivalence of definition in one direction.

Equivalence of two definitions

1. The differential equation (6) has very elegant and basic geometric interpretation. Suppose we take the function $P : \mathbb{C} \to \mathbb{P}^2_{\mathbb{C}}$ given by $P(u) = [\wp(u) : \wp'(u) : 1]$ if $u \notin \Lambda$ and $P(u) = [0 : 1 : 0]$.
2. The image of any non-lattice point is in xy-plane and coordinates satisfy the relation $y^2 = 4x^3 - g_2 x - g_3$ where cubic polynomial has distinct roots.
3. So P defines map from complex plane to a curve E in $\mathbb{P}^2_{\mathbb{C}}$. This map can be shown to be surjective (uses argument principal).
4. Since $\wp$ is Λ periodic, so we get a bijection from $\mathbb{C}/\Lambda$ to E (again injectivity uses agrument principal). So we established equivalence of definition in one direction.

Proposition

Given an elliptic curve $y^2 = 4x^3 - a_2 x - a_3$, there exists a lattice Λ s.t. $a_2 = 60G_4(\Lambda)$ and $a_3 = 140G_6(\Lambda)$.

5.

Equivalence of two definitions

1. The differential equation (6) has very elegant and basic geometric interpretation. Suppose we take the function $P : \mathbb{C} \to \mathbb{P}^2_{\mathbb{C}}$ given by $P(u) = [\wp(u) : \wp'(u) : 1]$ if $u \notin \Lambda$ and $P(u) = [0 : 1 : 0]$.
2. The image of any non-lattice point is in xy-plane and coordinates satisfy the relation $y^2 = 4x^3 - g_2 x - g_3$ where cubic polynomial has distinct roots.
3. So P defines map from complex plane to a curve E in $\mathbb{P}^2_{\mathbb{C}}$. This map can be shown to be surjective (uses argument principal).
4. Since $\wp$ is Λ periodic, so we get a bijection from $\mathbb{C}/\Lambda$ to E (again injectivity uses agrument principal). So we established equivalence of definition in one direction.

Proposition

Given an elliptic curve $y^2 = 4x^3 - a_2 x - a_3$, there exists a lattice Λ s.t. $a_2 = 60G_4(\Lambda)$ and $a_3 = 140G_6(\Lambda)$.

5.
6. So we have established equivalence of two definitions

Group law

1. Since $\mathbb{C}/\Lambda$ is a naturally group, the bijective map above induces a group structure on E.

4. $\mathbb{C}/\Lambda$ is torus (and thus a Riemann surface). So we can define topology (and Riemann surface structure) on complex elliptic curve via map $\tilde{P}$ and we obtain a torus.

5. A torus has topological genus 1 and there is concept of genus of curves. So intuitively, genus of an elliptic curve should be 1. In fact this is the case. This will be covered later in the course.

Group law

1. Since $\mathbb{C}/\Lambda$ is a naturally group, the bijective map above induces a group structure on E.
2. The most amazing thing about this group structure is that group law is given by the chord-tangent law that we have seen previously.

4. $\mathbb{C}/\Lambda$ is torus (and thus a Riemann surface). So we can define topology (and Riemann surface structure) on complex elliptic curve via map $\tilde{P}$ and we obtain a torus.
5. A torus has topological genus 1 and there is concept of genus of curves. So intuitively, genus of an elliptic curve should be 1. In fact this is the case. This will be covered later in the course.

Group law

1. Since $\mathbb{C}/\Lambda$ is a naturally group, the bijective map above induces a group structure on E.
2. The most amazing thing about this group structure is that group law is given by the chord-tangent law that we have seen previously.
3. This explains why group sturcture on elliptic curves exists at all. Ideally, one should do the above analysis to arrive at the group law on elliptic curves but as you can see, its very tedious. So most books directly start with group law definition.
4. $\mathbb{C}/\Lambda$ is torus (and thus a Riemann surface). So we can define topology (and Riemann surface structure) on complex elliptic curve via map $\tilde{P}$ and we obtain a torus.
5. A torus has topological genus 1 and there is concept of genus of curves. So intuitively, genus of an elliptic curve should be 1. In fact this is the case. This will be covered later in the course.

Points of finite order on complex elliptic curve

1. To find points of finite order, we again use the group isomorphism $\tilde{P}$. Suppose we want to find points of order diving m on E, we look for points in lattice $\mathbb{C}/L$ having order dividing m which are

$$\left\{ \frac{(a\omega_1 + b\omega_2)}{m} : 0 \leq a, b \leq m - 1 \right\} \tag{8}$$

Points of finite order on complex elliptic curve

1. To find points of finite order, we again use the group isomorphism $\tilde{P}$. Suppose we want to find points of order diving m on E, we look for points in lattice $\mathbb{C}/L$ having order dividing m which are

$$\left\{ \frac{(a\omega_1 + b\omega_2)}{m} : 0 \leq a, b \leq m-1 \right\} \tag{8}$$

2. So points of order dividing m on E are

$$E[m] = \left\{ \tilde{P}\left(\frac{a\omega_1 + b\omega_2}{m} \right) : 0 \leq a, b \leq m-1 \right\} \tag{9}$$

Points of finite order on complex elliptic curve

1. To find points of finite order, we again use the group isomorphism $\tilde{P}$. Suppose we want to find points of order diving m on E, we look for points in lattice $\mathbb{C}/L$ having order dividing m which are

$$\left\{ \frac{(a\omega_1 + b\omega_2)}{m} : 0 \leq a, b \leq m-1 \right\} \tag{8}$$

2. So points of order dividing m on E are

$$E[m] = \left\{ \tilde{P}\left(\frac{a\omega_1 + b\omega_2}{m} \right) : 0 \leq a, b \leq m-1 \right\} \tag{9}$$

3. So $|E[m]| = m^2$ and $E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} x \frac{\mathbb{Z}}{m\mathbb{Z}}$.

Elliptic curves over $\mathbb{R}$

1. A non-singular cubic curve C over $\mathbb{R}$ is said to be elliptic curve over $\mathbb{R}$. Addition of real points on C is continuous.

Elliptic curves over $\mathbb{R}$

1. A non-singular cubic curve C over $\mathbb{R}$ is said to be elliptic curve over $\mathbb{R}$. Addition of real points on C is continuous.
2. $C(\mathbb{R})$ can be shown to be compact one-dimensional Lie group.

Elliptic curves over $\mathbb{R}$

1. A non-singular cubic curve C over $\mathbb{R}$ is said to be elliptic curve over $\mathbb{R}$. Addition of real points on C is continuous.
2. $C(\mathbb{R})$ can be shown to be compact one-dimensional Lie group.

Theorem

Any one-dimensional compact connected Lie group is isomorphic to the group of rotations of the circle which is isomorphic to unit circle as subgroup of multiplicative group of complex numbers.

3.

Elliptic curves over $\mathbb{R}$

1. A non-singular cubic curve C over $\mathbb{R}$ is said to be elliptic curve over $\mathbb{R}$. Addition of real points on C is continuous.
2. $C(\mathbb{R})$ can be shown to be compact one-dimensional Lie group.

Theorem

Any one-dimensional compact connected Lie group is isomorphic to the group of rotations of the circle which is isomorphic to unit circle as subgroup of multiplicative group of complex numbers.

3.
4. If the curve is connected then it is isomorphic to unit circle group.

Elliptic curves over $\mathbb{R}$

1. A non-singular cubic curve C over $\mathbb{R}$ is said to be elliptic curve over $\mathbb{R}$. Addition of real points on C is continuous.
2. $C(\mathbb{R})$ can be shown to be compact one-dimensional Lie group.

Theorem

Any one-dimensional compact connected Lie group is isomorphic to the group of rotations of the circle which is isomorphic to unit circle as subgroup of multiplicative group of complex numbers.

3.
4. If the curve is connected then it is isomorphic to unit circle group.
5. If not, then the connected component which contains $\mathcal{O}$ is isomorphic to unit circle group.

Points of Finite order on Elliptic curves over $\mathbb{R}$

- Let E be a elliptic curve over $\mathbb{R}$ then for each m $\in \mathbb{Z}^+$ define

$$E[m] = \{P \in E : ord(P)|m\} \tag{10}$$

- On unit circle, points of finite order are roots of unity. For each m $\in \mathbb{Z}^+$, the points of order dividing m are.

$$\{e^{\frac{2\pi ik}{m}} : 0 \leq k \leq m-1\} \cong \mathbb{Z}/m\mathbb{Z} \tag{11}$$

- If E has only one component, then E[m] $\cong \mathbb{Z}/m\mathbb{Z}$.
- If E has two connected components then E($\mathbb{R}$) $\cong S^1 \oplus \mathbb{Z}/2\mathbb{Z}$. Hence

$$E[m] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{if m is odd} \\ \mathbb{Z}/m\mathbb{Z}x\mathbb{Z}/2\mathbb{Z} & \text{if m is even} \end{cases} \tag{12}$$

Elliptic curves over finite fields

1. Let $\mathbb{F}_q$ be a finite field of order q$= p^n$. Any rational elliptic curve coefficients can be made integers by cancelling denominators. And this in turn can be reduced modulo p to view it as curve over $\mathbb{F}_q$.

Elliptic curves over finite fields

1. Let $\mathbb{F}_q$ be a finite field of order q$= p^n$. Any rational elliptic curve coefficients can be made integers by cancelling denominators. And this in turn can be reduced modulo p to view it as curve over $\mathbb{F}_q$.
2. If we start with a non-singular cubic $y^2 = x^3 + ax^2 + bx + c$, after reducing mod p, it may happen that cubic does not remain singular. If it happens then we say reduction mod p is bad reduction. This will happen for finitely many primes (when $p|disc$).

Elliptic curves over finite fields

1. Let $\mathbb{F}_q$ be a finite field of order q$= p^n$. Any rational elliptic curve coefficients can be made integers by cancelling denominators. And this in turn can be reduced modulo p to view it as curve over $\mathbb{F}_q$.
2. If we start with a non-singular cubic $y^2 = x^3 + ax^2 + bx + c$, after reducing mod p, it may happen that cubic does not remain singular. If it happens then we say reduction mod p is bad reduction. This will happen for finitely many primes (when $p|disc$).
3. Otherwise it remains non-singular after reducing mod p. (i.e. an elliptic curve)

Elliptic curves over finite fields

1. Let $\mathbb{F}_q$ be a finite field of order q$= p^n$. Any rational elliptic curve coefficients can be made integers by cancelling denominators. And this in turn can be reduced modulo p to view it as curve over $\mathbb{F}_q$.
2. If we start with a non-singular cubic $y^2 = x^3 + ax^2 + bx + c$, after reducing mod p, it may happen that cubic does not remain singular. If it happens then we say reduction mod p is bad reduction. This will happen for finitely many primes (when $p|disc$).
3. Otherwise it remains non-singular after reducing mod p. (i.e. an elliptic curve)
4. Addition law from $\mathbb{C}$ carries over to finite field $\mathbb{F}_q$ because chord-tangent group law we have given can be described purely in algebraic terms (section 1.4- formulas for 2P and $P_1 + P_2$).

Elliptic curves over finite fields

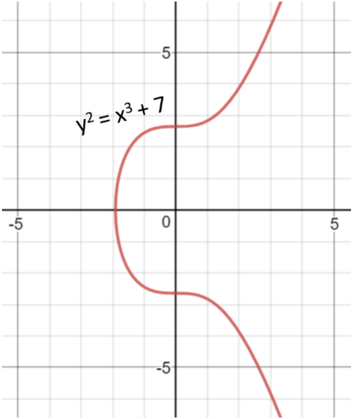

Figure: Bitcoin elliptic curve

Elliptic curves over finite fields

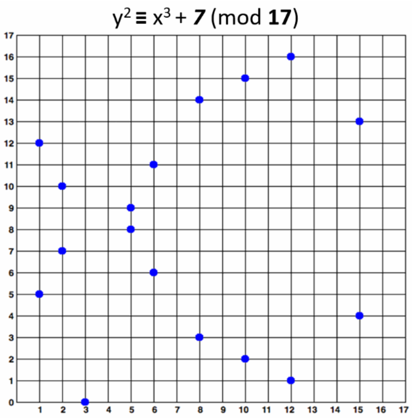

Figure: Bitcoin elliptic curve in $\mathbb{F}_{17}$

Reference-https://cryptobook.nakov.com/asymmetric-key-ciphers/elliptic-curve-cryptography-ecc

Elliptic curves over finite fields

1. Because in this case the group is finite, every point has finite order. But one can ask about points of various orders.

Elliptic curves over finite fields

1. Because in this case the group is finite, every point has finite order. But one can ask about points of various orders.
2. It turns out that E[p] is isomorphic to either $\mathbb{Z}/p\mathbb{Z}$ or trivial.

Elliptic curves over finite fields

1. Because in this case the group is finite, every point has finite order. But one can ask about points of various orders.
2. It turns out that E[p] is isomorphic to either $\mathbb{Z}/p\mathbb{Z}$ or trivial.
3. If r is prime different from p, then E[r] is isomorphic to either trivial or $\frac{\mathbb{Z}}{r\mathbb{Z}}$ or $\frac{\mathbb{Z}}{r\mathbb{Z}} x \frac{\mathbb{Z}}{r\mathbb{Z}}$

Elliptic curves over finite fields

1. Because in this case the group is finite, every point has finite order. But one can ask about points of various orders.
2. It turns out that E[p] is isomorphic to either $\mathbb{Z}/p\mathbb{Z}$ or trivial.
3. If r is prime different from p, then E[r] is isomorphic to either trivial or $\frac{\mathbb{Z}}{r\mathbb{Z}}$ or $\frac{\mathbb{Z}}{r\mathbb{Z}} x \frac{\mathbb{Z}}{r\mathbb{Z}}$
4. Why elliptic curves over finite fields?
    1. Elliptic curves over $\mathbb{F}_q$ are used in Elliptic Curve Cryptography (ECC).
    2. Certain algorithms (e.g. factorization algorithm) in computational number theory uses Elliptic curves properties

Summary

1. Saw why group law on elliptic curves exist.
2. Determined points of finite order on complex elliptic curves
3. Determined points of finite order on real elliptic curves
4. Saw elliptic curves over finite field and their importance in real world problems
5. Determined points of finite order on elliptic curves over finite field
6. - References:
    1. Introduction to elliptic curves and modular forms, Koblitz
    2. Rational points on elliptic curves, Silverman and Tate

Thank You!