Elliptic Curves over Finite Fields

Steven Jin
Advisor: Professor Lawrence Washington

Directed Reading Program Talks
University of Maryland
December 5, 2019

What is an Elliptic Curve?

Definition

Let k (char $k \neq 2, 3$) be a field. An **elliptic curve** E over k is a curve defined by a polynomial of the form $y^2 = x^3 + ax + b$ with coefficients $a, b \in k$, appended with a "point at infinity." Formally, an **elliptic curve** E over k is a nonsingular, projective algebraic curve of genus 1 with points lying in $\mathbb{P}^2_k$.

What is an Elliptic Curve?

Definition

Let k (char $k \neq 2, 3$) be a field. An **elliptic curve** E over k is a curve defined by a polynomial of the form $y^2 = x^3 + ax + b$ with coefficients $a, b \in k$, appended with a "point at infinity." Formally, an **elliptic curve** E over k is a nonsingular, projective algebraic curve of genus 1 with points lying in $\mathbb{P}^2_k$.

Definition

The set of k**-rational points** of an elliptic curve E is denoted $E(k)$.

What is an Elliptic Curve?

Definition

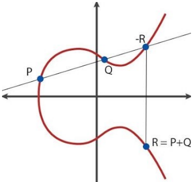
Let k (char $k \neq 2, 3$) be a field. An **elliptic curve** E over k is a curve defined by a polynomial of the form $y^2 = x^3 + ax + b$ with coefficients $a, b \in k$, appended with a "point at infinity." Formally, an **elliptic curve** E over k is a nonsingular, projective algebraic curve of genus 1 with points lying in $\mathbb{P}^2_k$.

Definition

The set of k**-rational points** of an elliptic curve E is denoted $E(k)$.

Remark

The points on an elliptic curve form a group.



Let $\mathbb{F}_q$ be the field of $q = p^s$ elements. Henceforth let E be an elliptic curve over $\mathbb{F}_q$.

Let $\mathbb{F}_q$ be the field of $q = p^s$ elements. Henceforth let E be an elliptic curve over $\mathbb{F}_q$.

Theorem 1

$E \cong \mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/L\mathbb{Z}$ for unique $L, M \in \mathbb{Z}$ where $L \mid M$.

Let $\mathbb{F}_q$ be the field of $q = p^s$ elements. Henceforth let E be an elliptic curve over $\mathbb{F}_q$.

Theorem 1

$E \cong \mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/L\mathbb{Z}$ for unique $L, M \in \mathbb{Z}$ where $L \mid M$.

Definition

The **order** of E is the number of elements in the group; this is $N = LM$ in the above notation. The integer M is the **group exponent**, which is the largest order of an element in the group.

Remark

Since $\mathbb{F}_q$ is a finite field, the set $E(\mathbb{F}_q)$ can be determined by iterating through all elements of $\mathbb{F}_q$ and seeing which ones satisfy the defining polynomial. (We must also remember to include the point at infinity.) This allows us to compute the group order. In practice, this might not be realistic.

Number of Points on E

Remark

Since $\mathbb{F}_q$ is a finite field, the set $E(\mathbb{F}_q)$ can be determined by iterating through all elements of $\mathbb{F}_q$ and seeing which ones satisfy the defining polynomial. (We must also remember to include the point at infinity.) This allows us to compute the group order. In practice, this might not be realistic.

Theorem 2 (Hasse)

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

Number of Points on E

Remark

Since $\mathbb{F}_q$ is a finite field, the set $E(\mathbb{F}_q)$ can be determined by iterating through all elements of $\mathbb{F}_q$ and seeing which ones satisfy the defining polynomial. (We must also remember to include the point at infinity.) This allows us to compute the group order. In practice, this might not be realistic.

Theorem 2 (Hasse)

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

Theorem 3

Let $\#E(\mathbb{F}_q) = q + 1 - a$. Write $x^2 - ax + q = (x - \alpha)(x - \beta)$. Then

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

for all $n \geq 1$.

Group Structure

Definition

Let E be an elliptic curve over k. Then $E[n] \subset E(\overline{k})$ is the kernel of the map that takes point P to $P + P + \cdots + P$ (n times).

Group Structure

Definition

Let E be an elliptic curve over k. Then $E[n] \subset E(\overline{k})$ is the kernel of the map that takes point P to $P + P + \cdots + P$ (n times).

Theorem 4

Let $\mu_n := \{x \in \overline{k} \mid x^n = 1\}$. If $E[n] \subset E(k)$, then $\mu_n \subset k$.

Group Structure

Definition

Let E be an elliptic curve over k. Then $E[n] \subset E(\overline{k})$ is the kernel of the map that takes point P to $P + P + \cdots + P$ (n times).

Theorem 4

Let $\mu_n := \{x \in \overline{k} \mid x^n = 1\}$. If $E[n] \subset E(k)$, then $\mu_n \subset k$.

Theorem 5

If char $k = p > 0$ and $p \mid n$, write $n = p^r n'$ with $p \nmid n'$. Then

$$E[n] \cong \mathbb{Z}/n'\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z}.$$

Group Structure

Definition

Let E be an elliptic curve over k. Then $E[n] \subset E(\overline{k})$ is the kernel of the map that takes point P to $P + P + \cdots + P$ (n times).

Theorem 4

Let $\mu_n := \{x \in \overline{k} \mid x^n = 1\}$. If $E[n] \subset E(k)$, then $\mu_n \subset k$.

Theorem 5

If char $k = p > 0$ and $p \mid n$, write $n = p^r n'$ with $p \nmid n'$. Then

$$E[n] \cong \mathbb{Z}/n'\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z}.$$

Theorem 6

Suppose

$$E(\mathbb{F}_q) \cong \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Then either $q = n^2 + 1$ or $q = n^2 \pm n + 1$ or $q = (n \pm 1)^2$.

Proof of Theorem 6

Proof.

Proof of Theorem 6

Proof.

By applying the Hasse bound, we have $n^2 = q + 1 - a$, where $|a| \leq 2\sqrt{q}$.

Proof of Theorem 6

Proof.

By applying the Hasse bound, we have $n^2 = q + 1 - a$, where $|a| \leq 2\sqrt{q}$.

Lemma

$a \equiv 2 \pmod{n}$.

Proof.

By applying the Hasse bound, we have $n^2 = q + 1 - a$, where $|a| \leq 2\sqrt{q}$.

Lemma

$a \equiv 2 \pmod{n}$.

Proof of Lemma.

Proof.

By applying the Hasse bound, we have $n^2 = q + 1 - a$, where $|a| \leq 2\sqrt{q}$.

Lemma

$a \equiv 2 \pmod{n}$.

Proof of Lemma.

Recall char $\mathbb{F}_q = p$.

Proof of Theorem 6

Proof.

By applying the Hasse bound, we have $n^2 = q + 1 - a$, where $|a| \leq 2\sqrt{q}$.

Lemma

$a \equiv 2 \pmod{n}$.

Proof of Lemma.

Recall $\operatorname{char} \mathbb{F}_q = p$.

If $p \mid n$, then there are p^2 points in $E[n]$.

Proof of Theorem 6

Proof.

By applying the Hasse bound, we have $n^2 = q + 1 - a$, where $|a| \leq 2\sqrt{q}$.

Lemma

$a \equiv 2 \pmod{n}$.

Proof of Lemma.

Recall $\operatorname{char} \mathbb{F}_q = p$.

If $p \mid n$, then there are p^2 points in $E[n]$.

This contradicts Theorem 5. Hence $p \nmid n$.

Proof of Theorem 6

Proof.

By applying the Hasse bound, we have $n^2 = q + 1 - a$, where $|a| \leq 2\sqrt{q}$.

Lemma

$a \equiv 2 \pmod{n}$.

Proof of Lemma.

Recall char $\mathbb{F}_q = p$.

If $p \mid n$, then there are p^2 points in $E[n]$.

This contradicts Theorem 5. Hence $p \nmid n$.

Since $E[n] \subset E(\mathbb{F}_q)$, by Theorem 4 we know that the nth roots of unity are in $\mathbb{F}_q$.

Proof.

By applying the Hasse bound, we have $n^2 = q + 1 - a$, where $|a| \leq 2\sqrt{q}$.

Lemma

$a \equiv 2 \pmod{n}$.

Proof of Lemma.

Recall char $\mathbb{F}_q = p$.

If $p \mid n$, then there are p^2 points in $E[n]$.

This contradicts Theorem 5. Hence $p \nmid n$.

Since $E[n] \subset E(\mathbb{F}_q)$, by Theorem 4 we know that the nth roots of unity are in $\mathbb{F}_q$.

So we conclude that $q - 1$ is a multiple of n.

Proof.

By applying the Hasse bound, we have $n^2 = q + 1 - a$, where $|a| \leq 2\sqrt{q}$.

Lemma

$a \equiv 2 \pmod{n}$.

Proof of Lemma.

Recall char $\mathbb{F}_q = p$.

If $p \mid n$, then there are p^2 points in $E[n]$.

This contradicts Theorem 5. Hence $p \nmid n$.

Since $E[n] \subset E(\mathbb{F}_q)$, by Theorem 4 we know that the nth roots of unity are in $\mathbb{F}_q$.

So we conclude that $q - 1$ is a multiple of n.

Therefore, $a = q + 1 - n^2 \equiv 2 \pmod{n}$. $\square$

Proof of Theorem 6 (cont.)

Write $a = 2 + kn$. Then substituting this into $n^2 = q + 1 - a$, we have

$$q = n^2 + kn + 1.$$

Write $a = 2 + kn$. Then substituting this into $n^2 = q + 1 - a$, we have

$$q = n^2 + kn + 1.$$

By the Hasse bound,

$$|2 + kn| \leq 2\sqrt{q}.$$

Write $a = 2 + kn$. Then substituting this into $n^2 = q + 1 - a$, we have

$$q = n^2 + kn + 1.$$

By the Hasse bound,

$$|2 + kn| \leq 2\sqrt{q}.$$

After squaring, we obtain

$$4 + 4kn + k^2n^2 \leq 4q = 4(n^2 + kn + 1).$$

Proof of Theorem 6 (cont.)

Write $a = 2 + kn$. Then substituting this into $n^2 = q + 1 - a$, we have

$$q = n^2 + kn + 1.$$

By the Hasse bound,

$$|2 + kn| \leq 2\sqrt{q}.$$

After squaring, we obtain

$$4 + 4kn + k^2n^2 \leq 4q = 4(n^2 + kn + 1).$$

After subtracting, we see that $|k| \leq 2$.

Proof of Theorem 6 (cont.)

Write $a = 2 + kn$. Then substituting this into $n^2 = q + 1 - a$, we have

$$q = n^2 + kn + 1.$$

By the Hasse bound,

$$|2 + kn| \leq 2\sqrt{q}.$$

After squaring, we obtain

$$4 + 4kn + k^2n^2 \leq 4q = 4(n^2 + kn + 1).$$

After subtracting, we see that $|k| \leq 2$.

The possibilities $k = 0, \pm 1, \pm 2$ precisely give us the values of q in our claim.

How Balanced Can $E(\mathbb{F}_q)$ be?

Question

So we have shown that the case of $E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ is very rare. When $E(\mathbb{F}_q)$ is an unbalanced direct sum, what can we say?

How Balanced Can $E(\mathbb{F}_q)$ be?

Question

So we have shown that the case of $E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ is very rare. When $E(\mathbb{F}_q)$ is an unbalanced direct sum, what can we say?

Theorem 7

Suppose $E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$. Then $q = mn^2 + kn + 1$ for some integer k.

How Balanced Can $E(\mathbb{F}_q)$ be?

Question

So we have shown that the case of $E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ is very rare. When $E(\mathbb{F}_q)$ is an unbalanced direct sum, what can we say?

Theorem 7

Suppose $E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$. Then $q = mn^2 + kn + 1$ for some integer k.

Theorem 8

For most values of q, an elliptic curve over $\mathbb{F}_q$ has a point of order greater than $4\sqrt{q}$.

How Balanced Can $E(\mathbb{F}_q)$ be?

Question

So we have shown that the case of $E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ is very rare. When $E(\mathbb{F}_q)$ is an unbalanced direct sum, what can we say?

Theorem 7

Suppose $E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$. Then $q = mn^2 + kn + 1$ for some integer k.

Theorem 8

For most values of q, an elliptic curve over $\mathbb{F}_q$ has a point of order greater than $4\sqrt{q}$.

Remark

This shows that in general, $E(\mathbb{F}_q)$ is substantially unbalanced. In particular, $E(\mathbb{F}_q)$ is "almost cyclic."

References

[1] Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves*. New York, NY: Springer New York.

[2] Washington, L. C. (2008). *Elliptic Curves: Number Theory and Cryptography*. Boca Raton, FL: Chapman & Hall/CRC.