Elliptic Curves Over Finite Fields

Jonathan Yu

July 14, 2025

Introduction

Motivating Question

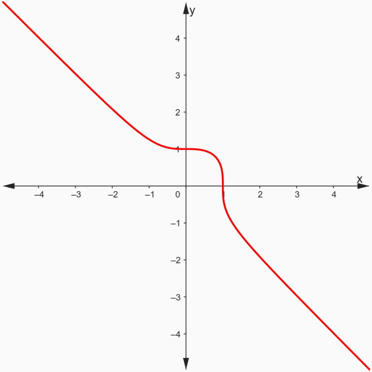
Problem

Consider the curve $x^3 + y^3 = 1$. *What points with rational coordinates lie on this curve?*

Motivating Question

Problem

Consider the curve $x^3 + y^3 = 1$. *What points with rational coordinates lie on this curve?*



$x^3 + y^3 = 1$

Fermat's Last Theorem

"It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."

> *"It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."*

Theorem (Fermat's last theorem)

For any integer $n > 2$, there are no positive integer solutions to the equation

$$a^n + b^n = c^n.$$

Corollary

For any integer $n > 2$, there are no nonzero integer solutions to the equation

$$a^n + b^n = c^n.$$

Corollary

For any integer $n > 2$, there are no nonzero integer solutions to the equation

$$a^n + b^n = c^n.$$

Corollary

For any integer $n > 2$, there are no rational solutions to the equation

$$x^n + y^n = 1$$

if both x and y are nonzero.

Fermat's Last Theorem

Corollary

For any integer $n > 2$, there are no nonzero integer solutions to the equation

$$a^n + b^n = c^n.$$

Corollary

For any integer $n > 2$, there are no rational solutions to the equation

$$x^n + y^n = 1$$

if both x and y are nonzero.

- Only rational points on $x^3 + y^3 = 1$: $(0, 1), (1, 0)$

Preliminaries

Definition (Characteristic)

The **characteristic** of a field K is the smallest positive integer n such that $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$. If no such n exists, the characteristic is defined to be 0.

Definition (Characteristic)

The **characteristic** of a field K is the smallest positive integer n such that $\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$. If no such n exists, the characteristic is defined to be 0.

Example

- Set of integers modulo prime p: $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$

Definition (Characteristic)

The **characteristic** of a field K is the smallest positive integer n such that $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$. If no such n exists, the characteristic is defined to be 0.

Example

- Set of integers modulo prime p: $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$
- Finite field with characteristic p

Characteristic

Definition (Characteristic)

The **characteristic** of a field K is the smallest positive integer n such that $\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$. If no such n exists, the characteristic is defined to be 0.

Example

- Set of integers modulo prime p: $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$
- Finite field with characteristic p
    - Finite number of elements

Characteristic

Definition (Characteristic)

The **characteristic** of a field K is the smallest positive integer n such that $\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$. If no such n exists, the characteristic is defined to be 0.

Example

- Set of integers modulo prime p: $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$
- Finite field with characteristic p
  - Finite number of elements
  - Smallest positive integer such that $\underbrace{1+1+\cdots+1}_{p \text{ times}} \equiv 0 \pmod{p}$ is p

Endomorphism

Definition (Endomorphism)

An **endomorphism** is a homomorphism between an algebraic object and itself.

Endomorphism

Definition (Endomorphism)

An **endomorphism** is a homomorphism between an algebraic object and itself.

Example

- Let $\mathbb{F}_p$ be field of characteristic p for some prime p

Definition (Endomorphism)

An **endomorphism** is a homomorphism between an algebraic object and itself.

Example

- Let $\mathbb{F}_p$ be field of characteristic p for some prime p
- $\varphi\colon \mathbb{F}_p \to \mathbb{F}_p$ defined by $\varphi(x) = x^p$ is endomorphism

Endomorphism

Definition (Endomorphism)

An **endomorphism** is a homomorphism between an algebraic object and itself.

Example

- Let $\mathbb{F}_p$ be field of characteristic p for some prime p
- $\varphi\colon \mathbb{F}_p \to \mathbb{F}_p$ defined by $\varphi(x) = x^p$ is endomorphism
  - Fermat's little theorem: $a^{p-1} \equiv 1 \pmod{p} \implies a^p \equiv a \pmod{p}$

Endomorphism

Definition (Endomorphism)

An **endomorphism** is a homomorphism between an algebraic object and itself.

Example

- Let $\mathbb{F}_p$ be field of characteristic p for some prime p
- $\varphi\colon \mathbb{F}_p \to \mathbb{F}_p$ defined by $\varphi(x) = x^p$ is endomorphism
  - Fermat's little theorem: $a^{p-1} \equiv 1 \pmod{p} \implies a^p \equiv a \pmod{p}$
  - $\varphi(x) = x$

Endomorphism

Definition (Endomorphism)

An **endomorphism** is a homomorphism between an algebraic object and itself.

Example

- Let $\mathbb{F}_p$ be field of characteristic p for some prime p
- $\varphi\colon \mathbb{F}_p \to \mathbb{F}_p$ defined by $\varphi(x) = x^p$ is endomorphism
  - Fermat's little theorem: $a^{p-1} \equiv 1 \pmod{p} \implies a^p \equiv a \pmod{p}$
  - $\varphi(x) = x$
- **Frobenius endomorphism**

Definition

An algebraic object is said to be **defined over** a field K if its coefficients lie in K.

Definition

An algebraic object is said to be **defined over** a field K if its coefficients lie in K.

Definition (K-rational points)

The set of points on a curve C with coordinates in a field K, denoted $C(K)$, is known as the K**-rational points**.

Curves Over Fields

Definition

An algebraic object is said to be **defined over** a field K if its coefficients lie in K.

Definition (K-rational points)

The set of points on a curve C with coordinates in a field K, denoted $C(K)$, is known as the K-**rational points**.

Example

- Let L be the line $y - x = 0$

Definition

An algebraic object is said to be **defined over** a field K if its coefficients lie in K.

Definition (K-rational points)

The set of points on a curve C with coordinates in a field K, denoted $C(K)$, is known as the K-**rational points**.

Example

- Let L be the line $y - x = 0$
- Defined over $\mathbb{Q}$, since coefficients $1, -1 \in \mathbb{Q}$

Definition

An algebraic object is said to be **defined over** a field K if its coefficients lie in K.

Definition (K-rational points)

The set of points on a curve C with coordinates in a field K, denoted $C(K)$, is known as the K**-rational points**.

Example

- Let L be the line $y - x = 0$
- Defined over $\mathbb{Q}$, since coefficients $1, -1 \in \mathbb{Q}$
- Set of $\mathbb{Q}$-rational points: $L(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y - x = 0\}$

Definition (General Weierstrass Equation)

A **general Weierstrass equation** over a field K is

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

where $a_1, a_2, a_3, a_4, a_6 \in K$.

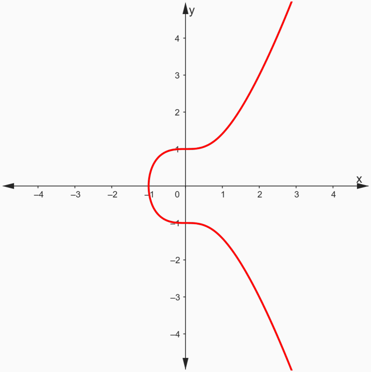
General Weierstrass Equations

Example

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

Example

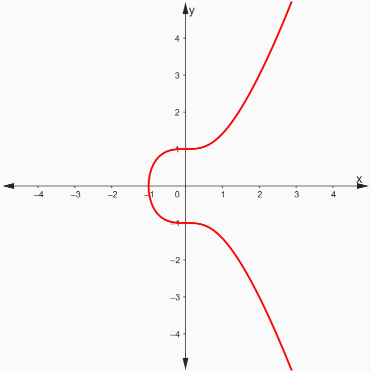
- $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$



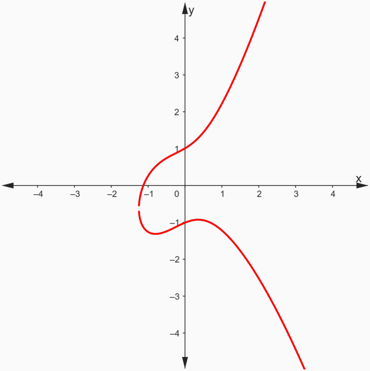
$y^2 = x^3 + 1$

Example

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



$y^2 = x^3 + 1$



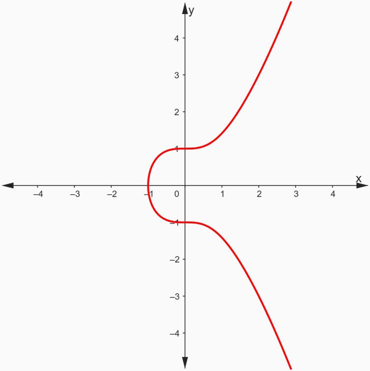
$y^2 - xy = x^3 + \frac{1}{2}x^2 + \frac{3}{16}x + \frac{65}{64}$

Definition (Elliptic Curve)

If E is the set of solutions to a general Weierstrass equation and the discriminant $\Delta \neq 0$, we call E an **elliptic curve**.

Definition (Elliptic Curve)

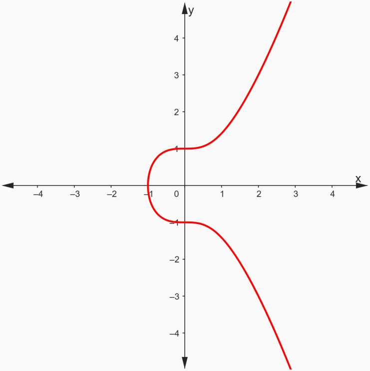
If E is the set of solutions to a general Weierstrass equation and the discriminant $\Delta \neq 0$, we call E an **elliptic curve**.



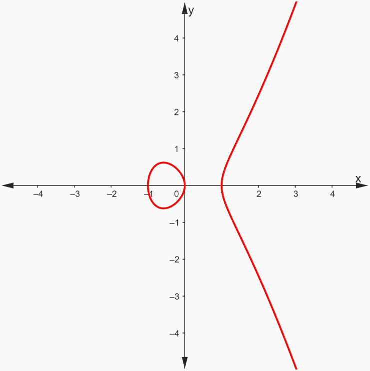
$y^2 = x^3 + 1$

Definition (Elliptic Curve)

If E is the set of solutions to a general Weierstrass equation and the discriminant $\Delta \neq 0$, we call E an **elliptic curve**.



$y^2 = x^3 + 1$



$y^2 = x^3 - x$

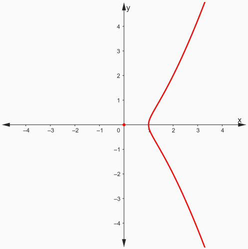
Singular Weierstrass Curves

Definition (Singular Weistrass Curve)

If E is the set of solutions to a general Weierstrass equation and the discriminant $\Delta = 0$, we call E a **singular Weierstrass curve**.

Definition (Singular Weistrass Curve)

If E is the set of solutions to a general Weierstrass equation and the discriminant $\Delta = 0$, we call E a **singular Weierstrass curve**.

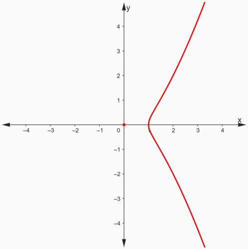


$y^2 = x^3 - x^2$

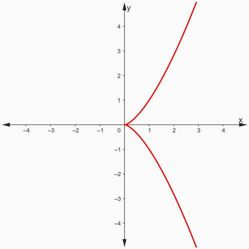
Singular Weierstrass Curves

Definition (Singular Weistrass Curve)

If E is the set of solutions to a general Weierstrass equation and the discriminant $\Delta = 0$, we call E a **singular Weierstrass curve**.



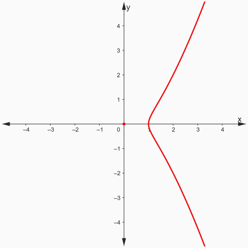
$y^2 = x^3 - x^2$



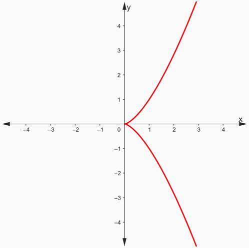
$y^2 = x^3$

Definition (Singular Weistrass Curve)

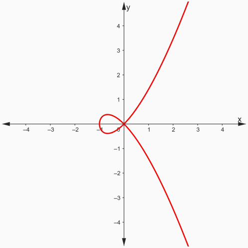
If E is the set of solutions to a general Weierstrass equation and the discriminant $\Delta = 0$, we call E a **singular Weierstrass curve**.



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



$y^2 = x^3$



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

Short Weierstrass Equation

Proposition

If E is a general Weierstrass equation defined over a field K of characteristic not 2 or 3, then it can be written in the form

$$y^2 = x^3 + ax + b.$$

This is known as a ***short Weierstrass equation****.*

Proposition

If E is a general Weierstrass equation defined over a field K of characteristic not 2 or 3, then it can be written in the form

$$y^2 = x^3 + ax + b.$$

This is known as a ***short Weierstrass equation****.*

Proof.

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

Short Weierstrass Equation

Proposition

If E is a general Weierstrass equation defined over a field K of characteristic not 2 or 3, then it can be written in the form

$$y^2 = x^3 + ax + b.$$

This is known as a ***short Weierstrass equation****.*

Proof.

- $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
- Let $y = y' - \dfrac{a_1x + a_3}{2}$ (valid for characteristic not 2)

Short Weierstrass Equation

Proposition

If E is a general Weierstrass equation defined over a field K of characteristic not 2 or 3, then it can be written in the form

$$y^2 = x^3 + ax + b.$$

This is known as a ***short Weierstrass equation****.*

Proof.

- $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
- Let $y = y' - \dfrac{a_1x + a_3}{2}$ (valid for characteristic not 2)
- $y'^2 = x^3 + a_2'x^2 + a_4'x + a_6'$

Short Weierstrass Equation

Proposition

If E is a general Weierstrass equation defined over a field K of characteristic not 2 or 3, then it can be written in the form

$$y^2 = x^3 + ax + b.$$

This is known as a ***short Weierstrass equation****.*

Proof.

- $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
- Let $y = y' - \dfrac{a_1x + a_3}{2}$ (valid for characteristic not 2)
- $y'^2 = x^3 + a_2'x^2 + a_4'x + a_6'$
- Let $x = x' - \dfrac{a_2'}{3}$ (valid for characteristic not 3)

Proposition

If E is a general Weierstrass equation defined over a field K of characteristic not 2 or 3, then it can be written in the form

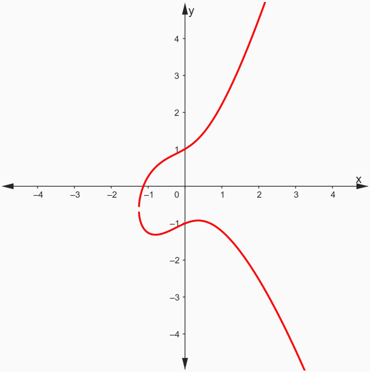
$$y^2 = x^3 + ax + b.$$

This is known as a ***short Weierstrass equation****.*

Proof.

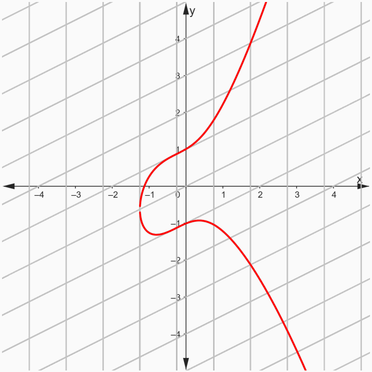
- $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
- Let $y = y' - \frac{a_1x + a_3}{2}$ (valid for characteristic not 2)
- $y'^2 = x^3 + a_2'x^2 + a_4'x + a_6'$
- Let $x = x' - \frac{a_2'}{3}$ (valid for characteristic not 3)
- $y'^2 = x'^3 + ax' + b$ □

Example



$$y^2 - xy = x^3 + \frac{1}{2}x^2 + \frac{3}{16}x + \frac{65}{64}$$

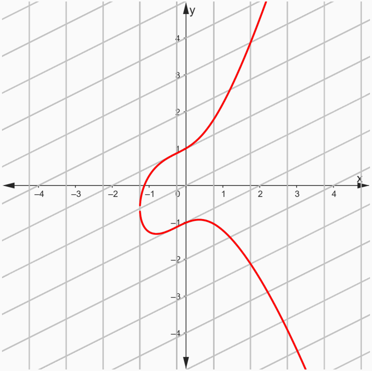
Example



$$y^2 - xy = x^3 + \frac{1}{2}x^2 + \frac{3}{16}x + \frac{65}{64}$$

Short Weierstrass Equation

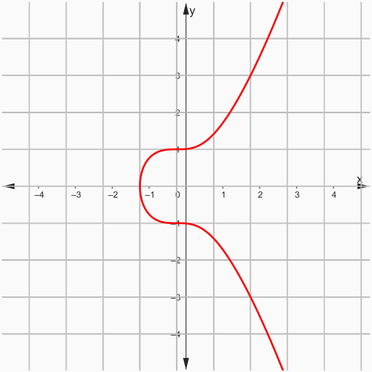
Example



$$y^2 - xy = x^3 + \frac{1}{2}x^2 + \frac{3}{16}x + \frac{65}{64}$$

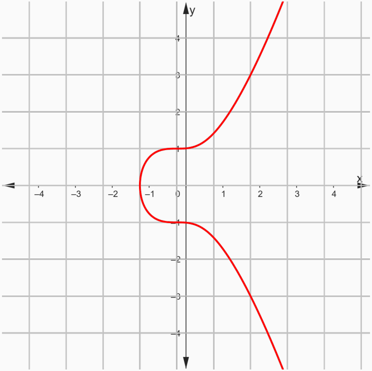
- $y = y' + \frac{1}{2}x$

Example



$$y^2 = x^3 + \frac{3}{4}x^2 + \frac{3}{16}x + \frac{65}{64}$$

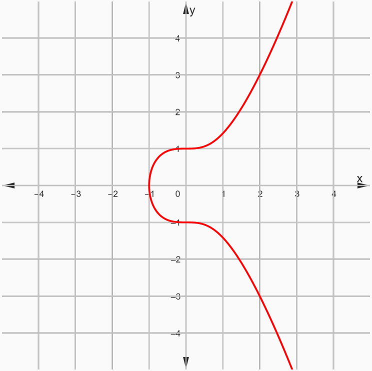
Example



$$y^2 = x^3 + \frac{3}{4}x^2 + \frac{3}{16}x + \frac{65}{64}$$

- $x = x' - \frac{1}{4}$

Example



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

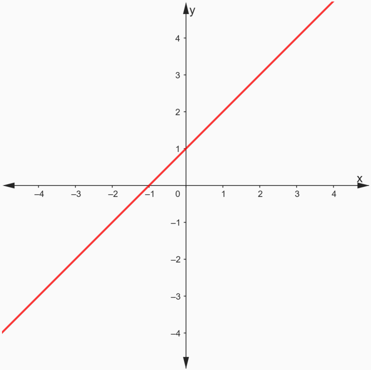
Rational Points on Curves

Proposition

The rational points on the rational line $ax + by + c = 0$ *are given by* $\left(t, -\frac{a}{b}t - \frac{c}{b}\right)$ *if* $b \neq 0$ *and* $\left(-\frac{c}{a}, t\right)$ *if* $b = 0$.

Proposition

The rational points on the rational line $ax + by + c = 0$ *are given by* $\left(t, -\frac{a}{b}t - \frac{c}{b}\right)$ *if* $b \neq 0$ *and* $\left(-\frac{c}{a}, t\right)$ *if* $b = 0$.



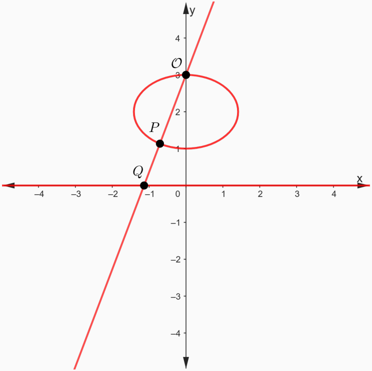
Rational Points on Conics

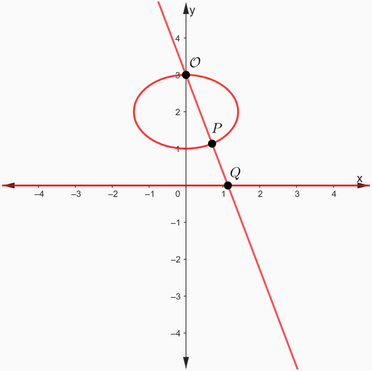
Proposition

There is a one-to-one correspondence between the points on a rational line and a rational conic.

Proposition

There is a one-to-one correspondence between the points on a rational line and a rational conic.





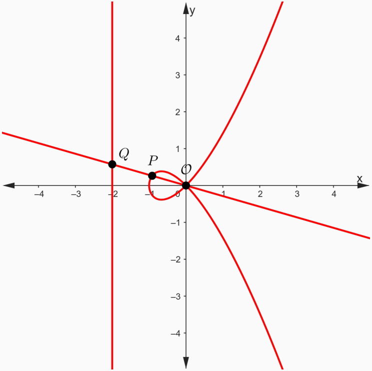
Rational Points on Singular Weierstrass Curves

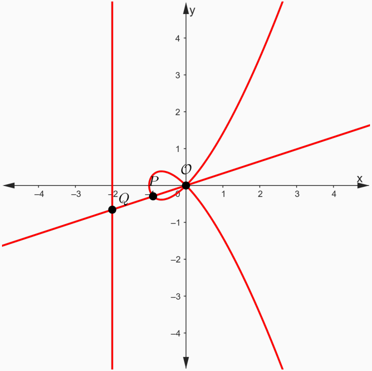
Proposition

There is a one-to-one correspondence between the points on a rational line and a singular Weierstrass curve except at the singular point.

Proposition

There is a one-to-one correspondence between the points on a rational line and a singular Weierstrass curve except at the singular point.





Geometry of Elliptic Curves

Adding Two Points

- Let $\mathcal{O}, P, Q$ be on elliptic curve for fixed $\mathcal{O}$

Adding Two Points

- Let $\mathcal{O}, P, Q$ be on elliptic curve for fixed $\mathcal{O}$
- Construct $\overleftrightarrow{PQ}$

Adding Two Points

- Let $\mathcal{O}, P, Q$ be on elliptic curve for fixed $\mathcal{O}$
- Construct $\overleftrightarrow{PQ}$
- This will intersect elliptic curve at a third point: $P * Q$

Adding Two Points

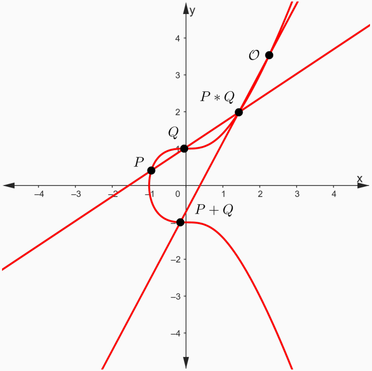
- Let $\mathcal{O}, P, Q$ be on elliptic curve for fixed $\mathcal{O}$
- Construct $\overleftrightarrow{PQ}$
- This will intersect elliptic curve at a third point: $P * Q$
- Construct $\overleftrightarrow{\mathcal{O}(P * Q)}$

Adding Two Points

- Let $\mathcal{O}, P, Q$ be on elliptic curve for fixed $\mathcal{O}$
- Construct $\overleftrightarrow{PQ}$
- This will intersect elliptic curve at a third point: $P * Q$
- Construct $\overleftrightarrow{\mathcal{O}(P * Q)}$
- This will intersect elliptic curve at a third point: $P + Q$

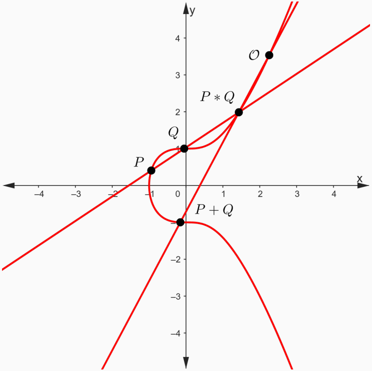
Adding Two Points

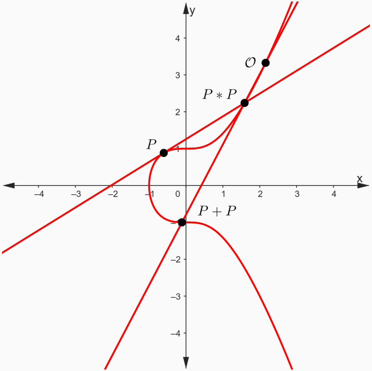
- Let $\mathcal{O}, P, Q$ be on elliptic curve for fixed $\mathcal{O}$
- Construct $\overleftrightarrow{PQ}$
- This will intersect elliptic curve at a third point: $P * Q$
- Construct $\overleftrightarrow{\mathcal{O}(P * Q)}$
- This will intersect elliptic curve at a third point: $P + Q$



Adding Two Points

- Let $\mathcal{O}, P, Q$ be on elliptic curve for fixed $\mathcal{O}$
- Construct $\overleftrightarrow{PQ}$
- This will intersect elliptic curve at a third point: $P * Q$
- Construct $\overleftrightarrow{\mathcal{O}(P * Q)}$
- This will intersect elliptic curve at a third point: $P + Q$



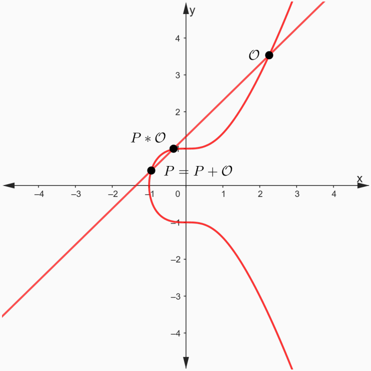


Proposition

Adding points forms an Abelian group with identity $\mathcal{O}$.

Proposition

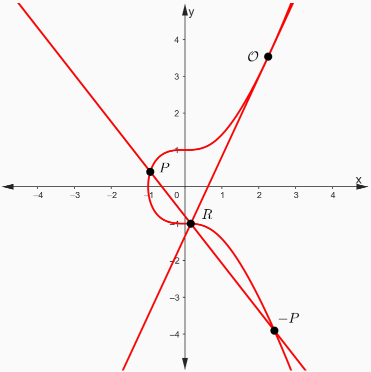
Adding points forms an Abelian group with identity $\mathcal{O}$.



Identity Element

Proposition

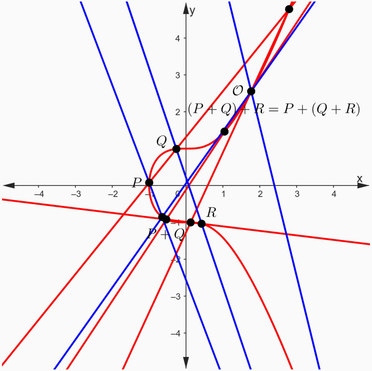
Adding points forms an Abelian group with identity $\mathcal{O}$.



Inverse Element

Proposition

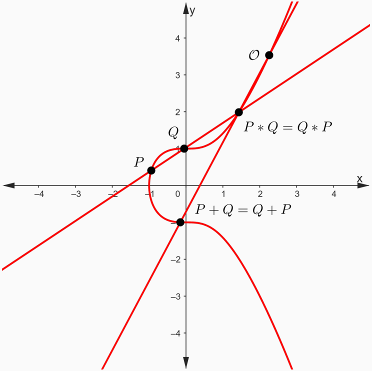
Adding points forms an Abelian group with identity $\mathcal{O}$.



Associative Property

Proposition

Adding points forms an Abelian group with identity $\mathcal{O}$.



Commutative Property

Hasse’s Theorem

Hasse's Theorem

Theorem (Hasse's theorem)

Let E be an elliptic curve and $\mathbb{F}_q$ a finite field of order $q = p^n$ for some prime p and positive integer n. Then

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

- Bounds number of points on elliptic curve

Hasse's Theorem

Theorem (Hasse's theorem)

Let E be an elliptic curve and $\mathbb{F}_q$ a finite field of order $q = p^n$ for some prime p and positive integer n. Then

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

- Bounds number of points on elliptic curve
- Expected number of $\mathbb{F}_q$-rational points is close to $q+1$

Hasse's Theorem

Theorem (Hasse's theorem)

Let E be an elliptic curve and $\mathbb{F}_q$ a finite field of order $q = p^n$ for some prime p and positive integer n. Then

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

- Bounds number of points on elliptic curve
- Expected number of $\mathbb{F}_q$-rational points is close to $q + 1$
- The $+1$ is because of point at infinity

Hasse's Theorem

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

Hasse's Theorem

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

Example

- $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$

Hasse's Theorem

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

Example

- $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$

x	$x^3 + x + 1 \pmod 5$	y	$\#$ of y
0	$0^3 + 0 + 1 = 1$	1, 4	2
1	$1^3 + 1 + 1 = 3$	none	0
2	$2^3 + 2 + 1 = 11 \equiv 1$	1, 4	2
3	$3^3 + 3 + 1 = 31 \equiv 1$	1, 4	2
4	$4^3 + 4 + 1 = 69 \equiv 4$	2, 3	2

Hasse's Theorem

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

Example

- $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$

x	$x^3 + x + 1 \pmod 5$	y	# of y
0	$0^3 + 0 + 1 = 1$	$1, 4$	2
1	$1^3 + 1 + 1 = 3$	none	0
2	$2^3 + 2 + 1 = 11 \equiv 1$	$1, 4$	2
3	$3^3 + 3 + 1 = 31 \equiv 1$	$1, 4$	2
4	$4^3 + 4 + 1 = 69 \equiv 4$	$2, 3$	2

- $\#E(\mathbb{F}_5) = 2 + 0 + 2 + 2 + 2 + 1 = 9$ distinct points, including point at infinity

Hasse's Theorem

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

Example

- $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$

x	$x^3 + x + 1 \pmod 5$	y	# of y
0	$0^3 + 0 + 1 = 1$	$1, 4$	2
1	$1^3 + 1 + 1 = 3$	none	0
2	$2^3 + 2 + 1 = 11 \equiv 1$	$1, 4$	2
3	$3^3 + 3 + 1 = 31 \equiv 1$	$1, 4$	2
4	$4^3 + 4 + 1 = 69 \equiv 4$	$2, 3$	2

- $\#E(\mathbb{F}_5) = 2 + 0 + 2 + 2 + 2 + 1 = 9$ distinct points, including point at infinity
- $|9 - (5+1)| = 3 \leq 2\sqrt{5}$

Proof.

- Consider Frobenius endomorphism: $\varphi_q : E \to E$, where $\varphi_q(x, y) = (x^q, y^q)$ and $\varphi(\mathcal{O}) = \mathcal{O}$, where $\mathcal{O}$ is point at infinity

Proof.

- Consider Frobenius endomorphism: $\varphi_q \colon E \to E$, where $\varphi_q(x, y) = (x^q, y^q)$ and $\varphi(\mathcal{O}) = \mathcal{O}$, where $\mathcal{O}$ is point at infinity
- $E(\mathbb{F}_q) = \ker(\varphi_q - 1)$

Proof.

- Consider Frobenius endomorphism: $\varphi_q \colon E \to E$, where $\varphi_q(x, y) = (x^q, y^q)$ and $\varphi(\mathcal{O}) = \mathcal{O}$, where $\mathcal{O}$ is point at infinity
- $E(\mathbb{F}_q) = \ker(\varphi_q - 1)$
- $\#E(\mathbb{F}_q) = \#\ker(\varphi_q - 1) = \deg(\varphi_q - 1)$

Hasse's Theorem

Proof.

- Consider Frobenius endomorphism: $\varphi_q : E \to E$, where $\varphi_q(x, y) = (x^q, y^q)$ and $\varphi(\mathcal{O}) = \mathcal{O}$, where $\mathcal{O}$ is point at infinity
- $E(\mathbb{F}_q) = \ker(\varphi_q - 1)$
- $\#E(\mathbb{F}_q) = \# \ker(\varphi_q - 1) = \deg(\varphi_q - 1)$
- Let $a = \#E(\mathbb{F}_q) - (q + 1)$

Proof.

- Consider Frobenius endomorphism: $\varphi_q : E \to E$, where $\varphi_q(x, y) = (x^q, y^q)$ and $\varphi(\mathcal{O}) = \mathcal{O}$, where $\mathcal{O}$ is point at infinity
- $E(\mathbb{F}_q) = \ker(\varphi_q - 1)$
- $\#E(\mathbb{F}_q) = \# \ker(\varphi_q - 1) = \deg(\varphi_q - 1)$
- Let $a = \#E(\mathbb{F}_q) - (q + 1)$
- $\deg(r\varphi_q - s) = r^2 q + s^2 + rsa \geq 0$

Proof.

- Consider Frobenius endomorphism: $\varphi_q : E \to E$, where $\varphi_q(x, y) = (x^q, y^q)$ and $\varphi(\mathcal{O}) = \mathcal{O}$, where $\mathcal{O}$ is point at infinity
- $E(\mathbb{F}_q) = \ker(\varphi_q - 1)$
- $\#E(\mathbb{F}_q) = \# \ker(\varphi_q - 1) = \deg(\varphi_q - 1)$
- Let $a = \#E(\mathbb{F}_q) - (q + 1)$
- $\deg(r\varphi_q - s) = r^2 q + s^2 + rsa \geq 0$
- $\deg(x\varphi_q - 1) = qx^2 + ax + 1 \geq 0$

Proof.

- Consider Frobenius endomorphism: $\varphi_q : E \to E$, where $\varphi_q(x, y) = (x^q, y^q)$ and $\varphi(\mathcal{O}) = \mathcal{O}$, where $\mathcal{O}$ is point at infinity
- $E(\mathbb{F}_q) = \ker(\varphi_q - 1)$
- $\# E(\mathbb{F}_q) = \# \ker(\varphi_q - 1) = \deg(\varphi_q - 1)$
- Let $a = \# E(\mathbb{F}_q) - (q + 1)$
- $\deg(r\varphi_q - s) = r^2 q + s^2 + rsa \geq 0$
- $\deg(x\varphi_q - 1) = qx^2 + ax + 1 \geq 0$
- $a^2 - 4q \leq 0$

Proof.

- Consider Frobenius endomorphism: $\varphi_q : E \to E$, where $\varphi_q(x, y) = (x^q, y^q)$ and $\varphi(\mathcal{O}) = \mathcal{O}$, where $\mathcal{O}$ is point at infinity
- $E(\mathbb{F}_q) = \ker(\varphi_q - 1)$
- $\#E(\mathbb{F}_q) = \#\ker(\varphi_q - 1) = \deg(\varphi_q - 1)$
- Let $a = \#E(\mathbb{F}_q) - (q + 1)$
- $\deg(r\varphi_q - s) = r^2 q + s^2 + rsa \geq 0$
- $\deg(x\varphi_q - 1) = qx^2 + ax + 1 \geq 0$
- $a^2 - 4q \leq 0$
- $|a| \leq 2\sqrt{q}$ $\square$

Riemann Hypothesis for Elliptic Curves

Theorem

Let $a = \#E(\mathbb{F}_q) - (q+1)$. *Let* α *and* β *be the roots of the characteristic polynomial* $T^2 - aT + q = 0$. *Then* $|\alpha| = |\beta| = \sqrt{q}$.

Theorem

Let $a = \#E(\mathbb{F}_q) - (q + 1)$. Let α and β be the roots of the characteristic polynomial $T^2 - aT + q = 0$. Then $|\alpha| = |\beta| = \sqrt{q}$.

Proof.

- $|a| \leq 2\sqrt{q}$

Theorem

Let $a = \#E(\mathbb{F}_q) - (q+1)$. *Let* α *and* β *be the roots of the characteristic polynomial* $T^2 - aT + q = 0$. *Then* $|\alpha| = |\beta| = \sqrt{q}$.

Proof.

- $|a| \leq 2\sqrt{q}$
- Vieta's formulas: $\alpha + \beta = a$ and $\alpha\beta = q$

Theorem

Let $a = \#E(\mathbb{F}_q) - (q+1)$. *Let* α *and* β *be the roots of the characteristic polynomial* $T^2 - aT + q = 0$. *Then* $|\alpha| = |\beta| = \sqrt{q}$.

Proof.

- $|a| \leq 2\sqrt{q}$
- Vieta's formulas: $\alpha + \beta = a$ and $\alpha\beta = q$
- α and β complex conjugates

Theorem

Let $a = \#E(\mathbb{F}_q) - (q+1)$. *Let* α *and* β *be the roots of the characteristic polynomial* $T^2 - aT + q = 0$. *Then* $|\alpha| = |\beta| = \sqrt{q}$.

Proof.

- $|a| \leq 2\sqrt{q}$
- Vieta's formulas: $\alpha + \beta = a$ and $\alpha\beta = q$
- α and β complex conjugates
- Let $\alpha = re^{i\theta}$ and $\beta = re^{-i\theta}$

Riemann Hypothesis for Elliptic Curves

Theorem

Let $a = \#E(\mathbb{F}_q) - (q+1)$*. Let* α *and* β *be the roots of the characteristic polynomial* $T^2 - aT + q = 0$*. Then* $|\alpha| = |\beta| = \sqrt{q}$*.*

Proof.

- $|a| \leq 2\sqrt{q}$
- Vieta's formulas: $\alpha + \beta = a$ and $\alpha\beta = q$
- α and β complex conjugates
- Let $\alpha = re^{i\theta}$ and $\beta = re^{-i\theta}$
- $\alpha\beta = r^2 = q \implies r = \sqrt{q} \implies \alpha = \sqrt{q}e^{i\theta}, \beta = \sqrt{q}e^{-i\theta}$

Theorem

Let $a = \#E(\mathbb{F}_q) - (q+1)$. *Let* α *and* β *be the roots of the characteristic polynomial* $T^2 - aT + q = 0$. *Then* $|\alpha| = |\beta| = \sqrt{q}$.

Proof.

- $|a| \leq 2\sqrt{q}$
- Vieta's formulas: $\alpha + \beta = a$ and $\alpha\beta = q$
- α and β complex conjugates
- Let $\alpha = re^{i\theta}$ and $\beta = re^{-i\theta}$
- $\alpha\beta = r^2 = q \implies r = \sqrt{q} \implies \alpha = \sqrt{q}e^{i\theta}, \beta = \sqrt{q}e^{-i\theta}$
- $|\alpha| = |\sqrt{q}e^{-i\theta}| = |\sqrt{q}|, |\beta| = |\sqrt{q}e^{-i\theta}| = |\sqrt{q}|$ $\square$

Proposition

The Riemann hypothesis for elliptic curves implies Hasse’s theorem.

Proposition

The Riemann hypothesis for elliptic curves implies Hasse's theorem.

Proof.

- $a = \alpha + \beta$

Proposition

The Riemann hypothesis for elliptic curves implies Hasse's theorem.

Proof.

- $a = \alpha + \beta$
- $|a| = |\alpha + \beta| \leq |\alpha| + |\beta| = 2\sqrt{q}$

Proposition

The Riemann hypothesis for elliptic curves implies Hasse's theorem.

Proof.

- $a = \alpha + \beta$
- $|a| = |\alpha + \beta| \leq |\alpha| + |\beta| = 2\sqrt{q}$
- $|a| = |\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}$ $\square$