Elliptic Curves

Ellie Hamer, Isabela Souza Cefrin da Silva

Mentor: Faisal Al-Faisal

University of Waterloo, WiM Directed Reading Program

August 8, 2025

Overview

1. Elliptic Curves
   - What Is An Elliptic Curve?
   - Elliptic Curve Group
2. Fermat's Last Theorem
   - What Is The Connection Between Elliptic Curves and FLT?
   - Proving Fermat's Last Theorem

What Is An Elliptic Curve?

Definition (Elliptic Curve)

A **rational elliptic curve** is a curve defined by an equation $y^2 = f(x) = x^3 + ax^2 + bx + c$ where $f(x)$ is a cubic polynomial with no repeated roots, and $a, b, c \in \mathbb{Q}$.

What Is An Elliptic Curve?

Definition (Elliptic Curve)

A **rational elliptic curve** is a curve defined by an equation $y^2 = f(x) = x^3 + ax^2 + bx + c$ where $f(x)$ is a cubic polynomial with no repeated roots, and $a, b, c \in \mathbb{Q}$.

- After a change of variables we can write it as: $y^2 = x^3 + Ax + B$ (Weierstrass Form)

What Is An Elliptic Curve?

Definition (Elliptic Curve)

A **rational elliptic curve** is a curve defined by an equation $y^2 = f(x) = x^3 + ax^2 + bx + c$ where $f(x)$ is a cubic polynomial with no repeated roots, and $a, b, c \in \mathbb{Q}$.

- After a change of variables we can write it as: $y^2 = x^3 + Ax + B$ (Weierstrass Form)
- No repeated roots: $\Delta = 4A^3 + 27B^2 \neq 0$

Examples: Elliptic Curve When $\Delta > 0$

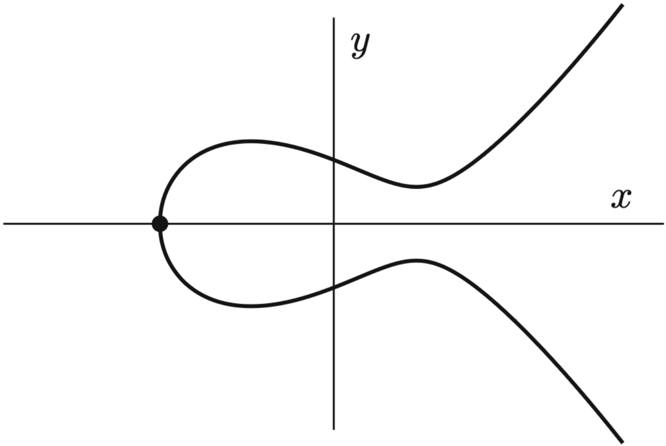


Figure: An elliptic curve with one real root

Examples: Elliptic Curve When $\Delta < 0$

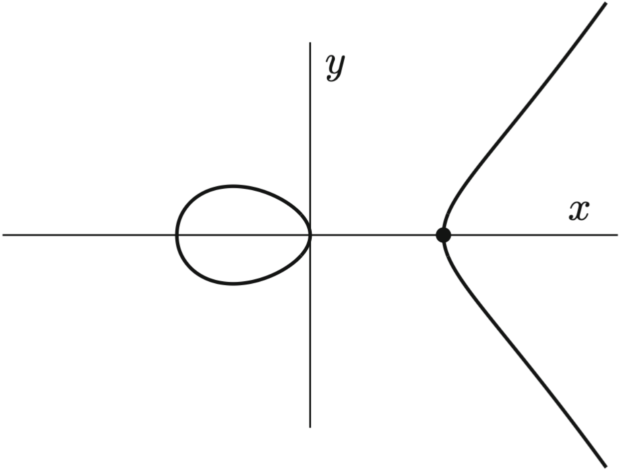


Figure: A elliptic curve with three real roots

Examples: Not An Elliptic Curve ($\Delta = 0$)

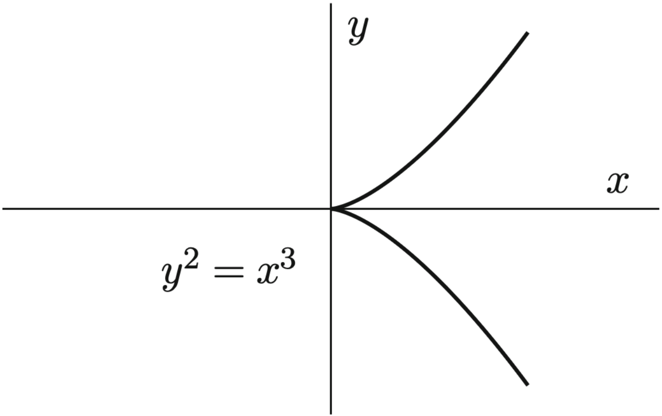


Figure: A cubic curve with a triple root

Examples: Not Elliptic Curves ($\Delta = 0$)

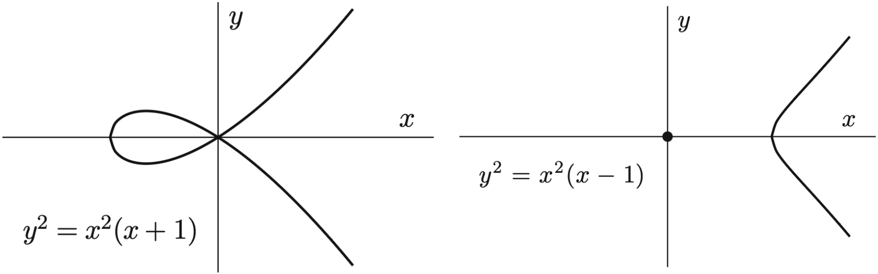


Figure: Cubic curves with a double root

The set of Rational Points $E(\mathbb{Q})$

Definition (Rational Point)

For an elliptic curve E, a **rational point** of E is a point (x, y) on E such that $x, y \in \mathbb{Q}$. The set of all rational points on E is denoted by $E(\mathbb{Q})$.

The set of Rational Points $E(\mathbb{Q})$

Definition (Rational Point)

For an elliptic curve E, a **rational point** of E is a point (x, y) on E such that $x, y \in \mathbb{Q}$. The set of all rational points on E is denoted by $E(\mathbb{Q})$.

- If we have some rational points on E, how do we find more?

The set of Rational Points $E(\mathbb{Q})$

Definition (Rational Point)

For an elliptic curve E, a **rational point** of E is a point (x, y) on E such that $x, y \in \mathbb{Q}$. The set of all rational points on E is denoted by $E(\mathbb{Q})$.

- If we have some rational points on E, how do we find more?
- Can we combine $(x_0, y_0), (x_1, y_1) \in E(\mathbb{Q})$ in some way to get a new rational point (x_2, y_2)?

Elliptic Curve Group

Definition (Group, Abelian)

A **group** $(G, \cdot)$ is a set G combined with an operation $\cdot$ that satisfies:

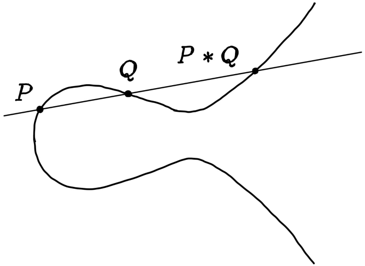
- Closure - $a, b \in G \implies a \cdot b \in G$
- Associativity - $(a \cdot b) \cdot c = a \cdot (b \cdot c)\ \forall a, b, c \in G$
- Identity - $\exists e \in G : a \cdot e = a = e \cdot a\ \forall a \in G$
- Inverse - $\forall a \in G, \exists a^{-1} \in G : a \cdot a^{-1} = e = a^{-1} \cdot a$

A group is **abelian** if for all $g, h \in G$, $g \cdot h = h \cdot g$

Adding Points in $E(\mathbb{Q})$

For $P, Q \in E(\mathbb{Q})$, define $P + Q$ geometrically:

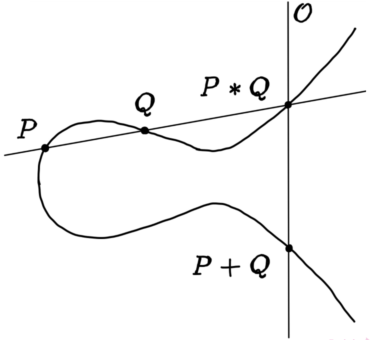
- Draw the line between P and Q. $P * Q$ is the third point of intersection between this line and E.



Adding Points in $E(\mathbb{Q})$

For $P, Q \in E(\mathbb{Q})$, define $P + Q$ geometrically:

- Draw the line between P and Q. $P * Q$ is the third point of intersection between this line and E.
- Draw the line between $\mathcal{O}$ and $P * Q$. $P + Q$ is the third point of intersection between this line and E. Here, $\mathcal{O}$ is the identity of the group.



Why is Adding Points Useful?

If we start with $P, Q \in E(\mathbb{Q})$, then $P + Q \in E(\mathbb{Q})$ as well!

Why is Adding Points Useful?

If we start with $P, Q \in E(\mathbb{Q})$, then $P + Q \in E(\mathbb{Q})$ as well!

Mordell's Theorem

Let E be a rational elliptic curve. Then the group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group.

Why is Adding Points Useful?

If we start with $P, Q \in E(\mathbb{Q})$, then $P + Q \in E(\mathbb{Q})$ as well!

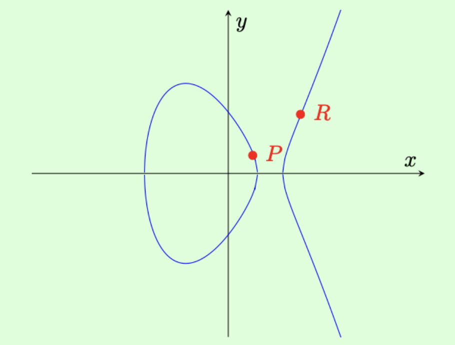
Mordell's Theorem

Let E be a rational elliptic curve. Then the group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group.

So we can generate the whole group with a finite amount of starting points of $E(\mathbb{Q})$!

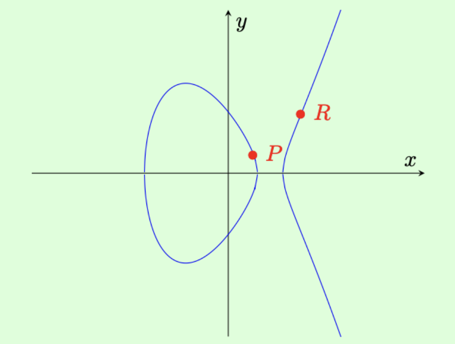
Adding Points: Example

Let E be the elliptic curve $y^2 = x^3 - 9x + 9$, and let $P = (1, 1)$, $R = (3, 3)$.



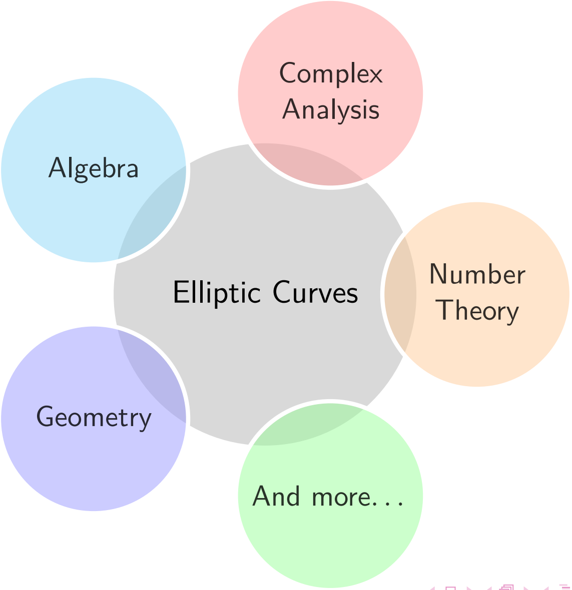
Adding Points: Example

Let E be the elliptic curve $y^2 = x^3 - 9x + 9$, and let $P = (1, 1)$, $R = (3, 3)$.



By adding linear combinations of these two points, we can generate any other rational point on this curve! More precisely, $E(\mathbb{Q}) = \{aP + bR : a, b \in \mathbb{Z}\}$.

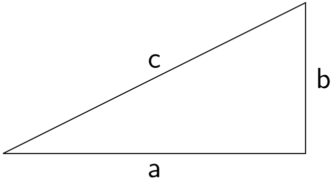
Connections



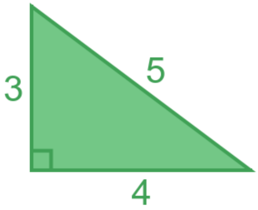
Pythagorean Triples

Definition (Pythagorean Triple)

A **Pythagorean triple** consists of three positive integers a, b, and c, such that $a^2 + b^2 = c^2$.

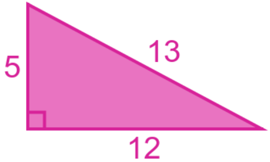


For Example...



$$5^2 = 3^2 + 4^2$$

$$25 = 9 + 16$$



$$13^2 = 5^2 + 12^2$$

$$169 = 25 + 144$$

Fermat's Last Theorem

Can we find any cubic, quartic, ... triples?

Fermat's Last Theorem

Can we find any cubic, quartic, ... triples?

Fermat's Last Theorem

Theorem (Fermat's Last Theorem)

For every integer $n \geq 3$ *the equation* $A^n + B^n = C^n$ *has no solutions in non-zero integers* A, B, *and* C.

Fermat's Last Theorem

Theorem (Fermat's Last Theorem)

For every integer $n \geq 3$ the equation $A^n + B^n = C^n$ has no solutions in non-zero integers A, B, and C.

- Fermat proved the case for $n = 4$.
- Other mathematicians provided proofs for specific cases (such as when $n \in \{3, 5, 7\}$).

What Is The Connection Between Elliptic Curves and FLT?

Hellegouarch's idea: We can use the equation's solutions to create a curve!

What Is The Connection Between Elliptic Curves and FLT?

Hellegouarch's idea: We can use the equation's solutions to create a curve!
Say there is a solution (A, B, C) to $A^n + B^n = C^n$.

What Is The Connection Between Elliptic Curves and FLT?

Hellegouarch's idea: We can use the equation's solutions to create a curve!
Say there is a solution (A, B, C) to $A^n + B^n = C^n$.
Then the **Frey Curve** is: $E_{A,B,C} : y^2 = x(x - A^n)(x + B^n)$.

Strategy: proof by contradiction!

- **Prove that rational elliptic curves are ______**
- **Prove that the Frey curve is not ______**

Then the Frey curve is not a rational elliptic curve.
But it is by its construction!
$\implies$ The Frey curve does not exist, i.e. no A, B, C exist

But what property should we use for ______?

Modularity

One property that appeared useful is called modularity.

Modularity Conjecture (Shimura, Taniyama, Weil)

Every rational elliptic curve is modular.

Frey theorized that $E_{A,B,C}$'s unusual properties made it unlikely for it to be modular.

When Is A Curve Modular?

- Take an elliptic curve E.

When Is A Curve Modular?

- Take an elliptic curve E.
- We can reduce it mod p for a prime p, and count the number of points.

When Is A Curve Modular?

- Take an elliptic curve E.
- We can reduce it mod p for a prime p, and count the number of points.
- By counting we can get a number ϵ_p, we can make a generating series: $\sum \epsilon_n q^n$.

When Is A Curve Modular?

- Take an elliptic curve E.
- We can reduce it mod p for a prime p, and count the number of points.
- By counting we can get a number ϵ_p, we can make a generating series: $\sum \epsilon_n q^n$.
- If we set $q = e^{2\pi i z}$, then the sum $\sum_{n=1}^{\infty} \epsilon_n e^{2\pi i z}$ turns into a Fourier series.

When Is A Curve Modular?

- Take an elliptic curve E.
- We can reduce it mod p for a prime p, and count the number of points.
- By counting we can get a number ϵ_p, we can make a generating series: $\sum \epsilon_n q^n$.
- If we set $q = e^{2\pi iz}$, then the sum $\sum_{n=1}^{\infty} \epsilon_n e^{2\pi iz}$ turns into a Fourier series.
- Then E is modular if $\sum_{n=1}^{\infty} \epsilon_n e^{2\pi iz}$ shows some specific behavior.

When Is A Curve Modular? Example

Let E be the curve $y^2 = x^3 + 1$.

We can calculate the values of ϵ_p and use them to make each ϵ_n. This gives us the series

$$f_E(q) = \sum_{n=1}^{\infty} \epsilon_n q^n = q - 4q^7 + 2q^{13} + 8q^{19} - 5q^{25} - 4q^{31} + \ldots$$

When Is A Curve Modular? Example

Let E be the curve $y^2 = x^3 + 1$.

We can calculate the values of ϵ_p and use them to make each ϵ_n. This gives us the series

$$f_E(q) = \sum_{n=1}^{\infty} \epsilon_n q^n = q - 4q^7 + 2q^{13} + 8q^{19} - 5q^{25} - 4q^{31} + ...$$

Then set $q = e^{2\pi iz}$ to get the Fourier series

$$F_E(z) = f_E(e^{2\pi iz}) = e^{2\pi iz} - 4e^{14\pi iz} + 2e^{26\pi iz} + ...$$

When Is A Curve Modular? Example

Let E be the curve $y^2 = x^3 + 1$. We have

$$F_E(z) = f_E(e^{2\pi iz}) = e^{2\pi iz} - 4e^{14\pi iz} + 2e^{26\pi iz} + \ldots.$$

This F_E is a convergent series for any $z \in \mathbb{C}$ with $Im(z) > 0$, and satisfies some interesting symmetries, such as

$$F_E(\tfrac{-1}{z}) = z^2 F_E(z) \text{ and } F_E(\tfrac{z}{36z+1}) = (36z+1)^2 F_E(z)$$

These types of symmetries mean that F_E is modular.

The Strategy Revisited

Strategy: proof by contradiction!

- **Prove that rational elliptic curves are modular.**
- **Prove that the Frey curve is not modular.**

Then the Frey curve is modular, and it is not modular
$\implies$ The Frey curve does not exist
$\implies$ no such A, B, C exist.

The Strategy Revisited

Ribet's Level-Lowering Theorem (1986)

The Frey Curve is not modular.

The Strategy Revisited

Ribet's Level-Lowering Theorem (1986)

The Frey Curve is not modular.

Corollary (Ribet)

Assume that elliptic curves over $\mathbb{Q}$ are modular. Then FLT is true.

The Strategy Revisited

Corollary (Ribet)

Assume that elliptic curves over $\mathbb{Q}$ are modular. Then FLT is true.

Why does this hold?

If the Modularity Conjecture is correct, the Frey curve, a rational elliptic curve, is modular.

But by Ribet's Theorem, the Frey curve is not modular.

So if the Modularity Conjecture is true, then the Frey curve doesn't exist, i.e. the solution (A, B, C) doesn't exist.

Proving the Modularity Theorem

- In 1994, Wiles and Taylor proved that the Modularity Conjecture holds for rational elliptic curves with semi-stable reduction.

Proving the Modularity Theorem

- In 1994, Wiles and Taylor proved that the Modularity Conjecture holds for rational elliptic curves with semi-stable reduction.
- Combined with Ribet's theorem that gives the non-modularity of the Frey curve $E_{A,B,C}$, this proves Fermat's Last Theorem.

Proving the Modularity Theorem

- In 1994, Wiles and Taylor proved that the Modularity Conjecture holds for rational elliptic curves with semi-stable reduction.
- Combined with Ribet's theorem that gives the non-modularity of the Frey curve $E_{A,B,C}$, this proves Fermat's Last Theorem.
- In 1999, Breuil, Conrad, Diamond, and Taylor proved the Modularity Theorem for all rational elliptic curves.

Theorem (Fermat's Last Theorem)

For every integer $n \geq 3$ the equation $A^n + B^n = C^n$ has no solutions in non-zero integers A, B, and C.

Plus, we can apply our elliptic curve knowledge to other areas!

References

Faisal Al-Faisal.
PMATH 340: Elementary number theory.

Martin McBride.
Pythagorean triples.

K.A. Ribet.
On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms.
Inventiones mathematicae, 1990.

Joseph H. Silverman and John T. Tate.
Rational Points on Elliptic Curves.
Springer, 2nd edition, 2015.

Thank you!