Heegner points on Elliptic curves

Xevi Guitart (UB)

BMS-BGSMath Junior Meeting 2022

Diophantine equations

Central problem in Number Theory

- Polynomial equations with rational coefficients
- Interested in: rational solutions

- $C: x^2 + y^2 - 1 = 0$
  - $C(\mathbb{Q}) = \{$ solutions of C with rational coordinates$\} \subset \mathbb{A}^2$
  - $(1, 0) \in C(\mathbb{Q})$
  - In fact, this equation has infinitely many solutions

Open question

Is there an algorithm that given a diophantine equation C computes $C(\mathbb{Q})$?

- Two variables: $f(x, y) = 0$ with $f \in \mathbb{Q}[x, y]$ is called a plane curve
  - This case is already open
  - But a lot is known: for example, topology plays a role!

Diophantine equations

Central problem in Number Theory

- Polynomial equations with rational coefficients
- Interested in: rational solutions

- $C\colon x^2 + y^2 - 1 = 0$
  - $C(\mathbb{Q}) = \{$ solutions of C with rational coordinates$\} \subset \mathbb{A}^2$
  - $(1,0) \in C(\mathbb{Q})$
  - In fact, this equation has infinitely many solutions

Open question

Is there an algorithm that given a diophantine equation C computes $C(\mathbb{Q})$?

- Two variables: $f(x,y) = 0$ with $f \in \mathbb{Q}[x,y]$ is called a plane curve
  - This case is already open
  - But a lot is known: for example, topology plays a role!

Diophantine equations

Central problem in Number Theory

- Polynomial equations with rational coefficients
- Interested in: rational solutions

- $C\colon x^2 + y^2 - 1 = 0$
  - $C(\mathbb{Q}) = \{$ solutions of C with rational coordinates$\} \subset \mathbb{A}^2$
  - $(1,0) \in C(\mathbb{Q})$
  - In fact, this equation has infinitely many solutions

Open question

Is there an algorithm that given a diophantine equation C computes $C(\mathbb{Q})$?

- Two variables: $f(x,y) = 0$ with $f \in \mathbb{Q}[x,y]$ is called a plane curve
  - This case is already open
  - But a lot is known: for example, topology plays a role!

Diophantine equations

Central problem in Number Theory

- Polynomial equations with rational coefficients
- Interested in: rational solutions

- $C\colon x^2 + y^2 - 1 = 0$
  - $C(\mathbb{Q}) = \{$ solutions of C with rational coordinates$\} \subset \mathbb{A}^2$
  - $(1, 0) \in C(\mathbb{Q})$
  - In fact, this equation has infinitely many solutions

Open question

Is there an algorithm that given a diophantine equation C computes $C(\mathbb{Q})$?

- Two variables: $f(x, y) = 0$ with $f \in \mathbb{Q}[x, y]$ is called a plane curve
  - This case is already open
  - But a lot is known: for example, topology plays a role!

Diophantine equations

Central problem in Number Theory

- Polynomial equations with rational coefficients
- Interested in: rational solutions

- $C\colon x^2 + y^2 - 1 = 0$
  - $C(\mathbb{Q}) = \{$ solutions of C with rational coordinates$\} \subset \mathbb{A}^2$
  - $(1, 0) \in C(\mathbb{Q})$
  - In fact, this equation has infinitely many solutions

Open question

Is there an algorithm that given a diophantine equation C computes $C(\mathbb{Q})$?

- Two variables: $f(x, y) = 0$ with $f \in \mathbb{Q}[x, y]$ is called a plane curve
  - This case is already open
  - But a lot is known: for example, topology plays a role!

Diophantine equations

Central problem in Number Theory

- Polynomial equations with rational coefficients
- Interested in: rational solutions

- $C\colon x^2 + y^2 - 1 = 0$
  - $C(\mathbb{Q}) = \{$ solutions of C with rational coordinates$\} \subset \mathbb{A}^2$
  - $(1, 0) \in C(\mathbb{Q})$, $(-3/5, 4/5) \in C(\mathbb{Q})$
  - In fact, this equation has infinitely many solutions

Open question

Is there an algorithm that given a diophantine equation C computes $C(\mathbb{Q})$?

- Two variables: $f(x, y) = 0$ with $f \in \mathbb{Q}[x, y]$ is called a plane curve
  - This case is already open
  - But a lot is known: for example, topology plays a role!

Diophantine equations

Central problem in Number Theory

- Polynomial equations with rational coefficients
- Interested in: rational solutions

- $C\colon x^2 + y^2 - 1 = 0$
  - $C(\mathbb{Q}) = \{$ solutions of C with rational coordinates$\} \subset \mathbb{A}^2$
  - $(1,0) \in C(\mathbb{Q})$, $(-3/5, 4/5) \in C(\mathbb{Q})$
  - In fact, this equation has infinitely many solutions

Open question

Is there an algorithm that given a diophantine equation C computes $C(\mathbb{Q})$?

- Two variables: $f(x,y) = 0$ with $f \in \mathbb{Q}[x,y]$ is called a plane curve
  - This case is already open
  - But a lot is known: for example, topology plays a role!

Diophantine equations

Central problem in Number Theory

- Polynomial equations with rational coefficients
- Interested in: rational solutions

- $C\colon x^2 + y^2 - 1 = 0$
  - $C(\mathbb{Q}) = \{$ solutions of C with rational coordinates$\} \subset \mathbb{A}^2$
  - $(1,0) \in C(\mathbb{Q})$, $(-3/5, 4/5) \in C(\mathbb{Q})$
  - In fact, this equation has infinitely many solutions

Open question

Is there an algorithm that given a diophantine equation C computes $C(\mathbb{Q})$?

- Two variables: $f(x,y) = 0$ with $f \in \mathbb{Q}[x,y]$ is called a plane curve
  - This case is already open
  - But a lot is known: for example, topology plays a role!

Diophantine equations

Central problem in Number Theory

- Polynomial equations with rational coefficients
- Interested in: rational solutions

- $C\colon x^2 + y^2 - 1 = 0$
  - $C(\mathbb{Q}) = \{$ solutions of C with rational coordinates$\} \subset \mathbb{A}^2$
  - $(1, 0) \in C(\mathbb{Q})$, $(-3/5, 4/5) \in C(\mathbb{Q})$
  - In fact, this equation has infinitely many solutions

Open question

Is there an algorithm that given a diophantine equation C computes $C(\mathbb{Q})$?

- Two variables: $f(x, y) = 0$ with $f \in \mathbb{Q}[x, y]$ is called a plane curve
  - This case is already open
  - But a lot is known: for example, topology plays a role!

Diophantine equations

Central problem in Number Theory

- Polynomial equations with rational coefficients
- Interested in: rational solutions

- $C\colon x^2 + y^2 - 1 = 0$
  - $C(\mathbb{Q}) = \{$ solutions of C with rational coordinates$\} \subset \mathbb{A}^2$
  - $(1, 0) \in C(\mathbb{Q})$, $(-3/5, 4/5) \in C(\mathbb{Q})$
  - In fact, this equation has infinitely many solutions

Open question

Is there an algorithm that given a diophantine equation C computes $C(\mathbb{Q})$?

- Two variables: $f(x, y) = 0$ with $f \in \mathbb{Q}[x, y]$ is called a plane curve
  - This case is already open
  - But a lot is known: for example, topology plays a role!

Diophantine equations

Central problem in Number Theory

- Polynomial equations with rational coefficients
- Interested in: rational solutions

- $C\colon x^2 + y^2 - 1 = 0$
  - $C(\mathbb{Q}) = \{$ solutions of C with rational coordinates$\} \subset \mathbb{A}^2$
  - $(1, 0) \in C(\mathbb{Q})$, $(-3/5, 4/5) \in C(\mathbb{Q})$
  - In fact, this equation has infinitely many solutions

Open question

Is there an algorithm that given a diophantine equation C computes $C(\mathbb{Q})$?

- Two variables: $f(x, y) = 0$ with $f \in \mathbb{Q}[x, y]$ is called a plane curve
  - This case is already open
  - But a lot is known: for example, topology plays a role!

Topology meets number theory

- $C\colon f(x,y)=0 \rightsquigarrow C(\mathbb{C}) = \{$ solutions with $x, y \in \mathbb{C}\}$
  - Write $x = a + bi$, $y = c + di$ with $a, b, c, d \in \mathbb{R}$
  - 2 equations in 4 unknnowns $\rightsquigarrow$ it is a surface (assume nonsingular)
  - non-compact, but can be compactified adding finitely many points:

$$\bar{C}\colon z^d f(\frac{x}{z}, \frac{y}{z}) = 0 \text{ and } \bar{C}(\mathbb{Q}) \subset \mathbb{P}^2$$

- $\bar{C}(\mathbb{C})$ is homeomorphic to a g-holed torus, where g is the genus
- Formula: $g = (d-1)(d-2)/2$ where d is the degree of f.
- $C\colon x^2 + y^2 - 1 = 0 \rightsquigarrow \bar{C}(\mathbb{C})$ is homeomorphic to a sphere

Falting's Theorem, 1984 (a.k.a. Mordell Conjecture)

If $g > 1$ then $C(\mathbb{Q})$ is finite.

- $g = 0$ is known: for $d = 2$ either $\bar{C}(\mathbb{Q}) = \emptyset$ or $\bar{C}(\mathbb{Q})$ can be parametrized by $\mathbb{Q} \cup \{\infty\}$.
- $g = 1$: there is no known method to determine whether $\bar{C}(\mathbb{Q}) = \emptyset$
  - If $\bar{C}(\mathbb{Q}) \neq \emptyset \rightsquigarrow C$ is called an elliptic curve

Topology meets number theory

- $C\colon f(x,y)=0 \rightsquigarrow C(\mathbb{C})=\{$ solutions with $x,y\in\mathbb{C}\}$
  - Write $x=a+bi$, $y=c+di$ with $a,b,c,d\in\mathbb{R}$
  - 2 equations in 4 unknnowns $\rightsquigarrow$ it is a surface (assume nonsingular)
  - non-compact, but can be compactified adding finitely many points:

$$\bar{C}\colon z^d f(\frac{x}{z},\frac{y}{z})=0 \text{ and } \bar{C}(\mathbb{Q})\subset\mathbb{P}^2$$

- $\bar{C}(\mathbb{C})$ is homeomorphic to a g-holed torus, where g is the genus
- Formula: $g=(d-1)(d-2)/2$ where d is the degree of f.
- $C\colon x^2+y^2-1=0 \rightsquigarrow \bar{C}(\mathbb{C})$ is homeomorphic to a sphere

Falting's Theorem, 1984 (a.k.a. Mordell Conjecture)

If $g>1$ then $C(\mathbb{Q})$ is finite.

- $g=0$ is known: for $d=2$ either $\bar{C}(\mathbb{Q})=\emptyset$ or $\bar{C}(\mathbb{Q})$ can be parametrized by $\mathbb{Q}\cup\{\infty\}$.
- $g=1$: there is no known method to determine whether $\bar{C}(\mathbb{Q})=\emptyset$
  - If $\bar{C}(\mathbb{Q})\neq\emptyset \rightsquigarrow C$ is called an elliptic curve

Topology meets number theory

- $C\colon f(x,y)=0 \rightsquigarrow C(\mathbb{C})=\{$ solutions with $x,y\in\mathbb{C}\}$
  - Write $x=a+bi$, $y=c+di$ with $a,b,c,d\in\mathbb{R}$
  - 2 equations in 4 unknnowns $\rightsquigarrow$ it is a surface (assume nonsingular)
  - non-compact, but can be compactified adding finitely many points:

$$\bar{C}\colon z^d f(\frac{x}{z},\frac{y}{z})=0 \text{ and } \bar{C}(\mathbb{Q})\subset\mathbb{P}^2$$

- $\bar{C}(\mathbb{C})$ is homeomorphic to a g-holed torus, where g is the genus
- Formula: $g=(d-1)(d-2)/2$ where d is the degree of f.
- $C\colon x^2+y^2-1=0 \rightsquigarrow \bar{C}(\mathbb{C})$ is homeomorphic to a sphere

Falting's Theorem, 1984 (a.k.a. Mordell Conjecture)

If $g>1$ then $C(\mathbb{Q})$ is finite.

- $g=0$ is known: for $d=2$ either $\bar{C}(\mathbb{Q})=\emptyset$ or $\bar{C}(\mathbb{Q})$ can be parametrized by $\mathbb{Q}\cup\{\infty\}$.
- $g=1$: there is no known method to determine whether $\bar{C}(\mathbb{Q})=\emptyset$
  - If $\bar{C}(\mathbb{Q})\neq\emptyset \rightsquigarrow C$ is called an elliptic curve

Topology meets number theory

- $C\colon f(x,y)=0 \rightsquigarrow C(\mathbb{C}) = \{$ solutions with $x,y\in\mathbb{C}\}$
  - Write $x=a+bi$, $y=c+di$ with $a,b,c,d\in\mathbb{R}$
  - 2 equations in 4 unknnowns $\rightsquigarrow$ it is a surface (assume nonsingular)
  - non-compact, but can be compactified adding finitely many points:

$$\bar{C}\colon z^d f(\frac{x}{z},\frac{y}{z})=0 \text{ and } \bar{C}(\mathbb{Q})\subset\mathbb{P}^2$$

- $\bar{C}(\mathbb{C})$ is homeomorphic to a g-holed torus, where g is the genus
- Formula: $g=(d-1)(d-2)/2$ where d is the degree of f.
- $C\colon x^2+y^2-1=0 \rightsquigarrow \bar{C}(\mathbb{C})$ is homeomorphic to a sphere

Falting's Theorem, 1984 (a.k.a. Mordell Conjecture)

If $g>1$ then $C(\mathbb{Q})$ is finite.

- $g=0$ is known: for $d=2$ either $\bar{C}(\mathbb{Q})=\emptyset$ or $\bar{C}(\mathbb{Q})$ can be parametrized by $\mathbb{Q}\cup\{\infty\}$.
- $g=1$: there is no known method to determine whether $\bar{C}(\mathbb{Q})=\emptyset$
  - If $\bar{C}(\mathbb{Q})\neq\emptyset \rightsquigarrow C$ is called an elliptic curve

Topology meets number theory

- $C\colon f(x,y)=0 \rightsquigarrow C(\mathbb{C}) = \{$ solutions with $x, y \in \mathbb{C}\}$
  - Write $x = a + bi$, $y = c + di$ with $a, b, c, d \in \mathbb{R}$
  - 2 equations in 4 unknnowns $\rightsquigarrow$ it is a surface (assume nonsingular)
  - non-compact, but can be compactified adding finitely many points:

$$\bar{C}\colon z^d f(\frac{x}{z}, \frac{y}{z}) = 0 \text{ and } \bar{C}(\mathbb{Q}) \subset \mathbb{P}^2$$

- $\bar{C}(\mathbb{C})$ is homeomorphic to a g-holed torus, where g is the genus
- Formula: $g = (d-1)(d-2)/2$ where d is the degree of f.
- $C\colon x^2 + y^2 - 1 = 0 \rightsquigarrow \bar{C}(\mathbb{C})$ is homeomorphic to a sphere

Falting's Theorem, 1984 (a.k.a. Mordell Conjecture)

If $g > 1$ then $C(\mathbb{Q})$ is finite.

- $g = 0$ is known: for $d = 2$ either $\bar{C}(\mathbb{Q}) = \emptyset$ or $\bar{C}(\mathbb{Q})$ can be parametrized by $\mathbb{Q} \cup \{\infty\}$.
- $g = 1$: there is no known method to determine whether $\bar{C}(\mathbb{Q}) = \emptyset$
  - If $\bar{C}(\mathbb{Q}) \neq \emptyset \rightsquigarrow C$ is called an elliptic curve

Topology meets number theory

- $C\colon f(x,y)=0 \rightsquigarrow C(\mathbb{C}) = \{$ solutions with $x,y\in\mathbb{C}\}$
  - Write $x=a+bi$, $y=c+di$ with $a,b,c,d\in\mathbb{R}$
  - 2 equations in 4 unknnowns $\rightsquigarrow$ it is a surface (assume nonsingular)
  - non-compact, but can be compactified adding finitely many points:

$$\bar{C}\colon z^d f(\frac{x}{z},\frac{y}{z})=0 \text{ and } \bar{C}(\mathbb{Q})\subset\mathbb{P}^2$$

- $\bar{C}(\mathbb{C})$ is homeomorphic to a g-holed torus, where g is the genus
- Formula: $g=(d-1)(d-2)/2$ where d is the degree of f.
- $C\colon x^2+y^2-1=0 \rightsquigarrow \bar{C}(\mathbb{C})$ is homeomorphic to a sphere

Falting's Theorem, 1984 (a.k.a. Mordell Conjecture)

If $g>1$ then $C(\mathbb{Q})$ is finite.

- $g=0$ is known: for $d=2$ either $\bar{C}(\mathbb{Q})=\emptyset$ or $\bar{C}(\mathbb{Q})$ can be parametrized by $\mathbb{Q}\cup\{\infty\}$.
- $g=1$: there is no known method to determine whether $\bar{C}(\mathbb{Q})=\emptyset$
  - If $\bar{C}(\mathbb{Q})\neq\emptyset \rightsquigarrow C$ is called an elliptic curve

Topology meets number theory

- $C\colon f(x,y)=0 \rightsquigarrow C(\mathbb{C})=\{$ solutions with $x,y\in\mathbb{C}\}$
  - Write $x=a+bi$, $y=c+di$ with $a,b,c,d\in\mathbb{R}$
  - 2 equations in 4 unknnowns $\rightsquigarrow$ it is a surface (assume nonsingular)
  - non-compact, but can be compactified adding finitely many points:

$$\bar{C}\colon z^d f(\frac{x}{z},\frac{y}{z})=0 \text{ and } \bar{C}(\mathbb{Q})\subset\mathbb{P}^2$$

- $\bar{C}(\mathbb{C})$ is homeomorphic to a g-holed torus, where g is the genus
- Formula: $g=(d-1)(d-2)/2$ where d is the degree of f.
- $C\colon x^2+y^2-1=0 \rightsquigarrow \bar{C}(\mathbb{C})$ is homeomorphic to a sphere

Falting's Theorem, 1984 (a.k.a. Mordell Conjecture)

If $g>1$ then $C(\mathbb{Q})$ is finite.

- $g=0$ is known: for $d=2$ either $\bar{C}(\mathbb{Q})=\emptyset$ or $\bar{C}(\mathbb{Q})$ can be parametrized by $\mathbb{Q}\cup\{\infty\}$.
- $g=1$: there is no known method to determine whether $\bar{C}(\mathbb{Q})=\emptyset$
  - If $\bar{C}(\mathbb{Q})\neq\emptyset \rightsquigarrow C$ is called an elliptic curve

Topology meets number theory

- $C\colon f(x,y)=0 \rightsquigarrow C(\mathbb{C}) = \{$ solutions with $x,y\in\mathbb{C}\}$
  - Write $x=a+bi$, $y=c+di$ with $a,b,c,d\in\mathbb{R}$
  - 2 equations in 4 unknnowns $\rightsquigarrow$ it is a surface (assume nonsingular)
  - non-compact, but can be compactified adding finitely many points:

$$\bar{C}\colon z^d f(\frac{x}{z},\frac{y}{z}) = 0 \text{ and } \bar{C}(\mathbb{Q})\subset\mathbb{P}^2$$

- $\bar{C}(\mathbb{C})$ is homeomorphic to a g-holed torus, where g is the genus
- Formula: $g=(d-1)(d-2)/2$ where d is the degree of f.
- $C\colon x^2+y^2-1=0 \rightsquigarrow \bar{C}(\mathbb{C})$ is homeomorphic to a sphere

Falting's Theorem, 1984 (a.k.a. Mordell Conjecture)

If $g>1$ then $C(\mathbb{Q})$ is finite.

- $g=0$ is known: for $d=2$ either $\bar{C}(\mathbb{Q})=\emptyset$ or $\bar{C}(\mathbb{Q})$ can be parametrized by $\mathbb{Q}\cup\{\infty\}$.
- $g=1$: there is no known method to determine whether $\bar{C}(\mathbb{Q})=\emptyset$
  - If $\bar{C}(\mathbb{Q})\neq\emptyset \rightsquigarrow C$ is called an elliptic curve

Topology meets number theory

- $C: f(x, y) = 0 \rightsquigarrow C(\mathbb{C}) = \{$ solutions with $x, y \in \mathbb{C}\}$
  - Write $x = a + bi$, $y = c + di$ with $a, b, c, d \in \mathbb{R}$
  - 2 equations in 4 unknnowns $\rightsquigarrow$ it is a surface (assume nonsingular)
  - non-compact, but can be compactified adding finitely many points:

$$\bar{C}\colon z^d f(\frac{x}{z}, \frac{y}{z}) = 0 \text{ and } \bar{C}(\mathbb{Q}) \subset \mathbb{P}^2$$

- $\bar{C}(\mathbb{C})$ is homeomorphic to a g-holed torus, where g is the genus
- Formula: $g = (d-1)(d-2)/2$ where d is the degree of f.
- $C: x^2 + y^2 - 1 = 0 \rightsquigarrow \bar{C}(\mathbb{C})$ is homeomorphic to a sphere

Falting's Theorem, 1984 (a.k.a. Mordell Conjecture)

If $g > 1$ then $C(\mathbb{Q})$ is finite.

- $g = 0$ is known: for $d = 2$ either $\bar{C}(\mathbb{Q}) = \emptyset$ or $\bar{C}(\mathbb{Q})$ can be parametrized by $\mathbb{Q} \cup \{\infty\}$.
- $g = 1$: there is no known method to determine whether $\bar{C}(\mathbb{Q}) = \emptyset$
  - If $\bar{C}(\mathbb{Q}) \neq \emptyset \rightsquigarrow C$ is called an elliptic curve

Topology meets number theory

- $C\colon f(x,y)=0 \rightsquigarrow C(\mathbb{C})=\{$ solutions with $x,y\in\mathbb{C}\}$
  - Write $x=a+bi$, $y=c+di$ with $a,b,c,d\in\mathbb{R}$
  - 2 equations in 4 unknnowns $\rightsquigarrow$ it is a surface (assume nonsingular)
  - non-compact, but can be compactified adding finitely many points:

$$\bar{C}\colon z^d f(\frac{x}{z},\frac{y}{z})=0 \text{ and } \bar{C}(\mathbb{Q})\subset\mathbb{P}^2$$

- $\bar{C}(\mathbb{C})$ is homeomorphic to a g-holed torus, where g is the genus
- Formula: $g=(d-1)(d-2)/2$ where d is the degree of f.
- $C\colon x^2+y^2-1=0 \rightsquigarrow \bar{C}(\mathbb{C})$ is homeomorphic to a sphere

Falting's Theorem, 1984 (a.k.a. Mordell Conjecture)

If $g>1$ then $C(\mathbb{Q})$ is finite.

- $g=0$ is known: for $d=2$ either $\bar{C}(\mathbb{Q})=\emptyset$ or $\bar{C}(\mathbb{Q})$ can be parametrized by $\mathbb{Q}\cup\{\infty\}$.
- $g=1$: there is no known method to determine whether $\bar{C}(\mathbb{Q})=\emptyset$
  - If $\bar{C}(\mathbb{Q})\neq\emptyset \rightsquigarrow C$ is called an elliptic curve

Topology meets number theory

- $C\colon f(x,y)=0 \rightsquigarrow C(\mathbb{C})=\{$ solutions with $x,y\in\mathbb{C}\}$
  - Write $x=a+bi$, $y=c+di$ with $a,b,c,d\in\mathbb{R}$
  - 2 equations in 4 unknnowns $\rightsquigarrow$ it is a surface (assume nonsingular)
  - non-compact, but can be compactified adding finitely many points:

$$\bar{C}\colon z^d f(\frac{x}{z},\frac{y}{z})=0 \text{ and } \bar{C}(\mathbb{Q})\subset\mathbb{P}^2$$

- $\bar{C}(\mathbb{C})$ is homeomorphic to a g-holed torus, where g is the genus
- Formula: $g=(d-1)(d-2)/2$ where d is the degree of f.
- $C\colon x^2+y^2-1=0 \rightsquigarrow \bar{C}(\mathbb{C})$ is homeomorphic to a sphere

Falting's Theorem, 1984 (a.k.a. Mordell Conjecture)

If $g>1$ then $C(\mathbb{Q})$ is finite.

- $g=0$ is known: for $d=2$ either $\bar{C}(\mathbb{Q})=\emptyset$ or $\bar{C}(\mathbb{Q})$ can be parametrized by $\mathbb{Q}\cup\{\infty\}$.
- $g=1$: there is no known method to determine whether $\bar{C}(\mathbb{Q})=\emptyset$
  - If $\bar{C}(\mathbb{Q})\neq\emptyset \rightsquigarrow C$ is called an elliptic curve

Elliptic curves

Elliptic curve

A non-singular genus 1 curve which has a rational point.

- By a rational change of variables they can be transformed into

$$E: y^2 = x^3 + Ax + B, \quad \text{with } A, B \in \mathbb{Z}, \;\; A^3 - 27B^2 \neq 0.$$

- $[0:1:0]$ point of $y^2z = x^3 + Axz^2 + Bz^3$, the only point at infinity
- Example:

$$E: y^2 = x^3 - 16x + 16$$

  - $(0,4), (4,4) \in E(\mathbb{Q})$

Key property

One can define a group operation

$$\begin{array}{rccc} +: & E(\mathbb{Q}) \times E(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q}) \\ & (P,Q) & \longmapsto & P+Q \end{array}$$

- From $P = (0,4)$ and $Q = (4,4) \rightsquigarrow P + Q \in E(\mathbb{Q})$

Elliptic curves

Elliptic curve

A non-singular genus 1 curve which has a rational point.

- By a rational change of variables they can be transformed into

$$E\colon y^2 = x^3 + Ax + B, \quad \text{with } A, B \in \mathbb{Z},\ A^3 - 27B^2 \neq 0.$$

- $[0:1:0]$ point of $y^2z = x^3 + Axz^2 + Bz^3$, the only point at infinity
- Example:

$$E\colon y^2 = x^3 - 16x + 16$$

  - $(0,4), (4,4) \in E(\mathbb{Q})$

Key property

One can define a group operation

$$\begin{array}{rccc} +\colon & E(\mathbb{Q}) \times E(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q}) \\ & (P,Q) & \longmapsto & P+Q \end{array}$$

- From $P = (0,4)$ and $Q = (4,4) \rightsquigarrow P + Q \in E(\mathbb{Q})$

Elliptic curves

Elliptic curve

A non-singular genus 1 curve which has a rational point.

- By a rational change of variables they can be transformed into
$$E\colon y^2 = x^3 + Ax + B, \quad \text{with } A, B \in \mathbb{Z},\ A^3 - 27B^2 \neq 0.$$
- $[0\colon 1\colon 0]$ point of $y^2z = x^3 + Axz^2 + Bz^3$, the only point at infinity
- Example:
$$E\colon y^2 = x^3 - 16x + 16$$
  - $(0,4), (4,4) \in E(\mathbb{Q})$

Key property

One can define a group operation

$$\begin{array}{rccc} +\colon & E(\mathbb{Q}) \times E(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q}) \\ & (P,Q) & \longmapsto & P+Q \end{array}$$

- From $P = (0,4)$ and $Q = (4,4) \rightsquigarrow P + Q \in E(\mathbb{Q})$

Elliptic curves

Elliptic curve

A non-singular genus 1 curve which has a rational point.

- By a rational change of variables they can be transformed into
$$E\colon y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Z},\ A^3 - 27B^2 \neq 0.$$
- $[0\colon 1\colon 0]$ point of $y^2z = x^3 + Axz^2 + Bz^3$, the only point at infinity
- Example:
$$E\colon y^2 = x^3 - 16x + 16$$
  - $(0,4),(4,4) \in E(\mathbb{Q})$

Key property

One can define a group operation

$$\begin{array}{rccc} +\colon & E(\mathbb{Q}) \times E(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q}) \\ & (P,Q) & \longmapsto & P+Q \end{array}$$

- From $P = (0,4)$ and $Q = (4,4) \rightsquigarrow P + Q \in E(\mathbb{Q})$

Elliptic curves

Elliptic curve

A non-singular genus 1 curve which has a rational point.

- By a rational change of variables they can be transformed into

$$E\colon y^2 = x^3 + Ax + B,\ \text{ with } A, B \in \mathbb{Z},\ A^3 - 27B^2 \neq 0.$$

- $[0\colon 1\colon 0]$ point of $y^2 z = x^3 + Axz^2 + Bz^3$, the only point at infinity
- Example:

$$E\colon y^2 = x^3 - 16x + 16$$

  - $(0,4), (4,4) \in E(\mathbb{Q})$

Key property

One can define a group operation

$$\begin{array}{rccc} +\colon & E(\mathbb{Q}) \times E(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q}) \\ & (P, Q) & \longmapsto & P + Q \end{array}$$

- From $P = (0,4)$ and $Q = (4,4) \rightsquigarrow P + Q \in E(\mathbb{Q})$

Elliptic curves

Elliptic curve

A non-singular genus 1 curve which has a rational point.

- By a rational change of variables they can be transformed into

$$E\colon y^2 = x^3 + Ax + B, \;\; \text{with } A, B \in \mathbb{Z}, \;\; A^3 - 27B^2 \neq 0.$$

- $[0\colon 1\colon 0]$ point of $y^2z = x^3 + Axz^2 + Bz^3$, the only point at infinity
- Example:

$$E\colon y^2 = x^3 - 16x + 16$$

  - $(0,4), (4,4) \in E(\mathbb{Q})$

Key property

One can define a group operation

$$\begin{array}{rccc} +\colon & E(\mathbb{Q}) \times E(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q}) \\ & (P, Q) & \longmapsto & P + Q \end{array}$$

- From $P = (0,4)$ and $Q = (4,4) \rightsquigarrow P + Q \in E(\mathbb{Q})$

Elliptic curves

Elliptic curve

A non-singular genus 1 curve which has a rational point.

- By a rational change of variables they can be transformed into

$$E\colon y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Z},\ A^3 - 27B^2 \neq 0.$$

- $[0 : 1 : 0]$ point of $y^2z = x^3 + Axz^2 + Bz^3$, the only point at infinity
- Example:

$$E\colon y^2 = x^3 - 16x + 16$$

  - $(0,4), (4,4) \in E(\mathbb{Q})$

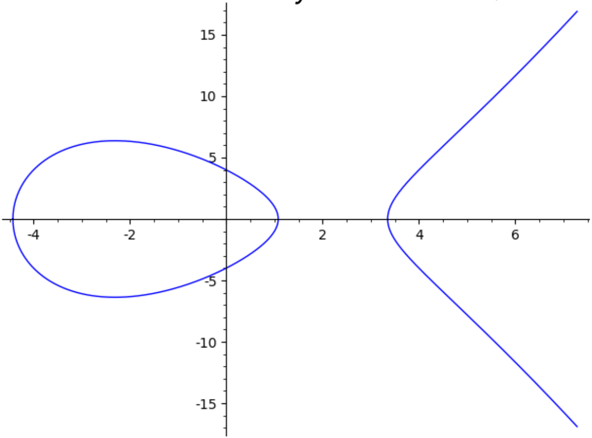
Key property

One can define a group operation

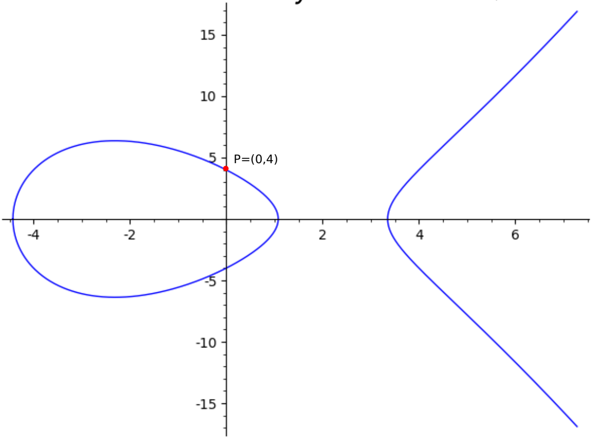
$$\begin{array}{rccc} +: & E(\mathbb{Q}) \times E(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q}) \\ & (P,Q) & \longmapsto & P+Q \end{array}$$

- From $P = (0,4)$ and $Q = (4,4) \rightsquigarrow P + Q \in E(\mathbb{Q})$

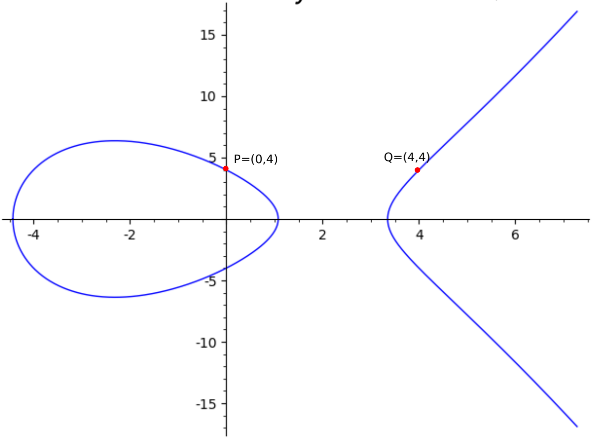
$$E\colon y^2 = x^3 - 16x + 16$$



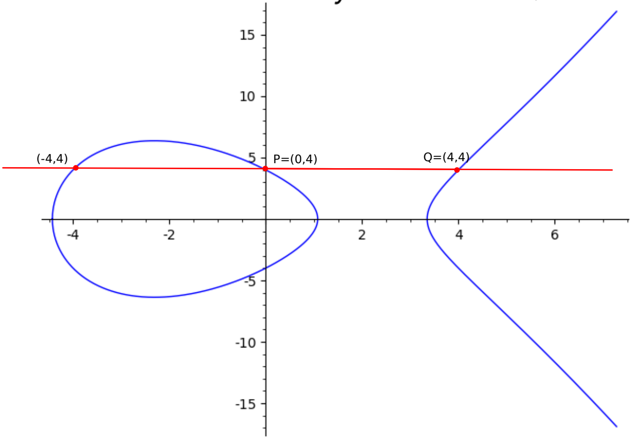
$$E\colon y^2 = x^3 - 16x + 16$$



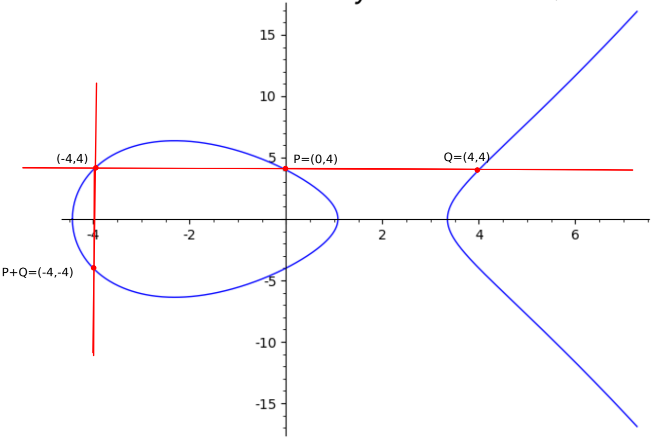
$$E\colon y^2 = x^3 - 16x + 16$$



$$E : y^2 = x^3 - 16x + 16$$



$$E\colon y^2 = x^3 - 16x + 16$$



The group of points

- This makes $E(\mathbb{Q})$ into an abelian group.

Mordell Theorem (1922)

$E(\mathbb{Q})$ is a finitely generated abelian group.

- Structure Theorem: $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$
  - T is finite, its points have finite order
  - r is called the rank of E.
- T is pretty well understood:

Theorem (Mazur, 1977)

$$T \simeq \begin{cases} \mathbb{Z}/N\mathbb{Z}, & 1 \leq N \leq 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, & 1 \leq N \leq 4. \end{cases}$$

- The rank is only understood conjecturally

The group of points

- This makes $E(\mathbb{Q})$ into an abelian group.

Mordell Theorem (1922)

$E(\mathbb{Q})$ is a finitely generated abelian group.

- Structure Theorem: $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$
  - T is finite, its points have finite order
  - r is called the rank of E.
- T is pretty well understood:

Theorem (Mazur, 1977)

$$T \simeq \begin{cases} \mathbb{Z}/N\mathbb{Z}, & 1 \leq N \leq 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, & 1 \leq N \leq 4. \end{cases}$$

- The rank is only understood conjecturally

The group of points

- This makes $E(\mathbb{Q})$ into an abelian group.

Mordell Theorem (1922)

$E(\mathbb{Q})$ is a finitely generated abelian group.

- Structure Theorem: $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$
  - T is finite, its points have finite order
  - r is called the rank of E.
- T is pretty well understood:

Theorem (Mazur, 1977)

$$T \simeq \begin{cases} \mathbb{Z}/N\mathbb{Z}, & 1 \leq N \leq 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, & 1 \leq N \leq 4. \end{cases}$$

- The rank is only understood conjecturally

The group of points

- This makes $E(\mathbb{Q})$ into an abelian group.

Mordell Theorem (1922)

$E(\mathbb{Q})$ is a finitely generated abelian group.

- Structure Theorem: $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$
  - T is finite, its points have finite order
  - r is called the rank of E.
- T is pretty well understood:

Theorem (Mazur, 1977)

$$T \simeq \begin{cases} \mathbb{Z}/N\mathbb{Z}, & 1 \leq N \leq 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, & 1 \leq N \leq 4. \end{cases}$$

- The rank is only understood conjecturally

The group of points

- This makes $E(\mathbb{Q})$ into an abelian group.

Mordell Theorem (1922)

$E(\mathbb{Q})$ is a finitely generated abelian group.

- Structure Theorem: $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$
  - T is finite, its points have finite order
  - r is called the rank of E.
- T is pretty well understood:

Theorem (Mazur, 1977)

$$T \simeq \begin{cases} \mathbb{Z}/N\mathbb{Z}, & 1 \leq N \leq 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, & 1 \leq N \leq 4. \end{cases}$$

- The rank is only understood conjecturally

The group of points

- This makes $E(\mathbb{Q})$ into an abelian group.

Mordell Theorem (1922)

$E(\mathbb{Q})$ is a finitely generated abelian group.

- Structure Theorem: $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$
  - T is finite, its points have finite order
  - r is called the rank of E.
- T is pretty well understood:

Theorem (Mazur, 1977)

$$T \simeq \begin{cases} \mathbb{Z}/N\mathbb{Z}, & 1 \leq N \leq 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, & 1 \leq N \leq 4. \end{cases}$$

- The rank is only understood conjecturally

Birch and Swinnerton-Dyer Conjecture

- $E\colon y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$
- For every prime number p:

$$y^2 \equiv x^3 + Ax + B \pmod{p}$$

- Define $a_p := p - \#\text{solutions}$
- $L(E,s) = \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}} = \sum_{n\geq 1} a_n n^{-s}$
  - Product only converges for $\mathrm{Re}(s) > 3/2$, but can be extended to $\mathbb{C}$

Birch and Swinnerton-Dyer Conjecture

The rank r of E equals $\mathrm{ord}_{s=1} L(E,s)$

Theorem (Gross–Zagier 1986, Kolyvagin 1990)

If $\mathrm{ord}_{s=1} L(E,s)$ is 0 or 1, the BSD Conjecture is true.

- In particular, if $\mathrm{ord}_{s=1} L(E,s) = 1$, E has a point of infinite order.
  - Main tool in the proof: Heegner Points

Birch and Swinnerton-Dyer Conjecture

- $E\colon y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$
- For every prime number p:

$$y^2 \equiv x^3 + Ax + B \pmod{p}$$

- Define $a_p := p - \#\text{solutions}$
- $L(E,s) = \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n \geq 1} a_n n^{-s}$
  - Product only converges for $\mathrm{Re}(s) > 3/2$, but can be extended to $\mathbb{C}$

Birch and Swinnerton-Dyer Conjecture

The rank r of E equals $\mathrm{ord}_{s=1} L(E,s)$

Theorem (Gross–Zagier 1986, Kolyvagin 1990)

If $\mathrm{ord}_{s=1} L(E,s)$ is 0 or 1, the BSD Conjecture is true.

- In particular, if $\mathrm{ord}_{s=1} L(E,s) = 1$, E has a point of infinite order.
  - Main tool in the proof: Heegner Points

Birch and Swinnerton-Dyer Conjecture

- $E\colon y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$
- For every prime number p:

$$y^2 \equiv x^3 + Ax + B \pmod p$$

- Define $a_p := p - \#\text{solutions}$
- $L(E,s) = \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n \geq 1} a_n n^{-s}$
  - Product only converges for $\mathrm{Re}(s) > 3/2$, but can be extended to $\mathbb{C}$

Birch and Swinnerton-Dyer Conjecture

The rank r of E equals $\mathrm{ord}_{s=1} L(E,s)$

Theorem (Gross–Zagier 1986, Kolyvagin 1990)

If $\mathrm{ord}_{s=1} L(E,s)$ is 0 or 1, the BSD Conjecture is true.

- In particular, if $\mathrm{ord}_{s=1} L(E,s) = 1$, E has a point of infinite order.
  - Main tool in the proof: Heegner Points

Birch and Swinnerton-Dyer Conjecture

- $E\colon y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$
- For every prime number p:

$$y^2 \equiv x^3 + Ax + B \pmod{p}$$

- Define $a_p := p - \#\text{solutions}$
- $L(E,s) = \prod_{p \nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}} = \sum_{n\geq 1} a_n n^{-s}$
  - Product only converges for $\mathrm{Re}(s) > 3/2$, but can be extended to $\mathbb{C}$

Birch and Swinnerton-Dyer Conjecture

The rank r of E equals $\mathrm{ord}_{s=1} L(E,s)$

Theorem (Gross–Zagier 1986, Kolyvagin 1990)

If $\mathrm{ord}_{s=1} L(E,s)$ is 0 or 1, the BSD Conjecture is true.

- In particular, if $\mathrm{ord}_{s=1} L(E,s) = 1$, E has a point of infinite order.
  - Main tool in the proof: Heegner Points

Birch and Swinnerton-Dyer Conjecture

- $E\colon y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$
- For every prime number p:

$$y^2 \equiv x^3 + Ax + B \pmod{p}$$

- Define $a_p := p - \#\text{solutions}$
- $L(E,s) = \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}} = \sum_{n\geq 1} a_n n^{-s}$
  - Product only converges for $\mathrm{Re}(s) > 3/2$, but can be extended to $\mathbb{C}$

Birch and Swinnerton-Dyer Conjecture

The rank r of E equals $\mathrm{ord}_{s=1} L(E,s)$

Theorem (Gross–Zagier 1986, Kolyvagin 1990)

If $\mathrm{ord}_{s=1} L(E,s)$ is 0 or 1, the BSD Conjecture is true.

- In particular, if $\mathrm{ord}_{s=1} L(E,s) = 1$, E has a point of infinite order.
  - Main tool in the proof: Heegner Points

Birch and Swinnerton-Dyer Conjecture

- $E\colon y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$
- For every prime number p:

$$y^2 \equiv x^3 + Ax + B \pmod{p}$$

- Define $a_p := p - \#\text{solutions}$
- $L(E,s) = \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}} = \sum_{n\geq 1} a_n n^{-s}$
  - Product only converges for $\mathrm{Re}(s) > 3/2$, but can be extended to $\mathbb{C}$

Birch and Swinnerton-Dyer Conjecture

The rank r of E equals $\mathrm{ord}_{s=1} L(E,s)$

Theorem (Gross–Zagier 1986, Kolyvagin 1990)

If $\mathrm{ord}_{s=1} L(E,s)$ is 0 or 1, the BSD Conjecture is true.

- In particular, if $\mathrm{ord}_{s=1} L(E,s) = 1$, E has a point of infinite order.
  - Main tool in the proof: Heegner Points

Birch and Swinnerton-Dyer Conjecture

- $E\colon y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$
- For every prime number p:

$$y^2 \equiv x^3 + Ax + B \pmod{p}$$

- Define $a_p := p - \#\text{solutions}$
- $L(E,s) = \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n \geq 1} a_n n^{-s}$
  - Product only converges for $\mathrm{Re}(s) > 3/2$, but can be extended to $\mathbb{C}$

Birch and Swinnerton-Dyer Conjecture

The rank r of E equals $\mathrm{ord}_{s=1} L(E,s)$

Theorem (Gross–Zagier 1986, Kolyvagin 1990)

If $\mathrm{ord}_{s=1} L(E,s)$ is 0 or 1, the BSD Conjecture is true.

- In particular, if $\mathrm{ord}_{s=1} L(E,s) = 1$, E has a point of infinite order.
  - Main tool in the proof: Heegner Points

Birch and Swinnerton-Dyer Conjecture

- $E: y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$
- For every prime number p:

$$y^2 \equiv x^3 + Ax + B \pmod{p}$$

- Define $a_p := p - \#\text{solutions}$
- $L(E,s) = \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}} = \sum_{n\geq 1} a_n n^{-s}$
  - Product only converges for $\mathrm{Re}(s) > 3/2$, but can be extended to $\mathbb{C}$

Birch and Swinnerton-Dyer Conjecture

The rank r of E equals $\mathrm{ord}_{s=1} L(E,s)$

Theorem (Gross–Zagier 1986, Kolyvagin 1990)

If $\mathrm{ord}_{s=1} L(E,s)$ is 0 or 1, the BSD Conjecture is true.

- In particular, if $\mathrm{ord}_{s=1} L(E,s) = 1$, E has a point of infinite order.
  - Main tool in the proof: Heegner Points

Complex analysis meets number theory

- $E\colon y^2 = x^3 + Ax + B \rightsquigarrow E(\mathbb{C})$ is homeomorphic to a torus

Weierstrass Uniformization Theorem

There is a lattice $\Lambda_E \subset \mathbb{C}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$ as complex varieties.

- $y^2 = x^3 - x$ is isomorphic to $\mathbb{C}/\mathbb{Z}[i]$
- $L(E,s) = \sum a_n n^{-s}$ with $a_p := p - \#\text{solutions} \pmod p$
- $f_E(z) := \sum_{n\geq 1} a_n e^{2\pi i n z}$ converges for $\mathrm{Im}(z) > 0$

Modularity Theorem (Wiles, Breuil-Conrad-Diamond-Taylor)

$f_E(z)$ is a modular form.

- $f_E(z)$ satisfies certain functional equations.
- This was known to imply Fermat's Last Theorem.

Complex analysis meets number theory

- $E\colon y^2 = x^3 + Ax + B \rightsquigarrow E(\mathbb{C})$ is homeomorphic to a torus

Weierstrass Uniformization Theorem

There is a lattice $\Lambda_E \subset \mathbb{C}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$ as complex varieties.

- $y^2 = x^3 - x$ is isomorphic to $\mathbb{C}/\mathbb{Z}[i]$
- $L(E,s) = \sum a_n n^{-s}$ with $a_p := p - \#\text{solutions} \pmod p$
- $f_E(z) := \sum_{n\geq 1} a_n e^{2\pi i n z}$ converges for $\mathrm{Im}(z) > 0$

Modularity Theorem (Wiles, Breuil-Conrad-Diamond-Taylor)

$f_E(z)$ is a modular form.

- $f_E(z)$ satisfies certain functional equations.
- This was known to imply Fermat's Last Theorem.

Complex analysis meets number theory

- $E\colon y^2 = x^3 + Ax + B \rightsquigarrow E(\mathbb{C})$ is homeomorphic to a torus

Weierstrass Uniformization Theorem

There is a lattice $\Lambda_E \subset \mathbb{C}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$ as complex varieties.

- $y^2 = x^3 - x$ is isomorphic to $\mathbb{C}/\mathbb{Z}[i]$
- $L(E,s) = \sum a_n n^{-s}$ with $a_p := p - \#\text{solutions} \pmod p$
- $f_E(z) := \sum_{n\geq 1} a_n e^{2\pi i n z}$ converges for $\mathrm{Im}(z) > 0$

Modularity Theorem (Wiles, Breuil-Conrad-Diamond-Taylor)

$f_E(z)$ is a modular form.

- $f_E(z)$ satisfies certain functional equations.
- This was known to imply Fermat's Last Theorem.

Complex analysis meets number theory

- $E\colon y^2 = x^3 + Ax + B \rightsquigarrow E(\mathbb{C})$ is homeomorphic to a torus

Weierstrass Uniformization Theorem

There is a lattice $\Lambda_E \subset \mathbb{C}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$ as complex varieties.

- $y^2 = x^3 - x$ is isomorphic to $\mathbb{C}/\mathbb{Z}[i]$
- $L(E,s) = \sum a_n n^{-s}$ with $a_p := p - \#\text{solutions} \pmod p$
- $f_E(z) := \sum_{n\geq 1} a_n e^{2\pi i n z}$ converges for $\mathrm{Im}(z) > 0$

Modularity Theorem (Wiles, Breuil-Conrad-Diamond-Taylor)

$f_E(z)$ is a modular form.

- $f_E(z)$ satisfies certain functional equations.
- This was known to imply Fermat's Last Theorem.

Complex analysis meets number theory

- $E\colon y^2 = x^3 + Ax + B \rightsquigarrow E(\mathbb{C})$ is homeomorphic to a torus

Weierstrass Uniformization Theorem

There is a lattice $\Lambda_E \subset \mathbb{C}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$ as complex varieties.

- $y^2 = x^3 - x$ is isomorphic to $\mathbb{C}/\mathbb{Z}[i]$
- $L(E,s) = \sum a_n n^{-s}$ with $a_p := p - \#\text{solutions} \pmod p$
- $f_E(z) := \sum_{n\geq 1} a_n e^{2\pi i n z}$ converges for $\mathrm{Im}(z) > 0$

Modularity Theorem (Wiles, Breuil-Conrad-Diamond-Taylor)

$f_E(z)$ is a modular form.

- $f_E(z)$ satisfies certain functional equations.
- This was known to imply Fermat's Last Theorem.

Complex analysis meets number theory

- $E\colon y^2 = x^3 + Ax + B \rightsquigarrow E(\mathbb{C})$ is homeomorphic to a torus

Weierstrass Uniformization Theorem

There is a lattice $\Lambda_E \subset \mathbb{C}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$ as complex varieties.

- $y^2 = x^3 - x$ is isomorphic to $\mathbb{C}/\mathbb{Z}[i]$
- $L(E,s) = \sum a_n n^{-s}$ with $a_p := p - \#\text{solutions} \pmod{p}$
- $f_E(z) := \sum_{n\geq 1} a_n e^{2\pi i n z}$ converges for $\mathrm{Im}(z) > 0$

Modularity Theorem (Wiles, Breuil-Conrad-Diamond-Taylor)

$f_E(z)$ is a modular form.

- $f_E(z)$ satisfies certain functional equations.
- This was known to imply Fermat's Last Theorem.

Complex analysis meets number theory

- $E\colon y^2 = x^3 + Ax + B \rightsquigarrow E(\mathbb{C})$ is homeomorphic to a torus

Weierstrass Uniformization Theorem

There is a lattice $\Lambda_E \subset \mathbb{C}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$ as complex varieties.

- $y^2 = x^3 - x$ is isomorphic to $\mathbb{C}/\mathbb{Z}[i]$
- $L(E, s) = \sum a_n n^{-s}$ with $a_p := p - \#\text{solutions} \pmod p$
- $f_E(z) := \sum_{n\geq 1} a_n e^{2\pi i n z}$ converges for $\mathrm{Im}(z) > 0$

Modularity Theorem (Wiles, Breuil-Conrad-Diamond-Taylor)

$f_E(z)$ is a modular form.

- $f_E(z)$ satisfies certain functional equations.
- This was known to imply Fermat's Last Theorem.

Complex analysis meets number theory

- $E\colon y^2 = x^3 + Ax + B \rightsquigarrow E(\mathbb{C})$ is homeomorphic to a torus

Weierstrass Uniformization Theorem

There is a lattice $\Lambda_E \subset \mathbb{C}$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$ as complex varieties.

- $y^2 = x^3 - x$ is isomorphic to $\mathbb{C}/\mathbb{Z}[i]$
- $L(E,s) = \sum a_n n^{-s}$ with $a_p := p - \#\text{solutions} \pmod p$
- $f_E(z) := \sum_{n\geq 1} a_n e^{2\pi i n z}$ converges for $\mathrm{Im}(z) > 0$

Modularity Theorem (Wiles, Breuil-Conrad-Diamond-Taylor)

$f_E(z)$ is a modular form.

- $f_E(z)$ satisfies certain functional equations.
- This was known to imply Fermat's Last Theorem.

Heegner points

- Associated to imaginary quadratic numbers $w = a + b\sqrt{-D}$
- $P_w = \int_{i\infty}^{w} f_E(z)dz \in \mathbb{C}/\Lambda_E \simeq E(\mathbb{C})$

Complex multiplication + Gross-Zagier

If $\mathrm{ord}_{s=1} L(E, s) = 1$ choosing w appropriately $P_w \in E(\mathbb{Q})$ and is of infinite order.

Heegner points

- Associated to imaginary quadratic numbers $w = a + b\sqrt{-D}$
- $P_w = \int_{i\infty}^{w} f_E(z)dz \in \mathbb{C}/\Lambda_E \simeq E(\mathbb{C})$

Complex multiplication + Gross-Zagier

If $\mathrm{ord}_{s=1} L(E, s) = 1$ choosing w appropriately $P_w \in E(\mathbb{Q})$ and is of infinite order.

Heegner points

- Associated to imaginary quadratic numbers $w = a + b\sqrt{-D}$
- $P_w = \int_{i\infty}^{w} f_E(z)dz \in \mathbb{C}/\Lambda_E \simeq E(\mathbb{C})$

Complex multiplication + Gross-Zagier

If $\mathrm{ord}_{s=1} L(E, s) = 1$ choosing w appropriately $P_w \in E(\mathbb{Q})$ and is of infinite order.

Stark-Heegner points

Natural question

Are there points P_w associated to real quadratic numbers $a + b\sqrt{D}$?

- Henri Darmon in 2000 proposed a construction using *p*-adic integrals instead of complex integrals.
- These are called Stark–Heegner (or Darmon) points, and have been constructed also for curves over other number fields.
- Rationality of the points is still conjectural, but the method can be used to compute points in practice: very efficient algorithm

Example (G.-Masdeu)

- $E: y^2 + xy = x^3 - 8x$
- $\left(\frac{3449809443179}{499880896975}, -\frac{3449809443179}{999761793950} + \frac{3600393040902501011}{393559729354696325 0}\sqrt{341}\right) \in E(\mathbb{Q}(\sqrt{341}))$

Stark-Heegner points

Natural question

Are there points P_w associated to real quadratic numbers $a + b\sqrt{D}$?

- Henri Darmon in 2000 proposed a construction using p-adic integrals instead of complex integrals.
- These are called Stark–Heegner (or Darmon) points, and have been constructed also for curves over other number fields.
- Rationality of the points is still conjectural, but the method can be used to compute points in practice: very efficient algorithm

Example (G.-Masdeu)

- $E\colon y^2 + xy = x^3 - 8x$
- $\left(\frac{3449809443179}{499880896975}, -\frac{3449809443179}{999761793950} + \frac{36003930409025010011}{393559729354696325O}\sqrt{341}\right) \in E(\mathbb{Q}(\sqrt{341}))$

Stark-Heegner points

Natural question

Are there points P_w associated to real quadratic numbers $a + b\sqrt{D}$?

- Henri Darmon in 2000 proposed a construction using p-adic integrals instead of complex integrals.
- These are called Stark–Heegner (or Darmon) points, and have been constructed also for curves over other number fields.
- Rationality of the points is still conjectural, but the method can be used to compute points in practice: very efficient algorithm

Example (G.-Masdeu)

- $E\colon y^2 + xy = x^3 - 8x$
- $\left(\frac{3449809443179}{499880896975}, -\frac{3449809443179}{999761793950} + \frac{3600393040902501011}{3935597293546963250}\sqrt{341}\right) \in E(\mathbb{Q}(\sqrt{341}))$

Stark-Heegner points

Natural question

Are there points P_w associated to real quadratic numbers $a + b\sqrt{D}$?

- Henri Darmon in 2000 proposed a construction using p-adic integrals instead of complex integrals.
- These are called Stark–Heegner (or Darmon) points, and have been constructed also for curves over other number fields.
- Rationality of the points is still conjectural, but the method can be used to compute points in practice: very efficient algorithm

Example (G.-Masdeu)

- $E: y^2 + xy = x^3 - 8x$
- $\left(\frac{3449809443179}{499880896975}, -\frac{3449809443179}{999761793950} + \frac{36003930409025010 11}{39355972935469632 50}\sqrt{341}\right) \in E(\mathbb{Q}(\sqrt{341}))$

Stark-Heegner points

Natural question

Are there points P_w associated to real quadratic numbers $a + b\sqrt{D}$?

- Henri Darmon in 2000 proposed a construction using p-adic integrals instead of complex integrals.
- These are called Stark–Heegner (or Darmon) points, and have been constructed also for curves over other number fields.
- Rationality of the points is still conjectural, but the method can be used to compute points in practice: very efficient algorithm

Example (G.-Masdeu)

- $E\colon y^2 + xy = x^3 - 8x$
- $\left(\frac{3449809443179}{499880896975}, -\frac{3449809443179}{999761793950} + \frac{3600393040902501011}{393559729354696325 0}\sqrt{341}\right) \in E(\mathbb{Q}(\sqrt{341}))$

Stark-Heegner points

Natural question

Are there points P_w associated to real quadratic numbers $a + b\sqrt{D}$?

- Henri Darmon in 2000 proposed a construction using *p*-adic integrals instead of complex integrals.
- These are called Stark–Heegner (or Darmon) points, and have been constructed also for curves over other number fields.
- Rationality of the points is still conjectural, but the method can be used to compute points in practice: very efficient algorithm

Example (G.-Masdeu)

- $E\colon y^2 + xy = x^3 - 8x$
- $\left(\frac{3449809443179}{499880896975}, -\frac{3449809443179}{999761793950} + \frac{3600393040902501011}{393559729354696325 0}\sqrt{341}\right) \in E(\mathbb{Q}(\sqrt{341}))$

Heegner points on Elliptic curves

Xevi Guitart (UB)

BMS-BGSMath Junior Meeting 2022