Heegner Points

Arshay Sheth

Talk at the number theory study group.

29th October, 2021

Goals of the talk

There are two goals of this talk:

- Introduce the definition and properties of Heegner points.
- Explain their applications.

Definition and properties of Heegner points

Modular curves

Let $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

Modular curves

Let $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. We have an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ by

$$\gamma \cdot z = \frac{az + b}{cz + d},$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathbb{H}$.

Modular curves

Let $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. We have an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ by

$$\gamma \cdot z = \frac{az + b}{cz + d},$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathbb{H}$.

Theorem (Uniformization theorem)

We have that $SL_2(\mathbb{Z})\backslash\mathbb{H}$ can be equipped with the structure of a Riemann surface

Modular curves

Let $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. We have an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ by

$$\gamma \cdot z = \frac{az + b}{cz + d},$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathbb{H}$.

Theorem (Uniformization theorem)

We have that $SL_2(\mathbb{Z})\backslash\mathbb{H}$ can be equipped with the structure of a Riemann surface and

$$j : SL_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}, \qquad [\tau] \mapsto j(\tau)$$

is an isomorphism of Riemann surfaces.

Congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$

Definition

For $N \in \mathbb{N}_{\geq 1}$, we define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$

Definition

For $N \in \mathbb{N}_{\geq 1}$, we define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Definition

A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup if there exists an $N \in \mathbb{N}_{\geq 1}$ such that $\Gamma(N) \subseteq \Gamma$.

Congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$

Definition

For $N \in \mathbb{N}_{\geq 1}$, we define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Definition

A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup if there exists an $N \in \mathbb{N}_{\geq 1}$ such that $\Gamma(N) \subseteq \Gamma$.

Definition

If Γ is any congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, then $Y(\Gamma) := \Gamma \backslash \mathbb{H}$ is called a modular curve.

Congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$

Definition

For $N \in \mathbb{N}_{\geq 1}$, we define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Definition

A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup if there exists an $N \in \mathbb{N}_{\geq 1}$ such that $\Gamma(N) \subseteq \Gamma$.

Definition

If Γ is any congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, then $Y(\Gamma) := \Gamma \backslash \mathbb{H}$ is called a modular curve.

Fact: $Y(\Gamma)$ can be equipped with the structure of a Riemann surface.

Compactified modular curves

Define $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{C})$,

Compactified modular curves

Define $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{C})$, where $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{C})$ via

$$\gamma \cdot (x : y) = \frac{ax + by}{cx + dy}$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $(x : y) \in \mathbb{P}^1(\mathbb{C})$.

Compactified modular curves

Define $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{C})$, where $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{C})$ via

$$\gamma \cdot (x : y) = \frac{ax + by}{cx + dy}$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $(x : y) \in \mathbb{P}^1(\mathbb{C})$.

Fact: $X(\Gamma) := \Gamma \backslash \mathbb{H}^*$ can be equipped with the structure of a compact Riemann surface.

Compactified modular curves

Define $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{C})$, where $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{C})$ via

$$\gamma \cdot (x : y) = \frac{ax + by}{cx + dy}$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $(x : y) \in \mathbb{P}^1(\mathbb{C})$.

Fact: $X(\Gamma) := \Gamma \backslash \mathbb{H}^*$ can be equipped with the structure of a compact Riemann surface.

Example

If $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, then $X(\Gamma)$ is isomorphic to the Riemann sphere.

The modular curves $Y_0(N)$ and $X_0(N)$

Definition

For $N \in \mathbb{N}_{\geq 1}$, we define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}.$$

The modular curves $Y_0(N)$ and $X_0(N)$

Definition

For $N \in \mathbb{N}_{\geq 1}$, we define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}.$$

Definition

The modular curve associated to $\Gamma_0(N)$ is denoted by $Y_0(N)$ and the compactified modular curve associated to $\Gamma_0(N)$ is denoted by $X_0(N)$.

The modular curves $Y_0(N)$ and $X_0(N)$

Definition

For $N \in \mathbb{N}_{\geq 1}$, we define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}.$$

Definition

The modular curve associated to $\Gamma_0(N)$ is denoted by $Y_0(N)$ and the compactified modular curve associated to $\Gamma_0(N)$ is denoted by $X_0(N)$.

Important fact: $X_0(N)$ can be defined as an algebraic curve over $\mathbb{Q}$

The modular curves $Y_0(N)$ and $X_0(N)$

Definition

For $N \in \mathbb{N}_{\geq 1}$, we define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}.$$

Definition

The modular curve associated to $\Gamma_0(N)$ is denoted by $Y_0(N)$ and the compactified modular curve associated to $\Gamma_0(N)$ is denoted by $X_0(N)$.

Important fact: $X_0(N)$ can be defined as an algebraic curve over $\mathbb{Q}$ and under this definition, $Y_0(N)$ is an open subvariety of $X_0(N)$.

Moduli interpretation of $Y_0(N)$

We have that $Y_0(N)(\mathbb{C})$ is in bijection with

$$\{\phi : E \to E' | E, E' \text{ e.c. over } \mathbb{C} \ \& \ \ker(\phi) \text{ cyclic subgroup of order } N\}/\cong$$

Moduli interpretation of $Y_0(N)$

We have that $Y_0(N)(\mathbb{C})$ is in bijection with

$$\{\phi : E \to E' | E, E' \text{ e.c. over } \mathbb{C} \ \& \ \ker(\phi) \text{ cyclic subgroup of order } N\}/\cong$$

If K is a number field, then $Y_0(N)(K)$ is in bijection with

$$\{\phi : E \to E' | E, E' \text{ e.c. over } K, \ \phi \text{ defined over } K$$

$$\& \ \ker(\phi) \text{ cyclic subgroup of order } N\}/\cong$$

Moduli interpretation of $Y_0(N)$

We have that $Y_0(N)(\mathbb{C})$ is in bijection with

$$\{\phi : E \to E' | E, E' \text{ e.c. over } \mathbb{C} \ \& \ \ker(\phi) \text{ cyclic subgroup of order } N\}/\cong$$

If K is a number field, then $Y_0(N)(K)$ is in bijection with

$$\{\phi : E \to E' | E, E' \text{ e.c. over } K, \ \ \phi \text{ defined over } K$$

$$\& \ \ \ker(\phi) \text{ cyclic subgroup of order } N\}/\cong$$

(here $\cong$ means over $\bar{K}$).

Moduli interpretation of $Y_0(N)$

We have that $Y_0(N)(\mathbb{C})$ is in bijection with

$$\{\phi : E \to E' | E, E' \text{ e.c. over } \mathbb{C} \ \& \ \ker(\phi) \text{ cyclic subgroup of order } N\}/\cong$$

If K is a number field, then $Y_0(N)(K)$ is in bijection with

$$\{\phi : E \to E' | E, E' \text{ e.c. over } K, \ \ \phi \text{ defined over } K$$

$$\& \ \ \ker(\phi) \text{ cyclic subgroup of order } N\}/\cong$$

(here $\cong$ means over $\bar{K}$).

The modular curve $Y_0(N)$ parameterizes isogenies $E \to E'$ with cyclic kernel of order N.

Definition of Heegner points on modular curves

Let K be an imaginary quadratic field.

Definition of Heegner points on modular curves

Let K be an imaginary quadratic field.

Definition

We say that $x_K = (\phi : E \to E') \in Y_0(N)(\mathbb{C})$ is a Heegner point

Definition of Heegner points on modular curves

Let K be an imaginary quadratic field.

Definition

We say that $x_K = (\phi : E \to E') \in Y_0(N)(\mathbb{C})$ is a Heegner point , if both E and E' have complex multiplication by some order $\mathcal{O} \subseteq K$.

Definition of Heegner points on modular curves

Let K be an imaginary quadratic field.

Definition

We say that $x_K = (\phi : E \to E') \in Y_0(N)(\mathbb{C})$ is a Heegner point , if both E and E' have complex multiplication by some order $\mathcal{O} \subseteq K$.

Theorem (Complex multiplication)

Let $\mathcal{O} \subseteq K$ be an order. The map

$$Cl(\mathcal{O}) \to \{elliptic\ curves\ with\ CM\ by\ \mathcal{O}\}$$

given by $[\mathfrak{a}] \mapsto \mathbb{C}/\mathfrak{a}$ is a bijection.

Definition of Heegner points on modular curves

Let K be an imaginary quadratic field.

Definition

We say that $x_K = (\phi : E \to E') \in Y_0(N)(\mathbb{C})$ is a Heegner point , if both E and E' have complex multiplication by some order $\mathcal{O} \subseteq K$.

Theorem (Complex multiplication)

Let $\mathcal{O} \subseteq K$ be an order. The map

$$Cl(\mathcal{O}) \to \{elliptic\ curves\ with\ CM\ by\ \mathcal{O}\}$$

given by $[\mathfrak{a}] \mapsto \mathbb{C}/\mathfrak{a}$ is a bijection.

Proposition

The set of Heegner points is non-empty if and only if there exists an order $\mathcal{O}$ and an ideal $\mathcal{N} \subseteq \mathcal{O}$ such that $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Proof of the proposition

Proof

" $\implies$ " Suppose we have a Heegner point $x_K = (\phi : E \to E')$ with $\ker\phi$ cyclic and E, E' have CM by $\mathcal{O}$.

Proof of the proposition

Proof

" $\implies$ " Suppose we have a Heegner point $x_K = (\phi : E \to E')$ with $\ker\phi$ cyclic and E, E' have CM by $\mathcal{O}$. We can write

$$E = \mathbb{C}/\mathfrak{a}, \quad E' = \mathbb{C}/\mathfrak{b}$$

for some invertible fractionals ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}$.

Proof of the proposition

Proof

" $\implies$ " Suppose we have a Heegner point $x_K = (\phi : E \to E')$ with $\ker\phi$ cyclic and E, E' have CM by $\mathcal{O}$. We can write

$$E = \mathbb{C}/\mathfrak{a}, \quad E' = \mathbb{C}/\mathfrak{b}$$

for some invertible fractionals ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}$. Then there exists an $\alpha \in K$ such $\alpha\mathfrak{a} \subseteq \mathfrak{b}$ and

$$\phi : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{b}, \quad \overline{x} \to \overline{\alpha \cdot x} \quad .$$

Proof of the proposition

Proof

" $\implies$ " Suppose we have a Heegner point $x_K = (\phi : E \to E')$ with $\ker\phi$ cyclic and E, E' have CM by $\mathcal{O}$. We can write

$$E = \mathbb{C}/\mathfrak{a}, \quad E' = \mathbb{C}/\mathfrak{b}$$

for some invertible fractionals ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}$. Then there exists an $\alpha \in K$ such $\alpha\mathfrak{a} \subseteq \mathfrak{b}$ and

$$\phi : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{b}, \quad \overline{x} \to \overline{\alpha \cdot x} \quad .$$

Note that

$$\ker(\phi) = (\alpha^{-1}\mathfrak{b})/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}.$$

Proof of the proposition

Proof

" $\implies$ " Suppose we have a Heegner point $x_K = (\phi : E \to E')$ with $\ker\phi$ cyclic and E, E' have CM by $\mathcal{O}$. We can write

$$E = \mathbb{C}/\mathfrak{a}, \quad E' = \mathbb{C}/\mathfrak{b}$$

for some invertible fractionals ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}$. Then there exists an $\alpha \in K$ such $\alpha\mathfrak{a} \subseteq \mathfrak{b}$ and

$$\phi : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{b}, \quad \overline{x} \to \overline{\alpha \cdot x} \quad .$$

Note that

$$\ker(\phi) = (\alpha^{-1}\mathfrak{b})/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}.$$

Thus if we set $\mathcal{N} = \alpha\mathfrak{a}\mathfrak{b}^{-1}$, then

$$\mathcal{O}/\mathcal{N} = (\mathfrak{b}\mathfrak{b}^{-1})/\alpha\mathfrak{a}\mathfrak{b}^{-1} \cong \mathfrak{b}/\alpha\mathfrak{a} \cong (\alpha^{-1}\mathfrak{b})/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}.$$

Proof of the proposition (contd.)

Proof

" $\Longleftarrow$ " Suppose there is an ideal $\mathcal{N} \subseteq \mathcal{O}$ such that $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Proof of the proposition (contd.)

Proof

" $\Longleftarrow$ " Suppose there is an ideal $\mathcal{N} \subseteq \mathcal{O}$ such that $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Choose an invertible fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ and set $E = \mathbb{C}/\mathfrak{a}$ and $E' = \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$.

Proof of the proposition (contd.)

Proof

" $\Longleftarrow$ " Suppose there is an ideal $\mathcal{N} \subseteq \mathcal{O}$ such that $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Choose an invertible fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ and set $E = \mathbb{C}/\mathfrak{a}$ and $E' = \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$. Both E and E' have CM by $\mathcal{O}$.

Proof of the proposition (contd.)

Proof

" $\Longleftarrow$ " Suppose there is an ideal $\mathcal{N} \subseteq \mathcal{O}$ such that $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Choose an invertible fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ and set $E = \mathbb{C}/\mathfrak{a}$ and $E' = \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$. Both E and E' have CM by $\mathcal{O}$. Consider the isogeny

$$\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}, \quad \overline{x} \mapsto \overline{x}.$$

Proof of the proposition (contd.)

Proof

" $\Longleftarrow$ " Suppose there is an ideal $\mathcal{N} \subseteq \mathcal{O}$ such that $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Choose an invertible fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ and set $E = \mathbb{C}/\mathfrak{a}$ and $E' = \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$. Both E and E' have CM by $\mathcal{O}$. Consider the isogeny

$$\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}, \quad \overline{x} \mapsto \overline{x}.$$

The kernel of this isogeny is

$$\mathfrak{a}\mathcal{N}^{-1}/\mathfrak{a}$$

Proof of the proposition (contd.)

Proof

" $\Longleftarrow$ " Suppose there is an ideal $\mathcal{N} \subseteq \mathcal{O}$ such that $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Choose an invertible fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ and set $E = \mathbb{C}/\mathfrak{a}$ and $E' = \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$. Both E and E' have CM by $\mathcal{O}$. Consider the isogeny

$$\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}, \quad \overline{x} \mapsto \overline{x}.$$

The kernel of this isogeny is

$$\mathfrak{a}\mathcal{N}^{-1}/\mathfrak{a} \cong \mathcal{O}/\mathcal{N}$$

Proof of the proposition (contd.)

Proof

" $\Longleftarrow$ " Suppose there is an ideal $\mathcal{N} \subseteq \mathcal{O}$ such that $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Choose an invertible fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ and set $E = \mathbb{C}/\mathfrak{a}$ and $E' = \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$. Both E and E' have CM by $\mathcal{O}$. Consider the isogeny

$$\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}, \quad \overline{x} \mapsto \overline{x}.$$

The kernel of this isogeny is

$$\mathfrak{a}\mathcal{N}^{-1}/\mathfrak{a} \cong \mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}. \qquad \square$$

The Heegner hypothesis

Proposition

Suppose that every prime p dividing N splits in K. Then there exists an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

The Heegner hypothesis

Proposition

Suppose that every prime p dividing N splits in K. Then there exists an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Proof.

Write $N = p_1^{e_1} \cdots p_r^{e_r}$ and suppose $p_1\mathcal{O}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}, \quad \ldots, p_r\mathcal{O}_K = \mathfrak{p}_{r1}\mathfrak{p}_{r2}$.

The Heegner hypothesis

Proposition

Suppose that every prime p dividing N splits in K. Then there exists an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Proof.

Write $N = p_1^{e_1} \cdots p_r^{e_r}$ and suppose $p_1\mathcal{O}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}, \quad \ldots, p_r\mathcal{O}_K = \mathfrak{p}_{r1}\mathfrak{p}_{r2}$. Since

$$\mathcal{O}_K/\mathfrak{p}_{11} \cong \mathbb{Z}/p_1\mathbb{Z}, \ldots, \mathcal{O}_K/\mathfrak{p}_{r1} \cong \mathbb{Z}/p_r\mathbb{Z},$$

The Heegner hypothesis

Proposition

Suppose that every prime p dividing N splits in K. Then there exists an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Proof.

Write $N = p_1^{e_1} \cdots p_r^{e_r}$ and suppose $p_1\mathcal{O}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}, \quad \ldots, p_r\mathcal{O}_K = \mathfrak{p}_{r1}\mathfrak{p}_{r2}$. Since

$$\mathcal{O}_K/\mathfrak{p}_{11} \cong \mathbb{Z}/p_1\mathbb{Z}, \ldots, \mathcal{O}_K/\mathfrak{p}_{r1} \cong \mathbb{Z}/p_r\mathbb{Z},$$

and since each $\mathfrak{p}_{i1}$ is unramified, one can check that

$$\mathcal{O}_K/\mathfrak{p}_{11}^{e_1} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z}, \ldots, \mathcal{O}_K/\mathfrak{p}_{r1}^{e_r} \cong \mathbb{Z}/p_r^{e_r}\mathbb{Z}.$$

The Heegner hypothesis

Proposition

Suppose that every prime p dividing N splits in K. Then there exists an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Proof.

Write $N = p_1^{e_1} \cdots p_r^{e_r}$ and suppose $p_1\mathcal{O}_K = \mathfrak{p}_{11}\mathfrak{p}_{12}, \quad \ldots, p_r\mathcal{O}_K = \mathfrak{p}_{r1}\mathfrak{p}_{r2}$. Since

$$\mathcal{O}_K/\mathfrak{p}_{11} \cong \mathbb{Z}/p_1\mathbb{Z}, \ldots, \mathcal{O}_K/\mathfrak{p}_{r1} \cong \mathbb{Z}/p_r\mathbb{Z},$$

and since each $\mathfrak{p}_{i1}$ is unramified, one can check that

$$\mathcal{O}_K/\mathfrak{p}_{11}^{e_1} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z}, \ldots, \mathcal{O}_K/\mathfrak{p}_{r1}^{e_r} \cong \mathbb{Z}/p_r^{e_r}\mathbb{Z}.$$

Set $\mathcal{N} = \mathfrak{p}_{11}^{e_1} \cdots \mathfrak{p}_{r1}^{e_r}$. Then

$$\mathcal{O}_K/\mathcal{N} \cong \mathcal{O}_K/\mathfrak{p}_{11}^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_{r1}^{e_r} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z} \cong \mathbb{Z}/N\mathbb{Z}.$$

Heegner hypothesis

Theorem

For a given N, there are infinitely many imaginary quadratic fields satisfying the Heegner hypothesis.

Heegner hypothesis

Theorem

For a given N, there are infinitely many imaginary quadratic fields satisfying the Heegner hypothesis.

Proof.

- For simplicity, we assume that $N = p$ and $p \equiv 1 \mod 4$.

Heegner hypothesis

Theorem

For a given N, there are infinitely many imaginary quadratic fields satisfying the Heegner hypothesis.

Proof.

- For simplicity, we assume that $N = p$ and $p \equiv 1 \mod 4$.
- By Dirichlet's theorem on primes in arithemtic progressions, there are infinitely many primes q such that $q \equiv 1 \mod p$.

Heegner hypothesis

Theorem

For a given N, there are infinitely many imaginary quadratic fields satisfying the Heegner hypothesis.

Proof.

- For simplicity, we assume that $N = p$ and $p \equiv 1 \mod 4$.
- By Dirichlet's theorem on primes in arithemtic progressions, there are infinitely many primes q such that $q \equiv 1 \mod p$.
- For each such q, $\left(\frac{q}{p}\right) = 1$.

Heegner hypothesis

Theorem

For a given N, there are infinitely many imaginary quadratic fields satisfying the Heegner hypothesis.

Proof.

- For simplicity, we assume that $N = p$ and $p \equiv 1 \bmod 4$.
- By Dirichlet's theorem on primes in arithemtic progressions, there are infinitely many primes q such that $q \equiv 1 \bmod p$.
- For each such q, $\left(\frac{q}{p}\right) = 1$.
- For each such q, $\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = 1$.

Heegner hypothesis

Theorem

For a given N, there are infinitely many imaginary quadratic fields satisfying the Heegner hypothesis.

Proof.

- For simplicity, we assume that $N = p$ and $p \equiv 1 \bmod 4$.
- By Dirichlet's theorem on primes in arithemtic progressions, there are infinitely many primes q such that $q \equiv 1 \bmod p$.
- For each such q, $\left(\frac{q}{p}\right) = 1$.
- For each such q, $\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = 1$.
- For each such q, p splits completely in $\mathbb{Q}(\sqrt{-q})$.

Heegner points of conductor n

- Fix an imaginary quadratic field K with discriminant D satisfying the Heegner hypothesis. Let $\mathcal{N}$ be an ideal such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Heegner points of conductor n

- Fix an imaginary quadratic field K with discriminant D satisfying the Heegner hypothesis. Let $\mathcal{N}$ be an ideal such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.
- Every order $\mathcal{O}$ is of the form $\mathcal{O} = \mathbb{Z} + n\mathcal{O}_K$ for some $n \geq 1$. Here n is called the conductor of $\mathcal{O}$ and we denote $\mathcal{O}$ by $\mathcal{O}_n$.

Heegner points of conductor n

- Fix an imaginary quadratic field K with discriminant D satisfying the Heegner hypothesis. Let $\mathcal{N}$ be an ideal such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.
- Every order $\mathcal{O}$ is of the form $\mathcal{O} = \mathbb{Z} + n\mathcal{O}_K$ for some $n \geq 1$. Here n is called the conductor of $\mathcal{O}$ and we denote $\mathcal{O}$ by $\mathcal{O}_n$.
- Let $\mathcal{N}_n := \mathcal{N} \cap \mathcal{O}_n$. For each n relatively prime to DN, one can check that $\mathcal{O}/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$.

Heegner points of conductor n

- Fix an imaginary quadratic field K with discriminant D satisfying the Heegner hypothesis. Let $\mathcal{N}$ be an ideal such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.
- Every order $\mathcal{O}$ is of the form $\mathcal{O} = \mathbb{Z} + n\mathcal{O}_K$ for some $n \geq 1$. Here n is called the conductor of $\mathcal{O}$ and we denote $\mathcal{O}$ by $\mathcal{O}_n$.
- Let $\mathcal{N}_n := \mathcal{N} \cap \mathcal{O}_n$. For each n relatively prime to DN, one can check that $\mathcal{O}/\mathcal{N}_n \cong \mathbb{Z}/N\mathbb{Z}$.

Definition

For each n relatively prime to ND, the Heegner point of conductor n is defined to be

$$x_n := [\mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathcal{N}_n^{-1}].$$

Heegner points lie in ring class fields

Proposition

The point $x_n \in X_0(N)(\mathbb{C})$ lies in $X_0(N)(H_n)$, where H_n is the ring class field of $\mathcal{O}_n$.

Heegner points lie in ring class fields

Proposition

The point $x_n \in X_0(N)(\mathbb{C})$ lies in $X_0(N)(H_n)$, where H_n is the ring class field of $\mathcal{O}_n$.

Proof.

By CM theory, $\mathbb{C}/\mathcal{O}_n$ is defined over H_n and

Heegner points lie in ring class fields

Proposition

The point $x_n \in X_0(N)(\mathbb{C})$ lies in $X_0(N)(H_n)$, where H_n is the ring class field of $\mathcal{O}_n$.

Proof.

By CM theory, $\mathbb{C}/\mathcal{O}_n$ is defined over H_n and so by the moduli interpretation, $x_n \in Y_0(N)(H_n) \subseteq X_0(N)(H_n)$. □

A reciprocity law

Note that $\mathrm{Gal}(H_n/K)$ acts on $X_0(N)(H_n)$. What is this action on Heegner points?

A reciprocity law

Note that $\mathrm{Gal}(H_n/K)$ acts on $X_0(N)(H_n)$. What is this action on Heegner points?

Theorem (Class field theory)

The map

$$Cl(\mathcal{O}) \to Gal(H_n/K), \quad [\mathfrak{a}] \mapsto \sigma_{\mathfrak{a}}$$

is an isomorphism of groups.

A reciprocity law

Note that $\mathrm{Gal}(H_n/K)$ acts on $X_0(N)(H_n)$. What is this action on Heegner points?

Theorem (Class field theory)

The map

$$Cl(\mathcal{O}) \to Gal(H_n/K), \quad [\mathfrak{a}] \mapsto \sigma_{\mathfrak{a}}$$

is an isomorphism of groups.

Theorem (A reciprocity law)

For $\sigma \in Gal(H_n/K)$ *and* $x_n = [\mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathcal{N}_n^{-1}] \in X_0(N)(H_n)$,

$$\sigma(x_n) = [\mathbb{C}/\mathfrak{a}_\sigma^{-1} \to \mathbb{C}/\mathfrak{a}_\sigma^{-1}\mathcal{N}_n^{-1}]$$

as elements of $X_0(N)(H_n)$.

Hecke correspondence

We let $\mathrm{Div}\ X_0(N)(H_n)$ to be the group of divisors which are stable under the action of $\mathrm{Gal}(\bar{K}/H_n)$.

Hecke correspondence

We let $\mathrm{Div}\ X_0(N)(H_n)$ to be the group of divisors which are stable under the action of $\mathrm{Gal}(\bar{K}/H_n)$. For p a prime not dividing N, we define a Hecke correspondence:

$$T_p : \mathrm{Div}\ X_0(N)(H_n) \to \mathrm{Div}\ X_0(N)(H_n)$$

Hecke correspondence

We let $\mathrm{Div}\ X_0(N)(H_n)$ to be the group of divisors which are stable under the action of $\mathrm{Gal}(\bar{K}/H_n)$. For p a prime not dividing N, we define a Hecke correspondence:

$$T_p : \mathrm{Div}\ X_0(N)(H_n) \to \mathrm{Div}\ X_0(N)(H_n)$$

by sending

$$[\phi : E \to E'] \mapsto \sum_{C \subseteq E[p], |C|=p} (E/C \to E'/\phi(C)).$$

and extending linearly.

Action of Hecke correspondence on Heegner points

Let n be a positive integer relatively prime to ND and let p be a prime not dividing nND.

Action of Hecke correspondence on Heegner points

Let n be a positive integer relatively prime to ND and let p be a prime not dividing nND. Define a trace map

$$\mathrm{Tr}_n : X_0(N)(H_{np}) \to X_0(N)(H_n), \quad z \mapsto \sum_{\sigma \in \mathrm{Gal}(H_{np}/H_n)} \sigma(z)$$

Action of Hecke correspondence on Heegner points

Let n be a positive integer relatively prime to ND and let p be a prime not dividing nND. Define a trace map

$$\mathrm{Tr}_n : X_0(N)(H_{np}) \to X_0(N)(H_n), \quad z \mapsto \sum_{\sigma \in \mathrm{Gal}(H_{np}/H_n)} \sigma(z)$$

Theorem

We have that $Tr_n(x_{np}) = T_p(x_n)$.

Definition of Heegner points on elliptic curves

Theorem (Shimura-Taniyama conjecture/Modularity theorem)

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N. Then there exists a non-zero morphism

$$\varphi : X_0(N) \to E.$$

defined over $\mathbb{Q}$.

Definition of Heegner points on elliptic curves

Theorem (Shimura-Taniyama conjecture/Modularity theorem)

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N. Then there exists a non-zero morphism

$$\varphi : X_0(N) \to E.$$

defined over $\mathbb{Q}$.

Definition

Let E be as above and let K be an imaginary quadratic field satisfying the Heegner hypothesis. Fix a modular parameterization φ as above. The Heegner point of conductor n is defined to be

$$y_n := \varphi(x_n).$$

Heegner points lie in ring class fields

Proposition

The point $y_n \in E(\mathbb{C})$ actually lies in $E(H_n)$.

Heegner points lie in ring class fields

Proposition

The point $y_n \in E(\mathbb{C})$ actually lies in $E(H_n)$.

Proof.

We know that x_n lies in $X_0(N)(H_n)$ and since φ is a morphism of algebraic curves defined over $\mathbb{Q}$, we conclude that y_n lies in $E(H_n)$. $\square$

Heegner points lie in ring class fields

Proposition

The point $y_n \in E(\mathbb{C})$ actually lies in $E(H_n)$.

Proof.

We know that x_n lies in $X_0(N)(H_n)$ and since φ is a morphism of algebraic curves defined over $\mathbb{Q}$, we conclude that y_n lies in $E(H_n)$. $\square$

Our work so far gives a systematic supply of points on elliptic curves defined over algebraic number fields.

Trace map on Heegner points

We define

$$\mathrm{Tr}_n : E(H_{np}) \to E(H_n), \quad z \mapsto \sum_{\sigma \in \mathrm{Gal}(H_{np}/H_n)} \sigma(z)$$

Trace map on Heegner points

We define

$$\mathrm{Tr}_n : E(H_{np}) \to E(H_n), \quad z \mapsto \sum_{\sigma \in \mathrm{Gal}(H_{np}/H_n)} \sigma(z)$$

Theorem

We have that $Tr(y_{np}) = a_p y_n$, *where* $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Trace map on Heegner points

We define

$$\mathrm{Tr}_n : E(H_{np}) \to E(H_n), \quad z \mapsto \sum_{\sigma \in \mathrm{Gal}(H_{np}/H_n)} \sigma(z)$$

Theorem

We have that $Tr(y_{np}) = a_p y_n$, *where* $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Proof.

By Eichler-Shimura theory, $\varphi \circ T_p = a_p \varphi$.

Trace map on Heegner points

We define

$$\mathrm{Tr}_n : E(H_{np}) \to E(H_n), \quad z \mapsto \sum_{\sigma \in \mathrm{Gal}(H_{np}/H_n)} \sigma(z)$$

Theorem

We have that $Tr(y_{np}) = a_p y_n$, *where* $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Proof.

By Eichler-Shimura theory, $\varphi \circ T_p = a_p \varphi$. So

$$\mathrm{Tr}_n(y_{np}) = \mathrm{Tr}_n(\varphi(x_{np}))$$

Trace map on Heegner points

We define

$$\mathrm{Tr}_n : E(H_{np}) \to E(H_n), \quad z \mapsto \sum_{\sigma \in \mathrm{Gal}(H_{np}/H_n)} \sigma(z)$$

Theorem

We have that $Tr(y_{np}) = a_p y_n$, *where* $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Proof.

By Eichler-Shimura theory, $\varphi \circ T_p = a_p \varphi$. So

$$\mathrm{Tr}_n(y_{np}) = \mathrm{Tr}_n(\varphi(x_{np})) = \varphi(\mathrm{Tr}_n(x_{np}))$$

Trace map on Heegner points

We define

$$\mathrm{Tr}_n : E(H_{np}) \to E(H_n), \quad z \mapsto \sum_{\sigma \in \mathrm{Gal}(H_{np}/H_n)} \sigma(z)$$

Theorem

We have that $Tr(y_{np}) = a_p y_n$, *where* $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Proof.

By Eichler-Shimura theory, $\varphi \circ T_p = a_p \varphi$. So

$$\mathrm{Tr}_n(y_{np}) = \mathrm{Tr}_n(\varphi(x_{np})) = \varphi(\mathrm{Tr}_n(x_{np})) = \varphi(T_p(x_n))$$

Trace map on Heegner points

We define

$$\mathrm{Tr}_n : E(H_{np}) \to E(H_n), \quad z \mapsto \sum_{\sigma \in \mathrm{Gal}(H_{np}/H_n)} \sigma(z)$$

Theorem

We have that $Tr(y_{np}) = a_p y_n$, *where* $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Proof.

By Eichler-Shimura theory, $\varphi \circ T_p = a_p \varphi$. So

$$\mathrm{Tr}_n(y_{np}) = \mathrm{Tr}_n(\varphi(x_{np})) = \varphi(\mathrm{Tr}_n(x_{np})) = \varphi(T_p(x_n)) = a_p(\varphi(x_n)) = a_p y_n.$$

□

The Basic Heegner point

Since the system $\{y_n\}$ satisfies these (and other) properties, this system is often called the 'Euler system of Heegner points'.

The Basic Heegner point

Since the system $\{y_n\}$ satisfies these (and other) properties, this system is often called the 'Euler system of Heegner points'. We define

$$y_K := \mathrm{tr}_{H_1/K}(y_1) = \sum_{\sigma \in \mathrm{Gal}(H_1/K)} \sigma(y_1) \in E(K)$$

and call it the Basic Heegner point.

Heegner points can be explicitly computed

Example

Let $E : y^2 = x^3 + 4x$ which has conductor 32. Let $K = \mathbb{Q}(\sqrt{-7})$. Then $H_1 = K$ and we can compute

$$y_K = \left(\frac{\sqrt{-7} - 1}{2}, \frac{\sqrt{-7} + 3}{2} \right) \in E(K).$$

Applications

Rational points on elliptic curves

Theorem (Mordell-Weil Theorem)

Let E be an elliptic curve defined over a number field K. Then the group $E(K)$ is a finitely generated abelian group

Rational points on elliptic curves

Theorem (Mordell-Weil Theorem)

Let E be an elliptic curve defined over a number field K. Then the group $E(K)$ is a finitely generated abelian group i.e.

$$E(K) \cong \mathbb{Z}^r \oplus \textit{finite group}$$

for some integer $r \geq 0$.

Rational points on elliptic curves

Theorem (Mordell-Weil Theorem)

Let E be an elliptic curve defined over a number field K. Then the group $E(K)$ is a finitely generated abelian group i.e.

$$E(K) \cong \mathbb{Z}^r \oplus \textit{finite group}$$

for some integer $r \geq 0$.

The integer r is often called the algebraic rank of E and will be denoted by $r_{\mathrm{al}}(E)$.

Height of a point on an elliptic curve

Let E be an elliptic curve defined over a number field K.

Definition (Naive height)

For $P \in E(K)$, define its naive height to be

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log \max\{|x|_v, |y|_v, |z|_v\},$$

where M_v is the set of (appropriately normalized) absolute values on K.

Height of a point on an elliptic curve

Let E be an elliptic curve defined over a number field K.

Definition (Naive height)

For $P \in E(K)$, define its naive height to be

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log \max\{|x|_v, |y|_v, |z|_v\},$$

where M_v is the set of (appropriately normalized) absolute values on K.

The definition of the naive height depends on the choice of the Weierstrass equation for E.

Neron-Tate height

Definition (Neron-Tate height)

For $P \in E(K)$, define the Neron-Tate height to be

$$\hat{h}(P) = \lim_{n \to \infty} \frac{h([2^n]P)}{4^n}.$$

Neron-Tate height

Definition (Neron-Tate height)

For $P \in E(K)$, define the Neron-Tate height to be

$$\hat{h}(P) = \lim_{n \to \infty} \frac{h([2^n]P)}{4^n}.$$

The definition of the Neron-Tate height does not depend on the choice of the Weierstrass equation for E.

Neron-Tate height

Definition (Neron-Tate height)

For $P \in E(K)$, define the Neron-Tate height to be

$$\hat{h}(P) = \lim_{n \to \infty} \frac{h([2^n]P)}{4^n}.$$

The definition of the Neron-Tate height does not depend on the choice of the Weierstrass equation for E.

Definition (Neron-Tate height pairing)

Define a pairing

$$\langle , \rangle : E(K) \times E(K) \to \mathbb{R}_{\geq 0}, \quad \langle P, Q \rangle = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)).$$

Neron-Tate height

Definition (Neron-Tate height)

For $P \in E(K)$, define the Neron-Tate height to be

$$\hat{h}(P) = \lim_{n \to \infty} \frac{h([2^n]P)}{4^n}.$$

The definition of the Neron-Tate height does not depend on the choice of the Weierstrass equation for E.

Definition (Neron-Tate height pairing)

Define a pairing

$$\langle , \rangle : E(K) \times E(K) \to \mathbb{R}_{\geq 0}, \quad \langle P, Q \rangle = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)).$$

Important fact: $\langle P, P \rangle = 0$ if and only if P is a torsion point.

The L-function of an elliptic curve

Definition

Let E be an elliptic curve defined over a number field K. We define its L-function to be

$$L(E,s) = \prod_{\mathfrak{p}:\text{good}} (1 - a_{\mathfrak{p}} N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-2s}) \prod_{\mathfrak{p}:\text{bad}} (1 - a_{\mathfrak{p}} N(\mathfrak{p})^{-s}),$$

where $a_{\mathfrak{p}} = p + 1 - \#E(\mathcal{O}_K/\mathfrak{p})$ if $\mathfrak{p}$ has good reduction and $a_{\mathfrak{p}} \in \{-1, 0, 1\}$ otherwise.

The L-function of an elliptic curve

Definition

Let E be an elliptic curve defined over a number field K. We define its L-function to be

$$L(E,s) = \prod_{\mathfrak{p}:\text{good}} (1 - a_{\mathfrak{p}} N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-2s}) \prod_{\mathfrak{p}:\text{bad}} (1 - a_{\mathfrak{p}} N(\mathfrak{p})^{-s}),$$

where $a_{\mathfrak{p}} = p + 1 - \#E(\mathcal{O}_K/\mathfrak{p})$ if $\mathfrak{p}$ has good reduction and $a_{\mathfrak{p}} \in \{-1, 0, 1\}$ otherwise.

$L(E,s)$ converges when $\mathrm{Re}(s) >> 0$ and is conjectured to have an analytic continuation to the entire complex plane.

The L-function of an elliptic curve

Definition

Let E be an elliptic curve defined over a number field K. We define its L-function to be

$$L(E,s) = \prod_{\mathfrak{p}:\text{good}} (1 - a_{\mathfrak{p}} N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-2s}) \prod_{\mathfrak{p}:\text{bad}} (1 - a_{\mathfrak{p}} N(\mathfrak{p})^{-s}),$$

where $a_{\mathfrak{p}} = p + 1 - \#E(\mathcal{O}_K/\mathfrak{p})$ if $\mathfrak{p}$ has good reduction and $a_{\mathfrak{p}} \in \{-1, 0, 1\}$ otherwise.

$L(E,s)$ converges when $\mathrm{Re}(s) >> 0$ and is conjectured to have an analytic continuation to the entire complex plane.

Definition

We define the analytic rank $r_{\mathrm{an}}(E) := \mathrm{ord}_{s=1} L(E,s)$ i.e.

The L-function of an elliptic curve

Definition

Let E be an elliptic curve defined over a number field K. We define its L-function to be

$$L(E,s) = \prod_{\mathfrak{p}:\text{good}} (1 - a_{\mathfrak{p}} N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-2s}) \prod_{\mathfrak{p}:\text{bad}} (1 - a_{\mathfrak{p}} N(\mathfrak{p})^{-s}),$$

where $a_{\mathfrak{p}} = p + 1 - \#E(\mathcal{O}_K/\mathfrak{p})$ if $\mathfrak{p}$ has good reduction and $a_{\mathfrak{p}} \in \{-1, 0, 1\}$ otherwise.

$L(E,s)$ converges when $\mathrm{Re}(s) >> 0$ and is conjectured to have an analytic continuation to the entire complex plane.

Definition

We define the analytic rank $r_{\mathrm{an}}(E) := \mathrm{ord}_{s=1} L(E,s)$ i.e.

$$L(E,s) = c(s-1)^{r_{\mathrm{an}}} + \cdots$$

The Birch and Swinnerton-Dyer conjecture

The BSD conjecture

Let E be an elliptic curve defined over a number field K. Then

$$r_{\mathrm{al}}(E) = r_{\mathrm{an}}(E).$$

The Gross-Zagier formula

Theorem

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. Let E_K denote the elliptic curve E over K.

The Gross-Zagier formula

Theorem

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. Let E_K denote the elliptic curve E over K. Then we have

$$L'(E_K, 1) = c_{E,K} \cdot \langle y_K, y_K \rangle$$

where $c_{E,K} \in \mathbb{C}$ is some constant depending on E and K.

The Gross-Zagier formula

Theorem

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. Let E_K denote the elliptic curve E over K. Then we have

$$L'(E_K, 1) = c_{E,K} \cdot \langle y_K, y_K \rangle$$

where $c_{E,K} \in \mathbb{C}$ is some constant depending on E and K.

This formula has the shape:

Derivative of L-function $=$ **Height of Heegner point**

The Gross-Zagier formula

Theorem

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. Let E_K denote the elliptic curve E over K. Then we have

$$L'(E_K, 1) = c_{E,K} \cdot \langle y_K, y_K \rangle$$

where $c_{E,K} \in \mathbb{C}$ is some constant depending on E and K.

This formula has the shape:

Derivative of L-function $=$ **Height of Heegner point**

Corollary

We have that $r_{an}(E_K) = 1 \implies r_{al}(E_K) \geq 1$.

The Gross-Zagier formula

Theorem

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. Let E_K denote the elliptic curve E over K. Then we have

$$L'(E_K, 1) = c_{E,K} \cdot \langle y_K, y_K \rangle$$

where $c_{E,K} \in \mathbb{C}$ is some constant depending on E and K.

This formula has the shape:

Derivative of L-function $=$ **Height of Heegner point**

Corollary

We have that $r_{an}(E_K) = 1 \implies r_{al}(E_K) \geq 1$.

Proof.

$r_{\mathrm{an}}(E_K) = 1 \implies L'(E_K, 1) \neq 0$

The Gross-Zagier formula

Theorem

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. Let E_K denote the elliptic curve E over K. Then we have

$$L'(E_K, 1) = c_{E,K} \cdot \langle y_K, y_K \rangle$$

where $c_{E,K} \in \mathbb{C}$ is some constant depending on E and K.

This formula has the shape:

Derivative of L-function $=$ **Height of Heegner point**

Corollary

We have that $r_{an}(E_K) = 1 \implies r_{al}(E_K) \geq 1$.

Proof.

$r_{\mathrm{an}}(E_K) = 1 \implies L'(E_K, 1) \neq 0$

The Gross-Zagier formula

Theorem

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. Let E_K denote the elliptic curve E over K. Then we have

$$L'(E_K, 1) = c_{E,K} \cdot \langle y_K, y_K \rangle$$

where $c_{E,K} \in \mathbb{C}$ is some constant depending on E and K.

This formula has the shape:

Derivative of L-function $=$ **Height of Heegner point**

Corollary

We have that $r_{an}(E_K) = 1 \implies r_{al}(E_K) \geq 1$.

Proof.

$r_{\mathrm{an}}(E_K) = 1 \implies L'(E_K, 1) \neq 0 \implies \langle y_K, y_K \rangle \neq 0$

The Gross-Zagier formula

Theorem

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. Let E_K denote the elliptic curve E over K. Then we have

$$L'(E_K, 1) = c_{E,K} \cdot \langle y_K, y_K \rangle$$

where $c_{E,K} \in \mathbb{C}$ is some constant depending on E and K.

This formula has the shape:

Derivative of L-function $=$ **Height of Heegner point**

Corollary

We have that $r_{an}(E_K) = 1 \implies r_{al}(E_K) \geq 1$.

Proof.

$r_{\mathrm{an}}(E_K) = 1 \implies L'(E_K, 1) \neq 0 \implies \langle y_K, y_K \rangle \neq 0 \implies y_K$ non-torsion point

The Gross-Zagier formula

Theorem

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. Let E_K denote the elliptic curve E over K. Then we have

$$L'(E_K, 1) = c_{E,K} \cdot \langle y_K, y_K \rangle$$

where $c_{E,K} \in \mathbb{C}$ is some constant depending on E and K.

This formula has the shape:

Derivative of L-function $=$ **Height of Heegner point**

Corollary

We have that $r_{an}(E_K) = 1 \implies r_{al}(E_K) \geq 1$.

Proof.

$r_{\mathrm{an}}(E_K) = 1 \implies L'(E_K, 1) \neq 0 \implies \langle y_K, y_K \rangle \neq 0 \implies y_K$ non-torsion point $\implies r_{\mathrm{al}}(E_K) \geq 1$. □

Remarks on the Gross-Zagier formula

Theorem (Kolyvagin)

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. If y_K has infinite order in $E(K)$, then $r_{al}(E_K) = 1$.

Remarks on the Gross-Zagier formula

Theorem (Kolyvagin)

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. If y_K has infinite order in $E(K)$, then $r_{al}(E_K) = 1$.

Thus, Gross-Zagier+Kolyvagin give:

$$r_{\mathrm{an}}(E_K) = 1 \implies r_{\mathrm{al}}(E_K) = 1.$$

Remarks on the Gross-Zagier formula

Theorem (Kolyvagin)

Let E be an elliptic curve over $\mathbb{Q}$ and let K be an imaginary quadratic field which satisfies the Heegner hypothesis. If y_K has infinite order in $E(K)$, then $r_{al}(E_K) = 1$.

Thus, Gross-Zagier+Kolyvagin give:

$$r_{\mathrm{an}}(E_K) = 1 \implies r_{\mathrm{al}}(E_K) = 1.$$

It is possible to use "descent" to prove the following:

$$r_{\mathrm{an}}(E) = 1 \implies r_{\mathrm{al}}(E) = 1.$$

Thank You!