Elliptic Curves and the Special Values of L-functions

ICTS, 2021

Introduction to Elliptic Curves: Lecture 2

Anupam Saikia

Department of Mathematics,
Indian Institute of Technology Guwahati

Sections

Sections

Height of a Point

- The notion of height is very useful in theory of elliptic curves. In this lecture, we will see its application in proving the Mordell-Weil Theorem. It also leads to the notion of regulator ('volume') associated with the Mordell-Weil group of an elliptic curve.
- Roughly speaking, '*the height of a rational point measures how complicated the point is from the viewpoint of number theory*'. For a rational number $x = \frac{m}{n}$ in its lowest form, we can define its height as

$$H(x) = \max\{|\ m\ |,\ |\ n\ |\}.$$

  For example, $H(1) = 1$, and $H(\frac{999}{1000}) = 1000$.
- For any given number B, the set $\{x \in \mathbb{Q} \mid H(x) \leq B\}$ is finite.
- For a point $P = (x, y) \in E(\mathbb{Q})$ on an elliptic curve $E/\mathbb{Q}$, we define

$$H(P) = H(x) \text{ for } P \neq \mathcal{O}, \qquad H(\mathcal{O}) = 1.$$

- The notion of height can be extended to points defined over any algebraic extension K of $\mathbb{Q}$ (see AEC, Ch VIII).

Height of a Point

- The notion of height is very useful in theory of elliptic curves. In this lecture, we will see its application in proving the Mordell-Weil Theorem. It also leads to the notion of regulator ('volume') associated with the Mordell-Weil group of an elliptic curve.

- Roughly speaking, '*the height of a rational point measures how complicated the point is from the viewpoint of number theory*'. For a rational number $x = \frac{m}{n}$ in its lowest form, we can define its height as

$$H(x) = \max\{|\, m \,|,\ |\, n \,|\}.$$

For example, $H(1) = 1$, and $H(\frac{999}{1000}) = 1000$.

- For any given number B, the set $\{x \in \mathbb{Q} \mid H(x) \leq B\}$ is finite.

- For a point $P = (x, y) \in E(\mathbb{Q})$ on an elliptic curve $E/\mathbb{Q}$, we define

$$H(P) = H(x) \text{ for } P \neq \mathcal{O}, \qquad H(\mathcal{O}) = 1.$$

- The notion of height can be extended to points defined over any algebraic extension K of $\mathbb{Q}$ (see AEC, Ch VIII).

Height of a Point

- The notion of height is very useful in theory of elliptic curves. In this lecture, we will see its application in proving the Mordell-Weil Theorem. It also leads to the notion of regulator ('volume') associated with the Mordell-Weil group of an elliptic curve.

- Roughly speaking, '*the height of a rational point measures how complicated the point is from the viewpoint of number theory*'. For a rational number $x = \frac{m}{n}$ in its lowest form, we can define its height as

$$H(x) = \max\{|\, m \,|,\ |\, n \,|\}.$$

  For example, $H(1) = 1$, and $H(\frac{999}{1000}) = 1000$.

- For any given number B, the set $\{x \in \mathbb{Q} \mid H(x) \leq B\}$ is finite.

- For a point $P = (x, y) \in E(\mathbb{Q})$ on an elliptic curve $E/\mathbb{Q}$, we define

$$H(P) = H(x) \text{ for } P \neq \mathcal{O}, \qquad H(\mathcal{O}) = 1.$$

- The notion of height can be extended to points defined over any algebraic extension K of $\mathbb{Q}$ (see AEC, Ch VIII).

Height of a Point

- The notion of height is very useful in theory of elliptic curves. In this lecture, we will see its application in proving the Mordell-Weil Theorem. It also leads to the notion of regulator ('volume') associated with the Mordell-Weil group of an elliptic curve.
- Roughly speaking, '*the height of a rational point measures how complicated the point is from the viewpoint of number theory*'. For a rational number $x = \frac{m}{n}$ in its lowest form, we can define its height as

$$H(x) = \max\{| m |, | n |\}.$$

For example, $H(1) = 1$, and $H(\frac{999}{1000}) = 1000$.

- For any given number B, the set $\{x \in \mathbb{Q} \mid H(x) \leq B\}$ is finite.
- For a point $P = (x, y) \in E(\mathbb{Q})$ on an elliptic curve $E/\mathbb{Q}$, we define

$$H(P) = H(x) \text{ for } P \neq \mathcal{O}, \qquad H(\mathcal{O}) = 1.$$

- The notion of height can be extended to points defined over any algebraic extension K of $\mathbb{Q}$ (see AEC, Ch VIII).

Height of a Point

- The notion of height is very useful in theory of elliptic curves. In this lecture, we will see its application in proving the Mordell-Weil Theorem. It also leads to the notion of regulator ('volume') associated with the Mordell-Weil group of an elliptic curve.
- Roughly speaking, '*the height of a rational point measures how complicated the point is from the viewpoint of number theory*'. For a rational number $x = \frac{m}{n}$ in its lowest form, we can define its height as
$$H(x) = \max\{\mid m \mid, \ \mid n \mid\}.$$
For example, $H(1) = 1$, and $H(\frac{999}{1000}) = 1000$.
- For any given number B, the set $\{x \in \mathbb{Q} \mid H(x) \leq B\}$ is finite.
- For a point $P = (x, y) \in E(\mathbb{Q})$ on an elliptic curve $E/\mathbb{Q}$, we define
$$H(P) = H(x) \text{ for } P \neq \mathcal{O}, \qquad H(\mathcal{O}) = 1.$$
- The notion of height can be extended to points defined over any algebraic extension K of $\mathbb{Q}$ (see AEC, Ch VIII).

Height of a Point

- The notion of height is very useful in theory of elliptic curves. In this lecture, we will see its application in proving the Mordell-Weil Theorem. It also leads to the notion of regulator ('volume') associated with the Mordell-Weil group of an elliptic curve.
- Roughly speaking, '*the height of a rational point measures how complicated the point is from the viewpoint of number theory*'. For a rational number $x = \frac{m}{n}$ in its lowest form, we can define its height as

$$H(x) = \max\{|\ m\ |,\ |\ n\ |\}.$$

For example, $H(1) = 1$, and $H(\frac{999}{1000}) = 1000$.

- For any given number B, the set $\{x \in \mathbb{Q} \mid H(x) \leq B\}$ is finite.
- For a point $P = (x, y) \in E(\mathbb{Q})$ on an elliptic curve $E/\mathbb{Q}$, we define

$$H(P) = H(x) \text{ for } P \neq \mathcal{O}, \qquad H(\mathcal{O}) = 1.$$

- The notion of height can be extended to points defined over any algebraic extension K of $\mathbb{Q}$ (see AEC, Ch VIII).

Height of a Point

- The notion of height is very useful in theory of elliptic curves. In this lecture, we will see its application in proving the Mordell-Weil Theorem. It also leads to the notion of regulator ('volume') associated with the Mordell-Weil group of an elliptic curve.
- Roughly speaking, '*the height of a rational point measures how complicated the point is from the viewpoint of number theory*'. For a rational number $x = \frac{m}{n}$ in its lowest form, we can define its height as

$$H(x) = \max\{| m |, | n |\}.$$

For example, $H(1) = 1$, and $H(\frac{999}{1000}) = 1000$.

- For any given number B, the set $\{x \in \mathbb{Q} \mid H(x) \leq B\}$ is finite.
- For a point $P = (x, y) \in E(\mathbb{Q})$ on an elliptic curve $E/\mathbb{Q}$, we define

$$H(P) = H(x) \text{ for } P \neq \mathcal{O}, \qquad H(\mathcal{O}) = 1.$$

- The notion of height can be extended to points defined over any algebraic extension K of $\mathbb{Q}$ (see AEC, Ch VIII).

Height of a Point

- The notion of height is very useful in theory of elliptic curves. In this lecture, we will see its application in proving the Mordell-Weil Theorem. It also leads to the notion of regulator ('volume') associated with the Mordell-Weil group of an elliptic curve.
- Roughly speaking, '*the height of a rational point measures how complicated the point is from the viewpoint of number theory*'. For a rational number $x = \frac{m}{n}$ in its lowest form, we can define its height as

$$H(x) = \max\{\mid m \mid, \mid n \mid\}.$$

  For example, $H(1) = 1$, and $H(\frac{999}{1000}) = 1000$.
- For any given number B, the set $\{x \in \mathbb{Q} \mid H(x) \leq B\}$ is finite.
- For a point $P = (x, y) \in E(\mathbb{Q})$ on an elliptic curve $E/\mathbb{Q}$, we define

$$H(P) = H(x) \text{ for } P \neq \mathcal{O}, \qquad H(\mathcal{O}) = 1.$$

- The notion of height can be extended to points defined over any algebraic extension K of $\mathbb{Q}$ (see AEC, Ch VIII).

Height of a Point

- The notion of height is very useful in theory of elliptic curves. In this lecture, we will see its application in proving the Mordell-Weil Theorem. It also leads to the notion of regulator ('volume') associated with the Mordell-Weil group of an elliptic curve.
- Roughly speaking, '*the height of a rational point measures how complicated the point is from the viewpoint of number theory*'. For a rational number $x = \frac{m}{n}$ in its lowest form, we can define its height as

$$H(x) = \max\{|\, m \,|, \ |\, n \,|\}.$$

  For example, $H(1) = 1$, and $H(\frac{999}{1000}) = 1000$.
- For any given number B, the set $\{x \in \mathbb{Q} \mid H(x) \leq B\}$ is finite.
- For a point $P = (x, y) \in E(\mathbb{Q})$ on an elliptic curve $E/\mathbb{Q}$, we define

$$H(P) = H(x) \text{ for } P \neq \mathcal{O}, \qquad H(\mathcal{O}) = 1.$$

- The notion of height can be extended to points defined over any algebraic extension K of $\mathbb{Q}$ (see AEC, Ch VIII).

Logarithmic Height

- It is more convenient to use logarithmic height $h(P)$ so that $h(P+Q)$ can be compared nicely with $h(P)$ and $h(Q)$. The (absolute) logarithmic height is defined as

$$h(P) := \log H(P) \qquad \forall P \in E(\overline{\mathbb{Q}}).$$

- **Lemma 1**: Let E be an elliptic curve over a number filed K. For any real number B, the set

$$\{P \in E(K) \mid h(P) \leq B\}$$

is finite.

- **Lemma 2**: Let P_0 be a fixed point on $E(K)$. Then there exists a constant c_0 depending on E and P_0 such that

$$h(P+P_0) \leq 2h(P) + c_0 \qquad \forall P \in E(K).$$

Logarithmic Height

- It is more convenient to use logarithmic height $h(P)$ so that $h(P+Q)$ can be compared nicely with $h(P)$ and $h(Q)$. The (absolute) logarithmic height is defined as

$$h(P) := \log H(P) \qquad \forall P \in E(\overline{\mathbb{Q}}).$$

- **Lemma 1**: Let E be an elliptic curve over a number filed K. For any real number B, the set

$$\{P \in E(K) \mid h(P) \leq B\}$$

is finite.

- **Lemma 2**: Let P_0 be a fixed point on $E(K)$. Then there exists a constant c_0 depending on E and P_0 such that

$$h(P+P_0) \leq 2h(P) + c_0 \qquad \forall P \in E(K).$$

Logarithmic Height

- It is more convenient to use logarithmic height $h(P)$ so that $h(P+Q)$ can be compared nicely with $h(P)$ and $h(Q)$. The (absolute) logarithmic height is defined as

$$h(P) := \log H(P) \qquad \forall P \in E(\overline{\mathbb{Q}}).$$

- **Lemma 1**: Let E be an elliptic curve over a number filed K. For any real number B, the set

$$\{P \in E(K) \mid h(P) \leq B\}$$

is finite.

- **Lemma 2**: Let P_0 be a fixed point on $E(K)$. Then there exists a constant c_0 depending on E and P_0 such that

$$h(P+P_0) \leq 2h(P) + c_0 \qquad \forall P \in E(K).$$

Logarithmic Height

- It is more convenient to use logarithmic height $h(P)$ so that $h(P+Q)$ can be compared nicely with $h(P)$ and $h(Q)$. The (absolute) logarithmic height is defined as

$$h(P) := \log H(P) \qquad \forall P \in E(\overline{\mathbb{Q}}).$$

- **Lemma 1**: Let E be an elliptic curve over a number filed K. For any real number B, the set

$$\{P \in E(K) \mid h(P) \leq B\}$$

is finite.

- **Lemma 2**: Let P_0 be a fixed point on $E(K)$. Then there exists a constant c_0 depending on E and P_0 such that

$$h(P+P_0) \leq 2h(P) + c_0 \qquad \forall P \in E(K).$$

The Canonical Height

- **Lemma 3**: There is a constant c depending on E such that

$$h(2P) \geq 4h(P) - c \qquad \forall P \in E(K).$$

- It is not difficult to show by induction that the logarithmic height function behaves almost likes a quadratic function, i.e,

$$h([n]P) = n^2 h(P) + O(1).$$

- A natural question arises whether one can find an actual quadratic form that differs from h by a bounded amount, and an affirmative answer is the notion of canonical height provided by work of Neron and Tate.

- The canonical height $\hat{h}(P)$ is defined as the function

$$\hat{h} : E(\overline{K}) \longrightarrow \mathbb{R}, \qquad \hat{h}(P) := \lim_{n \to \infty} 4^{-n} h([2^n]P).$$

The Canonical Height

- **Lemma 3**: There is a constant c depending on E such that

$$h(2P) \geq 4h(P) - c \qquad \forall P \in E(K).$$

- It is not difficult to show by induction that the logarithmic height function behaves almost likes a quadratic function, i.e,

$$h([n]P) = n^2 h(P) + O(1).$$

- A natural question arises whether one can find an actual quadratic form that differs from h by a bounded amount, and an affirmative answer is the notion of canonical height provided by work of Neron and Tate.

- The canonical height $\hat{h}(P)$ is defined as the function

$$\hat{h} : E(\overline{K}) \longrightarrow \mathbb{R}, \qquad \hat{h}(P) := \lim_{n \to \infty} 4^{-n} h([2^n]P).$$

The Canonical Height

- **Lemma 3**: There is a constant c depending on E such that

$$h(2P) \geq 4h(P) - c \qquad \forall P \in E(K).$$

- It is not difficult to show by induction that the logarithmic height function behaves almost likes a quadratic function, i.e,

$$h([n]P) = n^2 h(P) + O(1).$$

- A natural question arises whether one can find an actual quadratic form that differs from h by a bounded amount, and an affirmative answer is the notion of canonical height provided by work of Neron and Tate.

- The canonical height $\hat{h}(P)$ is defined as the function

$$\hat{h} : E(\overline{K}) \longrightarrow \mathbb{R}, \qquad \hat{h}(P) := \lim_{n \to \infty} 4^{-n} h([2^n]P).$$

The Canonical Height

- **Lemma 3**: There is a constant c depending on E such that

$$h(2P) \geq 4h(P) - c \qquad \forall P \in E(K).$$

- It is not difficult to show by induction that the logarithmic height function behaves almost likes a quadratic function, i.e,

$$h([n]P) = n^2 h(P) + O(1).$$

- A natural question arises whether one can find an actual quadratic form that differs from h by a bounded amount, and an affirmative answer is the notion of canonical height provided by work of Neron and Tate.

- The canonical height $\hat{h}(P)$ is defined as the function

$$\hat{h} : E(\overline{K}) \longrightarrow \mathbb{R}, \qquad \hat{h}(P) := \lim_{n \to \infty} 4^{-n} h([2^n]P).$$

Properties of the Canonical Height

Let E be an elliptic curve over a number field K with algebraic closure $\overline{K}$. The canonical height $\hat{h}$ of Neron and Tate on E satisfies the following properties:

(a) $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q) \qquad \forall P, Q \in E(\overline{K})$.

(b) $\hat{h}([n]P) = n^2\hat{h}(P) \qquad \forall P \in E(\overline{K}), \qquad \forall n \in \mathbb{Z}$.

(c) $\hat{h}$ gives rise to the Neron-Tate height pairing

$$\langle , \rangle : E(\overline{K}) \times E(\overline{K}) \longrightarrow \mathbb{R}, \qquad \langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

(d) $\hat{h}(P) \geq 0$ for all $P \in E(\overline{K})$, and $\hat{h}(P) = 0$ if and only if P is a torsion point.

(e) $\hat{h} = h + O(1)$.

(f) Any function satisfying the properties above is unique.

Properties of the Canonical Height

Let E be an elliptic curve over a number field K with algebraic closure $\overline{K}$. The canonical height $\hat{h}$ of Neron and Tate on E satisfies the following properties:

(a) $\hat{h}(P+Q)+\hat{h}(P-Q)=2\hat{h}(P)+2\hat{h}(Q) \qquad \forall P,Q \in E(\overline{K})$.

(b) $\hat{h}([n]P)=n^2\hat{h}(P) \qquad \forall P \in E(\overline{K}), \qquad \forall n \in \mathbb{Z}$.

(c) $\hat{h}$ gives rise to the Neron-Tate height pairing

$$\langle , \rangle : E(\overline{K}) \times E(\overline{K}) \longrightarrow \mathbb{R}, \qquad \langle P,Q \rangle = \hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q).$$

(d) $\hat{h}(P) \geq 0$ for all $P \in E(\overline{K})$, and $\hat{h}(P)=0$ if and only if P is a torsion point.

(e) $\hat{h}=h+O(1)$.

(f) Any function satisfying the properties above is unique.

Properties of the Canonical Height

Let E be an elliptic curve over a number field K with algebraic closure $\overline{K}$. The canonical height $\hat{h}$ of Neron and Tate on E satisfies the following properties:

(a) $\hat{h}(P+Q)+\hat{h}(P-Q)=2\hat{h}(P)+2\hat{h}(Q) \qquad \forall P,Q \in E(\overline{K})$.

(b) $\hat{h}([n]P)=n^2\hat{h}(P) \qquad \forall P \in E(\overline{K}), \qquad \forall n \in \mathbb{Z}$.

(c) $\hat{h}$ gives rise to the Neron-Tate height pairing

$$\langle , \rangle : E(\overline{K}) \times E(\overline{K}) \longrightarrow \mathbb{R}, \qquad \langle P,Q\rangle = \hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q).$$

(d) $\hat{h}(P) \geq 0$ for all $P \in E(\overline{K})$, and $\hat{h}(P)=0$ if and only if P is a torsion point.

(e) $\hat{h}=h+O(1)$.

(f) Any function satisfying the properties above is unique.

Properties of the Canonical Height

Let E be an elliptic curve over a number field K with algebraic closure $\overline{K}$. The canonical height $\hat{h}$ of Neron and Tate on E satisfies the following properties:

(a) $\hat{h}(P+Q)+\hat{h}(P-Q)=2\hat{h}(P)+2\hat{h}(Q) \qquad \forall P, Q \in E(\overline{K})$.

(b) $\hat{h}([n]P)=n^2\hat{h}(P) \qquad \forall P \in E(\overline{K}), \qquad \forall n \in \mathbb{Z}$.

(c) $\hat{h}$ gives rise to the Neron-Tate height pairing

$$\langle , \rangle : E(\overline{K}) \times E(\overline{K}) \longrightarrow \mathbb{R}, \qquad \langle P, Q\rangle = \hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q).$$

(d) $\hat{h}(P) \geq 0$ for all $P \in E(\overline{K})$, and $\hat{h}(P)=0$ if and only if P is a torsion point.

(e) $\hat{h}=h+O(1)$.

(f) Any function satisfying the properties above is unique.

Properties of the Canonical Height

Let E be an elliptic curve over a number field K with algebraic closure $\overline{K}$. The canonical height $\hat{h}$ of Neron and Tate on E satisfies the following properties:

(a) $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q) \qquad \forall P, Q \in E(\overline{K})$.

(b) $\hat{h}([n]P) = n^2\hat{h}(P) \qquad \forall P \in E(\overline{K}), \qquad \forall n \in \mathbb{Z}$.

(c) $\hat{h}$ gives rise to the Neron-Tate height pairing

$$\langle , \rangle : E(\overline{K}) \times E(\overline{K}) \longrightarrow \mathbb{R}, \qquad \langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

(d) $\hat{h}(P) \geq 0$ for all $P \in E(\overline{K})$, and $\hat{h}(P) = 0$ if and only if P is a torsion point.

(e) $\hat{h} = h + O(1)$.

(f) Any function satisfying the properties above is unique.

Properties of the Canonical Height

Let E be an elliptic curve over a number field K with algebraic closure $\overline{K}$. The canonical height $\hat{h}$ of Neron and Tate on E satisfies the following properties:

(a) $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q) \qquad \forall P, Q \in E(\overline{K})$.

(b) $\hat{h}([n]P) = n^2\hat{h}(P) \qquad \forall P \in E(\overline{K}), \qquad \forall n \in \mathbb{Z}$.

(c) $\hat{h}$ gives rise to the Neron-Tate height pairing

$$\langle , \rangle : E(\overline{K}) \times E(\overline{K}) \longrightarrow \mathbb{R}, \qquad \langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

(d) $\hat{h}(P) \geq 0$ for all $P \in E(\overline{K})$, and $\hat{h}(P) = 0$ if and only if P is a torsion point.

(e) $\hat{h} = h + O(1)$.

(f) Any function satisfying the properties above is unique.

Properties of the Canonical Height

Let E be an elliptic curve over a number field K with algebraic closure $\overline{K}$. The canonical height $\hat{h}$ of Neron and Tate on E satisfies the following properties:

(a) $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q) \qquad \forall P, Q \in E(\overline{K})$.

(b) $\hat{h}([n]P) = n^2\hat{h}(P) \qquad \forall P \in E(\overline{K}), \qquad \forall n \in \mathbb{Z}$.

(c) $\hat{h}$ gives rise to the Neron-Tate height pairing

$$\langle , \rangle : E(\overline{K}) \times E(\overline{K}) \longrightarrow \mathbb{R}, \qquad \langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

(d) $\hat{h}(P) \geq 0$ for all $P \in E(\overline{K})$, and $\hat{h}(P) = 0$ if and only if P is a torsion point.

(e) $\hat{h} = h + O(1)$.

(f) Any function satisfying the properties above is unique.

Sections

Sections

The Notion of Height

Sketch of the Proof of Mordell-Weil Theorem

Elliptic Curves over Complex Numbers

- The Weak Mordell-Weil Theorem: Let E be an elliptic curve over a number field K. Then the quotient group $E(K)/2E(K)$ is finite.

  This theorem can be proved by embedding $E(K)/2E(K)$ in a subgroup of the Galois cohomology group $H^1(\mathrm{Gal}(\bar{K}/K), E[2])$, consisting of classes that satisfy certain local conditions. The subgroup is called the 2-Selmer groups, which turns out to be finite.

- We sketch the proof of Mordell-Weil Theorem using the weak version and the canonical height function $\hat{h}$. Observe that
  1. $\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h([2^n]P) \implies \hat{h}([2]P) = 4\hat{h}(P)$.
  2. For any given real number B, the set

$$\{P \in E(K) \mid \hat{h}(P) \leq B\}$$

  is finite, which clearly follows from the finiteness of such set with respect to the height $h(P) = \log\big(\mid H(P) \mid\big)$ and the fact that $\mid \hat{h}(P) - h(P) \mid$ is bounded for all $P \in E(K)$.

The Weak Mordell-Weil Theorem

- The Weak Mordell-Weil Theorem: Let E be an elliptic curve over a number field K. Then the quotient group $E(K)/2E(K)$ is finite.

  This theorem can be proved by embedding $E(K)/2E(K)$ in a subgroup of the Galois cohomology group $H^1(\mathrm{Gal}(\bar{K}/K), E[2])$, consisting of classes that satisfy certain local conditions. The subgroup is called the 2-Selmer groups, which turns out to be finite.

- We sketch the proof of Mordell-Weil Theorem using the weak version and the canonical height function $\hat{h}$. Observe that
  1. $\hat{h}(P) = \lim_{n\to\infty} 4^{-n}h([2^n]P) \implies \hat{h}([2]P) = 4\hat{h}(P)$.
  2. For any given real number B, the set

     $$\{P \in E(K) \mid \hat{h}(P) \leq B\}$$

     is finite, which clearly follows from the finiteness of such set with respect to the height $h(P) = \log\left(\mid H(P) \mid \right)$ and the fact that $\mid \hat{h}(P) - h(P) \mid$ is bounded for all $P \in E(K)$.

The Weak Mordell-Weil Theorem

- The Weak Mordell-Weil Theorem: Let E be an elliptic curve over a number field K. Then the quotient group $E(K)/2E(K)$ is finite.

  This theorem can be proved by embedding $E(K)/2E(K)$ in a subgroup of the Galois cohomology group $H^1(\text{Gal}(\bar{K}/K), E[2])$, consisting of classes that satisfy certain local conditions. The subgroup is called the 2-Selmer groups, which turns out to be finite.

- We sketch the proof of Mordell-Weil Theorem using the weak version and the canonical height function $\hat{h}$. Observe that
  1. $\hat{h}(P) = \lim_{n\to\infty} 4^{-n}h([2^n]P) \implies \hat{h}([2]P) = 4\hat{h}(P)$.
  2. For any given real number B, the set

  $$\{P \in E(K) \mid \hat{h}(P) \leq B\}$$

  is finite, which clearly follows from the finiteness of such set with respect to the height $h(P) = \log\left(\mid H(P) \mid\right)$ and the fact that $\mid \hat{h}(P) - h(P) \mid$ is bounded for all $P \in E(K)$.

The Weak Mordell-Weil Theorem

- The Weak Mordell-Weil Theorem: Let E be an elliptic curve over a number field K. Then the quotient group $E(K)/2E(K)$ is finite.

  This theorem can be proved by embedding $E(K)/2E(K)$ in a subgroup of the Galois cohomology group $H^1(\text{Gal}(\bar{K}/K), E[2])$, consisting of classes that satisfy certain local conditions. The subgroup is called the 2-Selmer groups, which turns out to be finite.

- We sketch the proof of Mordell-Weil Theorem using the weak version and the canonical height function $\hat{h}$. Observe that

  1. $\hat{h}(P) = \lim_{n\to\infty} 4^{-n}h([2^n]P) \implies \hat{h}([2]P) = 4\hat{h}(P)$.
  2. For any given real number B, the set

  $$\{P \in E(K) \mid \hat{h}(P) \le B\}$$

  is finite, which clearly follows from the finiteness of such set with respect to the height $h(P) = \log\left(\mid H(P) \mid\right)$ and the fact that $\mid \hat{h}(P) - h(P) \mid$ is bounded for all $P \in E(K)$.

The Weak Mordell-Weil Theorem

- The Weak Mordell-Weil Theorem: Let E be an elliptic curve over a number field K. Then the quotient group $E(K)/2E(K)$ is finite.

  This theorem can be proved by embedding $E(K)/2E(K)$ in a subgroup of the Galois cohomology group $H^1(\text{Gal}(\bar{K}/K), E[2])$, consisting of classes that satisfy certain local conditions. The subgroup is called the 2-Selmer groups, which turns out to be finite.

- We sketch the proof of Mordell-Weil Theorem using the weak version and the canonical height function $\hat{h}$. Observe that
  1. $\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h([2^n]P) \implies \hat{h}([2]P) = 4\hat{h}(P)$.
  2. For any given real number B, the set

$$\{P \in E(K) \mid \hat{h}(P) \leq B\}$$

     is finite, which clearly follows from the finiteness of such set with respect to the height $h(P) = \log\left(\mid H(P) \mid \right)$ and the fact that $\mid \hat{h}(P) - h(P) \mid$ is bounded for all $P \in E(K)$.

The Weak Mordell-Weil Theorem

- **The Weak Mordell-Weil Theorem**: Let E be an elliptic curve over a number field K. Then the quotient group $E(K)/2E(K)$ is finite.

  This theorem can be proved by embedding $E(K)/2E(K)$ in a subgroup of the Galois cohomology group $H^1(\text{Gal}(\bar{K}/K), E[2])$, consisting of classes that satisfy certain local conditions. The subgroup is called the 2-Selmer groups, which turns out to be finite.

- We sketch the proof of Mordell-Weil Theorem using the weak version and the canonical height function $\hat{h}$. Observe that
  1. $\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h([2^n]P) \implies \hat{h}([2]P) = 4\hat{h}(P).$
  2. For any given real number B, the set

     $$\{P \in E(K) \mid \hat{h}(P) \leq B\}$$

     is finite, which clearly follows from the finiteness of such set with respect to the height $h(P) = \log\left(\mid H(P) \mid\right)$ and the fact that $\mid \hat{h}(P) - h(P) \mid$ is bounded for all $P \in E(K)$.

Proof of the Mordell-Weil Theorem

- Let $S_0 = \{Q_1, Q_2, \ldots, Q_k\}$ be a finite set of representatives of $E(K)$ modulo $2E(K)$. Let $B = \max_i \hat{h}(Q_i)$.
- Consider the finite set $S = \{P \in E(K) \mid \hat{h}(P) \leq B\}$. We claim that $E(K)$ is generated as an abelian group by the elements of the finite set S, i.e., $E(K) = \langle S \rangle$.
- If possible, let $U = E(K) \setminus \langle S \rangle$ be a non-empty set. Then there exists a point $R \in U$ such that $\hat{h}(R) = \min\{\hat{h}(T) \mid T \in U\}$. Existence of such a point R in a non-empty subset U of $E(K)$ follows from the finiteness of points of bounded height in $E(K)$.

- Let $S_0 = \{Q_1, Q_2, \ldots, Q_k\}$ be a finite set of representatives of $E(K)$ modulo $2E(K)$. Let $B = \max_i \hat{h}(Q_i)$.
- Consider the finite set $S = \{P \in E(K) \mid \hat{h}(P) \leq B\}$. We claim that $E(K)$ is generated as an abelian group by the elements of the finite set S, i.e., $E(K) = \langle S \rangle$.
- If possible, let $U = E(K) \setminus \langle S \rangle$ be a non-empty set. Then there exists a point $R \in U$ such that $\hat{h}(R) = \min\{\hat{h}(T) \mid T \in U\}$. Existence of such a point R in a non-empty subset U of $E(K)$ follows from the finiteness of points of bounded height in $E(K)$.

Proof of the Mordell-Weil Theorem

- Let $S_0 = \{Q_1, Q_2, \ldots, Q_k\}$ be a finite set of representatives of $E(K)$ modulo $2E(K)$. Let $B = \max_i \hat{h}(Q_i)$.

- Consider the finite set $S = \{P \in E(K) \mid \hat{h}(P) \leq B\}$. We claim that $E(K)$ is generated as an abelian group by the elements of the finite set S, i.e., $E(K) = \langle S \rangle$.

- If possible, let $U = E(K) \setminus \langle S \rangle$ be a non-empty set. Then there exists a point $R \in U$ such that $\hat{h}(R) = \min\{\hat{h}(T) \mid T \in U\}$. Existence of such a point R in a non-empty subset U of $E(K)$ follows from the finiteness of points of bounded height in $E(K)$.

Proof of the Mordell-Weil Theorem

- Let $S_0 = \{Q_1, Q_2, \ldots, Q_k\}$ be a finite set of representatives of $E(K)$ modulo $2E(K)$. Let $B = \max_i \hat{h}(Q_i)$.

- Consider the finite set $S = \{P \in E(K) \mid \hat{h}(P) \leq B\}$. We claim that $E(K)$ is generated as an abelian group by the elements of the finite set S, i.e., $E(K) = \langle S \rangle$.

- If possible, let $U = E(K) \setminus \langle S \rangle$ be a non-empty set. Then there exists a point $R \in U$ such that $\hat{h}(R) = \min\{\hat{h}(T) \mid T \in U\}$. Existence of such a point R in a non-empty subset U of $E(K)$ follows from the finiteness of points of bounded height in $E(K)$.

Proof of the Mordell-Weil Theorem

- Let $S_0 = \{Q_1, Q_2, \ldots, Q_k\}$ be a finite set of representatives of $E(K)$ modulo $2E(K)$. Let $B = \max_i \hat{h}(Q_i)$.

- Consider the finite set $S = \{P \in E(K) \mid \hat{h}(P) \leq B\}$. We claim that $E(K)$ is generated as an abelian group by the elements of the finite set S, i.e., $E(K) = \langle S \rangle$.

- If possible, let $U = E(K) \setminus \langle S \rangle$ be a non-empty set. Then there exists a point $R \in U$ such that $\hat{h}(R) = \min\{\hat{h}(T) \mid T \in U\}$. Existence of such a point R in a non-empty subset U of $E(K)$ follows from the finiteness of points of bounded height in $E(K)$.

Proof of the Mordell-Weil Theorem

- Let $S_0 = \{Q_1, Q_2, \ldots, Q_k\}$ be a finite set of representatives of $E(K)$ modulo $2E(K)$. Let $B = \max_i \hat{h}(Q_i)$.
- Consider the finite set $S = \{P \in E(K) \mid \hat{h}(P) \leq B\}$. We claim that $E(K)$ is generated as an abelian group by the elements of the finite set S, i.e., $E(K) = \langle S \rangle$.
- If possible, let $U = E(K) \setminus \langle S \rangle$ be a non-empty set. Then there exists a point $R \in U$ such that $\hat{h}(R) = \min\{\hat{h}(T) \mid T \in U\}$. Existence of such a point R in a non-empty subset U of $E(K)$ follows from the finiteness of points of bounded height in $E(K)$.

Proof of the Mordell-Weil Theorem

- We have $R = Q_i + 2P$ for some Q_i in the set S_0 of representatives of $E(K)/2E(K)$ and $P \in E(K)$.
- Since $Q_i \in \langle S \rangle$ and $R \notin \langle S \rangle$, so $P \notin \langle S \rangle$. Therefore, $\hat{h}(P) \geq \hat{h}(R)$.
- By properties of the canonical height,

$$\begin{aligned} 2\hat{h}(R) + 2\hat{h}(Q_i) &= \hat{h}(R + Q_i) + \hat{h}(R - Q_i) \\ \implies 2\hat{h}(Q_i) &= \hat{h}(R + Q_i) + \hat{h}(2P) - 2\hat{h}(R) \\ \implies 2\hat{h}(Q_i) &\geq 0 + 4\hat{h}(P) - 2\hat{h}(R) \\ \implies 2\hat{h}(Q_i) &\geq 4\hat{h}(R) - 2\hat{h}(R) \geq 2\hat{h}(R), \end{aligned}$$

i.e., $\hat{h}(R) \leq \hat{h}(Q_i) \leq B$ and $R \in S \subset \langle S \rangle$, a contradiction.

- Therefore, $U = E(K) \setminus \langle S \rangle$ must be empty, and $E(K)$ is generated as an abelian group by the finite set S.

Proof of the Mordell-Weil Theorem

- We have $R = Q_i + 2P$ for some Q_i in the set S_0 of representatives of $E(K)/2E(K)$ and $P \in E(K)$.
- Since $Q_i \in \langle S \rangle$ and $R \notin \langle S \rangle$, so $P \notin \langle S \rangle$. Therefore, $\hat{h}(P) \geq \hat{h}(R)$.
- By properties of the canonical height,

$$
\begin{aligned}
& 2\hat{h}(R) + 2\hat{h}(Q_i) = \hat{h}(R + Q_i) + \hat{h}(R - Q_i) \\
\implies & 2\hat{h}(Q_i) = \hat{h}(R + Q_i) + \hat{h}(2P) - 2\hat{h}(R) \\
\implies & 2\hat{h}(Q_i) \geq 0 + 4\hat{h}(P) - 2\hat{h}(R) \\
\implies & 2\hat{h}(Q_i) \geq 4\hat{h}(R) - 2\hat{h}(R) \geq 2\hat{h}(R),
\end{aligned}
$$

  i.e., $\hat{h}(R) \leq \hat{h}(Q_i) \leq B$ and $R \in S \subset \langle S \rangle$, a contradiction.
- Therefore, $U = E(K) \setminus \langle S \rangle$ must be empty, and $E(K)$ is generated as an abelian group by the finite set S.

Proof of the Mordell-Weil Theorem

- We have $R = Q_i + 2P$ for some Q_i in the set S_0 of representatives of $E(K)/2E(K)$ and $P \in E(K)$.
- Since $Q_i \in \langle S \rangle$ and $R \notin \langle S \rangle$, so $P \notin \langle S \rangle$. Therefore, $\hat{h}(P) \geq \hat{h}(R)$.
- By properties of the canonical height,

$$2\hat{h}(R) + 2\hat{h}(Q_i) = \hat{h}(R + Q_i) + \hat{h}(R - Q_i)$$
$$\implies 2\hat{h}(Q_i) = \hat{h}(R + Q_i) + \hat{h}(2P) - 2\hat{h}(R)$$
$$\implies 2\hat{h}(Q_i) \geq 0 + 4\hat{h}(P) - 2\hat{h}(R)$$
$$\implies 2\hat{h}(Q_i) \geq 4\hat{h}(R) - 2\hat{h}(R) \geq 2\hat{h}(R),$$

  i.e., $\hat{h}(R) \leq \hat{h}(Q_i) \leq B$ and $R \in S \subset \langle S \rangle$, a contradiction.
- Therefore, $U = E(K) \setminus \langle S \rangle$ must be empty, and $E(K)$ is generated as an abelian group by the finite set S.

Proof of the Mordell-Weil Theorem

- We have $R = Q_i + 2P$ for some Q_i in the set S_0 of representatives of $E(K)/2E(K)$ and $P \in E(K)$.
- Since $Q_i \in \langle S \rangle$ and $R \notin \langle S \rangle$, so $P \notin \langle S \rangle$. Therefore, $\hat{h}(P) \geq \hat{h}(R)$.
- By properties of the canonical height,

$$\begin{aligned} & 2\hat{h}(R) + 2\hat{h}(Q_i) = \hat{h}(R + Q_i) + \hat{h}(R - Q_i) \\ \implies & 2\hat{h}(Q_i) = \hat{h}(R + Q_i) + \hat{h}(2P) - 2\hat{h}(R) \\ \implies & 2\hat{h}(Q_i) \geq 0 + 4\hat{h}(P) - 2\hat{h}(R) \\ \implies & 2\hat{h}(Q_i) \geq 4\hat{h}(R) - 2\hat{h}(R) \geq 2\hat{h}(R), \end{aligned}$$

i.e., $\hat{h}(R) \leq \hat{h}(Q_i) \leq B$ and $R \in S \subset \langle S \rangle$, a contradiction.

- Therefore, $U = E(K) \setminus \langle S \rangle$ must be empty, and $E(K)$ is generated as an abelian group by the finite set S.

Proof of the Mordell-Weil Theorem

- We have $R = Q_i + 2P$ for some Q_i in the set S_0 of representatives of $E(K)/2E(K)$ and $P \in E(K)$.
- Since $Q_i \in \langle S \rangle$ and $R \notin \langle S \rangle$, so $P \notin \langle S \rangle$. Therefore, $\hat{h}(P) \geq \hat{h}(R)$.
- By properties of the canonical height,

$$
\begin{aligned}
& 2\hat{h}(R) + 2\hat{h}(Q_i) = \hat{h}(R + Q_i) + \hat{h}(R - Q_i) \\
\implies & 2\hat{h}(Q_i) = \hat{h}(R + Q_i) + \hat{h}(2P) - 2\hat{h}(R) \\
\implies & 2\hat{h}(Q_i) \geq 0 + 4\hat{h}(P) - 2\hat{h}(R) \\
\implies & 2\hat{h}(Q_i) \geq 4\hat{h}(R) - 2\hat{h}(R) \geq 2\hat{h}(R),
\end{aligned}
$$

  i.e., $\hat{h}(R) \leq \hat{h}(Q_i) \leq B$ and $R \in S \subset \langle S \rangle$, a contradiction.

- Therefore, $U = E(K) \setminus \langle S \rangle$ must be empty, and $E(K)$ is generated as an abelian group by the finite set S.

Proof of the Mordell-Weil Theorem

- We have $R = Q_i + 2P$ for some Q_i in the set S_0 of representatives of $E(K)/2E(K)$ and $P \in E(K)$.
- Since $Q_i \in \langle S \rangle$ and $R \notin \langle S \rangle$, so $P \notin \langle S \rangle$. Therefore, $\hat{h}(P) \geq \hat{h}(R)$.
- By properties of the canonical height,

$$
\begin{aligned}
& 2\hat{h}(R) + 2\hat{h}(Q_i) = \hat{h}(R + Q_i) + \hat{h}(R - Q_i) \\
\implies & 2\hat{h}(Q_i) = \hat{h}(R + Q_i) + \hat{h}(2P) - 2\hat{h}(R) \\
\implies & 2\hat{h}(Q_i) \geq 0 + 4\hat{h}(P) - 2\hat{h}(R) \\
\implies & 2\hat{h}(Q_i) \geq 4\hat{h}(R) - 2\hat{h}(R) \geq 2\hat{h}(R),
\end{aligned}
$$

  i.e., $\hat{h}(R) \leq \hat{h}(Q_i) \leq B$ and $R \in S \subset \langle S \rangle$, a contradiction.
- Therefore, $U = E(K) \setminus \langle S \rangle$ must be empty, and $E(K)$ is generated as an abelian group by the finite set S.

The Regulator of an Elliptic Curve

- The regulator of an elliptic curve E/K is an important arithmetic invariant, which can be compared to the regulator of a number field.

- By Mordell-Weil Theorem, $E(K) \otimes \mathbb{R}$ is a finite dimensional vector space. We can consider the $E(K)/E(K)_{tors}$ as a complete lattice in $E(K) \otimes \mathbb{R}$. The regulator of E/K is the volume of a fundamental domain of $E(K)/E(K)_{tors}$ with respect to the positive definite quadratic form defined by Neron-Tate height pairing.

- Let $P_1, P_2, \ldots, P_r \in E(K)$ be a set of generators for $E(K)/E(K)_{tors}$. The regulator of of E/K is defined as

$$R_{E/K} = \det\Big(\langle P_i, P_j\rangle\Big)_{\substack{1\le i\le r,\\ 1\le j\le r}}$$

where $\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ is the Neron-Tate height pairing. If $r = 0$, then we set $R_{E/K} = 1$ by convention.

The Regulator of an Elliptic Curve

- The regulator of an elliptic curve E/K is an important arithmetic invariant, which can be compared to the regulator of a number field.
- By Mordell-Weil Theorem, $E(K) \otimes \mathbb{R}$ is a finite dimensional vector space. We can consider the $E(K)/E(K)_{tors}$ as a complete lattice in $E(K) \otimes \mathbb{R}$. The regulator of E/K is the volume of a fundamental domain of $E(K)/E(K)_{tors}$ with respect to the positive definite quadratic form defined by Neron-Tate height pairing.
- Let $P_1, P_2, \ldots, P_r \in E(K)$ be a set of generators for $E(K)/E(K)_{tors}$. The regulator of of E/K is defined as

$$R_{E/K} = \det \left(\langle P_i, P_j \rangle \right)_{\substack{1 \le i \le r, \\ 1 \le j \le r}}$$

where $\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ is the Neron-Tate height pairing. If $r = 0$, then we set $R_{E/K} = 1$ by convention.

The Regulator of an Elliptic Curve

- The regulator of an elliptic curve E/K is an important arithmetic invariant, which can be compared to the regulator of a number field.
- By Mordell-Weil Theorem, $E(K) \otimes \mathbb{R}$ is a finite dimensional vector space. We can consider the $E(K)/E(K)_{tors}$ as a complete lattice in $E(K) \otimes \mathbb{R}$. The regulator of E/K is the volume of a fundamental domain of $E(K)/E(K)_{tors}$ with respect to the positive definite quadratic form defined by Neron-Tate height pairing.
- Let $P_1, P_2, \ldots, P_r \in E(K)$ be a set of generators for $E(K)/E(K)_{tors}$. The regulator of of E/K is defined as

$$R_{E/K} = \det\left(\langle P_i, P_j \rangle\right)_{\substack{1 \le i \le r,\\ 1 \le j \le r}}$$

where $\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ is the Neron-Tate height pairing. If $r = 0$, then we set $R_{E/K} = 1$ by convention.

The Regulator of an Elliptic Curve

- The regulator of an elliptic curve E/K is an important arithmetic invariant, which can be compared to the regulator of a number field.
- By Mordell-Weil Theorem, $E(K) \otimes \mathbb{R}$ is a finite dimensional vector space. We can consider the $E(K)/E(K)_{tors}$ as a complete lattice in $E(K) \otimes \mathbb{R}$. The regulator of E/K is the volume of a fundamental domain of $E(K)/E(K)_{tors}$ with respect to the positive definite quadratic form defined by Neron-Tate height pairing.
- Let $P_1, P_2, \ldots, P_r \in E(K)$ be a set of generators for $E(K)/E(K)_{tors}$. The regulator of of E/K is defined as

$$R_{E/K} = \det\Big(\langle P_i, P_j\rangle\Big)_{\substack{1\le i\le r,\\ 1\le j\le r}}$$

where $\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ is the Neron-Tate height pairing. If $r=0$, then we set $R_{E/K}=1$ by convention.

The Regulator of an Elliptic Curve

- The regulator of an elliptic curve E/K is an important arithmetic invariant, which can be compared to the regulator of a number field.
- By Mordell-Weil Theorem, $E(K) \otimes \mathbb{R}$ is a finite dimensional vector space. We can consider the $E(K)/E(K)_{tors}$ as a complete lattice in $E(K) \otimes \mathbb{R}$. The regulator of E/K is the volume of a fundamental domain of $E(K)/E(K)_{tors}$ with respect to the positive definite quadratic form defined by Neron-Tate height pairing.
- Let $P_1, P_2, \ldots, P_r \in E(K)$ be a set of generators for $E(K)/E(K)_{tors}$. The regulator of of E/K is defined as

$$R_{E/K} = \det\Big(\langle P_i, P_j\rangle\Big)_{\substack{1\leq i\leq r\\ 1\leq j\leq r}},$$

where $\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ is the Neron-Tate height pairing. If $r = 0$, then we set $R_{E/K} = 1$ by convention.

The Regulator of an Elliptic Curve

- The regulator of an elliptic curve E/K is an important arithmetic invariant, which can be compared to the regulator of a number field.
- By Mordell-Weil Theorem, $E(K) \otimes \mathbb{R}$ is a finite dimensional vector space. We can consider the $E(K)/E(K)_{tors}$ as a complete lattice in $E(K) \otimes \mathbb{R}$. The regulator of E/K is the volume of a fundamental domain of $E(K)/E(K)_{tors}$ with respect to the positive definite quadratic form defined by Neron-Tate height pairing.
- Let $P_1, P_2, \ldots, P_r \in E(K)$ be a set of generators for $E(K)/E(K)_{tors}$. The regulator of of E/K is defined as

$$R_{E/K} = \det \Big(\langle P_i, P_j \rangle \Big)_{\substack{1 \le i \le r \\ 1 \le j \le r}},$$

where $\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ is the Neron-Tate height pairing. If $r = 0$, then we set $R_{E/K} = 1$ by convention.

Importance of the Regulator

- The Analytic Class Number Formula of Dirichlet gives the residue of the Dedekind zeta function $\zeta_K(s)$ of K at the pole $s = 1$ in terms of certain arithmetic invariants associated with the number field, namely, the number w_K of roots of unity in K, the class number number h_K, the discriminant d_K, and the regulator Reg_K of the number field K:

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot h_K \cdot \text{Reg}_K}{w_K \cdot \sqrt{|\, d_K \,|}}.$$

- Analogously, the second part of the BSD Conjecture expresses the first non-vanishing coefficient in the Taylor series expansion of the '*Hasse-Weil L-function*' of an elliptic curve E/K in terms of arithmetic invariants associated with the elliptic curve such as the order of $E(K)_{tors}$, the '*local Tamagawa numbers*', the order of the '*Shafarevich-Tate group*' and the regulator of E/K.

Importance of the Regulator

- The Analytic Class Number Formula of Dirichlet gives the residue of the Dedekind zeta function $\zeta_K(s)$ of K at the pole $s = 1$ in terms of certain arithmetic invariants associated with the number field, namely, the number w_K of roots of unity in K, the class number number h_K, the discriminant d_K, and the regulator Reg_K of the number field K:

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}\cdot(2\pi)^{r_2}\cdot h_K\cdot \text{Reg}_K}{w_K\cdot\sqrt{|\,d_K\,|}}.$$

- Analogously, the second part of the BSD Conjecture expresses the first non-vanishing coefficient in the Taylor series expansion of the '*Hasse-Weil L-function*' of an elliptic curve E/K in terms of arithmetic invariants associated with the elliptic curve such as the order of $E(K)_{tors}$, the '*local Tamagawa numbers*', the order of the '*Shafarevich-Tate group*' and the regulator of E/K.

Importance of the Regulator

- The Analytic Class Number Formula of Dirichlet gives the residue of the Dedekind zeta function $\zeta_K(s)$ of K at the pole $s = 1$ in terms of certain arithmetic invariants associated with the number field, namely, the number w_K of roots of unity in K, the class number number h_K, the discriminant d_K, and the regulator Reg_K of the number field K:

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot h_K \cdot \text{Reg}_K}{w_K \cdot \sqrt{| d_K |}}.$$

- Analogously, the second part of the BSD Conjecture expresses the first non-vanishing coefficient in the Taylor series expansion of the '*Hasse-Weil L-function*' of an elliptic curve E/K in terms of arithmetic invariants associated with the elliptic curve such as the order of $E(K)_{tors}$, the '*local Tamagawa numbers*', the order of the '*Shafarevich-Tate group*' and the regulator of E/K.

Importance of the Regulator

- The Analytic Class Number Formula of Dirichlet gives the residue of the Dedekind zeta function $\zeta_K(s)$ of K at the pole $s = 1$ in terms of certain arithmetic invariants associated with the number field, namely, the number w_K of roots of unity in K, the class number number h_K, the discriminant d_K, and the regulator Reg_K of the number field K:

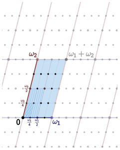
$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot h_K \cdot \text{Reg}_K}{w_K \cdot \sqrt{| d_K |}}.$$

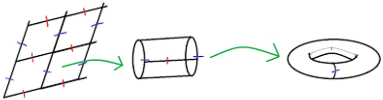
- Analogously, the second part of the BSD Conjecture expresses the first non-vanishing coefficient in the Taylor series expansion of the '*Hasse-Weil L-function*' of an elliptic curve E/K in terms of arithmetic invariants associated with the elliptic curve such as the order of $E(K)_{tors}$, the '*local Tamagawa numbers*', the order of the '*Shafarevich-Tate group*' and the regulator of E/K.

Sections

Sections

Lattices in $\mathbb{C}$



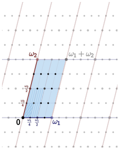


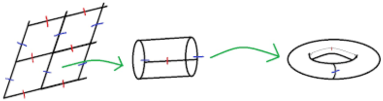
- A lattice Λ in $\mathbb{C}$ is a group consisting of elements which are integral linear combination of two fixed non-zero complex numbers $\omega_1,\ \omega_2$, where ω_1 is not a real multiple of ω_2. I.e.,

$$\Lambda := \{m\omega_1 + n\omega_2 \mid m,\ n \in \mathbb{Z}\}, \qquad \omega_1 \notin \mathbb{R}\omega_2.$$

- Note also that $\mathbb{C}/\Lambda$ is *topologically* a torus (a parallelogram with opposite sides identified, or a dough-nut), and *complex analytically* a Riemann surface (an object with nice analytic structure) of genus 1 (‘*one hole*’).

Lattices in $\mathbb{C}$



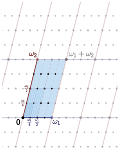


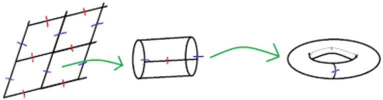
- A lattice Λ in $\mathbb{C}$ is a group consisting of elements which are integral linear combination of two fixed non-zero complex numbers $\omega_1,\ \omega_2$, where ω_1 is not a real multiple of ω_2. I.e.,

$$\Lambda := \{m\omega_1 + n\omega_2 \mid m,\ n \in \mathbb{Z}\}, \qquad \omega_1 \notin \mathbb{R}\omega_2.$$

- Note also that $\mathbb{C}/\Lambda$ is *topologically* a torus (a parallelogram with opposite sides identified, or a dough-nut), and *complex analytically* a Riemann surface (an object with nice analytic structure) of genus 1 (‘*one hole*’).

Lattices in $\mathbb{C}$





- A lattice Λ in $\mathbb{C}$ is a group consisting of elements which are integral linear combination of two fixed non-zero complex numbers $\omega_1,\ \omega_2$, where ω_1 is not a real multiple of ω_2. I.e.,

$$\Lambda := \{m\omega_1 + n\omega_2 \mid m,\ n \in \mathbb{Z}\}, \qquad \omega_1 \notin \mathbb{R}\omega_2.$$

- Note also that $\mathbb{C}/\Lambda$ is *topologically* a torus (a parallelogram with opposite sides identified, or a dough-nut), and *complex analytically* a Riemann surface (an object with nice analytic structure) of genus 1 ('*one hole*').

Elliptic Functions

- An elliptic function relative to a lattice Λ is a meromorphic function on $\mathbb{C}$ that satisfies

$$f(z+w) = f(z) \qquad \forall z \in \mathbb{C}, \quad \forall \omega \in \Lambda.$$

  The set of all such functions is denoted by $\mathbb{C}(\Lambda)$, which is clearly a field. We can think of f as a function of the quotient group $\mathbb{C}/\Lambda$.

- It follows easily from Liouville's theorem that an elliptic function with no poles (or with no zeroes) must be constant.

- The Weierstrass $\wp$-function associated with a given lattice Λ is given by

$$\wp(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda,\ \omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

  The series above converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. It defines an even, meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.

Elliptic Functions

- An elliptic function relative to a lattice Λ is a meromorphic function on $\mathbb{C}$ that satisfies

$$f(z+w) = f(z) \qquad \forall z \in \mathbb{C}, \quad \forall \omega \in \Lambda.$$

The set of all such functions is denoted by $\mathbb{C}(\Lambda)$, which is clearly a field. We can think of f as a function of the quotient group $\mathbb{C}/\Lambda$.

- It follows easily from Liouville's theorem that an elliptic function with no poles (or with no zeroes) must be constant.

- The Weierstrass $\wp$-function associated with a given lattice Λ is given by

$$\wp(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda,\ \omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

The series above converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. It defines an even, meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.

Elliptic Functions

- An elliptic function relative to a lattice Λ is a meromorphic function on $\mathbb{C}$ that satisfies

$$f(z+w) = f(z) \qquad \forall z \in \mathbb{C}, \quad \forall \omega \in \Lambda.$$

  The set of all such functions is denoted by $\mathbb{C}(\Lambda)$, which is clearly a field. We can think of f as a function of the quotient group $\mathbb{C}/\Lambda$.

- It follows easily from Liouville's theorem that an elliptic function with no poles (or with no zeroes) must be constant.

- The Weierstrass $\wp$-function associated with a given lattice Λ is given by

$$\wp(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda,\ \omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

  The series above converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. It defines an even, meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.

Elliptic Functions

- An elliptic function relative to a lattice Λ is a meromorphic function on $\mathbb{C}$ that satisfies

$$f(z+w) = f(z) \qquad \forall z \in \mathbb{C}, \quad \forall \omega \in \Lambda.$$

The set of all such functions is denoted by $\mathbb{C}(\Lambda)$, which is clearly a field. We can think of f as a function of the quotient group $\mathbb{C}/\Lambda$.

- It follows easily from Liouville's theorem that an elliptic function with no poles (or with no zeroes) must be constant.

- The Weierstrass $\wp$-function associated with a given lattice Λ is given by

$$\wp(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda,\ \omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

The series above converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. It defines an even, meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.

Elliptic Functions

- An elliptic function relative to a lattice Λ is a meromorphic function on $\mathbb{C}$ that satisfies

$$f(z+w) = f(z) \qquad \forall z \in \mathbb{C}, \quad \forall \omega \in \Lambda.$$

The set of all such functions is denoted by $\mathbb{C}(\Lambda)$, which is clearly a field. We can think of f as a function of the quotient group $\mathbb{C}/\Lambda$.

- It follows easily from Liouville's theorem that an elliptic function with no poles (or with no zeroes) must be constant.

- The Weierstrass $\wp$-function associated with a given lattice Λ is given by

$$\wp(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda,\ \omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

The series above converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. It defines an even, meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.

Elliptic Functions

- An elliptic function relative to a lattice Λ is a meromorphic function on $\mathbb{C}$ that satisfies

$$f(z+w) = f(z) \qquad \forall z \in \mathbb{C}, \quad \forall \omega \in \Lambda.$$

  The set of all such functions is denoted by $\mathbb{C}(\Lambda)$, which is clearly a field. We can think of f as a function of the quotient group $\mathbb{C}/\Lambda$.

- It follows easily from Liouville's theorem that an elliptic function with no poles (or with no zeroes) must be constant.

- The Weierstrass $\wp$-function associated with a given lattice Λ is given by

$$\wp(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda,\ \omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

  The series above converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. It defines an even, meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.

Elliptic Functions

- An elliptic function relative to a lattice Λ is a meromorphic function on $\mathbb{C}$ that satisfies

$$f(z+w) = f(z) \qquad \forall z \in \mathbb{C}, \quad \forall \omega \in \Lambda.$$

  The set of all such functions is denoted by $\mathbb{C}(\Lambda)$, which is clearly a field. We can think of f as a function of the quotient group $\mathbb{C}/\Lambda$.

- It follows easily from Liouville's theorem that an elliptic function with no poles (or with no zeroes) must be constant.

- The Weierstrass $\wp$-function associated with a given lattice Λ is given by

$$\wp(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda,\ \omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right].$$

  The series above converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. It defines an even, meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.

The Weierstrass $\wp$-function

- We can compute the derivative of $\wp(z)$ by term-by-term differentiation and obtain

$$\wp'(z) = -2 \sum_{\omega \in \Lambda,\ \omega \neq 0} \frac{1}{(z-\omega)^3}.$$

- Clearly, $\wp'$ is an elliptic function, i.e., $\wp'(z+w) = \wp'(z)$ for all $\omega \in \Lambda$.
- Integrating with respect z, we obtain $\wp(z+w) = \wp(z) + c(\omega)$, where $c(\omega) \in \mathbb{C}$ is independent of z. Putting $z = -\frac{\omega}{2}$ and noting that $\wp(z)$ is an even function, we find that $c(\omega) = 0$, i.e., $\wp(z)$ is an elliptic function.
- One can show that every elliptic function is a rational combination of $\wp$ and $\wp'$, i.e.,

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp').$$

The Weierstrass $\wp$-function

- We can compute the derivative of $\wp(z)$ by term-by-term differentiation and obtain

$$\wp'(z) = -2 \sum_{\omega \in \Lambda,\ \omega \neq 0} \frac{1}{(z-\omega)^3}.$$

- Clearly, $\wp'$ is an elliptic function, i.e., $\wp'(z+w) = \wp'(z)$ for all $\omega \in \Lambda$.
- Integrating with respect z, we obtain $\wp(z+w) = \wp(z) + c(\omega)$, where $c(\omega) \in \mathbb{C}$ is independent of z. Putting $z = -\frac{\omega}{2}$ and noting that $\wp(z)$ is an even function, we find that $c(\omega) = 0$, i.e., $\wp(z)$ is an elliptic function.
- One can show that every elliptic function is a rational combination of $\wp$ and $\wp'$, i.e.,

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp').$$

The Weierstrass $\wp$-function

- We can compute the derivative of $\wp(z)$ by term-by-term differentiation and obtain

$$\wp'(z) = -2 \sum_{\omega \in \Lambda,\ \omega \neq 0} \frac{1}{(z-\omega)^3}.$$

- Clearly, $\wp'$ is an elliptic function, i.e., $\wp'(z+w) = \wp'(z)$ for all $\omega \in \Lambda$.
- Integrating with respect z, we obtain $\wp(z+w) = \wp(z) + c(\omega)$, where $c(\omega) \in \mathbb{C}$ is independent of z. Putting $z = -\frac{\omega}{2}$ and noting that $\wp(z)$ is an even function, we find that $c(\omega) = 0$, i.e., $\wp(z)$ is an elliptic function.
- One can show that every elliptic function is a rational combination of $\wp$ and $\wp'$, i.e.,

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp').$$

The Weierstrass $\wp$-function

- We can compute the derivative of $\wp(z)$ by term-by-term differentiation and obtain

$$\wp'(z) = -2 \sum_{\omega \in \Lambda,\ \omega \neq 0} \frac{1}{(z-\omega)^3}.$$

- Clearly, $\wp'$ is an elliptic function, i.e., $\wp'(z+w) = \wp'(z)$ for all $\omega \in \Lambda$.
- Integrating with respect z, we obtain $\wp(z+w) = \wp(z) + c(\omega)$, where $c(\omega) \in \mathbb{C}$ is independent of z. Putting $z = -\frac{\omega}{2}$ and noting that $\wp(z)$ is an even function, we find that $c(\omega) = 0$, i.e., $\wp(z)$ is an elliptic function.
- One can show that every elliptic function is a rational combination of $\wp$ and $\wp'$, i.e.,

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp').$$

The Weierstrass $\wp$-function

- We can compute the derivative of $\wp(z)$ by term-by-term differentiation and obtain

$$\wp'(z) = -2 \sum_{\omega \in \Lambda,\ \omega \neq 0} \frac{1}{(z-\omega)^3}.$$

- Clearly, $\wp'$ is an elliptic function, i.e., $\wp'(z+w) = \wp'(z)$ for all $\omega \in \Lambda$.
- Integrating with respect z, we obtain $\wp(z+w) = \wp(z) + c(\omega)$, where $c(\omega) \in \mathbb{C}$ is independent of z. Putting $z = -\frac{\omega}{2}$ and noting that $\wp(z)$ is an even function, we find that $c(\omega) = 0$, i.e., $\wp(z)$ is an elliptic function.
- One can show that every elliptic function is a rational combination of $\wp$ and $\wp'$, i.e.,

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp').$$

Algebraic Relation between $\wp$ and $\wp'$

- It can be shown that the Laurent series for $\wp(z)$ around $z = 0$ is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\Lambda)z^{2k},$$

where $G_{2k}(\Lambda)$ is the Eisenstein series of weight $2k$ defined as

$$G_{2k}(\Lambda) = \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{w^{2k}}.$$

- As any holomorphic elliptic function is constant, it follows that

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \quad g_2 = 60G_4(\Lambda), \quad g_3 = 140G_6(\Lambda).$$

- It can be shown that the polynomial $4x^3 - g_2x - g_3$ has distinct roots, i.e., its discriminant $g_2^3 - 27g_3^2$ is non-zero. Thus, $(\wp(z), \wp'(z))$ gives a point on the elliptic curve $E_\Lambda : y^2 = 4x^3 - g_2x - g_3$ defined over $\mathbb{C}$.

Algebraic Relation between $\wp$ and $\wp'$

- It can be shown that the Laurent series for $\wp(z)$ around $z = 0$ is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\Lambda)z^{2k},$$

where $G_{2k}(\Lambda)$ is the Eisenstein series of weight $2k$ defined as

$$G_{2k}(\Lambda) = \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{w^{2k}}.$$

- As any holomorphic elliptic function is constant, it follows that

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \quad g_2 = 60G_4(\Lambda), \quad g_3 = 140G_6(\Lambda).$$

- It can be shown that the polynomial $4x^3 - g_2x - g_3$ has distinct roots, i.e., its discriminant $g_2^3 - 27g_3^2$ is non-zero. Thus, $(\wp(z), \wp'(z))$ gives a point on the elliptic curve $E_\Lambda : y^2 = 4x^3 - g_2x - g_3$ defined over $\mathbb{C}$.

Algebraic Relation between $\wp$ and $\wp'$

- It can be shown that the Laurent series for $\wp(z)$ around $z = 0$ is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\Lambda)z^{2k},$$

where $G_{2k}(\Lambda)$ is the Eisenstein series of weight $2k$ defined as

$$G_{2k}(\Lambda) = \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{w^{2k}}.$$

- As any holomorphic elliptic function is constant, it follows that

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \quad g_2 = 60G_4(\Lambda), \quad g_3 = 140G_6(\Lambda).$$

- It can be shown that the polynomial $4x^3 - g_2x - g_3$ has distinct roots, i.e., its discriminant $g_2^3 - 27g_3^2$ is non-zero. Thus, $(\wp(z), \wp'(z))$ gives a point on the elliptic curve $E_\Lambda : y^2 = 4x^3 - g_2x - g_3$ defined over $\mathbb{C}$.

Algebraic Relation between $\wp$ and $\wp'$

- It can be shown that the Laurent series for $\wp(z)$ around $z = 0$ is given by
$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\Lambda)z^{2k},$$
where $G_{2k}(\Lambda)$ is the Eisenstein series of weight $2k$ defined as
$$G_{2k}(\Lambda) = \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{w^{2k}}.$$
- As any holomorphic elliptic function is constant, it follows that
$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \quad g_2 = 60G_4(\Lambda), \quad g_3 = 140G_6(\Lambda).$$
- It can be shown that the polynomial $4x^3 - g_2x - g_3$ has distinct roots, i.e., its discriminant $g_2^3 - 27g_3^2$ is non-zero. Thus, $(\wp(z), \wp'(z))$ gives a point on the elliptic curve $E_\Lambda : y^2 = 4x^3 - g_2x - g_3$ defined over $\mathbb{C}$.

Isomorphism between $\mathbb{C}/\Lambda$ and $E_\Lambda(\mathbb{C})$

- The map $\mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}), \qquad z \pmod{\Lambda} \longmapsto [\wp(z) : \wp'(z) : 1]$

  is a group isomorphism, i.e.,

  $$[\wp(z_1+z_2) : \wp'(z_1+z_2) : 1] = [\wp(z_1) : \wp'(z_1) : 1] \oplus [\wp(z_2) : \wp'(z_2) : 1].$$

  The homomorhism can be shown by constructing a suitable function on $\mathbb{C}/\Lambda$ with $(z_1+z_2) - (z_1) - (z_2) + (0)$ as divisors by using '*Weierstrass σ-function*'.

- The surjectivity is shown by using the fact the non-constant elliptic function $\wp(z) - x$ must have a zero.

- The inverse map is obtained by integrating the invariant holomorphic differential form $\frac{dx}{2y}$ from a given point $\mathcal{O}$ to an arbitrary point P on $E(\mathbb{C})$. The values of the integral modulo Λ is path-independent.

Isomorphism between $\mathbb{C}/\Lambda$ and $E_\Lambda(\mathbb{C})$

- The map $\mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}), \qquad z \pmod{\Lambda} \longmapsto [\wp(z) : \wp'(z) : 1]$

  is a group isomorphism, i.e.,

  $$[\wp(z_1+z_2) : \wp'(z_1+z_2) : 1] = [\wp(z_1) : \wp'(z_1) : 1] \oplus [\wp(z_2) : \wp'(z_2) : 1].$$

  The homomorhism can be shown by constructing a suitable function on $\mathbb{C}/\Lambda$ with $(z_1+z_2) - (z_1) - (z_2) + (0)$ as divisors by using '*Weierstrass σ-function*'.

- The surjectivity is shown by using the fact the non-constant elliptic function $\wp(z) - x$ must have a zero.

- The inverse map is obtained by integrating the invariant holomorphic differential form $\frac{dx}{2y}$ from a given point $\mathcal{O}$ to an arbitrary point P on $E(\mathbb{C})$. The values of the integral modulo Λ is path-independent.

Isomorphism between $\mathbb{C}/\Lambda$ and $E_\Lambda(\mathbb{C})$

- The map $\mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$, $\quad z \pmod{\Lambda} \longmapsto [\wp(z) : \wp'(z) : 1]$

  is a group isomorphism, i.e.,

  $[\wp(z_1+z_2) : \wp'(z_1+z_2) : 1] = [\wp(z_1) : \wp'(z_1) : 1] \oplus [\wp(z_2) : \wp'(z_2) : 1].$

  The homomorhism can be shown by constructing a suitable function on $\mathbb{C}/\Lambda$ with $(z_1+z_2) - (z_1) - (z_2) + (0)$ as divisors by using '*Weierstrass σ-function*'.

- The surjectivity is shown by using the fact the non-constant elliptic function $\wp(z) - x$ must have a zero.

- The inverse map is obtained by integrating the invariant holomorphic differential form $\frac{dx}{2y}$ from a given point $\mathcal{O}$ to an arbitrary point P on $E(\mathbb{C})$. The values of the integral modulo Λ is path-independent.

- The map $\mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}), \qquad z \pmod{\Lambda} \longmapsto [\wp(z) : \wp'(z) : 1]$

  is a group isomorphism, i.e.,

  $[\wp(z_1+z_2) : \wp'(z_1+z_2) : 1] = [\wp(z_1) : \wp'(z_1) : 1] \oplus [\wp(z_2) : \wp'(z_2) : 1].$

  The homomorhism can be shown by constructing a suitable function on $\mathbb{C}/\Lambda$ with $(z_1+z_2) - (z_1) - (z_2) + (0)$ as divisors by using '*Weierstrass σ-function*'.

- The surjectivity is shown by using the fact the non-constant elliptic function $\wp(z) - x$ must have a zero.

- The inverse map is obtained by integrating the invariant holomorphic differential form $\frac{dx}{2y}$ from a given point $\mathcal{O}$ to an arbitrary point P on $E(\mathbb{C})$. The values of the integral modulo Λ is path-independent.

Isomorphism between $\mathbb{C}/\Lambda$ and $E_\Lambda(\mathbb{C})$

- The map $\mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}), \qquad z \pmod{\Lambda} \longmapsto [\wp(z) : \wp'(z) : 1]$

  is a group isomorphism, i.e.,

  $$[\wp(z_1+z_2) : \wp'(z_1+z_2) : 1] = [\wp(z_1) : \wp'(z_1) : 1] \oplus [\wp(z_2) : \wp'(z_2) : 1].$$

  The homomorhism can be shown by constructing a suitable function on $\mathbb{C}/\Lambda$ with $(z_1+z_2) - (z_1) - (z_2) + (0)$ as divisors by using '*Weierstrass σ-function*'.

- The surjectivity is shown by using the fact the non-constant elliptic function $\wp(z) - x$ must have a zero.

- The inverse map is obtained by integrating the invariant holomorphic differential form $\frac{dx}{2y}$ from a given point $\mathcal{O}$ to an arbitrary point P on $E(\mathbb{C})$. The values of the integral modulo Λ is path-independent.

Isomorphism between $\mathbb{C}/\Lambda$ and $E_\Lambda(\mathbb{C})$

- The map $\mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}), \qquad z \pmod{\Lambda} \longmapsto [\wp(z) : \wp'(z) : 1]$

  is a group isomorphism, i.e.,

  $$[\wp(z_1+z_2) : \wp'(z_1+z_2) : 1] = [\wp(z_1) : \wp'(z_1) : 1] \oplus [\wp(z_2) : \wp'(z_2) : 1].$$

  The homomorhism can be shown by constructing a suitable function on $\mathbb{C}/\Lambda$ with $(z_1+z_2) - (z_1) - (z_2) + (0)$ as divisors by using '*Weierstrass σ-function*'.

- The surjectivity is shown by using the fact the non-constant elliptic function $\wp(z) - x$ must have a zero.

- The inverse map is obtained by integrating the invariant holomorphic differential form $\frac{dx}{2y}$ from a given point $\mathcal{O}$ to an arbitrary point P on $E(\mathbb{C})$. The values of the integral modulo Λ is path-independent.

Isomorphism between $\mathbb{C}/\Lambda$ and $E_\Lambda(\mathbb{C})$

- The map $\mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}), \qquad z \pmod{\Lambda} \longmapsto [\wp(z) : \wp'(z) : 1]$

  is a group isomorphism, i.e.,

  $$[\wp(z_1+z_2) : \wp'(z_1+z_2) : 1] = [\wp(z_1) : \wp'(z_1) : 1] \oplus [\wp(z_2) : \wp'(z_2) : 1].$$

  The homomorhism can be shown by constructing a suitable function on $\mathbb{C}/\Lambda$ with $(z_1 + z_2) - (z_1) - (z_2) + (0)$ as divisors by using '*Weierstrass σ-function*'.

- The surjectivity is shown by using the fact the non-constant elliptic function $\wp(z) - x$ must have a zero.

- The inverse map is obtained by integrating the invariant holomorphic differential form $\frac{dx}{2y}$ from a given point $\mathcal{O}$ to an arbitrary point P on $E(\mathbb{C})$. The values of the integral modulo Λ is path-independent.

Associating Elliptic Curves over $\mathbb{C}$ with Lattices

- We just saw that starting with a lattice Λ in $\mathbb{C}$, we can we can associate an elliptic curve $E_\Lambda/\mathbb{C}$.

- The converse is also true. The equation for an elliptic curve $E/\mathbb{C}$ can be written as $y^2 = 4x^3 - ax - b$ for some $a, b \in \mathbb{C}$ such that $a^3 - 27b^2 \neq 0$. Given such a and b, one case show that

$$\exists \text{ lattice } \Lambda \text{ such that } g_2 = 60G_4(\Lambda) = a, \quad g_3 = 140G_6(\Lambda) = b.$$

The proof uses the surjectivity of the modular function

$$j : \mathfrak{h} \longrightarrow \mathbb{C}, \qquad j(\tau) = 1728\frac{\big(g_2(\tau)\big)^3}{\big(g_2(\tau)\big)^3 - 27\big(g_3(\tau)\big)^2}.$$

- Thus, *the set of lattices in $\mathbb{C}$ and the set of elliptic curves defined over $\mathbb{C}$ have a one-to-one correspondence.*

- As a consequence, the subgroup of n-torsion points in $E(\mathbb{C})$ is

$$E(\mathbb{C})[n] \simeq (\mathbb{C}/\Lambda)[n] \simeq \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

Associating Elliptic Curves over $\mathbb{C}$ with Lattices

- We just saw that starting with a lattice Λ in $\mathbb{C}$, we can we can associate an elliptic curve $E_\Lambda/\mathbb{C}$.

- The converse is also true. The equation for an elliptic curve $E/\mathbb{C}$ can be written as $y^2 = 4x^3 - ax - b$ for some $a, b \in \mathbb{C}$ such that $a^3 - 27b^2 \neq 0$. Given such a and b, one case show that

$$\exists \text{ lattice } \Lambda \text{ such that } g_2 = 60G_4(\Lambda) = a, \quad g_3 = 140G_6(\Lambda) = b.$$

The proof uses the surjectivity of the modular function

$$j : \mathfrak{h} \longrightarrow \mathbb{C}, \qquad j(\tau) = 1728 \frac{\big(g_2(\tau)\big)^3}{\big(g_2(\tau)\big)^3 - 27\big(g_3(\tau)\big)^2}.$$

- Thus, *the set of lattices in $\mathbb{C}$ and the set of elliptic curves defined over $\mathbb{C}$ have a one-to-one correspondence.*

- As a consequence, the subgroup of n-torsion points in $E(\mathbb{C})$ is

$$E(\mathbb{C})[n] \simeq (\mathbb{C}/\Lambda)[n] \simeq \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

Associating Elliptic Curves over $\mathbb{C}$ with Lattices

- We just saw that starting with a lattice Λ in $\mathbb{C}$, we can we can associate an elliptic curve $E_\Lambda/\mathbb{C}$.

- The converse is also true. The equation for an elliptic curve $E/\mathbb{C}$ can be written as $y^2 = 4x^3 - ax - b$ for some $a, b \in \mathbb{C}$ such that $a^3 - 27b^2 \neq 0$. Given such a and b, one case show that

$$\exists \text{ lattice } \Lambda \text{ such that } g_2 = 60G_4(\Lambda) = a, \quad g_3 = 140G_6(\Lambda) = b.$$

The proof uses the surjectivity of the modular function

$$j : \mathfrak{h} \longrightarrow \mathbb{C}, \qquad j(\tau) = 1728 \frac{\big(g_2(\tau)\big)^3}{\big(g_2(\tau)\big)^3 - 27\big(g_3(\tau)\big)^2}.$$

- Thus, *the set of lattices in $\mathbb{C}$ and the set of elliptic curves defined over $\mathbb{C}$ have a one-to-one correspondence.*

- As a consequence, the subgroup of n-torsion points in $E(\mathbb{C})$ is

$$E(\mathbb{C})[n] \simeq (\mathbb{C}/\Lambda)[n] \simeq \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

Associating Elliptic Curves over $\mathbb{C}$ with Lattices

- We just saw that starting with a lattice Λ in $\mathbb{C}$, we can we can associate an elliptic curve $E_\Lambda/\mathbb{C}$.
- The converse is also true. The equation for an elliptic curve $E/\mathbb{C}$ can be written as $y^2 = 4x^3 - ax - b$ for some $a, b \in \mathbb{C}$ such that $a^3 - 27b^2 \neq 0$. Given such a and b, one case show that

$$\exists \text{ lattice } \Lambda \text{ such that } g_2 = 60G_4(\Lambda) = a, \quad g_3 = 140G_6(\Lambda) = b.$$

The proof uses the surjectivity of the modular function

$$j : \mathfrak{h} \longrightarrow \mathbb{C}, \qquad j(\tau) = 1728 \frac{\left(g_2(\tau)\right)^3}{\left(g_2(\tau)\right)^3 - 27\left(g_3(\tau)\right)^2}.$$

- Thus, *the set of lattices in $\mathbb{C}$ and the set of elliptic curves defined over $\mathbb{C}$ have a one-to-one correspondence*.
- As a consequence, the subgroup of n-torsion points in $E(\mathbb{C})$ is

$$E(\mathbb{C})[n] \simeq (\mathbb{C}/\Lambda)[n] \simeq \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

Associating Elliptic Curves over $\mathbb{C}$ with Lattices

- We just saw that starting with a lattice Λ in $\mathbb{C}$, we can we can associate an elliptic curve $E_\Lambda/\mathbb{C}$.

- The converse is also true. The equation for an elliptic curve $E/\mathbb{C}$ can be written as $y^2 = 4x^3 - ax - b$ for some $a, b \in \mathbb{C}$ such that $a^3 - 27b^2 \neq 0$. Given such a and b, one case show that

  $$\exists \text{ lattice } \Lambda \text{ such that } g_2 = 60G_4(\Lambda) = a, \quad g_3 = 140G_6(\Lambda) = b.$$

  The proof uses the surjectivity of the modular function

  $$j : \mathfrak{h} \longrightarrow \mathbb{C}, \qquad j(\tau) = 1728 \frac{\big(g_2(\tau)\big)^3}{\big(g_2(\tau)\big)^3 - 27\big(g_3(\tau)\big)^2}.$$

- Thus, *the set of lattices in $\mathbb{C}$ and the set of elliptic curves defined over $\mathbb{C}$ have a one-to-one correspondence*.

- As a consequence, the subgroup of n-torsion points in $E(\mathbb{C})$ is

  $$E(\mathbb{C})[n] \simeq (\mathbb{C}/\Lambda)[n] \simeq \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

Associating Elliptic Curves over $\mathbb{C}$ with Lattices

- We just saw that starting with a lattice Λ in $\mathbb{C}$, we can we can associate an elliptic curve $E_\Lambda/\mathbb{C}$.
- The converse is also true. The equation for an elliptic curve $E/\mathbb{C}$ can be written as $y^2 = 4x^3 - ax - b$ for some $a, b \in \mathbb{C}$ such that $a^3 - 27b^2 \neq 0$. Given such a and b, one case show that

  $$\exists \text{ lattice } \Lambda \text{ such that } g_2 = 60G_4(\Lambda) = a, \quad g_3 = 140G_6(\Lambda) = b.$$

  The proof uses the surjectivity of the modular function

  $$j : \mathfrak{h} \longrightarrow \mathbb{C}, \qquad j(\tau) = 1728 \frac{\big(g_2(\tau)\big)^3}{\big(g_2(\tau)\big)^3 - 27\big(g_3(\tau)\big)^2}.$$

- Thus, *the set of lattices in $\mathbb{C}$ and the set of elliptic curves defined over $\mathbb{C}$ have a one-to-one correspondence*.
- As a consequence, the subgroup of n-torsion points in $E(\mathbb{C})$ is

  $$E(\mathbb{C})[n] \simeq (\mathbb{C}/\Lambda)[n] \simeq \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

Associating Elliptic Curves over $\mathbb{C}$ with Lattices

- We just saw that starting with a lattice Λ in $\mathbb{C}$, we can we can associate an elliptic curve $E_\Lambda/\mathbb{C}$.
- The converse is also true. The equation for an elliptic curve $E/\mathbb{C}$ can be written as $y^2 = 4x^3 - ax - b$ for some $a, b \in \mathbb{C}$ such that $a^3 - 27b^2 \neq 0$. Given such a and b, one case show that

$$\exists \text{ lattice } \Lambda \text{ such that } g_2 = 60G_4(\Lambda) = a, \quad g_3 = 140G_6(\Lambda) = b.$$

The proof uses the surjectivity of the modular function

$$j : \mathfrak{h} \longrightarrow \mathbb{C}, \qquad j(\tau) = 1728 \frac{\big(g_2(\tau)\big)^3}{\big(g_2(\tau)\big)^3 - 27\big(g_3(\tau)\big)^2}.$$

- Thus, *the set of lattices in $\mathbb{C}$ and the set of elliptic curves defined over $\mathbb{C}$ have a one-to-one correspondence*.
- As a consequence, the subgroup of n-torsion points in $E(\mathbb{C})$ is

$$E(\mathbb{C})[n] \simeq (\mathbb{C}/\Lambda)[n] \simeq \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

Homothety and Isomorphism

- Two lattice Λ_1 and Λ_2 in $\mathbb{C}$ are called homothetic if there exists $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda_1 = \Lambda_2$.
- Multiplication by α induces a holomorphic isomomorphism

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2, \qquad \phi_\alpha(z) = \alpha z \mod \Lambda_2.$$

- The induced map on the corresponding elliptic curves

$$E_{\Lambda_1} \longrightarrow E_{\Lambda_2}, \quad [\wp(z,\Lambda_1) : \wp'(z,\Lambda_1) : 1] \mapsto [\wp(\alpha z,\Lambda_2) : \wp'(\alpha z,\Lambda_2) : 1]$$

is an isomorphism of elliptic curves over $\mathbb{C}$. The essential step is to realize that $\wp(\alpha z,\Lambda_2) \in \mathbb{C}(\Lambda_1) = \mathbb{C}((\wp(z,\Lambda_1), \wp'(z,\Lambda_1)))$.

- Therefore, we have a one-to-one correspondence between

$$\{\text{Lattice in } \mathbb{C}/\text{Homothety}\} \leftrightarrow \{\text{Elliptic Curves over } \mathbb{C}/\text{Isomorphim}\}.$$

Homothety and Isomorphism

- Two lattice Λ_1 and Λ_2 in $\mathbb{C}$ are called homothetic if there exists $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda_1 = \Lambda_2$.
- Multiplication by α induces a holomorphic isomomorphism

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2, \qquad \phi_\alpha(z) = \alpha z \mod \Lambda_2.$$

- The induced map on the corresponding elliptic curves

$$E_{\Lambda_1} \longrightarrow E_{\Lambda_2}, \; [\wp(z,\Lambda_1) : \wp'(z,\Lambda_1) : 1] \mapsto [\wp(\alpha z,\Lambda_2) : \wp'(\alpha z,\Lambda_2) : 1]$$

is an isomorphism of elliptic curves over $\mathbb{C}$. The essential step is to realize that $\wp(\alpha z,\Lambda_2) \in \mathbb{C}(\Lambda_1) = \mathbb{C}\big((\wp(z,\Lambda_1), \wp'(z,\Lambda_1)\big)$.

- Therefore, we have a one-to-one correspondence between

$$\{\text{Lattice in } \mathbb{C}/\text{Homothety}\} \leftrightarrow \{\text{Elliptic Curves over } \mathbb{C}/\text{Isomorphim}\}.$$

Homothety and Isomorphism

- Two lattice Λ_1 and Λ_2 in $\mathbb{C}$ are called homothetic if there exists $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda_1 = \Lambda_2$.
- Multiplication by α induces a holomorphic isomomorphism

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2, \qquad \phi_\alpha(z) = \alpha z \mod \Lambda_2.$$

- The induced map on the corresponding elliptic curves

$$E_{\Lambda_1} \longrightarrow E_{\Lambda_2}, \ \ [\wp(z,\Lambda_1) : \wp'(z,\Lambda_1) : 1] \mapsto [\wp(\alpha z,\Lambda_2) : \wp'(\alpha z,\Lambda_2) : 1]$$

is an isomorphism of elliptic curves over $\mathbb{C}$. The essential step is to realize that $\wp(\alpha z,\Lambda_2) \in \mathbb{C}(\Lambda_1) = \mathbb{C}\big((\wp(z,\Lambda_1), \wp'(z,\Lambda_1)\big)$.

- Therefore, we have a one-to-one correspondence between

$$\{\text{Lattice in } \mathbb{C}/\text{Homothety}\} \leftrightarrow \{\text{Elliptic Curves over } \mathbb{C}/\text{Isomorphim}\}.$$

Homothety and Isomorphism

- Two lattice Λ_1 and Λ_2 in $\mathbb{C}$ are called homothetic if there exists $\alpha \in \mathbb{C}^{\times}$ such that $\alpha\Lambda_1 = \Lambda_2$.
- Multiplication by α induces a holomorphic isomomorphism

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2, \qquad \phi_\alpha(z) = \alpha z \mod \Lambda_2.$$

- The induced map on the corresponding elliptic curves

$$E_{\Lambda_1} \longrightarrow E_{\Lambda_2}, \ [\wp(z,\Lambda_1) : \wp'(z,\Lambda_1) : 1] \mapsto [\wp(\alpha z,\Lambda_2) : \wp'(\alpha z,\Lambda_2) : 1]$$

is an isomorphism of elliptic curves over $\mathbb{C}$. The essential step is to realize that $\wp(\alpha z,\Lambda_2) \in \mathbb{C}(\Lambda_1) = \mathbb{C}\big((\wp(z,\Lambda_1), \wp'(z,\Lambda_1)\big)$.

- Therefore, we have a one-to-one correspondence between

$$\{\text{Lattice in } \mathbb{C}/\text{Homothety}\} \leftrightarrow \{\text{Elliptic Curves over } \mathbb{C}/\text{Isomorphim}\}.$$

Homothety and Isomorphism

- Two lattice Λ_1 and Λ_2 in $\mathbb{C}$ are called homothetic if there exists $\alpha \in \mathbb{C}^{\times}$ such that $\alpha\Lambda_1 = \Lambda_2$.
- Multiplication by α induces a holomorphic isomomorphism

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2, \qquad \phi_\alpha(z) = \alpha z \mod \Lambda_2.$$

- The induced map on the corresponding elliptic curves

$$E_{\Lambda_1} \longrightarrow E_{\Lambda_2}, \ \ [\wp(z,\Lambda_1) : \wp'(z,\Lambda_1) : 1] \mapsto [\wp(\alpha z,\Lambda_2) : \wp'(\alpha z,\Lambda_2) : 1]$$

  is an isomorphism of elliptic curves over $\mathbb{C}$. The essential step is to realize that $\wp(\alpha z,\Lambda_2) \in \mathbb{C}(\Lambda_1) = \mathbb{C}\big((\wp(z,\Lambda_1), \wp'(z,\Lambda_1)\big)$.
- Therefore, we have a one-to-one correspondence between

$$\{\text{Lattice in } \mathbb{C}/\text{Homothety}\} \leftrightarrow \{\text{Elliptic Curves over } \mathbb{C}/\text{Isomorphim}\}.$$

Homothetic Lattices and the Upper Half Plane

- Let $\mathfrak{h} = \{\tau \in \mathbb{C} \mid Im(\tau) > 0\}$ be the complex upper half plane. Each $\tau \in \mathfrak{h}$ gives a corresponding lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.
- Given any lattice $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$, either $Im(w_2/w_1) > 0$ or $Im(w_1/w_2) > 0$. Assuming the latter and letting $\tau = w_1/w_2$, we find that $\Lambda = w_2(\mathbb{Z}\tau + \mathbb{Z}) = w_2\Lambda_\tau$. Thus any lattice in $\mathbb{C}$ is homothetic to Λ_τ for some $\tau \in \mathfrak{h}$.
- For $\tau,\ \tau' \in \mathfrak{h}$, the lattice Λ_τ is homothetic to $\Lambda_{\tau'}$ if and only if

  $$\tau' = \gamma\tau = \frac{a\tau + b}{c\tau + d} \text{ for some } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}):$$

  Clearly, $\tau' = \frac{a\tau+b}{c\tau+d}$ implies $(c\tau + d)\Lambda_{\tau'} = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) = \Lambda_\tau$.

  Conversely, $\alpha\Lambda_{\tau'} = \Lambda_\tau$ implies that $\alpha\tau' = a\tau + b$ and $\alpha = c\tau + d$ for some integers a, b, c, d such that $ad - bc = \pm 1$.

  Thus, $\tau' = \frac{a\tau+b}{c\tau+d}$, and $ad - bc = 1$ since $Im(\tau'),\ \ Im(\tau) > 0$.

Homothetic Lattices and the Upper Half Plane

- Let $\mathfrak{h} = \{\tau \in \mathbb{C} \mid Im(\tau) > 0\}$ be the complex upper half plane. Each $\tau \in \mathfrak{h}$ gives a corresponding lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.
- Given any lattice $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$, either $Im(w_2/w_1) > 0$ or $Im(w_1/w_2) > 0$. Assuming the latter and letting $\tau = w_1/w_2$, we find that $\Lambda = w_2(\mathbb{Z}\tau + \mathbb{Z}) = w_2\Lambda_\tau$. Thus any lattice in $\mathbb{C}$ is homothetic to Λ_τ for some $\tau \in \mathfrak{h}$.
- For $\tau,\ \tau' \in \mathfrak{h}$, the lattice Λ_τ is homothetic to $\Lambda_{\tau'}$ if and only if

  $$\tau' = \gamma\tau = \frac{a\tau + b}{c\tau + d} \text{ for some } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}):$$

  Clearly, $\tau' = \frac{a\tau+b}{c\tau+d}$ implies $(c\tau + d)\Lambda_{\tau'} = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) = \Lambda_\tau$.

  Conversely, $\alpha\Lambda_{\tau'} = \Lambda_\tau$ implies that $\alpha\tau' = a\tau + b$ and $\alpha = c\tau + d$ for some integers a, b, c, d such that $ad - bc = \pm 1$.

  Thus, $\tau' = \frac{a\tau+b}{c\tau+d}$, and $ad - bc = 1$ since $Im(\tau'),\ \ Im(\tau) > 0$.

Homothetic Lattices and the Upper Half Plane

- Let $\mathfrak{h} = \{\tau \in \mathbb{C} \mid Im(\tau) > 0\}$ be the complex upper half plane. Each $\tau \in \mathfrak{h}$ gives a corresponding lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.
- Given any lattice $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$, either $Im(w_2/w_1) > 0$ or $Im(w_1/w_2) > 0$. Assuming the latter and letting $\tau = w_1/w_2$, we find that $\Lambda = w_2(\mathbb{Z}\tau + \mathbb{Z}) = w_2\Lambda_\tau$. Thus any lattice in $\mathbb{C}$ is homothetic to Λ_τ for some $\tau \in \mathfrak{h}$.
- For $\tau,\ \tau' \in \mathfrak{h}$, the lattice Λ_τ is homothetic to $\Lambda_{\tau'}$ if and only if $\tau' = \gamma\tau = \dfrac{a\tau + b}{c\tau + d}$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$:

  Clearly, $\tau' = \frac{a\tau+b}{c\tau+d}$ implies $(c\tau + d)\Lambda_{\tau'} = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) = \Lambda_\tau$.

  Conversely, $\alpha\Lambda_{\tau'} = \Lambda_\tau$ implies that $\alpha\tau' = a\tau + b$ and $\alpha = c\tau + d$ for some integers a, b, c, d such that $ad - bc = \pm 1$.

  Thus, $\tau' = \frac{a\tau+b}{c\tau+d}$, and $ad - bc = 1$ since $Im(\tau'),\ \ Im(\tau) > 0$.

Homothetic Lattices and the Upper Half Plane

- Let $\mathfrak{h} = \{\tau \in \mathbb{C} \mid Im(\tau) > 0\}$ be the complex upper half plane. Each $\tau \in \mathfrak{h}$ gives a corresponding lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.
- Given any lattice $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$, either $Im(w_2/w_1) > 0$ or $Im(w_1/w_2) > 0$. Assuming the latter and letting $\tau = w_1/w_2$, we find that $\Lambda = w_2(\mathbb{Z}\tau + \mathbb{Z}) = w_2\Lambda_\tau$. Thus any lattice in $\mathbb{C}$ is homothetic to Λ_τ for some $\tau \in \mathfrak{h}$.
- For $\tau,\ \tau' \in \mathfrak{h}$, the lattice Λ_τ is homothetic to $\Lambda_{\tau'}$ if and only if $\tau' = \gamma\tau = \dfrac{a\tau + b}{c\tau + d}$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$:

  Clearly, $\tau' = \frac{a\tau+b}{c\tau+d}$ implies $(c\tau + d)\Lambda_{\tau'} = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) = \Lambda_\tau$.

  Conversely, $\alpha\Lambda_{\tau'} = \Lambda_\tau$ implies that $\alpha\tau' = a\tau + b$ and $\alpha = c\tau + d$ for some integers a, b, c, d such that $ad - bc = \pm 1$.

  Thus, $\tau' = \frac{a\tau+b}{c\tau+d}$, and $ad - bc = 1$ since $Im(\tau'),\ \ Im(\tau) > 0$.

Homothetic Lattices and the Upper Half Plane

- Let $\mathfrak{h} = \{\tau \in \mathbb{C} \mid Im(\tau) > 0\}$ be the complex upper half plane. Each $\tau \in \mathfrak{h}$ gives a corresponding lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.
- Given any lattice $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$, either $Im(w_2/w_1) > 0$ or $Im(w_1/w_2) > 0$. Assuming the latter and letting $\tau = w_1/w_2$, we find that $\Lambda = w_2(\mathbb{Z}\tau + \mathbb{Z}) = w_2\Lambda_\tau$. Thus any lattice in $\mathbb{C}$ is homothetic to Λ_τ for some $\tau \in \mathfrak{h}$.
- For $\tau,\ \tau' \in \mathfrak{h}$, the lattice Λ_τ is homothetic to $\Lambda_{\tau'}$ if and only if $\tau' = \gamma\tau = \dfrac{a\tau + b}{c\tau + d}$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$:

  Clearly, $\tau' = \frac{a\tau+b}{c\tau+d}$ implies $(c\tau + d)\Lambda_{\tau'} = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) = \Lambda_\tau$.

  Conversely, $\alpha\Lambda_{\tau'} = \Lambda_\tau$ implies that $\alpha\tau' = a\tau + b$ and $\alpha = c\tau + d$ for some integers a, b, c, d such that $ad - bc = \pm 1$.

  Thus, $\tau' = \frac{a\tau+b}{c\tau+d}$, and $ad - bc = 1$ since $Im(\tau'),\ \ Im(\tau) > 0$.

Homothetic Lattices and the Upper Half Plane

- Let $\mathfrak{h} = \{\tau \in \mathbb{C} \mid Im(\tau) > 0\}$ be the complex upper half plane. Each $\tau \in \mathfrak{h}$ gives a corresponding lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.
- Given any lattice $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$, either $Im(w_2/w_1) > 0$ or $Im(w_1/w_2) > 0$. Assuming the latter and letting $\tau = w_1/w_2$, we find that $\Lambda = w_2(\mathbb{Z}\tau + \mathbb{Z}) = w_2\Lambda_\tau$. Thus any lattice in $\mathbb{C}$ is homothetic to Λ_τ for some $\tau \in \mathfrak{h}$.
- For $\tau,\ \tau' \in \mathfrak{h}$, the lattice Λ_τ is homothetic to $\Lambda_{\tau'}$ if and only if $\tau' = \gamma\tau = \dfrac{a\tau + b}{c\tau + d}$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$:

  Clearly, $\tau' = \frac{a\tau+b}{c\tau+d}$ implies $(c\tau + d)\Lambda_{\tau'} = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) = \Lambda_\tau$.

  Conversely, $\alpha\Lambda_{\tau'} = \Lambda_\tau$ implies that $\alpha\tau' = a\tau + b$ and $\alpha = c\tau + d$ for some integers a, b, c, d such that $ad - bc = \pm 1$.

  Thus, $\tau' = \frac{a\tau+b}{c\tau+d}$, and $ad - bc = 1$ since $Im(\tau'),\ \ Im(\tau) > 0$.

Homothetic Lattices and the Upper Half Plane

- Let $\mathfrak{h} = \{\tau \in \mathbb{C} \mid Im(\tau) > 0\}$ be the complex upper half plane. Each $\tau \in \mathfrak{h}$ gives a corresponding lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.
- Given any lattice $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$, either $Im(w_2/w_1) > 0$ or $Im(w_1/w_2) > 0$. Assuming the latter and letting $\tau = w_1/w_2$, we find that $\Lambda = w_2(\mathbb{Z}\tau + \mathbb{Z}) = w_2\Lambda_\tau$. Thus any lattice in $\mathbb{C}$ is homothetic to Λ_τ for some $\tau \in \mathfrak{h}$.
- For $\tau,\ \tau' \in \mathfrak{h}$, the lattice Λ_τ is homothetic to $\Lambda_{\tau'}$ if and only if $\tau' = \gamma\tau = \dfrac{a\tau + b}{c\tau + d}$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$:

  Clearly, $\tau' = \frac{a\tau+b}{c\tau+d}$ implies $(c\tau + d)\Lambda_{\tau'} = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) = \Lambda_\tau$.

  Conversely, $\alpha\Lambda_{\tau'} = \Lambda_\tau$ implies that $\alpha\tau' = a\tau + b$ and $\alpha = c\tau + d$ for some integers a, b, c, d such that $ad - bc = \pm 1$.

  Thus, $\tau' = \frac{a\tau+b}{c\tau+d}$, and $ad - bc = 1$ since $Im(\tau'),\ \ Im(\tau) > 0$.

- Let $\mathfrak{h} = \{\tau \in \mathbb{C} \mid Im(\tau) > 0\}$ be the complex upper half plane. Each $\tau \in \mathfrak{h}$ gives a corresponding lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.
- Given any lattice $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$, either $Im(w_2/w_1) > 0$ or $Im(w_1/w_2) > 0$. Assuming the latter and letting $\tau = w_1/w_2$, we find that $\Lambda = w_2(\mathbb{Z}\tau + \mathbb{Z}) = w_2\Lambda_\tau$. Thus any lattice in $\mathbb{C}$ is homothetic to Λ_τ for some $\tau \in \mathfrak{h}$.
- For $\tau,\ \tau' \in \mathfrak{h}$, the lattice Λ_τ is homothetic to $\Lambda_{\tau'}$ if and only if $$\tau' = \gamma\tau = \frac{a\tau + b}{c\tau + d} \text{ for some } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}):$$

  Clearly, $\tau' = \frac{a\tau+b}{c\tau+d}$ implies $(c\tau + d)\Lambda_{\tau'} = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) = \Lambda_\tau.$

  Conversely, $\alpha\Lambda_{\tau'} = \Lambda_\tau$ implies that $\alpha\tau' = a\tau + b$ and $\alpha = c\tau + d$ for some integers a, b, c, d such that $ad - bc = \pm 1$.

  Thus, $\tau' = \frac{a\tau+b}{c\tau+d}$, and $ad - bc = 1$ since $Im(\tau'),\ \ Im(\tau) > 0$.

Homothetic Lattices and the Upper Half Plane

- Let $\mathfrak{h} = \{\tau \in \mathbb{C} \mid Im(\tau) > 0\}$ be the complex upper half plane. Each $\tau \in \mathfrak{h}$ gives a corresponding lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.
- Given any lattice $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$, either $Im(w_2/w_1) > 0$ or $Im(w_1/w_2) > 0$. Assuming the latter and letting $\tau = w_1/w_2$, we find that $\Lambda = w_2(\mathbb{Z}\tau + \mathbb{Z}) = w_2\Lambda_\tau$. Thus any lattice in $\mathbb{C}$ is homothetic to Λ_τ for some $\tau \in \mathfrak{h}$.
- For $\tau,\ \tau' \in \mathfrak{h}$, the lattice Λ_τ is homothetic to $\Lambda_{\tau'}$ if and only if

  $$\tau' = \gamma\tau = \frac{a\tau + b}{c\tau + d} \text{ for some } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}):$$

  Clearly, $\tau' = \frac{a\tau+b}{c\tau+d}$ implies $(c\tau + d)\Lambda_{\tau'} = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) = \Lambda_\tau.$

  Conversely, $\alpha\Lambda_{\tau'} = \Lambda_\tau$ implies that $\alpha\tau' = a\tau + b$ and $\alpha = c\tau + d$ for some integers a, b, c, d such that $ad - bc = \pm 1$.

  Thus, $\tau' = \frac{a\tau+b}{c\tau+d}$, and $ad - bc = 1$ since $Im(\tau'),\ \ Im(\tau) > 0$.

Moduli Space of Elliptic Curves

- We just saw that the set of homothetic classes of lattices is represented by the quotient $\dfrac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- It follows that each isomorphism class of elliptic curves over $\mathbb{C}$ is represented by a point on the quotient $\dfrac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- An isomorphism class (E, C) of an elliptic curve E with a cyclic subgroup C of order of order N is represented by a point $[\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle]$ in $\dfrac{\mathfrak{h}}{\Gamma_0(N)} =: Y_0(N)$, where $\Gamma_0(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0 \pmod{N}$.
- Compactifying $Y_0(N)$, one obtains $X_0(N) := \dfrac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_0(N)}$. The compact Riemann surface $X_0(N)$ is a curve defined by polynomials with rational coefficients.

Moduli Space of Elliptic Curves

- We just saw that the set of homothetic classes of lattices is represented by the quotient $\dfrac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- It follows that each isomorphism class of elliptic curves over $\mathbb{C}$ is represented by a point on the quotient $\dfrac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- An isomorphism class (E, C) of an elliptic curve E with a cyclic subgroup C of order of order N is represented by a point $[\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle]$ in $\dfrac{\mathfrak{h}}{\Gamma_0(N)} =: Y_0(N)$, where $\Gamma_0(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0$ (mod N).
- Compactifying $Y_0(N)$, one obtains $X_0(N) := \dfrac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_0(N)}$. The compact Riemann surface $X_0(N)$ is a curve defined by polynomials with rational coefficients.

Moduli Space of Elliptic Curves

- We just saw that the set of homothetic classes of lattices is represented by the quotient $\dfrac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- It follows that each isomorphism class of elliptic curves over $\mathbb{C}$ is represented by a point on the quotient $\dfrac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- An isomorphism class (E, C) of an elliptic curve E with a cyclic subgroup C of order of order N is represented by a point $[\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle]$ in $\dfrac{\mathfrak{h}}{\Gamma_0(N)} =: Y_0(N)$, where $\Gamma_0(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0 \pmod N$.
- Compactifying $Y_0(N)$, one obtains $X_0(N) := \dfrac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_0(N)}$. The compact Riemann surface $X_0(N)$ is a curve defined by polynomials with rational coefficients.

Moduli Space of Elliptic Curves

- We just saw that the set of homothetic classes of lattices is represented by the quotient $\dfrac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- It follows that each isomorphism class of elliptic curves over $\mathbb{C}$ is represented by a point on the quotient $\dfrac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- An isomorphism class (E, C) of an elliptic curve E with a cyclic subgroup C of order of order N is represented by a point $[\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle]$ in $\dfrac{\mathfrak{h}}{\Gamma_0(N)} =: Y_0(N)$, where $\Gamma_0(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0$ (mod N).
- Compactifying $Y_0(N)$, one obtains $X_0(N) := \dfrac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_0(N)}$. The compact Riemann surface $X_0(N)$ is a curve defined by polynomials with rational coefficients.

Moduli Space of Elliptic Curves

- We just saw that the set of homothetic classes of lattices is represented by the quotient $\frac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- It follows that each isomorphism class of elliptic curves over $\mathbb{C}$ is represented by a point on the quotient $\frac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- An isomorphism class (E, C) of an elliptic curve E with a cyclic subgroup C of order of order N is represented by a point $[\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle]$ in $\frac{\mathfrak{h}}{\Gamma_0(N)} =: Y_0(N)$, where $\Gamma_0(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0$ (mod N).
- Compactifying $Y_0(N)$, one obtains $X_0(N) := \frac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_0(N)}$. The compact Riemann surface $X_0(N)$ is a curve defined by polynomials with rational coefficients.

Moduli Space of Elliptic Curves

- We just saw that the set of homothetic classes of lattices is represented by the quotient $\frac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- It follows that each isomorphism class of elliptic curves over $\mathbb{C}$ is represented by a point on the quotient $\frac{\mathfrak{h}}{SL_2(\mathbb{Z})}$.
- An isomorphism class (E, C) of an elliptic curve E with a cyclic subgroup C of order of order N is represented by a point $[\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle]$ in $\frac{\mathfrak{h}}{\Gamma_0(N)} =: Y_0(N)$, where $\Gamma_0(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0$ (mod N).
- Compactifying $Y_0(N)$, one obtains $X_0(N) := \frac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_0(N)}$. The compact Riemann surface $X_0(N)$ is a curve defined by polynomials with rational coefficients.

An Application

- An isomorphism class (E, P) of an elliptic curve E with a specified point P of order of order N is represented by a point $[\Lambda_\tau, \frac{1}{N} + \Lambda_\tau]$ in $\dfrac{\mathfrak{h}}{\Gamma_1(N)} =: Y_1(N)$, where $\Gamma_1(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0 \pmod N$, $a \equiv d \equiv 1 \pmod N$.
- For example, by compactifying $Y_1(11)$ one obtains $X_1(11) := \dfrac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_1(N)}$, whose defining equation turns out to be

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

One can further check that $X_1(11)(\mathbb{Q})$ has only five points, all of which are 'cusps', i.,e., these points do not belong to $Y_1(11)(\mathbb{Q})$. One can then conclude that there is no elliptic curve defined over $\mathbb{Q}$ with a point of order 11.

An Application

- An isomorphism class (E, P) of an elliptic curve E with a specified point P of order of order N is represented by a point $[\Lambda_\tau, \frac{1}{N} + \Lambda_\tau]$ in $\dfrac{\mathfrak{h}}{\Gamma_1(N)} =: Y_1(N)$, where $\Gamma_1(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0$ (mod N), $a \equiv d \equiv 1$ (mod N).

- For example, by compactifying $Y_1(11)$ one obtains $X_1(11) := \dfrac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_1(N)}$, whose defining equation turns out to be

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

One can further check that $X_1(11)(\mathbb{Q})$ has only five points, all of which are 'cusps', i.,e., these points do not belong to $Y_1(11)(\mathbb{Q})$. One can then conclude that there is no elliptic curve defined over $\mathbb{Q}$ with a point of order 11.

An Application

- An isomorphism class (E, P) of an elliptic curve E with a specified point P of order of order N is represented by a point $[\Lambda_\tau, \frac{1}{N} + \Lambda_\tau]$ in $\frac{\mathfrak{h}}{\Gamma_1(N)} =: Y_1(N)$, where $\Gamma_1(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0$ (mod N), $a \equiv d \equiv 1$ (mod N).
- For example, by compactifying $Y_1(11)$ one obtains $X_1(11) := \frac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_1(N)}$, whose defining equation turns out to be

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

One can further check that $X_1(11)(\mathbb{Q})$ has only five points, all of which are 'cusps', i.,e., these points do not belong to $Y_1(11)(\mathbb{Q})$. One can then conclude that there is no elliptic curve defined over $\mathbb{Q}$ with a point of order 11.

An Application

- An isomorphism class (E, P) of an elliptic curve E with a specified point P of order of order N is represented by a point $[\Lambda_\tau, \frac{1}{N} + \Lambda_\tau]$ in $\frac{\mathfrak{h}}{\Gamma_1(N)} =: Y_1(N)$, where $\Gamma_1(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0$ (mod N), $a \equiv d \equiv 1$ (mod N).
- For example, by compactifying $Y_1(11)$ one obtains $X_1(11) := \frac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_1(N)}$, whose defining equation turns out to be

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

One can further check that $X_1(11)(\mathbb{Q})$ has only five points, all of which are 'cusps', i.,e., these points do not belong to $Y_1(11)(\mathbb{Q})$. One can then conclude that there is no elliptic curve defined over $\mathbb{Q}$ with a point of order 11.

An Application

- An isomorphism class (E, P) of an elliptic curve E with a specified point P of order of order N is represented by a point $[\Lambda_\tau, \frac{1}{N} + \Lambda_\tau]$ in $\dfrac{\mathfrak{h}}{\Gamma_1(N)} =: Y_1(N)$, where $\Gamma_1(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0$ (mod N), $a \equiv d \equiv 1$ (mod N).
- For example, by compactifying $Y_1(11)$ one obtains $X_1(11) := \dfrac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_1(N)}$, whose defining equation turns out to be

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

One can further check that $X_1(11)(\mathbb{Q})$ has only five points, all of which are 'cusps', i.,e., these points do not belong to $Y_1(11)(\mathbb{Q})$. One can then conclude that there is no elliptic curve defined over $\mathbb{Q}$ with a point of order 11.

An Application

- An isomorphism class (E, P) of an elliptic curve E with a specified point P of order of order N is represented by a point $[\Lambda_\tau, \frac{1}{N} + \Lambda_\tau]$ in $\dfrac{\mathfrak{h}}{\Gamma_1(N)} =: Y_1(N)$, where $\Gamma_1(N)$ is a subgroup of $SL_2(\mathbb{Z})$ consisting of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $c \equiv 0 \pmod{N}$, $a \equiv d \equiv 1 \pmod{N}$.
- For example, by compactifying $Y_1(11)$ one obtains $X_1(11) := \dfrac{\mathfrak{h} \cup \{\infty\} \cup \mathbb{Q}}{\Gamma_1(N)}$, whose defining equation turns out to be

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

One can further check that $X_1(11)(\mathbb{Q})$ has only five points, all of which are 'cusps', i.,e., these points do not belong to $Y_1(11)(\mathbb{Q})$. One can then conclude that there is no elliptic curve defined over $\mathbb{Q}$ with a point of order 11.

Possible Torsion for $E/\mathbb{Q}$

For $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$, one can check that $X_1(N)$ has genus 0. Thus, $X_1(N)(\mathbb{Q})$ has infinitely many rational points, and correspondingly, we have infinitely many elliptic curves over $\mathbb{Q}$ with an N-torsion point.

Additional References

- *A First Course in Modular Forms*, F. Diamond and J. Shurman, Springer 2005.
- *The Modular Curves $X_0(11)$ and $X_1(11)$*, Tom Weston.

Possible Torsion for $E/\mathbb{Q}$

For $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$, one can check that $X_1(N)$ has genus 0. Thus, $X_1(N)(\mathbb{Q})$ has infinitely many rational points, and correspondingly, we have infinitely many elliptic curves over $\mathbb{Q}$ with an N-torsion point.

Additional References

- *A First Course in Modular Forms*, F. Diamond and J. Shurman, Springer 2005.
- *The Modular Curves $X_0(11)$ and $X_1(11)$*, Tom Weston.

Possible Torsion for $E/\mathbb{Q}$

For $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$, one can check that $X_1(N)$ has genus 0. Thus, $X_1(N)(\mathbb{Q})$ has infinitely many rational points, and correspondingly, we have infinitely many elliptic curves over $\mathbb{Q}$ with an N-torsion point.

Additional References

- *A First Course in Modular Forms*, F. Diamond and J. Shurman, Springer 2005.
- *The Modular Curves $X_0(11)$ and $X_1(11)$*, Tom Weston.

THANK YOU