Lecture 3

Introduction

In this lecture, we will finally connect points of $\text{SL}_2(\mathbb{Z}) \backslash \mathcal{H}$ with isomorphism classes of elliptic curves over $\mathbb{C}$. To do so, we will first establish a correspondence between points of $\text{SL}_2(\mathbb{Z}) \backslash \mathcal{H}$ and equivalence classes of certain subgroups of $\mathbb{C}$. We will then establish a correspondence between those equivalence classes and isomorphism classes of elliptic curves over $\mathbb{C}$.

Lattices

**Definition 1** A lattice $\Lambda \subset \mathbb{C}$ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}$-basis for $\mathbb{C}$. Such a subgroup is given by

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

Here, $\{\omega_1, \omega_2\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.

**Remark 2** Throughout, we make the convention that the basis $\{\omega_1, \omega_2\}$ is oriented so that $\omega_1/\omega_2 \in \mathcal{H}$.

It is important to note that oriented bases are not unique.

**Proposition 3** Let $\Lambda \subset \mathbb{C}$ be a lattice. Then $\{\omega_1, \omega_2\}$ and $\{\omega'_1, \omega'_2\}$ are two oriented bases for $\Lambda$ if and only if

$$\gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix},$$

for some $\gamma \in \text{SL}_2(\mathbb{Z})$.

The proof of this proposition is one of the exercises in the problem set for this lecture.

We now introduce an equivalence relation on the lattices of $\mathbb{C}$; first, we have the following definition:

**Definition 4** Two lattices $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ are homothetic if $\Lambda_1 = \alpha \Lambda_2$ for some $\alpha \in \mathbb{C}^*$.

**Claim 5** Homothety is an equivalence relation

**Proposition 6** (A) Each lattice $\Lambda$ is homothetic to a lattice $\Lambda_\tau$ with basis $\{\tau, 1\}$ for some $\tau \in \mathcal{H}$.

(B) For $\tau_1, \tau_2 \in \mathcal{H}$, the lattices $\Lambda_{\tau_1}$ (with basis $\{\tau_1, 1\}$) and $\Lambda_{\tau_2}$ (with basis $\{\tau_2, 1\}$) are homothetic if and only if $\gamma \tau_1 = \tau_2$ for some $\gamma \in \text{SL}_2(\mathbb{Z})$.

**Proof:** (A) This is an exercise in the problem set for this lecture.

(B) Suppose $\Lambda_{\tau_1}$ and $\Lambda_{\tau_2}$ are homothetic. Then $\alpha \Lambda_{\tau_1} = (\alpha \tau_1)Z + \alpha Z = \Lambda_{\tau_2}$ for some $\alpha \in \mathbb{C}^*$. Since $\{\alpha \tau_1, \alpha\}$ is an oriented basis for $\Lambda_{\tau_2}$, by Prop. 3 there is some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \begin{pmatrix} \alpha \tau_1 \\ \alpha \end{pmatrix} = \begin{pmatrix} \alpha & \tau_2 \\ c & d \end{pmatrix}.$$ 

It follows then that

$$\tau_2 = \frac{\tau_2}{1} = \frac{\alpha \tau_1 + \alpha b}{\alpha c \tau_1 + \alpha d} = \frac{a \tau_1 + b}{c \tau_1 + d} = \gamma \tau_1.$$
Next, suppose that $\gamma \tau_1 = \tau_2$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Then since $\tau_1 \in \mathcal{H}$ and at least one of $c, d$ is nonzero, we have $1/(ct_1 + d) \in \mathbb{C}^*$ and
\[
\left(\frac{1}{ct_1 + d}\right)\Lambda_2 = \left(\frac{1}{ct_1 + d}\right)(\tau_2 \mathbb{Z} + \mathbb{Z}) = (a\tau_1 + b)\mathbb{Z} + (ct_1 + d)\mathbb{Z}.
\]
By Prop. 3, this is an oriented basis for $\Lambda_1$. □

From part (A) of this proposition, we have that every lattice $\Lambda \subset \mathbb{C}$ is homothetic to some lattice $\Lambda_\tau$ with basis $\{\tau, 1\}$ and $\tau \in \mathcal{H}$. By part (B), we can say more:

**Corollary 7** There is a one-to-one correspondence
\[
\{\text{Homothety classes of lattices } \Lambda \subset \mathbb{C}\} \overset{1:1}{\longleftrightarrow} SL_2(\mathbb{Z})/\mathcal{H}
\]

The quotient $\mathbb{C}/\Lambda$

Later in this lecture, we will show that given a lattice $\Lambda \subset \mathbb{C}$, there is a map from quotient $\mathbb{C}/\Lambda$ to $E(\mathbb{C})$, the $\mathbb{C}$ points of an elliptic curve $E$. Even at this stage, we can establish some important facts about $\mathbb{C}/\Lambda$.

**Theorem 8** Holomorphic maps $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ with $\varphi(0) = 0$ correspond to scalar multiplication $a\Lambda \subseteq \Lambda'$.

Such maps are group homomorphisms and have finite kernel unless $\varphi$ is the zero map. A complex analytic isomorphism $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ exists if and only if $\Lambda$ and $\Lambda'$ are homothetic.

The Weierstrass $\wp$-function of $\Lambda$

In this section, we will see how a lattice $\Lambda$ gives rise to an elliptic curve. For this and the following section, we will highlight the key results, then we will state the necessary theorems that lead to these key results. We will assume a level of familiarity with holomorphic functions. We also state a number of results without proof, but for a more complete discussion, Complex Analysis by Ahlfors ([1]), The Arithmetic of Elliptic Curves by Silverman ([2]), or Sutherland’s notes ([Lecture 15, 3]) are nice references.

Given a lattice $\Lambda$, we first define a very important function, the Weierstrass $\wp$-function.

**Definition 9** Let $\Lambda \subset \mathbb{C}$ be a lattice. The Weierstrass $\wp$-function of $\Lambda$ is
\[
\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda'} \left( \frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right),
\]
where $\sum_{\lambda \in \Lambda'}$ indicates that the sum is taken over nonzero $\lambda \in \Lambda$.

**Remark 10** Fixing a lattice $\Lambda$, we will write $\wp(z)$ to ease notation.

The Weierstrass $\wp$-function is an example of an elliptic function.

**Definition 11** An elliptic function for a lattice $\Lambda$ is a complex function $f(z)$ such that
(i) $f$ is meromorphic on $\mathbb{C}$ (i.e., holomorphic except for a discrete set of poles).
(ii) $f(z + \lambda) = f(z)$ for all $\lambda \in \Lambda$. 
In order to show that \( \wp \) is meromorphic, one shows that it has poles of order two for each \( \lambda \in \Lambda \) (which is hopefully easy to see from the definition) and that it has no other poles in \( \mathbb{C} \). In fact, \( \wp \) is holomorphic, with the series defining \( \wp \) converge absolutely and uniformly on all compact subset of \( \mathbb{C} \) disjoint from \( \Lambda \) \( ([2] \text{ VI.3.1}) \).

To show that \( \wp \) is periodic with respect to \( \Lambda \), it is easier to first show that its derivative

\[
\wp'(z) = -2 \sum_{\lambda \in \Lambda} \frac{1}{(z - \lambda)^3}
\]

is periodic. Since \( \wp' \) is periodic, one has \( \wp'(z + \omega_k) - \wp'(z) = 0 \) for each \( z \notin \Lambda \) (where \( \{\omega_1, \omega_2\} \) is a basis for \( \Lambda \)), so that \( \wp(z + \omega_k) - \wp(z) \) is constant for each \( k = 1, 2 \). Using the fact that \( \omega_k/2 \notin \Lambda \) and the fact that \( \wp \) is an even function, one then concludes that \( \wp(-\omega_k/2 + \omega_k) = \wp(\omega_k/2) = \wp(-\omega_k/2) \), so that \( \wp(z + \omega_k) - \wp(z) = 0 \).

One will note that since \( \wp \) is meromorphic, so too is \( \wp' \) - it has poles of order three at each \( \lambda \in \Lambda \), and poles nowhere else. In order to associate to a lattice \( \Lambda \) an elliptic curve \( E/\mathbb{C} \), the following series will also be important:

**Definition 12** The Eisenstein series of weight \( 2k \) for \( \Lambda \) is the series

\[
G_{2k}(\Lambda) = \sum_{\lambda \in \Lambda} \lambda^{-2k}
\]

These series appear in the Laurent series expansion of \( \wp \) ([1], §7.3.3]), and using this expansion, one can finally relate the lattice \( \Lambda \) to an equation for an elliptic curve: Again fixing a lattice \( \Lambda \), we define \( g_2 = g_2(\Lambda) = 60G_4(\Lambda) \) and \( g_3 = g_3(\Lambda) = 140G_6(\Lambda) \). With these definitions in place, we can state the key results for this section.

**Theorem 13** For \( \mathbb{C} \setminus \Lambda \), the Weierstrass \( \wp \)-function and its derivative satisfy the relation

\[
\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3
\]

(For a proof, see [3] Thm. 15.29.) If we let \( y = \wp'(z) \), \( x = \wp(z) \), then \( y^2 = 4x^3 - g_2x - g_3 \) will define an elliptic curve, provided \( g_3^3 - 27g_2^2 \neq 0 \). This equation can be put into Weierstrass form by letting \( A = \frac{g_2}{4} \) and \( B = \frac{g_3}{4} \). Moreover, using \( \wp \) and \( \wp' \), we obtain a map from \( \mathbb{C}/\Lambda \) to complex points \( E(\mathbb{C}) \) for the elliptic curve \( E \) defined by \( y^2 = 4x^3 - g_2x - g_3 \).

**Theorem 14** Let \( \Lambda \) be a lattice, and let \( g_2 = g_2(\Lambda) \) and \( g_3 = g_3(\Lambda) \) be as above. Then
(A) The polynomial \( 4x^3 - g_2x - g_3 \) has distinct roots so that its discriminant \( g_2^3 - 27g_3^2 \neq 0 \).
(B) Let \( E/\mathbb{C} \) be the elliptic curve

\[
E : y^2 = 4x^3 - g_2x - g_3.
\]

The map

\[
z \mapsto \begin{cases} (\wp(z), \wp'(z)) & \text{if } z \notin \Lambda \\ O & \text{if } z \in \Lambda \end{cases}
\]

yields a group isomorphism \( \mathbb{C}/\Lambda \to E(\mathbb{C}) \).
Given an elliptic curve

Definition 17

A, B ∈ \mathbb{K}

satisfy

Thus \( g'(\omega_k/2) = -g'(\omega_k/2). \) Therefore, if \( e_k = \omega_k/2 \) is a zero of \( 4g(z)^3g_2g(z) - g_3. \) The same holds for \( e_3 = \frac{\omega_1 + \omega_2}{2}; \) therefore, if \( g'(e_1), g'(e_2), \) and \( g'(e_3) \) are all distinct, \( g_3^2 - 27g_2^3 \) will be nonzero.

To establish this last fact, we use the fact that in a fundamental parallelogram for \( \Lambda, \) an elliptic function for \( \Lambda \) has as many zeros as it does poles. Since the function \( g(z) - g(e_k) \) has a double pole only at the lattice point in a fundamental parallelogram and it has a double zero at \( e_k, \) these are its only zeros, so if \( e_j \neq e_k, \) then \( g(e_j) - g(e_k) \neq 0. \)

Elliptic curves and their associated Lattices

In the first section, we established that equivalence classes of lattices (i.e., lattices up to homothety) are in bijection with the set \( \text{SL}_2(\mathbb{Z}) \backslash \mathcal{H}. \) In the previous section, we showed that a lattice \( \Lambda \) gives rise to a complex torus \( \mathbb{C}/\Lambda \) which is isomorphic to an elliptic curve. In this section, we will show that an elliptic curve \( E/\mathbb{C} \) can be associated to a lattice. Having done so, we will have established the following

Proposition 15

Isomorphism classes of elliptic curves are isomorphism classes of elliptic curves \( E/\mathbb{C} \) are in one-to-one correspondence with homothety classes of lattices \( \Lambda \subset \mathbb{C}, \) which are in one-to-one correspondence with orbits of \( \mathcal{H} \) under the \( \text{SL}_2(\mathbb{Z}) \) action.

To show that we can associate an elliptic curve \( E/\mathbb{C} \) to a lattice, we must first introduce the \( j \)-invariant of a lattice and the \( j \)-invariant of an elliptic curve.

Definition 16

Given a lattice \( \Lambda \subset \mathbb{C}, \) the \( j \)-invariant of \( \Lambda \) is defined by

\[
j(\Lambda) = 1728 \frac{g_3(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}
\]

Recall that in the first lecture, we stated that an elliptic curve \( E \) defined over a field \( \mathbb{K} \) of characteristic zero (for example, \( \mathbb{K} = \mathbb{C} \)) can be described by an equation \( E : y^2 = x^3 + Ax + B, \) where \( A, B \in \mathbb{K} \) satisfy \(-16(4A^3 + 27B^2) \neq 0.\)

Definition 17

Given an elliptic curve \( E : y^2 = x^3 + Ax + B, \) where \( A, B \in \mathbb{K} \) satisfy \(-16(4A^3 + 27B^2) \neq 0, \) the \( j \)-invariant of \( E \) is defined by

\[
j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}
\]

If \( \Lambda \subset \mathbb{C} \) is a lattice and \( E_\Lambda : y^2 = 4x^3 - g_2x - g_3 \) is the elliptic curve isomorphic to \( \mathbb{C}/\Lambda, \) then \( E_\Lambda \) is isomorphic to an elliptic curve given by \( E : y^2 = x^3 + Ax + B, \) where \( A = -\frac{g_2}{4} \) and \( B = -\frac{g_3}{4}, \) and we have \( j(\Lambda) = j(E). \) Moreover, if two lattices \( \Lambda_1 \) and \( \Lambda_2 \) are homothetic, then \( j(\Lambda_1) = j(\Lambda_2). \) It is not the case in general that the elliptic curves \( E_1 \) and \( E_2, \) associated to \( \Lambda_1 \) and \( \Lambda_2 \) respectively, but they are isomorphic.

Finally, to conclude the lecture, we state the Uniformization Theorem for elliptic curves...
Theorem 18 Let $E/\mathbb{C}$ be an elliptic curve given by $E : y^2 = 4x^3 - a_2x - a_3$. Then there is a lattice $\Lambda \subset \mathbb{C}$ such that $a_2 = g_2(\Lambda)$ and $a_3 = g_3(\Lambda)$.

We will briefly explain the role of the $j$-invariant here, and discuss the function further in the next lecture. Among the relevant facts about the function $j$ is that it defines a surjection $j : \mathcal{H} \to \mathbb{C}, \tau \mapsto \tau(\Lambda_\tau)$. Thus, given an elliptic curve $E$ with $j$-invariant $j(E)$, we can find a lattice $\Lambda_\tau$ whose $j$-invariant equals $j(E)$, and the elliptic curve $E_\tau$ associated to $\Lambda_\tau$ is isomorphic to $E$.

References

