16 Elliptic curves over $\mathbb{C}$ (part 2)

Last time we showed that every lattice $L \subseteq \mathbb{C}$ gives rise to an elliptic curve

$$E_L\colon y^2 = 4x^3 - g_2(L)x - g_3(L),$$

where

$$g_2(L) = 60G_4(L) := 60\sum_{L^*}\frac{1}{\omega^4}, \qquad g_3(L) = 140G_6(L) = 140\sum_{L^*}\frac{1}{\omega^6},$$

with $L^* := L - \{0\}$, and we defined a map

$$\begin{aligned}\Phi\colon \mathbb{C}/L &\to E_L(\mathbb{C})\\ z &\mapsto \begin{cases}(\wp(z), \wp'(z)) & z \notin L\\ 0 & z \in L\end{cases}\end{aligned}$$

where

$$\wp(z) = \wp(z;L) = \frac{1}{z^2} + \sum_{\omega\in L^*}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

is the Weierstrass $\wp$-function for the lattice L, and

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

In this lecture is to prove two theorems. First we will prove that Φ is an isomorphism of additive groups; it is also an isomorphism of complex manifolds [3, Cor. 5.1.1], and of complex Lie groups, but we won't prove this now.[1] Second, we will prove that every elliptic curve $E/\mathbb{C}$ is isomorphic to E_L for some lattice L; this is also known as the Uniformization Theorem.

16.1 The isomorphism from a torus to the corresponding elliptic curve

Theorem 16.1. *Let $L \subseteq \mathbb{C}$ be a lattice and let $E_L\colon y^2 = 4x^3 - g_2(L)x - g_3(L)$ be the corresponding elliptic curve. The map $\Phi\colon \mathbb{C}/L \to E_L(\mathbb{C})$ is a group isomorphism.*

Proof. We first note that $\Phi(0) = 0$, so Φ preserves the identity, and for all $z \notin L$ we have

$$\Phi(-z) = (\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z)) = -\Phi(z),$$

since $\wp$ is even and $\wp'$ is odd, so Φ is compatible with taking inverses.

Let $L = [\omega_1, \omega_2]$. There are three points of order 2 in $\mathbb{C}/L$; if $L = [\omega_1, \omega_2]$ these are $\omega_1/2, \omega_2/2$, and $(\omega_1 + \omega_2)/2$. By Lemma 15.31, $\wp'$ vanishes these points, hence Φ maps points of order 2 in $\mathbb{C}/L$ to points of order 2 in $E_L(\mathbb{C})$, since the latter are the points with y-coordinate zero. Moreover, Φ is injective on points of order 2, since $\wp(z)$ maps each point of order 2 in $\mathbb{C}/L$ to a distinct root of $4\wp(z)^3 - g_2(L)\wp(z) - g_3(L)$, as shown in the proof of Lemma 15.32. The restriction of Φ to $(\mathbb{C}/L)[2]$ defines a bijection of $(\mathbb{C}/L)[2] \xrightarrow{\sim} E_L[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with $\Phi(0) = 0$, which must be a group isomorphism.

[1] This is not difficult to show, but it would distract us from our immediate goal. We will see an explicit isomorphism of complex manifolds in a few lectures when we study modular curves, and in that case we will take the time to define precisely what this means and to prove it.

Lecture by Andrew Sutherland

To show that Φ is surjective, let $(x_0, y_0) \in E_L(\mathbb{C})$. The elliptic function $f(z) = \wp(z) - x_0$ has order 2, hence it has two zeros in the fundamental parallelogram $\mathcal{F}_0$, by Theorem 15.18. Neither of these zeros occurs at $z = 0$, since f has a pole at 0. So let $z_0 \neq 0$ be a zero of $f(z)$ in $\mathcal{F}_0$. Then $\wp(z_0) = x_0$, which implies $\Phi(z_0) = (x_0, \pm y_0)$ and therefore $(x_0, y_0) = \Phi(\pm z_0)$; thus Φ is surjective.

We now show that Φ is injective. Let $z_1, z_2 \in \mathcal{F}_0$ and suppose that $\Phi(z_1) = \Phi(z_2)$. If $2z_1 \in L$ then z_1 is a 2-torsion element and we have already shown that Φ restricts to a bijection on $(\mathbb{C}/L)[2]$, so we must have $z_1 = z_2$. We now assume $2z_1 \notin L$, which implies $\wp'(z_1) \neq 0$. As argued above, the roots of $f(z) = \wp(z) - \wp(z_1)$ in $\mathcal{F}_0$ are $\pm z_1$, thus $z_2 \equiv \pm z_1 \bmod L$. We also have $\wp'(z_1) = \wp'(z_2)$, and this forces $z_2 \equiv z_1 \bmod L$, since $\wp'(-z_1) = -\wp'(z_1) \neq \wp'(z_1)$ because $\wp'(z_1) \neq 0$.

It remains only to show that $\Phi(z_1 + z_2) = \Phi(z_1) + \Phi(z_2)$. So let $z_1, z_2 \in \mathcal{F}_0$; we may assume that $z_1, z_2, z_1 + z_2 \notin L$ since the case where either z_1 or z_2 lies in L is immediate, and if $z_1 + z_2 \in L$ then z_1 and z_2 are inverses modulo L, a case treated above.

The points $P_1 = \Phi(z_1)$ and $P_2 = \Phi(z_2)$ are affine points in $E_L(\mathbb{C})$, and the line ℓ between them cannot be vertical because P_1 and P_2 are not inverses (since z_1 and z_2 are not). So let $y = mx + b$ be an equation for this line, and let P_3 be the third point where the line intersects the curve E_L. Then $P_1 + P_2 + P_3 = 0$, by the definition of the group law on $E_L(\mathbb{C})$.

Now consider the function $\ell(z) = -\wp'(z) + m\wp(z) + b$. It is an elliptic function of order 3 with a triple pole at 0, so it has three zeros in the fundamental region $\mathcal{F}_0$, two of which are z_1 and z_2. Let z_3 be the third zero in $\mathcal{F}_0$. The point $\Phi(z_3)$ lies on both the line ℓ and the elliptic curve $E_L(C)$, hence it must lie in $\{P_1, P_2, P_3\}$; moreover, we have a bijection from $\{z_1, z_2, z_3\}$ to $\{\Phi(z_1), \Phi(z_2), \Phi(z_3)\} = \{P_1, P_2, P_3\}$, and this bijection must send z_3 to P_3 if P_3 is distinct from P_1 and P_2. If P_3 coincides with exactly one of P_1 or P_2, say P_1, then $\ell(z)$ has a double zero at z_1 and we must have $z_3 = z_1$; and if $P_1 = P_2 = P_3$ then clearly $z_1 = z_2 = z_3$. Thus in every case we must have $P_3 = \Phi(z_3)$.

We have $P_1 + P_2 + P_3 = 0$, so it suffices to show $z_1 + z_2 + z_3 \in L$, since this implies

$$\Phi(z_1 + z_2) = \Phi(-z_3) = -\Phi(z_3) = -P_3 = P_1 + P_2 = \Phi(z_1) + \Phi(z_2).$$

Let $\mathcal{F}_\alpha$ be a fundamental region for L whose boundary does not contain any zeros or poles of $\ell(z)$ and replace z_1, z_2, z_3 by equivalent points in $\mathcal{F}_\alpha$ if necessary.

Applying Theorem 15.17 to $g(z) = z$ and $f(z) = \ell(z)$ yields

$$\frac{1}{2\pi i}\int_{\partial \mathcal{F}_\alpha} z\frac{\ell'(z)}{\ell(z)}dz = \sum_{w \in F_\alpha} \operatorname{ord}_w(\ell) w = z_1 + z_2 + z_3 - 3\cdot 0 = z_1 + z_2 + z_3, \tag{1}$$

where the boundary $\partial \mathcal{F}_\alpha$ of $\mathcal{F}_\alpha$ is oriented counter-clockwise.

Let us now evaluate the integral in (1); to ease the notation, define $f(z) := \ell'(z)/\ell(z)$, which we note is an elliptic function (hence periodic with respect to L). We then have

$$\begin{aligned}\int_{\partial F_\alpha} zf(z)\,dz &= \int_\alpha^{\alpha+\omega_1} zf(z)dz + \int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} zf(z)dz + \int_{\alpha+\omega_1+\omega_2}^{\alpha+\omega_2} zf(z)dz + \int_{\alpha+\omega_2}^{\alpha} zf(z)dz\\ &= \int_\alpha^{\alpha+\omega_1} zf(z)dz + \int_\alpha^{\alpha+\omega_2}(z+\omega_1)f(z)dz + \int_{\alpha+\omega_1}^{\alpha}(z+\omega_2)f(z)dz + \int_{\alpha+\omega_2}^{\alpha} zf(z)dz\\ &= \omega_1\int_\alpha^{\alpha+\omega_2} f(z)dz + \omega_2\int_{\alpha+\omega_1}^{\alpha} f(z)dz.\end{aligned} \tag{2}$$

Note that we have used the periodicity of $f(z)$ to replace $f(z+\omega_i)$ by $f(z)$, and to cancel integrals in opposite directions along lines that are equivalent modulo L.

For any closed (not necessarily simple) curve C and a point $z_0 \notin C$, the quantity

$$\frac{1}{2\pi i}\int_C \frac{dz}{z-z_0}$$

is the *winding number* of C about z_0, and it is an integer (it counts the number of times the curve C "winds around" the point z_0); see [1, Lem. 4.2.1] or [4, Lem. B.1.3].

The function $\ell(\alpha+t\omega_2)$ parametrizes a closed curve C_1 from $\ell(\alpha)$ to $\ell(\alpha+\omega_2)=\ell(\alpha)$, as t ranges from 0 to 1. The winding number of C_1 about the point 0 is the integer

$$c_1 := \frac{1}{2\pi i}\int_{C_1}\frac{dz}{z-0} = \frac{1}{2\pi i}\int_0^1 \frac{\ell'(\alpha+t\omega_2)}{\ell(\alpha+t\omega_2)}\omega_2 dt = \frac{1}{2\pi i}\int_\alpha^{\alpha+w_2}\frac{\ell'(z)}{\ell(z)}dz = \frac{1}{2\pi i}\int_\alpha^{\alpha+\omega_2} f(z)dz. \quad (3)$$

Similarly, the function $\ell(\alpha+t\omega_1)$ parameterizes a closed curve C_2 from $\ell(\alpha)$ to $\ell(\alpha+\omega_1)$, and we obtain the integer

$$c_2 := \frac{1}{2\pi i}\int_{C_2}\frac{dz}{z-0} = \frac{1}{2\pi i}\int_0^1 \frac{\ell'(\alpha+t\omega_1)}{\ell(\alpha+t\omega_1)}\omega_1 dt = \frac{1}{2\pi i}\int_\alpha^{\alpha+\omega_1}\frac{\ell'(z)}{\ell(z)}dz = \frac{1}{2\pi i}\int_\alpha^{\alpha+\omega_1} f(z)\,dz. \quad (4)$$

Plugging (3), and (4) into (2), and applying (1), we see that

$$z_1+z_2+z_3 = c_1\omega_1 - c_2\omega_2 \in L,$$

as desired. □

16.2 The j-invariant of a lattice

Definition 16.2. The *j-invariant* of a lattice L is defined by

$$j(L) = 1728\frac{g_2(L)^3}{\Delta(L)} = 1728\frac{g_2(L)^3}{g_2(L)^3-27g_3(L)^2}.$$

Recall that $\Delta(L)\neq 0$, by Lemma 15.32, so $j(L)$ is always defined.

The elliptic curve $E_L\colon y^2 = 4x^3 - g_2(L)x - g_3(L)$ is isomorphic to the elliptic curve $y^2 = x^3+Ax+B$, where $g_2(L) = -4A$ and $g_3(L) = -4B$. Thus

$$j(L) = 1728\frac{g_2(L)^3}{g_2(L)^3-27g_3(L)^2} = 1728\frac{(-4A)^3}{(-4A)^3-27(-4B)^2} = 1728\frac{4A^3}{4A^3+27B^2} = j(E_L).$$

Thus the j-invariant of a lattice L is the same as the j-invariant of the corresponding elliptic curve E_L. We now define the discriminant of an elliptic curve so that it agrees with the discriminant of the corresponding lattice.

Definition 16.3. The *discriminant* of an elliptic curve $E\colon y^2 = x^3+Ax+B$ is

$$\Delta(E) = -16(4A^3+27B^2).$$

This definition applies to any elliptic curve E/k defined by a short Weierstrass equation, whether $k=\mathbb{C}$ or not, but for the moment we continue to focus on elliptic curves over $\mathbb{C}$.

Recall from Theorem 14.14 that elliptic curves E/k and E'/k are isomorphic over $\bar{k}$ if and only if $j(E) = j(E')$. Thus over an algebraically closed field like $\mathbb{C}$, the j-invariant characterizes elliptic curves up to isomorphism. We now define an analogous notion of isomorphism for lattices.

Definition 16.4. Lattices L and L' are said to be *homothetic* if $L' = \lambda L$ for some $\lambda \in \mathbb{C}^\times$.

Theorem 16.5. *Two lattices L and L' are homothetic if and only if $j(L) = j(L')$.*

Proof. Suppose L and L' are homothetic, with $L' = \lambda L$. Then

$$g_2(L') \;=\; 60\sum_{\omega\in L'^*}\frac{1}{w^4} \;=\; 60\sum_{\omega\in L^*}\frac{1}{(\lambda\omega)^4} \;=\; \lambda^{-4}g_2(L).$$

Similarly, $g_3(L') = \lambda^{-6}g_3L$, and we have

$$j(L') = 1728\frac{(\lambda^{-4}g_2(L))^3}{(\lambda^{-4}g_2(L))^3 - 27(\lambda^{-6}g_3(L))^2} = 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2} = j(L).$$

To show the converse, let us now assume $j(L) = j(L')$. Let E_L and $E_{L'}$ be the corresponding elliptic curves. Then $j(E_L) = j(E_{L'})$. We may write

$$E_L\colon y^2 = x^3 + Ax + B,$$

with $-4A = g_2(L)$ and $-4B = g_3(L)$, and similarly for $E_{L'}$, with $-4A' = g_2(L')$ and $-4B' = g_3(L')$. By Theorem 14.13, there is a $\mu \in \mathbb{C}^\times$ such that $A' = \mu^4 A$ and $B' = \mu^6 B$, and if we let $\lambda = 1/\mu$, then $g_2(L') = \lambda^{-4}g_2(L) = g_2(\lambda L)$ and $g_3(L') = \lambda^{-6}g_3(L) = g_3(\lambda L)$, as above. We now show that this implies $L' = \lambda L$.

Recall from Theorem 15.29 that the Weierstrass $\wp$-function satisfies

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Differentiating both sides yields

$$\begin{aligned} 2\wp'(z)\wp''(z) &= 12\wp(z)^2\wp'(z) - g_2\wp'(z)\\ \wp''(z) &= 6\wp(z)^2 - \frac{g_2}{2}. \end{aligned} \tag{5}$$

By Theorem 15.28, the Laurent series for $\wp(z;L)$ at $z = 0$ is

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

where $a_1 = g_2/20$ and $a_2 = g_3/28$.

Comparing coefficients for the z^{2n} term in (5), we find that for $n \ge 2$ we have

$$(2n+2)(2n+1)a_{n+1} = 6\left(\sum_{k=1}^{n-1}a_k a_{n-k} + 2a_{n+1}\right),$$

and therefore

$$a_{n+1} = \frac{6}{(2n+2)(2n+1) - 12}\sum_{k=1}^{n-1}a_k a_{n-k}.$$

This allows us to compute a_{n+1} from $a_1, \ldots, a_{n-1}$, for all $n \ge 2$. It follows that $g_2(L)$ and $g_3(L)$ uniquely determine the function $\wp(z) = \wp(z;L)$ (and therefore the lattice L where $\wp(z)$ has poles), since $\wp(z)$ is uniquely determined by its Laurent series expansion about 0.

Now consider L' and λL, where we have $g_2(L') = g_2(\lambda L)$ and $g_3(L') = g_3(\lambda L)$. It follows that $\wp(z;L') = \wp(z;\lambda L)$ and $L' = \lambda L$, as desired. □

Corollary 16.6. *Two lattices L and L' are homothetic if and only if the corresponding elliptic curves E_L and $E_{L'}$ are isomorphic.*

Thus homethety classes of lattices correspond to isomorphism classes of elliptic curves over $\mathbb{C}$, and both are classified by the j-invariant. Recall from Theorem 14.12 that every complex number is the j-invariant of an elliptic curve $E/\mathbb{C}$. To prove the Uniformization Theorem we just need to show that the same is true of lattices.

16.3 The j-function

Every lattice $[\omega_1, \omega_2]$ is homothetic to a lattice of the form $[1, \tau]$, with τ in the upper half plane $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{im} z > 0\}$; we may take $\tau = \pm\omega_2/\omega_1$ with the sign chosen so that $\operatorname{im} \tau > 0$. This leads to the following definition of the j-function.

Definition 16.7. The *j-function* $j\colon \mathbb{H} \to \mathbb{C}$ is defined by $j(\tau) = j([1, \tau])$. We similarly define $g_2(\tau) = g_2([1, \tau])$, $g_3(\tau) = g_3([1, \tau])$, and $\Delta(\tau) = \Delta([1, \tau])$.

Note that for any $\tau \in \mathbb{H}$, both $-1/\tau$ and $\tau + 1$ lie in $\mathbb{H}$ (the maps $\tau \mapsto 1/\tau$ and $\tau \mapsto -\tau$ both swap the upper and lower half-planes; their composition preserves them).

Theorem 16.8. *The j-function is holomorphic on $\mathbb{H}$, and satisfies $j(-1/\tau) = j(\tau)$ and $j(\tau + 1) = j(\tau)$.*

Proof. From the definition of $j(\tau) = j([1, \tau])$ we have

$$j(\tau) = 1728\frac{g_2(\tau)^3}{\Delta(\tau)} = 1728\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2}.$$

The series defining

$$g_2(\tau) = 60 \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0}} \frac{1}{(m + n\tau)^4} \qquad \text{and} \qquad g_3(\tau) = 140 \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m + n\tau)^6}$$

converge absolutely for any fixed $\tau \in \mathbb{H}$, by Lemma 15.22, and they converge uniformly over τ in any compact subset of $\mathbb{H}$. The proof of this last fact is straight-forward but slightly technical; see [2, Thm. 1.15] for the details. It follows that $g_2(\tau)$ and $g_3(\tau)$ are holomorphic on $\mathbb{H}$, and therefore $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$ is also holomorphic on $\mathbb{H}$. Since $\Delta(\tau)$ is nonzero for all $\tau \in \mathbb{H}$, by Lemma 15.32, the j-function $j(\tau)$ is holomorphic on $\mathbb{H}$ as well.

The lattices $[1, \tau]$ and $[1, -1/\tau] = -{}^1\!/\!_\tau[1, \tau]$ are homothetic, and the lattices $[1, \tau + 1]$ and $[1, \tau]$ are equal; thus $j(-1/\tau) = j(\tau)$ and $j(\tau + 1) = j(\tau)$, by Theorem 16.5. □

16.4 The modular group

We now consider the *modular group*

$$\Gamma = \mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

As proved in Problem Set 8, the group Γ acts on $\mathbb{H}$ via linear fractional transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d},$$

and it is generated by the matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. This implies that the j-function is invariant under the action of the modular group; in fact, more is true.

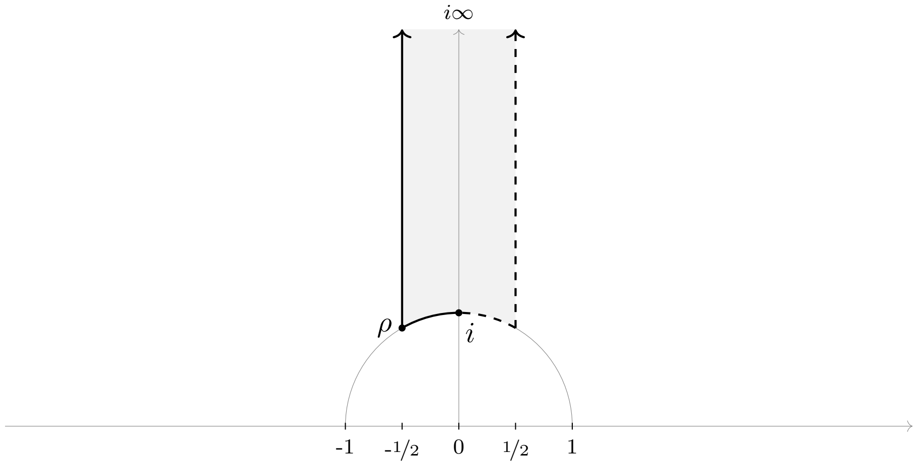

Figure 1: Fundamental domain $\mathcal{F}$ for $\mathbb{H}/\Gamma$, with $i = e^{\pi/2}$ and $\rho = e^{2\pi i/3}$.

Lemma 16.9. *We have $j(\tau) = j(\tau')$ if and only if $\tau' = \gamma\tau$ for some $\gamma \in \Gamma$.*

Proof. We have $j(S\tau) = j(-1/\tau) = j(\tau)$ and $j(T\tau) = j(\tau+1) = j(\tau)$, by Theorem 16.8, It follows that if $\tau' = \gamma\tau$ then $j(\tau') = j(\tau)$, since S and T generate Γ.

To prove the converse, let us suppose that $j(\tau) = j(\tau')$. Then by Theorem 16.5, the lattices $[1,\tau]$ and $[1,\tau']$ are homothetic So $[1,\tau'] = \lambda[1,\tau]$, for some $\lambda \in \mathbb{C}^\times$. There thus exist integers a, b, c, and d such that

$$\begin{aligned}\tau' &= a\lambda\tau + b\lambda\\ 1 &= c\lambda\tau + d\lambda\end{aligned}$$

From the second equation, we see that $\lambda = \frac{1}{c\tau+d}$. Substituting this into the first, we have

$$\tau' = \frac{a\tau+b}{c\tau+d} = \gamma\tau, \qquad \text{where } \gamma = \begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathbb{Z}^{2\times 2}.$$

Similarly, using $[1,\tau] = \lambda^{-1}[1,\tau']$, we can write $\tau = \gamma'\tau'$ for some integer matrix γ'. The fact that $\tau' = \gamma\gamma'\tau'$ implies that $\det\gamma = \pm 1$ (since γ and γ' are integer matrices). But τ and τ' both lie in $\mathbb{H}$, so we must have $\det\gamma = 1$; therefore $\gamma \in \Gamma$ as desired. □

Lemma 16.9 implies that when studying the j-function it suffices to study its behavior on Γ-equivalence classes of $\mathbb{H}$, that is, the orbits of $\mathbb{H}$ under the action of Γ. We thus consider the quotient of $\mathbb{H}$ modulo Γ-equivalence, which we denote by $\mathbb{H}/\Gamma$.[2] The actions of γ and $-\gamma$ are identical, so taking the quotient by $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$ yields the same result, but for the sake of clarity we will stick with $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

We now wish to determine a fundamental domain for $\mathbb{H}/\Gamma$, a set of unique representatives in $\mathbb{H}$ for each Γ-equivalence class. For this purpose we will use the set

$$\mathcal{F} = \{\tau \in \mathbb{H} : \mathrm{re}(\tau) \in [-1/2, 1/2) \text{ and } |\tau| \ge 1, \text{ such that } |\tau| > 1 \text{ if } \mathrm{re}(\tau) > 0\}.$$

Lemma 16.10. *The set $\mathcal{F}$ is a fundamental domain for $\mathbb{H}/\Gamma$.*

[2] Some authors write this quotient as $\Gamma\backslash\mathbb{H}$ to indicate that the action is on the left.

Proof. We need to show that for every $\tau \in \mathbb{H}$, there is a unique $\tau' \in \mathcal{F}$ such that $\tau' = \gamma\tau$, for some $\gamma \in \Gamma$. We first prove existence. Let us fix $\tau \in \mathbb{H}$. For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ we have

$$\operatorname{im}(\gamma\tau) = \operatorname{im}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{\operatorname{im}((a\tau+b)(c\bar{\tau}+d))}{|c\tau+d|^2} = \frac{(ad-bc)\operatorname{im}\tau}{|c\tau+d|^2} = \frac{\operatorname{im}\tau}{|c\tau+d|^2} \tag{6}$$

Let $c\tau + d$ be a shortest vector in the lattice $[1, \tau]$. Then c and d must be relatively prime, and we can pick integers a and b so that $ad - bc = 1$. The matrix $\gamma_0 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ then maximizes the value of $\operatorname{im}(\gamma\tau)$ over $\gamma \in \Gamma$. Let us now choose $\gamma = T^k\gamma_0$, where k is chosen so that $\operatorname{re}(\gamma\tau) \in [1/2, 1/2)$, and note that $\operatorname{im}(\gamma\tau) = \operatorname{im}(\gamma_0\tau)$ remains maximal. We must have $|\gamma\tau| \geq 1$, since otherwise $\operatorname{im}(S\gamma\tau) > \operatorname{im}(\gamma\tau)$, contradicting the maximality of $\operatorname{im}(\gamma\tau)$. Finally, if $\tau' = \gamma\tau \notin \mathcal{F}$, then we must have $|\gamma\tau| = 1$ and $\operatorname{re}(\gamma\tau) > 0$, in which case we replace γ by $S\gamma$ so that $\tau' = \gamma\tau \in \mathcal{F}$.

It remains to show that τ' is unique. This is equivalent to showing that any two Γ-equivalent points in $\mathcal{F}$ must coincide. So let τ_1 and $\tau_2 = \gamma_1\tau_1$ be two elements of $\mathcal{F}$, with $\gamma_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, and assume $\operatorname{im}\tau_1 \leq \operatorname{im}\tau_2$. By (6), we must have $|c\tau_1 + d|^2 \leq 1$, thus

$$1 \geq |c\tau_1 + d|^2 = (c\tau_1 + d)(c\bar{\tau}_1 + d) = c^2|\tau_1|^2 + d^2 + 2cd\operatorname{re}\tau_1 \geq c^2|\tau_1|^2 + d^2 - |cd| \geq 1,$$

where the last inequality follows from $|\tau_1| \geq 1$ and the fact that c and d cannot both be zero (since $\det\gamma = 1$). Thus $|c\tau_1 + d| = 1$, which implies $\operatorname{im}\tau_2 = \operatorname{im}\tau_1$. We also have $|c|, |d| \leq 1$, and by replacing γ_1 by $-\gamma_1$ if necessary, we may assume that $c \geq 0$. This leaves 3 cases:

1. $c = 0$: then $|d| = 1$ and $a = d$. So $\tau_2 = \tau_1 \pm b$, but $|\operatorname{re}\tau_2 - \operatorname{re}\tau_1| < 1$, so $\tau_2 = \tau_1$.
2. $c = 1, d = 0$: then $b = -1$ and $|\tau_1| = 1$. So τ_1 is on the unit circle and $\tau_2 = a - 1/\tau_1$. Either $a = 0$ and $\tau_2 = \tau_1 = i$, or $a = -1$ and $\tau_2 = \tau_1 = \rho$.
3. $c = 1, |d| = 1$: then $|\tau_1 + d| = 1$, so $\tau_1 = \rho$, and $\operatorname{im}\tau_2 = \operatorname{im}\tau_1 = \sqrt{3}/2$ implies $\tau_2 = \rho$.

In every case we have $\tau_1 = \tau_2$ as desired. □

Theorem 16.11. *The restriction of the j-function to $\mathcal{F}$ defines a bijection from $\mathcal{F}$ to $\mathbb{C}$.*

Proof. Injectivity follows immediately from Lemmas 16.9 and 16.10. It remains to prove surjectivity. We have

$$g_2(\tau) \;=\; 60 \sum_{\substack{n,m\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^4} \;=\; 60\left(2\sum_{m=1}^{\infty}\frac{1}{m^4} + \sum_{\substack{n,m\in\mathbb{Z}\\ n\neq 0}}\frac{1}{(m+n\tau)^4}\right).$$

The second sum tends to 0 as $\operatorname{im}\tau \to \infty$. Thus we have

$$\lim_{\operatorname{im}\tau\to\infty} g_2(\tau) = 120\sum_{m=1}^{\infty} m^{-4} = 120\,\zeta(4) = 120\,\frac{\pi^4}{90} = \frac{4\pi^4}{3},$$

where $\zeta(s)$ is the Riemann zeta function. Similarly,

$$\lim_{\operatorname{im}\tau\to\infty} g_3(\tau) = 280\,\zeta(6) = 280\,\frac{\pi^6}{945} = \frac{8\pi^6}{27}.$$

Thus

$$\lim_{\operatorname{im}\tau\to\infty} \Delta(\tau) = \left(\frac{4}{3}\pi^4\right)^3 - 27\left(\frac{8}{27}\pi^6\right)^2 = 0.$$

(this explains the coefficients 60 and 140 in the definitions of g_2 and g_3; they are the smallest pair of integers that ensure this limit is 0). Since $\Delta(\tau)$ is the denominator of $j(\tau)$, the quantity $j(\tau) = g_2(\tau)^3/\Delta(\tau)$ is unbounded as $\operatorname{im}\tau \to \infty$.

In particular, the j-function is non-constant, and by Theorem 16.8 it is holomorphic on $\mathbb{H}$. The open mapping theorem implies that $j(\mathbb{H})$ is an open subset of $\mathbb{C}$; see [4, Thm. 3.4.4].

We claim that $j(\mathbb{H})$ is also a closed subset of $\mathbb{C}$. Let $j(\tau_1), j(\tau_2), \ldots$ be an arbitrary convergent sequence in $j(\mathbb{H})$, converging to $w \in \mathbb{C}$. The j-function is Γ-invariant, by Lemma 16.9, so we may assume the τ_n all lie in $\mathcal{F}$. The sequence $\operatorname{im}\tau_1, \operatorname{im}\tau_2, \ldots$ must be bounded, say be B, since $j(\tau) \to \infty$ as $\operatorname{im}\tau \to \infty$, but the sequence $j(\tau_)), j(\tau_2), \ldots$ converges; it follows that the τ_n all lie in the compact set

$$\Omega = \{\tau : \operatorname{re}\tau \in [-1/2, 1/2], \operatorname{im}\tau \in [1/2, B]\}.$$

There is thus a subsequence of the τ_n that converges to some $\tau \in \Omega \subset \mathbb{H}$. The j-function is holomorphic, hence continuous, so $j(\tau) = w$. It follows that the open set $j(\mathbb{H})$ contains all its limit points and is therefore closed.

The fact that the non-empty set $j(\mathbb{H}) \subseteq \mathbb{C}$ is both open and closed implies that $j(\mathbb{H}) = \mathbb{C}$, since $\mathbb{C}$ is connected. It follows that $j(\mathcal{F}) = \mathbb{C}$, since every element of $\mathbb{H}$ is Γ-equivalent to an element of $\mathcal{F}$ (Lemma 16.10) and the j-function is Γ-invariant (Lemma 16.9). □

Corollary 16.12 (Uniformization Theorem)**.** *For every elliptic curve $E/\mathbb{C}$ there exists a lattice L such that $E = E_L$.*

Proof. Given $E/\mathbb{C}$, pick $\tau \in \mathbb{H}$ so that $j(\tau) = j(E)$ and let $L' = [1, \tau]$. We have

$$j(E) = j(\tau) = j(L') = j(E_{L'}),$$

so E is isomorphic to $E_{L'}$, by Theorem 14.13, where the isomorphism is given by the map $(x, y) \mapsto (\mu^2 x, \mu^3 y)$ for some $\mu \in \mathbb{C}^\times$. If now let $L = \frac{1}{\mu}L'$, then $E = E_L$. □

References

[1] L. Ahlfors, *Complex analysis*, third edition, McGraw Hill, 1979.

[2] Tom M. Apostol, *Modular functions and Dirichlet series in number theory*, second edition, Springer, 1990.

[3] J.H. Silverman, *The arithmetic of elliptic curves*, second edition, Springer 2009.

[4] E.M. Stein and R. Shakarchi, *Complex analysis*, Princeton University Press, 2003.

18.783 Elliptic Curves
Spring 2019