Last time we showed that every lattice L in the complex plane gives rise to an elliptic curve $E/\mathbb{C}$ corresponding to the torus $\mathbb{C}/L$. In this lecture we establish a group isomorphism between $\mathbb{C}/L$ and $E(\mathbb{C})$, in which addition of complex numbers (modulo the lattice L) corresponds to addition of points on the elliptic curve. Before we begin, let us note a generalization of the argument principle (Theorem 16.7).

Theorem 17.1. *Let f be a meromorphic function, let F be a region whose boundary ∂F is a simple curve that contains no zeros or poles of f, and let g be a function that is holomorphic on an open set containing F. Then*

$$\frac{1}{2\pi i}\int_{\partial F} g(z)\frac{f'(z)}{f(z)}\,dz = \sum_{a\in F} \mathrm{ord}_a(f)g(a),$$

where the integer $\mathrm{ord}_a(f)$ is defined by

$$\mathrm{ord}_a(f) = \begin{cases} n & \text{if } f \text{ has a zero of order } n \text{ at } a,\\ -n & \text{if } f \text{ has a pole of order } n \text{ at } a,\\ 0 & \text{otherwise.}\end{cases}$$

If we let $g(z) = 1$, this reduces to the usual argument principle.

Proof. This may be derived from the residue formula ([1, Thm. 4.19] or [2, Thm. 3.2.3]), but for the benefit of those who have not taken complex analysis, we give a direct proof that explains both the factor of $\frac{1}{2\pi i}$ and the appearance of the logarithmic derivative f'/f in the formula. We will not be overly concerned with making the details rigorous, our goal is to clearly convey the main ideas used in the proof.

If $f(z)$ has a zero of order n at a, then we may write

$$f(z) = (z-a)^n h(z)$$

where the function $h(z)$ is holomorphic and nonzero on some open disc D about a. Similarly, if $f(z)$ has a pole of order n at a we have $f(z) = (z-a)^{-n}h(z)$, and in either case

$$f(z) = (z-a)^m h(z),$$

where m is the integer $\mathrm{ord}_a(f)$. If we then compute the logarithmic derivative, we have

$$\frac{f'(z)}{f(z)} = \frac{m(z-a)^{m-1}h(z) + (z-a)^m h'(z)}{(z-a)^m h(z)} = \frac{m}{z-a} + \frac{h'(z)}{h(z)},$$

where h'/h is holomorphic on D. Thus f'/f has only a simple pole at a. The same is true at every zero or pole of f, and f'/f is holomorphic everywhere else.

We now compute $\int_{\partial F} \frac{f'(z)}{f(z)} g(z)$. For the sake of illustration, let us suppose that ∂F is a circle C, oriented counter-clockwise, and that $f'(z)/f(z)$ has just one pole inside C, at the point a. Rather than computing the integral along C, we instead consider the curve C' depicted below, which mostly follows the path of C, but makes a detour around a along an

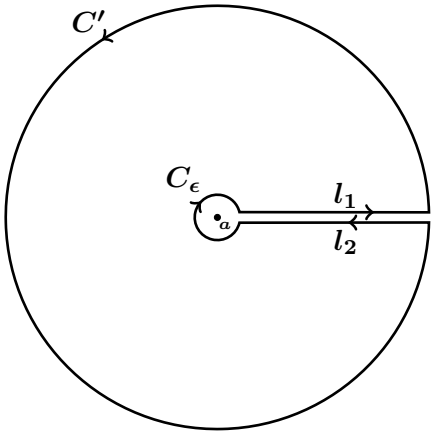

Figure 1: A keyhole contour.

infinitesimally small circle C_ϵ of radius ϵ, so that its interior contains no poles of $f'(z)/f(z)$. The curve C' is known as a *keyhole contour*.

In the limit as ϵ tends to zero, the portions of the integral along the anti-parallel lines l_1 and l_2 cancel, and we may view C as the sum of C' and C_ϵ, where C_ϵ now has a counter clockwise-orientation, cancelling the clockwise detour along C_ϵ in C'. The integral about C' is zero, by Cauchy's theorem [2, Thm. 3.5.3], since the integrand is holomorphic on a simply connected region that contains C' and its interior.

Thus we are left with

$$\begin{aligned}\int_C \frac{f'(x)}{f(z)} g(z)\, dz &= \lim_{\epsilon\to 0} \int_{C_\epsilon} \frac{f'(x)}{f(z)} g(z) dz \\ &= \lim_{\epsilon\to 0} \int_{C_\epsilon} \frac{mg(z)}{z-a} + \frac{h'(z)g(z)}{h(z)} dz.\end{aligned}$$

The term on the right is holomorphic, so its integral along C_ϵ is zero, and we have

$$\begin{aligned}\int_C \frac{f'(x)}{f(z)} g(z)\, dz &= m \lim_{\epsilon\to 0} \int_{C_\epsilon} \frac{g(z)}{z-a} dz \\ &= m \lim_{\epsilon\to 0} \int_{C_\epsilon} \frac{g(z)-g(a)}{z-a} + \frac{g(a)}{z-a} dz.\end{aligned}$$

The term on the left is bounded, since $g(z)$ is holomorphic, so as $\epsilon \to 0$ its integral about C_ϵ vanishes. Thus

$$\begin{aligned}\int_C \frac{f'(x)}{f(z)} g(z)\, dz &= mg(a) \lim_{\epsilon\to 0} \int_{C_\epsilon} \frac{dz}{z-a} \\ &= mg(a) \lim_{\epsilon\to 0} \int_0^{2\pi} \frac{\epsilon i e^{it}}{\epsilon e^{it}} dt \\ &= mg(a) 2\pi i\end{aligned}$$

This argument easily generalizes: we know let C' be a a curve that follows ∂F but makes an infinitesimal detour about each of the poles of $f'(z)/f(z)$, yielding the desired formula

$$\frac{1}{2\pi i} \int_C \frac{f'(x)}{f(z)} g(z)\, dz = \sum_{a\in F} \mathrm{ord}_a(f) g(a) \qquad \square$$

17.1 The isomorphism from a torus to its corresponding elliptic curve

Theorem 17.2. *Let L be a lattice, and let E be the elliptic curve $y^2 = 4x^3 - g_2(L)x - g_3(L)$ over $\mathbb{C}$. The map $\Phi\colon \mathbb{C}/L \to E(\mathbb{C})$ that sends $z \in L$ to 0 and each $z \notin L$ to the affine point $\big(\wp(z), \wp'(z)\big)$ on $E(\mathbb{C})$ is an isomorphism between the additive group of $\mathbb{C}/L$ and $E(\mathbb{C})$.*

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

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

since $\wp$ is even and $\wp'$ is odd, so Φ maps inverses to inverses.

There are exactly 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 16.20, $\wp'$ vanishes at each of these points, hence Φ maps points of order 2 in $\mathbb{C}/$Ł to points of order 2 in $E(\mathbb{C})$, since these are precisely the points with y-coordinate zero. Moreover, Φ is injective on points of order 2, since the roots of $4\wp(z)^3 - g_2(L)\wp(z) - g_3(L)$ are distinct; see the proof of Lemma 16.20. Thus Φ restricts to an isomorphism from $(\mathbb{C}/L)[2]$ to $E(\mathbb{C})[2]$.

To show that Φ is surjective, let $(x_0, y_0) \in E(\mathbb{C})$. The elliptic function $f(z) = \wp(z) - x_0$ has order 2, hence it has 2 zeros in the fundamental parallelogram $\mathcal{F}_0$, by Theorem 16.6, and neither of these is 0, since f has a pole at 0. Let $z_0 \neq 0$ be a zero of $f(z)$ in $\mathcal{F}_0$. Then $\Phi(z_0) = (x_0, \pm y_0)$, and therefore $(x_0, y_0) = \Phi(\pm z_0)$, hence Φ is surjective.

We now show that Φ is injective. Let $z_1, z_2 \in \mathbb{C}$ be distinct modulo L and suppose for the sake of contradiction that $\Phi(z_1) = \Phi(z_2)$. We may assume $2z_1 \notin L$, since we have already shown that Φ is injective on $(\mathbb{C}/L)[2]$. As 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 $\wp'(-z_1) = -\wp'(z_1) \neq \wp'(z_1)$ for $2z_1 \notin L$, since $\wp'(z_1) \neq 0$.

It only remains to show that $\Phi(z_1 + z_2) = \Phi(z_1) + \Phi(z_2)$, and we may assume that $z_1, z_2, 2z_1, z_1 + z_2 \notin L$; the case where either z_1 or z_2 lies in L is immediate, and we addressed points of order 2 and inverses above. Let $P_i = (x_i, y_i) = (\wp(z_i), \wp'(z_i))$ for $i = 1, 2$, and let $y = ax + b$ be the line $\overline{P_1P_2}$, or the line tangent to P_1 on $E/\mathbb{C}$ if $P_1 = P_2$ (note that this line cannot be vertical, since $2z_1 \notin L$ means that P_1 is not a point of order 2). Let $P_3 = (x_3, y_3)$ be the third point where the line intersects the curve E. Then $P_1 + P_2 + P_3 = 0$, by the definition of the group law on $E(\mathbb{C})$.

Now consider the function $\ell(z) = -\wp'(z) + a\wp(z) + b$. It is an elliptic function of order 3 with a triple pole at 0, so it has three zeros in any fundamental region, two of which are equivalent to z_1 and z_2. Pick a fundamental region $\mathcal{F}_\alpha$ whose boundary does not contain any zeros or poles of $\ell(z)$, replace z_1 and z_2 by equivalent points in $\mathcal{F}_\alpha$, and let z_3 be the third zero of $\ell(z)$ in $\mathcal{F}_\alpha$ (z_1, z_2, and z_3 need not be distinct, we count zeros with multiplicity).

Applying Theorem 17.1 with $g(z) = z$ yields

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

Let us now evaluate the integral in (1), with the parallelogram $\partial\mathcal{F}_\alpha$ oriented counterclockwise. To ease the notation, let $f(z) = \ell'(z)/\ell(z)$, which we note is an elliptic function.

Assuming $L = [\omega_1, \omega_2]$, we have

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

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 curve C in the complex plane and any 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. 4.1] or [2, Lem. B.1.3].

The function $g_1(t) = \ell(\alpha + t\omega_2)$ parametrizes a closed curve C_1 from $\ell(\alpha)$ to $\ell(\alpha+\omega_2)$, as t ranges from 0 to 1, since $\ell(\alpha+\omega_2) = \ell(\alpha)$. The winding number of C_1 about the point 0 is the integer

$$c = \frac{1}{2\pi i}\int_\alpha^{\alpha+w_2} \frac{\ell'(z)\,dz}{\ell(z) - 0} = \frac{1}{2\pi i}\int_\alpha^{\alpha+\omega_2} f(z)\,dz. \tag{3}$$

Applying the same logic to the closed curve C_2 from $\ell(\alpha+\omega_1)$ to $\ell(\alpha)$ parameterized by the function $g_2(t) = \ell(\alpha + (1-t)\omega_1)$, we obtain the integer

$$d = \frac{1}{2\pi i}\int_{\alpha+\omega_1}^{\alpha} \frac{\ell'(z)dz}{\ell(z) - 0}\,dz = \frac{1}{2\pi i}\int_{\alpha+\omega_1}^{\alpha} f(z)\,dz. \tag{4}$$

Plugging (2), (3), and (4) into the LHS of (1), we see that

$$cw_1 + dw_2 = z_1 + z_2 + z_3.$$

Thus $z_1 + z_2 + z_3$ lies in L, which implies that $\wp(z_3) = \wp(-z_3) = \wp(z_1+z_2) = x_3$.

Thus $\Phi(z_1+z_2) = \pm(\Phi(z_1) + \Phi(z_2))$, it remains only to show that the sign is positive. Suppose not. Then $\Phi(z_1) + \Phi(z_2) = -\Phi(z_1+z_2)$, and it follows that

$$\Phi(z_1) = -\Phi(z_1+z_2) - \Phi(z_2) = \pm\Phi(z_1+2z_2).$$

This implies $\wp(z_1) = \wp(z_1+2z_2)$. The function $f(z) = \wp(z_1+z) - \wp(z_1)$ is an elliptic function of order 2, thus, up to equivalence modulo L there are only two possible values of $2z_2$, and at most eight possible values of z_2.

For any fixed z_1, there is therefore only a finite set S of z_2 in any fundamental region for which we might not have $\Phi(z_1+z_2) = \Phi(z_1) + \Phi(z_2)$. We can assume that none of these points lie in L, and also that $z_1 + z_2 \notin L$ for any $z_2 \in S$ (recall our assumption that $z_1, z_2, z_1+z_2 \notin L$). Now let R be an open set containing at least one point equivalent to each point in the set $\{z_1\} \cup S \cup \{z_1 + z_2 : z_2 \in S\}$, but no points in L. Then $\wp(z)$ and $\wp'(z)$ are both holomorphic on R, and by continuity we must have $\Phi(z_1+z_2) = \Phi(z_1) + \Phi(z_2)$ for every $z_2 \in S$. Therefore $\Phi(z_1+z_2) = \Phi(z_1) + \Phi(z_2)$. □

17.2 The j-invariant

Definition 17.3. 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 16.21, so $j(L)$ is always defined.

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

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

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

Definition 17.4. The *discriminant* of the elliptic curve $E\colon y^2 = x^3 + Ax + B$ is

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

This definition extends 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 15.11 that elliptic curves E/k and E'/k are isomorphic over $\bar{k}$ if and only if $j(E) = j(E')$. When $k = \mathbb{C}$, we have $\bar{k} = k$, so up to isomorphism, elliptic curves over $\mathbb{C}$ are completely characterized by their j-invariant. We now define an analogous notion of isomorphism for lattices.

Definition 17.5. Lattices L and L' are said to be *homothetic* if $L' = \lambda L$ for some $\lambda \in \mathbb{C}^*$.

Theorem 17.6. *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

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

where $\sum'$ sums over nonzero lattice points. 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 and E' be the elliptic curves corresponding to L and L', respectively. Then $j(E) = j(E')$, and as above, we may write E in the form $y^2 = x^3 + Ax + B$, with $-4A = g_2(L)$ and $-4B = g_3(L)$, and similarly for E', with $-4A' = g_2(L')$ and $-4B' = g_3(L')$. By Theorem 15.10, there is a $\mu \in \mathbb{C}^*$ 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 the differential equation for $\wp(z)$ from Theorem 16.18:

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

Differentiating, we get

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

By Theorem 16.17, 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 $n \geq 2$ 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

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

Thus we can compute a_{n+1} from $a_1, \ldots, a_{n-1}$, for all $n \geq 2$. It follows that $g_2(L)$ and $g_3(L)$ uniquely determine the function $\wp(z;L)$, and therefore the lattice L, since $\wp(z;L)$ is uniquely determined by its Laurent series expansion about 0 (consider an open set containing the fundamental region $\mathcal{F}_0$ but no points in L besides 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 17.7. *Two lattices are homothetic if and only if their corresponding elliptic curves 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.

We have seen that every lattice L gives rise to a corresponding elliptic curve over $E/\mathbb{C}$ that is related to L via an analytic group isomorphism $\Phi\colon \mathbb{C}/L \to E(\mathbb{C})$. Our next task is to prove the Uniformization Theorem: every elliptic curve $E/\mathbb{C}$ arises from a lattice L. We know from Theorem 15.9 that every complex number is the j-invariant of some elliptic curve $E/\mathbb{C}$. To prove the uniformization theorem we need to show that every complex number is also the j-invariant of some lattice. This lattice must of course correspond to an elliptic curve $E/\mathbb{C}$ with the same j-invariant, but the existence of the elliptic curve E does not immediately imply the existence of a corresponding lattice L. The coefficients of the equation $y^2 = x^3 + Ax + B$ for the elliptic curve tell us that we must have $g_2(L) = -A/4$ and $g_3(L) = -B/4$, but it requires some work to show that such a lattice actually exists.

References

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

[2] Elias M. Stein and Rami Shakarchi, *Complex analysis*, Princeton University Press, 2003.

18.783 Elliptic Curves
Spring 2013