18.783 Elliptic Curves
Lecture 15

Andrew Sutherland

November 2, 2023

Elliptic curves over $\mathbb{C}$

Recall our goal from last lecture to prove **Uniformization Theorem**, an explicit correspondence between elliptic curves over $\mathbb{C}$ and tori $\mathbb{C}/L$ defined by lattices $L \subseteq \mathbb{C}$.

Our goal is to prove that:

- Every lattice $L \subseteq \mathbb{C}$ can be used to define an elliptic curve $E_L/\mathbb{C}$.
- Every elliptic curve $E/\mathbb{C}$ arises as E_L for some lattice L.
- There is an analytic isomorphism

  $$\mathbb{C}/L \xrightarrow{\Phi} E_L/\mathbb{C}$$

  that induces an isomorphism of abelian groups $\mathbb{C}/L \simeq E(\mathbb{C})$ (addition in $\mathbb{C}$ modulo L induces the elliptic curve group law on $E(\mathbb{C})$).

Recall the Weierstrass $\wp$-function

Definition

The Weierstrass $\wp$-function of a lattice L in $\mathbb{C}$ is defined by

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

It is an even elliptic function of order 2 and $\wp'$ is an odd elliptic function of order 3.

Theorem

The function $\wp(z) = \wp(z; L)$ satisfies the differential equation

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

where $g_2(L) := 60G_4(L)$ and $g_3(L) := 140G_6(L)$.

Elliptic curves from lattices

If we put $x := \wp(z)$ and $y := \wp'(z)$, the differential equation for $\wp$ looks like

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

which is an elliptic curve over $\mathbb{C}$ because

$$\Delta(L) := g_2(L)^3 - 27g_3(L)^2 \neq 0.$$

Morever, the map

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

sends points on $\mathbb{C}/L$ to points on the elliptic curve E_L.

Φ is a group isomorphism

Last time we showed that the points of order 2 in $\mathbb{C}/L$ are $\omega_1/2, \omega_2/2, (\omega_1+\omega_2)/2$, where $L = [\omega_1, \omega_2]$. These are the roots of $4x^3 - g_2(L) - g_3(L)$ and the zeros of $\wp'(z)$.

Theorem

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: To the board!

For our proof we will need to use Cauchy's argument principle and the notion of the winding number of a closed curve (see the next slide for precise statements).

Some results from complex analysis

Theorem (Cauchy's argument principle)

Let γ be a simple closed curve with positive orientation, let $f(z)$ be a function that is meromorphic on an open set Ω containing γ and its interior Γ, with no zeros or poles on γ, and let $g(z)$ be a nonzero function that is holomorphic on Ω. Then

$$\frac{1}{2\pi i}\int_{\gamma} g(z)\frac{f'(z)}{f(z)}\,dz = \sum_{w\in\Gamma} g(w)\,\mathrm{ord}_w(f).$$

Definition

For any closed curve C and a point $z_0 \notin C$, the winding number of C about z_0 is

$$\frac{1}{2\pi i}\int_{C}\frac{dz}{z-z_0}.$$

It is an integer that counts how many times the curve C "winds around" the point z_0.

The j-invariant of a lattice

Definition

The j-invariant of a lattice L is defined by

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

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 $g_3(L) = -4B$. We have

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

The j-invariant of a lattice L is the same as the j-invariant of the elliptic curve E_L. Recall that the discriminant of $E\colon y^2 = x^3 + Ax + B$ is $\Delta(E) := -16(4A^3 + 27B^2)$, thus we also have $\Delta(L) = \Delta(E_L)$ (this is where the leading 16 comes from).

Lattices up to homethety

Recall that for elliptic curves E/k and E'/k we have $E_{\bar{k}} \simeq E'_{\bar{k}} \iff j(E) = j(E')$.

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

Lattices L and L' in $\mathbb{C}$ are homothetic if $L' = \lambda L$ for some $\lambda \in \mathbb{C}^\times$.

Theorem

Lattices L and L' in $\mathbb{C}$ are homothetic if and only if $j(L) = j(L')$.
Proof: see notes.

Corollary

Lattices L and L' in $\mathbb{C}$ are homothetic if and only if E_L and $E_{L'}$ are isomorphic.

The j-function

Definition

The j-function $j\colon \mathcal{H} \to \mathbb{C}$ 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 $\tau \in \mathcal{H}$, both $-1/\tau$ and $\tau + 1$ lie in $\mathcal{H}$ (the maps $\tau \mapsto 1/\tau$ and $\tau \mapsto -\tau$ both swap the upper and lower half-planes; their composition preserves them).

Theorem

The j-function is holomorphic on $\mathcal{H}$, with $j(-1/\tau) = j(\tau)$ and $j(\tau + 1) = j(\tau)$.

Proof: To the board!

The modular group

Definition

The modular group is

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

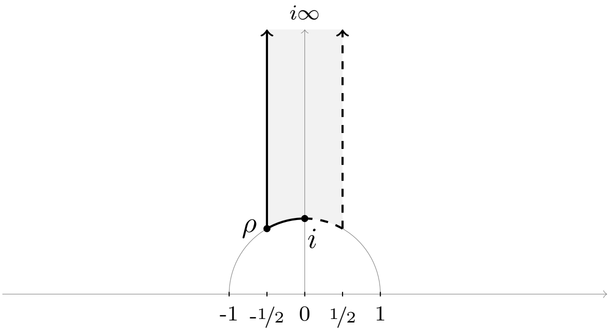
It acts on $\mathcal{H}$ via linear fractional transformations $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \tau = \frac{a\tau + b}{c\tau + d}$, and it is generated by the matrices $S := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

Lemma

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

Proof: To the board!

A fundamental domain for the modular group



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

Lemma

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

Proof: To the board!

The isomorphism given by the j-function

Theorem

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

Proof: To the board!

Corollary (Uniformization Theorem)

For every elliptic curve $E/\mathbb{C}$ there exists a lattice L such that $E = E_L$.

Proof: Given E, let $\tau \in \mathcal{F}$ satisfy $j(\tau) = j(E)$ and let $L' = [1, \tau]$ so $j(E) = j(L')$.
Then $E \simeq E_{L'}$ via an isomorphism $(x, y) \mapsto (\mu^2 x, \mu^3 y)$ and $E = E_L$ for $L := \frac{1}{\mu} L'$.