Modular Curve $X(1)$ and the j-invariant

1 Modular Functions and Uniformization

In last lecture, we discussed that isomorphism classes of elliptic curves defined over the complex numbers correspond to lattices $\Lambda \subset \mathbb{C}$ up to homothety. Thus, we can parameterize isomorphism classes of elliptic curves over $\mathbb{C}$ by parameterizing lattices up to homothety.

For any lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, we can find a homothetic lattice $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathbb{C}$ satisfying $\operatorname{Im}\tau > 0$. Thus, there is a surjective map from the upper half plane

$$\mathbb{H} = \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}$$

to the set of homothety classes of lattices given by $\tau \mapsto \Lambda_\tau := \mathbb{Z} + \mathbb{Z}\tau$.

But the choice from Λ to such a τ is not unique.

The modular group

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

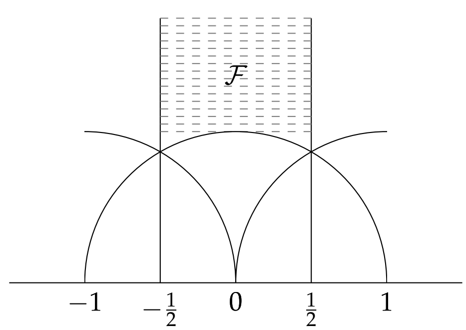
acts on $\mathbb{H}$ by linear fractional transformations.

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad \gamma(\tau) = \frac{a\tau + b}{c\tau + d}, \quad \forall \tau \in \mathbb{H}.$$

For any $\tau_1, \tau_2 \in \mathbb{H}$, the lattices Λ_{τ_1} and Λ_{τ_2} are homothetic if and only if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau_2 = \gamma(\tau_1)$. Thus lattices up to homothety are parameterized by the upper plane $\mathbb{H}$ modulo the action of $\mathrm{SL}_2(\mathbb{Z})$. And this set $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$ is in bijection to the region

$$\mathcal{F} = \left\{\tau \in \mathbb{H} \mid |\Re(\tau)| \leq \frac{1}{2}, |\tau| \geq 1\right\}.$$

This region is called a *fundamental domain* for $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$ and every lattice $\Lambda \subset \mathbb{C}$ is homothetic to a lattice Λ_τ for some $\tau \in \mathcal{F}$.



The quotient $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}$ (denoted as $Y(1)$) has a natural structure of a genus 0 Riemann surface with a puncture, a 2-sphere with one point missing. Then it's natural to want to compactify this topological space. To add this missing point and give it a moduli interpretation, we define the extended upper half plane

$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}.$$

Then $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}^*$ and the quotient $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathbb{H}^*$ (denoted as $X(1)$) is a compact genus 0 Riemann surface. There is one point in the compliment of $Y(1) \subset X(1)$ and this point is called the cusp of $X(1)$.

Next, we introduce a function j on homothety classes of lattices which is a complex analytic isomorphism of (open) Riemann surfaces $j : Y(1) \to \mathbb{C}$ and it extends to $j : X(1) \simeq \mathbb{P}^1(\mathbb{C})$.

Recall from Lecture 2, given a lattice Λ and $k \in \mathbb{Z}_{>1}$, we defined Eisenstein series

$$G_{2k}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-2k}.$$

Given $\tau \in \mathbb{H}$, it is naturally associated to the lattice $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$ and thus we can consider $G_{2k}(\tau)$ as a meromorphic function defined on the upper half plane $\mathbb{H}$. Note that for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$G_{2k}(\gamma\tau) = (c\tau + d)^{2k} G_{2k}(\tau).$$

(Meromorphic functions on $\mathbb{H}$ satisfying this condition are called weakly modular of weight $2k$. The Eisenstein series G_{2k}, $k > 1$ is not only weakly modular, it is also holomorphic on $\mathbb{H}$ and at ∞. It is an example of a *modular form* of weight $2k$.)

The function G_{2k} is defined on the set of lattices but it is not a function on homothety classes of lattices. However, we can construct a function on homothety classes of lattices using G_{2k}.

Definition 1.1. Let $\mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$ be a lattice. The j-invariant is defined to be the complex number

$$j(\tau) := 1728 \frac{(60G_4(\tau))^3}{(60G_4(\tau))^3 - 27(140G_6(\tau))^2}.$$

For any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we have $j(\gamma\tau) = j(\tau)$.

Theorem 1.2. *If $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ are two lattices, then they are homothetic if and only if*

$$j(\Lambda_1) = j(\Lambda_2).$$

Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, the function $j : \mathbb{H} \to \mathbb{C}$ satisfies $j(\tau + 1) = j(\tau)$. Thus, let $q = e^{2\pi i \tau}$, the function j has a Laurent expansion in the variable q. Explicitly,

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n,$$

where the coefficients c_n are integers for all $n \geq 0$.

2 The j-invariant of an Elliptic Curve

From our discussion in lecture 2, a lattice $\Lambda \subset \mathbb{C}$ corresponds to an elliptic curve defined by a Weierstrass equation

$$y^2 = 4x^3 - 60G_4x - 140G_6 \quad (y^2 = x^3 - 15G_4x - 35G_6).$$

Following the definition of j-invariant for a lattice Λ, given an elliptic curve E over some field K with Weierstrass equation

$$y^2 = x^3 + Ax + B,$$

we can define its j-invariant to be

$$j = 1728 \frac{(4A)^3}{16(4A^3 + 27B^2)}.$$

When K is a subfield of $\mathbb{C}$, our discussion implies that the j-invariant determines the isomorphism class of E over $\mathbb{C}$. Although we won't prove it, but it's true that, the j-invariant determines the isomorphism class of an elliptic curve E over $\overline{K}$ for any field K.

From the definition, we see that for E defined over any field K (thus $A, B \in K$), its j-invariant takes value in K. Conversely, given a j-invariant $j_0 \in K$ for some field K, the elliptic curve

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

has its j-invariant equal to j_0 unless $j_0 = 0$ or 1728. Values 0 and 1728 are j-invariants of elliptic curves $y^2 + y = x^3$ and $y^2 = x^3 + x$ respectively. Thus, over an algebraically closed field $\overline{K}$, the set of isomorphism classes of elliptic curves is in bijection to the set of all j values in $\overline{K}$.

Note that the cusp of $X(1)$ corresponds to j-invariant value ∞. Thus, let $\mathfrak{p}$ be a prime of a field K and E/K an elliptic curve, if the valuation of the j-invariant is negative at $\mathfrak{p}$ ("having a power of $\mathfrak{p}$ in the denominator of $j(E)$"), then the reduction of E at $\mathfrak{p}$ is singular and we call this reduction a bad reduction. If the valuation of the j-invariant is non-negative at $\mathfrak{p}$, then E has potential good reduction at $\mathfrak{p}$, meaning there is a finite extension L/K such that $E \otimes \operatorname{Spec} L$ has good reduction at a prime above $\mathfrak{p}$.

Moreover, let E_1, E_2 be two elliptic curves defined over a number field K and let $\mathfrak{p}$ be a prime of K at which E_1, E_2 admit good reduction. For each E_i there exists a Weierstrass equation $y^2 = x^3 + A_i x + B_i$ such that $y^2 = x^3 + \overline{A_i}x + \overline{B_i}$ with $\overline{A_i}, \overline{B_i} \in \mathbb{F}_{\mathfrak{p}}$ the reduction of A, B in the residue field of $\mathfrak{p}$ defines an elliptic curve $\mathscr{E}_i$ over $\mathbb{F}_{\mathfrak{p}}$. The j-invariants $j(E_1) \equiv j(E_2) \bmod \mathfrak{p}$ if and only if $\mathscr{E}_1$ is isomorphic to $\mathscr{E}_2$ over $\overline{\mathbb{F}_{\mathfrak{p}}}$.

3 The j-invariant of a CM Elliptic Curve

Recall from Lecture 2, a lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$ corresponds to a CM elliptic curve when τ is an imaginary quadratic number. Now let's talk about the j-invariant $j(\tau)$ of a CM elliptic curve, which is often called a singular moduli.

Proposition 3.1. *The j-invariant of a CM elliptic curve is an algebraic number.*

Proof. Let $E/\mathbb{C} : y^2 = x^3 + Ax + B$ be an elliptic curve and $\phi \in \operatorname{End}(E)$. For any $\sigma \in \operatorname{Aut}(\mathbb{C})$, let E^σ be the elliptic curve with Weierstrass equation $y^2 = x^3 + \sigma(A)x + \sigma(B)$. Then $\sigma \circ \phi \circ \sigma^{-1}$ is an Endomorphism of E^σ. Thus, if E has CM by an order $\mathcal{O}$, so does E^σ.

The isomorphism classes of E and E^σ are determined by their j-invariants and $j(E^\sigma) = \sigma(j(E))$ following the definition of the j-invariant. Recall from lecture 2, that the isomorphism classes of elliptic curves with CM by $\mathcal{O}$ are parameterized by the class group of $\mathcal{O}$ which is a finite group. We conclude that $j(E)$ is algebraic. $\square$

Let h be the class number of an order $\mathcal{O}$ of an imaginary quadratic field. From the above proof, we see that $\mathbb{Q}(j(E))$ is a number field of degree at most h where E is an elliptic curve with CM by $\mathcal{O}$. In fact $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h$.

Theorem 3.2. *The j-invariant of a CM elliptic curve is an algebraic integer. Thus, a CM elliptic curve has potential good reduction at every prime.*

Sketch of proof. First, recall the degree of the multiplication by m isogeny is m^2 for any positive integer m. Let $\alpha \in \mathcal{O} \subset \mathbb{C}$ be an endomorphism of an elliptic curve E. Then the degree of $\alpha : E \to E$ is its norm, or simply $\alpha\overline{\alpha}$ where $\overline{\alpha}$ its complex conjugate. Thus, an elliptic curve having CM by an order $\mathcal{O} \subset \mathbb{Q}(\sqrt{-d})$ can be characterized by the existence of an endomorphism whose degree m is not a perfect square.

Consider a lattice $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$, the elliptic curve $\mathbb{C}/\Lambda_\tau$ admits a degree m isogeny to $\mathbb{C}/\Lambda_{m\tau}$ by $z \mapsto mz$. Using the existence of dual isogeny, admitting a degree m isogeny to or from $\mathbb{C}/\Lambda_\tau$ are equivalent. In fact, all lattices Λ for which $\mathbb{C}/\Lambda$ admitting a degree m isogeny to $\mathbb{C}/\Lambda_\tau$ takes the form $\mathbb{Z} + \mathbb{Z}(m\gamma\tau)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Up to homothety, there are finitely many homothety classes of lattices Λ for which $\mathbb{C}/\Lambda$ admits a degree m isogeny to $\mathbb{C}/\Lambda_\tau$ for a fixed Λ_τ. We list a representative of this set of $m\gamma\tau$ as $\tau_1, \cdots, \tau_n$.

Now we can define a polynomial in variable x in the following way

$$\Phi_m(X, \tau) := \prod_{i=1}^{n} (X - j(\tau_i)).$$

This theorem follows from the following facts about the polynomial Φ_m. The proof of these statements all base on the q-expansion of the j-function.

If

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n,$$

then

$$j(m\gamma\tau) = \frac{\zeta_m^{-ab}}{(q^{1/m})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{abn} (q^{1/m})^{a^2 n}, \text{ in which we take } m\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

- If we vary τ, the coefficients of $\Phi_m(X, \tau)$ varies in the following way: $\Phi_m(X, \tau) \in \mathbb{C}(j(\tau))[X]$.

  This follows from the coefficients of Φ_m as symmetric polynomials of $j(m\gamma\tau)$ are holomorphic functions on $\tau \in \mathbb{H}$ and invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. These coefficients are meromorphic at the cusps, thus are modular functions (weakly modular+meromorphic at ∞). All holomorphic modular functions of $\mathrm{SL}_2(\mathbb{Z})$ are polynomials of $j(\tau)$.

- Consider $\Phi_m(X, \tau)$ as a polynomial with two variables $\Phi_m(X, Y) \in \mathbb{C}[X, Y]$ by setting $Y = j(\tau)$. Then, in fact $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$.

  Using the explicit Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $j(m\gamma\tau)$ using the q-expansion, we can conclude $\Phi_m(X, Y) \in \mathbb{Q}[X, Y]$. Since the coefficients of the q-expansions of $j(m\gamma\tau)$ are algebraic integers, we conclude that $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$.

- When m is not a perfect square, $\Phi_m(X, X)$ is an integral polynomial of X with leading coefficients ± 1.

  This again follows from the explicit q-expansion of $j(m\gamma\tau)$, where $m\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Note that we need $m = ad$ to not be a perfect square in this argument.

$\square$