Lecture 5

The modular curves $X(\Gamma)$

In Lecture 3, we saw that the set of isomorphism classes of elliptic curves $E\mathbb{C}$ were in bijection with classes of homothetic lattices $\Lambda \subset \mathbb{C}$, which were in turn in bijection with elements of $Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$. In Lecture 4, we then saw that $X(1)$ is a compact Riemann surface.

Recall that given a lattice Λ, we define the j-invariant of Λ

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

where g_2 and g_3 are defined in terms of the Eisenstein series of weights 4 and 6, respectively. Homothetic lattices Λ and Λ' have $j(\Lambda) = j(\Lambda')$, and every lattice Λ is homothetic to a lattice $\Lambda_\tau = \tau\mathbb{Z} + \mathbb{Z}$, where $\tau \in \mathcal{H}$. We then define the function $j : \mathcal{H} \to \mathbb{C}$, $j(\tau) = j(\Lambda_\tau)$. This function is holomorphic on $\mathcal{H}$ and satisfies $j(S\tau) = j(\tau)$ and $j(T\tau) = j(\tau)$ for the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which generate $\mathrm{SL}_2(\mathbb{Z})$; thus we have a well-defined map $j : Y(1) \to \mathbb{C}$. This map is surjective, and by defining $j(\infty) = \infty$, we have a meromorphic function $j : X(1) \to \mathbb{P}^1(\mathbb{C})$ which is, in fact, an isomorphism of Riemann Surfaces. The modular curve $X(1)$, can therefore, be identified with the Riemann sphere S^2.

More generally, for a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$, we may again define the quotient space $Y(\Gamma)$. This space is not compact, but by adjoining finitely many cusps (corresponding to the orbits of $\mathbb{Q} \cup \{\infty\}$ under the action of Γ), we obtain the modular curves $X(\Gamma)$ which is again a compact Riemann surface. Each $X(\Gamma)$ is, topologically, a sphere with g handles. This nonnegative integer g is the genus of the surface. The Riemann sphere has 0 handles, thus its genus is 0. The genus of a curve is not only a topological invariant, it has "arithmetic" signifcance as well: for example, by Faltings's Theorem, a curve of genus $g > 1$ can have only finitely many $\mathbb{Q}$-rational points (or more generally only finitely many K-rational points for any finite degree extension of $\mathbb{Q}$). We will see some of the implications of this in the next lecture. For now, we discuss how to determine the genus g of a modular curve $X(\Gamma)$.

The genus of $X(\Gamma)$

If $f : X \to Y$ is a holomorphic map between Riemann surfaces, then f is surjective and there is a fixed positive integer d (the degree of the map) such that for all but finitely many $y \in Y$, $|f^{-1}(y)| = d$ so that the map f is d-to-1. In other words, for most $x \in X$, the multiplicity of x is $e_x = 1$, so that f is 1-1 about x. This integer e_x is known as the ramification index of x. There are sometimes points $x \in X$ for which $e_x > 1$; these points are said to be ramified. The Riemann-Hurwitz formula gives us a way to relate the genus g_X of X to the genus g_Y of Y.

Theorem 1 (Riemann-Hurwitz Formula) *Let X and Y be compact Riemann surfaces, and let $f : X \to Y$ be a nonconstant holomorphic map of degree d. Then*

$$2g_X - 2 = d(2g_Y - 2) + \sum_{x \in X}(e_x - 1).$$

As $X(1)$ is of genus 0, for a congruence subgroup Γ we can use the natural map

$$f : X(\Gamma) \to X(1),$$

$$\Gamma\tau \mapsto \mathrm{SL}_2(\mathbb{Z})\tau$$

to determine the genus of $X(\Gamma)$.

Theorem 2 *Let $\Gamma_1 \subseteq \Gamma_2$ be congruence subgroups. Then the map*

has degree

$$m = \begin{cases} [\Gamma_2 : \Gamma_1]/2 & \text{if } -I_2 \in \Gamma_2 \setminus \Gamma_1 \\ [\Gamma_2 : \Gamma_1] & \text{otherwise} \end{cases}$$

For example, since $-I_2 \in \Gamma(2)$ and $|SL_2(\mathbb{Z}/2\mathbb{Z})| = 6$, the map $X(2) \to X(1)$ is of degree 6.

We saw in the last lecture that for each $x \in X(1)$ corresponding to $\tau \in \mathcal{F}^*$ (a fundamental domain for the action on $\mathcal{H}^*$), there is some neighborhood U_x of τ_x such that $\gamma U_x \cap U_x = \emptyset$ for all $\gamma \neq \tau_x$. From this, we obtain an open cover $\{\pi(U_x)\}$ of $X(1)$ along with maps $\psi_x : \pi(U_x) \to \mathbb{D}$ which give a complex structure on $X(1)$. For most $x \in X(1)$, the projection map $\pi : \mathcal{H}^* \to X(1)$ restricted to U_x is a homeomorphism, but for $x \in \{i, e^{\frac{\pi i}{3}}, \infty\}$ the map is not injective. To correct for this, we had to define the homeomorphisms ψ_x in a slightly different fashion for these points than for the other points of $X(1)$. A similar issue arises for $X(\Gamma)$. In a fundamental domain F_Γ for Γ, the set $\{\pm I_2\}Stab_{\Gamma_\tau} = \{\pm I_2\}\{\gamma \in \Gamma : \gamma\tau = \tau\}$ will consist only of $\{\pm I_2\}$, and on an appropriate neighhborhood of τ, the restriction of the quotient map $\mathcal{H}^* \to X(\Gamma)$ will be a homeomorphism. The possible exceptions are those τ in the orbit of $i, e^{\pi i/3}$, or ∞.

Definition 3 *Let Γ be a subgroup of $SL_2(\mathbb{Z})$. A point $\tau \in \mathcal{H}$ is an elliptic point for Γ if $\{\pm I_2\} \subsetneq \{\pm I_2\}Stab_\tau$. We say $x = \Gamma\tau \in X(\Gamma)$ is elliptic if τ is an elliptic point.*

Example 4 *The elliptic points for $SL_2(\mathbb{Z})$ are i and $-\bar{\omega} = e^{\pi i/3}$.*

Definition 5 *If $\Gamma\tau \in X(\Gamma)$ is an elliptic point, its period is*

$$|\{\pm I_2\}Stab_{\Gamma_\tau} : \{\pm I_2\}| = \begin{cases} |Stab_{\Gamma_\tau}|/2 & \text{if } -I_2 \in \Gamma \\ |Stab_{\Gamma_\tau}| & \text{otherwise} \end{cases}$$

Now, two points of $\mathcal{H}^*$ may be in different Γ orbits despite being in the same $\mathrm{SL}_2(\mathbb{Z})$ orbit. By keeping track of elliptic points of Γ and determining their ramification indices, we can compute the genus of $X(\Gamma)$.

Theorem 6 *Let $\Gamma \subseteq SL_2(\mathbb{Z})$ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let m be the degree of the natural map $X(\Gamma) \to X(1)$. Let ϵ_2 denote the number of elliptic points of period 2, ϵ_3 the number of elliptic points of period 3, and ϵ_∞ the number of cusps of Γ (i.e., the number of orbits of Γ on $\mathbb{Q} \cup \{\infty\}$. Then then genus of $X(\Gamma)$ is*

$$g(X(\Gamma)) = 1 + \frac{m}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2}$$

For a proof, see [2, Thm. 2.22].

Example 7 *$X(2)$ has no elliptic points of order 2 or 3 and has 3 cusps. Thus $g(X(2)) = 0$.*

Points on $Y(\Gamma)$

Just as the points of $Y(1)$ parametrize elliptic curves, the points on the other modular curves we are most interested parameterize elliptic curves, but this time with additional torsion data.

Recall, for a positive integer N, the principal subgroup of level N, denoted $\Gamma(N)$ is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\},$$

where we reduce the entries of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ modulo N. A subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup if $\Gamma(N) \subseteq \Gamma$ for some N. The two we will most focus on are

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\},$$

(where the $*$ indicates that there are no conditions on b modulo N) and

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\},$$

To see how points of these curves parameterize elliptic curves with additional torsion data, first recall that if $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is a holomorphic map, then there are $m, b \in \mathbb{C}$ with $m\Lambda_1 \subset \Lambda_2$ and $\phi(z + \Lambda_1) = (mz + b) + \Lambda_2$.

When $\phi(0 + \Lambda_1) = 0 + \Lambda_2$, this map is a group homomorphism.

Definition 8 *A holomorphic group homomorphism of complex tori is called an isogeny.*

When $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is not the zero map, it is nonconstant. Therefore, ϕ is surjective. Moreover, the kernel, being a discrete subgroup of a compact space, is finite. To understand the kernel, we can use two kinds of isogenies. The first is the multiplication by N map. For $N \in \mathbb{Z}^+$, the map $[N]$ is given by

$$[N] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$$

$$z + \Lambda \mapsto Nz + \Lambda$$

If Λ has an oriented basis $\{\omega_1, \omega_2\}$, then the kernel of this map consists of points P of the form

$$P = \frac{c\omega_1 + d\omega_2}{N} + \Lambda$$

Let $E = \mathbb{C}/\Lambda$ be an elliptic curve. As an abstract group, the set of N-torsion points denoted $E[N]$ (i.e., the kernel of $[N]$ is isomorphic as an abstract group to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

In addition to the multiplication by N map, for a cyclic subgroup C of $E[N]$, we obtain a map

$$\mathbb{C}/\Lambda \to \mathbb{C}/C$$

$$z + \lambda \mapsto z + C$$

so that C is the kernel of the isogeny. Again refering to an oriented basis $\{\omega_1, \omega_2\}$, a cyclic subgroup of order N can be given by the lattice generated by ω_1 and ω_2/N. If, for example, $\Lambda = \Lambda_\tau$, then the cyclic subgroup C is $\tau\mathbb{Z} + \frac{1}{N}\mathbb{Z}$.

We are nearly ready to state the correspondence between points on $Y(N), Y_1(N)$ and $Y_0(N)$ and isomorphism classes of "elliptic curves with certain torsion data." For identifying points of $Y(N)$, we first need to define the Weil pairing. Note that we will be following Diamond and Shurman's definition ([1, §1.3]), but it is possible to define the Weil pairing using, for example, divisors (see for example [3, §3.8]).

Given an elliptic curve E corresponding to a lattice $\Lambda = \omega_1\mathbb{Z}+\omega_2\mathbb{Z}$ with $\omega_1/\omega_2 \in \mathcal{H}$, and given points P, Q in $E[N]$ there is some matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}/N\mathbb{Z})$ such that $P = \frac{a\omega_1}{N} + \frac{b\omega_2}{N} + \Lambda$ and $Q = \frac{c\omega_1}{N} + \frac{d\omega_2}{N} + \Lambda$, we define $e_N(P,Q)$ to be

$$e_N(P,Q) = e^{2\pi i \det(\gamma)/N}$$

. This pairing has

$$e_N : E[N] \times E[N] \to \mu_N,$$

where μ_N denotes the Nth roots of unity. We make the following claims:

Theorem 9 *The Weil pairing is*

(i) Bilinear:

$$e_N(P_1 + P_2, Q) = e_N(P_1, Q)e_N(P_2, Q)$$

and

$$e_N(P, Q_1 + Q + 2) = e_N(P, Q_1)e_N(P, Q_2)$$

(ii) Alternating:

$$e_N(P,P) = 1 \textit{ and in particular, } e_N(P,Q) = e_N(Q,P)^{-1}$$

(iii) Nondegenerate:

$$\textit{If } e_N(P,Q) = 1 \textit{ for all } P \in E[N], \textit{ then } Q = 0$$

Having introduced the Weil pairing, we can describe points of $Y(N)$: A point of $Y(N)$ corresponds to an isomorphism class of a triple $[E,P,Q]$ where P and Q are a basis for $E[N]$ and $e_N(P,Q) = e^{2\pi i/N}$. The triples $[E,P,Q]$ and $[E',P',Q']$ are equivalent if there is an isomorphism $\phi : E \to E'$ such that $\phi(P) = P'$ and $\phi(Q) = Q'$.

A point on $Y_1(N)$ corresponds to a pair $[E,P]$, where P is a point of E of order N. Two such pairs $[E,P]$ and $[E',P']$ are equivalent if there is an isomorphism $\phi : E \to E'$ such that $\phi(P) = P'$.

A point on $Y_0(N)$ corresponds to a pair $[E,C]$ where C is a cyclic subgroup of E of order N. Two such pairs $[E,C]$ and $[E',C']$ are equivalent if there is an isomorphism $\phi : E \to E'$ such that $\phi(C) = C'$.

We can identify an elliptic curve E with $\mathbb{C}/\Lambda$, but we can actually do more.

Theorem 10 *Let N be a positive integer.*

(i) Each point $[E,P,Q]$ of $Y(N)$ is equivalent to $[\mathbb{C}/\Lambda_\tau, \tau/N + \Lambda_\tau, 1/N + \Lambda_\tau]$ for some $\tau \in \mathcal{H}$. Two points $[\mathbb{C}/\Lambda_\tau, \tau/N+\Lambda_\tau, 1/N+\Lambda_\tau] = [\mathbb{C}/\Lambda'_\tau, \tau'/N+\Lambda'_\tau, 1/N+\Lambda'_\tau]$ if and only if $\Gamma(N)\tau = \Gamma(N)\tau'$

(ii) Each point $[E,P]$ of $Y_1(N)$ is equivalent to $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau]$ for some $\tau \in \mathcal{H}$. Two points $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau]$ and $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau]$ are equal if and only if $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$

(iii) Each point $[E,C]$ of $Y_0(N)$ is equivalent to $[\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle]$ for some $\tau \in \mathcal{H}$. Two points $[\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle]$ and $[\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau]\rangle$ are equal if and only if $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$

For a proof of part (ii), see [1, Thm. 1.5.1]

References

[1] Diamond, F. and Shurman, J. *A First Course in Modular Forms.* Springer 2016, 4th. printing.

[2] Milne, J.S., *Modular Functions and Modular Forms*, `https://www.jmilne.org/math/CourseNotes/mf.html`

[3] Silverman, J. *The Arithmetic of Elliptic curves, second edition*, Springer 2009.