19.1 The j-function

Let L be a lattice in $\mathbb{C}$ (a discrete cocompact subgroup). The weight-k Eisentstein series for L is

$$G_k(L) := \sum_{\omega \in L - \{0\}} \frac{1}{\omega^k},$$

which vanishes for odd k and converges for all $k > 2$. After replacing L with λL for some $\lambda \in \mathbb{C}^\times$ we may assume L is the lattice spanned by $[1, \tau]$ for some $\tau \in \mathbf{H}$. We then have

$$G_k(z) := G_k([1,\tau]) = \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m+nz)^k},$$

thus for $k > 2$ we may view $G_k(\tau)$ as a holomorphic function $\mathbf{H} \to \mathbb{C}$ that satisfies

$$G_k(\tau+1) = G_k(\tau) \qquad \text{and} \qquad G_k(-1/\tau) = \tau^k G_k(\tau).$$

This implies that $G_k|_k\gamma = G_k$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z}) = \langle \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\rangle$. For even k we have

$$\lim_{\operatorname{Im}\tau\to\infty} G_k(\tau) = 2\zeta(k),$$

and $G_k(z)$ is holomorphic and nonvanishing at the cusps, makeing it a (non-cuspidal) modular form of weight k for $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$.

The Weierstrass $\wp$-function for L is defined by

$$\wp(z:L) := \frac{1}{z^2} + \sum_{\omega\in L-\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

It is a meromorphic function on $\mathbb{C}$ that is periodic with respect to L: $\wp(z+\omega) = \wp(z)$ for $\omega \in L$; in other words, it is an elliptic function. It has poles of order 2 at each $\omega \in L$ is holomorphic elsewhere. The Laurent series expansion of $\wp(z)$ as $z = 0$ is

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

and one can use this to show that $\wp(z) = \wp(z;L)$ satisfies the differential equation

$$\wp'(z) = 4\wp(z)^3 - g_4(L)\wp(z) - g_6(L),$$

where $g_4(L) := 60G_4(L)$ and $g_6(L) := 140G_6(L)$. The map $z \mapsto (\wp(z), \wp'(z))$ defines an isomorphism from the torus $\mathbb{C}/L$ (which is a Riemann surface of genus 1) to the elliptic curve

$$E_L\colon y^2 = 4x^3 - g_4(L)x - g_6(L),$$

with nonzero discriminant $\Delta(L) := g_4(L)^3 - 27g_6(L)^2$, which sends $\omega \in L$ to the projective point $\infty := (0:1:0)$ on E_L, which serves as the identity element of the group $E_L(\mathbb{C})$. The discriminant function $\Delta(\tau) := \Delta([1,\tau])$ is a cusp form of weight 12.

Definition 19.1. The j-invariant of the lattice L, and of the elliptic curve E_L, is defined by

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

Lecture by Andrew V. Sutherland, notes by Andrew V. Sutherland

If we write the E_L in the form $y^2 = x^3 + Ax + B$ with $g_4(L) = -4A$ and $g_6(L) = -4B$ then

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

which defined the j-invariant of elliptic curves E/k for any field k whose characteristic is not 2 or 3 (and there are generalizations that work over any field).

We call lattices L and L' homothetic if $L' = \lambda L$ for some $\lambda \in \mathbb{C}^\times$.

Theorem 19.2. *Lattices L and L' are homothetic if and only if $j(L) = j(L')$, and if and only if the corresponding elliptic curves E_L and $E_{L'}$ are isomorphic.*

Proof. See Theorem 15.5 and Corollary 15.6 in [1]. ☐

Theorem 19.3 (Uniformization theorem)**.** *The functor $L \mapsto E_L$ defines an equivalence of categories of complex tori $\mathbb{C}/L$ up to homethety and elliptic curves $E/\mathbb{C}$ up to isomorphism. The map $\mathbb{C}/L \to E_L(\mathbb{C})$ defined by $z \mapsto (\wp(z), \wp'(z))$ is an isomorphism of compact Lie groups.*

Proof. See Corollary 15.12 in [1]. ☐

Now consider $j(\tau) := j([1,\tau])$ as a holomorphic function $\mathbf{H} \to \mathbb{C}$. We have $j(\gamma\tau) = j(\tau)$ for all $\gamma \in \Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$, thus $j(\tau)$ is a modular function. It is not a modular form (of weight 0) because it is not holomorphic at the cusps: it has a pole at ∞.

The function $j(\tau)$ defines an isomorphism from $Y(1) := \mathbf{H}/\Gamma(1)$ to the affine line $\mathbb{A}^1(\mathbb{C})$ that extends to an isomorphism from $X(1) := \mathbf{H}^*/\Gamma(1)$ to the projective line $\mathbb{P}^1(\mathbb{C})$.

If we put $q = e^{2\pi i\tau}$ the q-expansion of the j-function is

$$j(\tau) = \frac{1}{q} + 744 + \sum_{n\geq 1} a_n q^n$$

with $a_n \in \mathbb{Z}$. This explains the factor 1728 in the definition of $j(\tau)$; it is the least integer that makes the q-expansion of $j(\tau)$ integral.

19.2 Isogenies

Morphisms of complex tori $\varphi: \mathbb{C}/L_1 \to \mathbb{C}/L_2$ are induced by holomorphic functions $f: \mathbb{C} \to \mathbb{C}$ for which the following diagram commutes

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{C} \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ \mathbb{C}/L_1 & \xrightarrow{\varphi} & \mathbb{C}/L_2 \end{array}$$

One can show that, up to homethety, we can always take f to be a multiplication-by-α map $z \mapsto \alpha z$ for some $\alpha \in \mathbb{C}^\times$ for which $\alpha L_1 \subseteq L_2$. The corresponding homomorphism φ_α is then defined by $z + L_1 \mapsto \alpha z + L_2$. We have an isomorphism of abelian groups

$$\left\{\alpha \in \mathbb{C} : \alpha L_1 \subseteq L_2\right\} \xrightarrow{\sim} \left\{\varphi: \mathbb{C}/L_1 \to \mathbb{C}/L_2\right\} = \mathrm{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_2),$$

and if $L_1 = L_2$ this is an isomorphism of commutative rings. For most lattice L we have $\mathrm{End}(\mathbb{C}/L) = \mathbb{Z}$, but if L is homothetic to an ideal in an imaginary quadratic order $\mathcal{O}$ then $\mathrm{End}(\mathbb{C}/L) \simeq \mathcal{O}$ (this is the theory of complex multiplication).

Definition 19.4. An isogeny of elliptic curves is a nonconstant morphism $\phi\colon E_1 \to E_2$ that is compatible with the group law. The degree of an isogeny ϕ is its degree as a rational map, equivalently, the degree of the extension of function fields induced by ϕ (for each $f \in k(E_2)$ we have $f \circ \phi \in k(E_1)$ and a field extension $k(E_1)/\phi^*(k(E_2)$. We say that ϕ is separable if the extension $k(E_1)/\phi^*(k(E_2))$ is separable (always true in characteristic zero).

If $L_1 \subseteq L_2$ then L_2/L_1 is a finite abelian group and the inclusion $L_1 \subseteq L_2$ induces a morphism $\mathbb{C}/L_1 \to \mathbb{C}/L_2$ via $z + L_1 \mapsto z + L_2$ and a corresponding isogeny of elliptic curves $\phi\colon E_{L_1} \to E_{L_2}$ whose kernel is isomorphic to L_2/L_1 with $\deg \phi = [L_2 : L_1]$. If we put $N = [L_2 : L_1]$ then we also have an inclusion $NL_2 \subseteq L_1$ that induces an isogeny in the reverse direction of the same degree called the dual isogeny. The composition of these two isogenies (in either order) is equivalent to multiplication-by-N.

The kernel of the multiplication-by-N map on any lattice L or elliptic curve $E/\mathbb{C}$ is isomorphic to $\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$. We call an isogeny cyclic if its kernel is a cyclic group. If $\phi\colon E_1 \to E_2$ is a cyclic isogeny of degree N then its kernel is isomorphic to $\mathbb{Z}/N\mathbb{Z}$ and $\phi(E_1[N])$ is a cyclic subgroup of $E_2[N]$ that is the kernel of the dual isogeny $\hat{\phi}$.

For any elliptic curve E/k the kernel of any isogeny $\phi\colon E \to E'$ is a finite subgroup of $E(\bar{k})$ whose order divides $\deg \phi$, with equality if and only if ϕ is separable. Conversely, every finite subgroup of $E(\bar{k})$ is the kernel of a separable isogeny that is unique up to isomorphism; Vélu's formulas allow one to explicit construct this isogeny and an equation for its codomain.

19.3 Modular curves

Recall the modular curves $X_0(N) := \mathbf{H}^*/\Gamma_0(N)$ and $X_1(N) := \mathbf{H}^*/\Gamma_1(N)$. These are compact Riemann surfaces, hence smooth projective curves over $\mathbb{C}$, but in fact they have models over $\mathbb{Q}$ that allow us to view them as smooth projective curves over any field whose characteristic does not divide N.

For $X_0(1) = X_1(1) = X(1)$, we have $\mathbb{C}(X(1)) = \mathbb{C}(j)$ generated by the j-function (this follows from the fact that $j(\tau)$ defines an isomorphism $X(1) \simeq \mathbb{P}^1$ and meromorphic functions on $\mathbb{P}^1$ are rational functions).

If Γ is any congruence subgroup, the inclusion $\Gamma \subseteq \Gamma(1)$ induces morphism of modular curves $X_\Gamma \to X(1)$. Thus every modular curve comes equipped with a map to the j-line $X(1) \simeq \mathbb{P}^1$. It follows that each non-cuspidal point on X_Γ can be associated to an elliptic curve, and this makes applies not only over $\mathbb{C}$, but for any field over which X_Γ is defined.

Assuming Γ contains -1, the degree of the morphism $X_\Gamma \to X(1)$ is $[\Gamma(1)\colon \Gamma]$, which is the degree of the function field extension $\mathbb{C}(X_\Gamma)/\mathbb{C}(j)$. We now consider the function field $\mathbb{C}(X_0(N))$.

Theorem 19.5. *For each positive integer N the function $j_N(\tau) := j(N\tau)$ is a modular function for $\Gamma_0(N)$ that generates the extension $\mathbb{C}(X_0(N))/\mathbb{C}(j)$, in other words, $\mathbb{C}(X_0(N)) = \mathbb{C}(j, j_N)$.*

Proof. See Theorems 19.13 and 19.14 in [1]. □

Note that while $\mathbb{C}(j)$ is a transcendental extension of $\mathbb{C}$, the field $\mathbb{C}(j, j_N)$ is a finite (hence algebraic) extension of $\mathbb{C}(j)$.

Definition 19.6. The (classical) modular polynomial $\Phi_N(Y) \in \mathbb{C}(j)[Y]$ is the minimal polynomial of j_N over $\mathbb{C}(j)$. If we replace each occurrence of j in the coefficients of Φ_N with X, we obtain a bivariate polynomial $\Phi_N \in \mathbb{Z}[X, Y]$ that satisfies $\Phi_N(X, Y) = \Phi_N(Y, X)$.

Theorem 19.7. *For $j_1, j_2 \in \mathbb{C}$ we have $\Phi_N(j_1, j_2) = 0$ if and only if j_1 and j_2 are the j-invariants of elliptic curves E_1, E_2 over $\mathbb{C}$ for which there exists a cyclic isogeny $\phi\colon E_1 \to E_2$ of degree N.*

Proof. See Theorem 20.3 in [1] for a proof in the case where N is prime. □

Remark 19.8. If E_1 and E_2 are related by an isogeny $\phi\colon E_1 \to E_2$ of degree N, the pair $(j(E_1), j(E_2))$ does not necessarily determine ϕ uniquely (not even up to isomorphism), as it is possible for there to be two cyclic isogenies of degree N from E_1 to E_2 that have distinct kernels. This occurs precisely when $j(E_2)$ is a double root of the polynomial $\Phi_N(j(E_1), Y)$.

The connection between $\Gamma_0(N)$ and isogenies can be seen in two ways. First, there is a one-to-one correspondence between cyclic subgroups H of $\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ of order N and cosets of $\Gamma_0(N)$ in $\Gamma(1)$. Alternatively, if we fix a basis $\langle P, Q\rangle$ of $\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ so that $H = \langle P\rangle$, then the matrices in $GL_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ that send P to a multiple of P and therefore stabilize H are precisely the upper triangular matrices; if we restrict to matrices of determinant 1, these are precisely the reductions of elements of $\Gamma_0(N)$ modulo N.

This leads to the moduli interpretation of $X_0(N)$. There is a one-to-one correspondence between non-cuspidal points in $X_0(N)(\mathbb{C})$ and equivalence classes of pairs $(E, \langle P\rangle)$, where E is an elliptic curve and $P \in E[N]$ is a point of order N. We regard two pairs $(E, \langle P\rangle)$ and $(E', \langle P'\rangle)$ to be equivalent whenever there is an isomorphism $\iota\colon E \to E'$ for which $\langle P'\rangle = \langle \iota(P)\rangle$.

Let us now consider the modular curve $X_1(N)$. Matrices in $\Gamma_1(N)$ don't just fix a cyclic subgroup of $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ of order N, they fix a point of order N, and there is a one-to-one correspondence between non-cuspidal points in $X_1(N)(\mathbb{C})$ and equivalence classes of pairs (E, P), where E is an elliptic curve and $P \in E[N]$ is a point of order N, where we now regard pairs (E, P) and (E', P') as equivalent if there is an isomorphism $\iota\colon E \to E'$ for which $P' = \iota(P)$.

For the modular curve $X(N)$ we have a one-to-one correspondence between non-cuspidal points in $X(N)(\mathbb{C})$ and equivalence classes of triples (E, P, Q) where $E[N] = \langle P, Q\rangle$ and equivalence involves an isomorphism $\iota\colon E \to E'$ with $\iota(P) = P'$ and $\iota(Q) = Q'$.

Every matrix in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ defines an automorphism of $X(N)$ via its action on P and Q, so given any subgroup $H \le \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we can consider the quotient curve $X(N)/H$. If we take H to be the subgroup of upper triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, this quotient is $X_0(N)$, and restricting to upper triangular matrices with a 1 in the upper left corner yields $X_1(N)$.

Unlike the curves $X_0(N)$ and $X_1(N)$, which have models over $\mathbb{Q}$, the curve $X(N)$ is defined over $\mathbb{Q}(\zeta_N)$(so over $\mathbb{Q}$ only when $N \le 2$). But if H is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for which $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$, the quotient $X(N)/H$ will have a model over $\mathbb{Q}$.

References

[1] Andrew V. Sutherland, *Lecture notes for Elliptic Curves (18.783)*, 2023.