18.783 Elliptic Curves
Lecture 19

Andrew Sutherland

November 16, 2023

Modular curves

Definition

The principal congruence subgroup $\Gamma(N)$ is defined by

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

A congruence subgroup (of level N) is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that contains $\Gamma(N)$, e.g.

$$\Gamma_1(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \bmod N \right\};$$
$$\Gamma_0(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod N \right\}.$$

A classical modular curve is a quotient of $\mathcal{H}^*$ or $\mathcal{H}$ by a congruence subgroup.

We now define the classical modular curves

$$X(N) := \mathcal{H}^*/\Gamma(N), \qquad X_1(N) := \mathcal{H}^*/\Gamma_1(N), \qquad X_0(N) := \mathcal{H}^*/\Gamma_0(N).$$

q-expansions

Let $\mathcal{D} = \{z \in \mathbb{C} : |z| < 1\}$ denote the (open) unit disk. The map $q\colon \mathcal{H} \to \mathcal{D}$ defined by

$$q(\tau) = e^{2\pi i\tau} = e^{-2\pi\,\mathrm{im}\,\tau}\left(\cos(2\pi\,\mathrm{re}\,\tau) + i\sin(2\pi\,\mathrm{re}\,\tau)\right)$$

bijectively maps each vertical strip $\mathcal{H}_n := \{\tau \in \mathcal{H} : n \le \mathrm{re}\,\tau < n+1\}$ (for any $n \in \mathbb{Z}$) to the punctured unit disk $\mathcal{D}_0 := \mathcal{D} - \{0\}$. Note that $q(\tau) \to 0$ as $\mathrm{im}\,\tau \to \infty$.

If $f\colon \mathcal{H} \to \mathbb{C}$ is a meromorphic function that satisfies $f(\tau+1) = f(\tau)$ for all $\tau \in \mathcal{H}$, then we can write f in the form $f(\tau) = f^*(q(\tau))$, where $f^*\colon \mathcal{D}_0 \to \mathbb{C}$ is a meromorphic function that we can define by fixing a vertical strip $\mathcal{H}_n$ and putting $f^* := f \circ (q_{|\mathcal{H}_n})^{-1}$.

Definition

The q-expansion (or q-series) of a meromorphic $f\colon \mathcal{H} \to \mathbb{C}$ with $f(\tau+1) = f(\tau)$ is

$$f(\tau) = f^*(q(\tau)) = \sum_{n=-\infty}^{+\infty} a_n q(\tau)^n = \sum_{n=-\infty}^{+\infty} a_n q^n.$$

Cusps

Let Γ be a congruence subgroup of level N. Then $\gamma = \left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$, and $\gamma\tau = \tau + N$. If $f \colon \mathcal{H} \to \mathbb{C}$ is meromorphic and Γ-invariant, then $f(\tau + N) = f(\tau)$ and we can write

$$f(\tau) = f^*(q(\tau)^{1/N}) = \sum_{n=-\infty}^{\infty} a_n q^{n/N}.$$

If f^* is meromorphic at 0 then

$$f(\tau) = \sum_{n=n_0}^{\infty} a_n q^{n/N} \qquad (a_{n_0} \neq 0).$$

and say that f is meromorphic at ∞ (with order n_0 at ∞). If $f(\gamma\tau)$ is meromorphic at ∞ for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ then we say that f is meromorphic at the cusps.

Recall that the $\mathrm{SL}_2(\mathbb{Z})$-orbit of ∞ in $\mathcal{H}^*$ is $\mathcal{H}^* - \mathcal{H} = \mathbb{P}^1(\mathbb{Q})$; the $\gamma\infty$ are called cusps, and Γ partitions $\mathbb{P}^1(\mathbb{Q})$ into a finite set of Γ-orbits called the cusps of Γ.

Modular functions

If $f\colon \mathcal{H} \to \mathbb{C}$ is a Γ-invariant meromorphic function then for every $\gamma \in \Gamma$ we have

$$\lim_{\operatorname{im}\tau\to\infty} f(\gamma\tau) = \lim_{\operatorname{im}\tau\to\infty} f(\tau)$$

whenever either limit exists.

If f is meromorphic at the cusps it must have the same order at ∞ and $\gamma\infty$ and thus defines a meromorphic function $g\colon X_\Gamma \to \mathbb{C}$ on the modular curve $X_\Gamma := \mathcal{H}^*/\Gamma$.

Conversely, each meromorphic $g\colon X_\Gamma \to \mathbb{C}$ determines a Γ-invariant meromorphic $f\colon \mathcal{H} \to \mathbb{C}$ that is meromorphic at the cusps via $f = g \circ \pi$, where $\pi\colon \mathcal{H}^* \to \mathcal{H}^*/\Gamma$.

Definition

A modular function for a congruence subgroup Γ is a Γ-invariant meromorphic function $f\colon \mathcal{H} \to \mathbb{C}$ that is meromorphic at the cusps, equivalently, a meromorphic $g\colon X_\Gamma \to \mathbb{C}$.

Function fields of modular curves

For any congruence subgroup Γ the modular functions for Γ for a field $\mathbb{C}(\Gamma)$ that is a transcendental extension of $\mathbb{C}$. As we will prove for $\Gamma = \Gamma_0(N)$, the Riemann surface $X_\Gamma := \mathcal{H}^*/\Gamma$ is an algebraic curve, and $\mathbb{C}(\Gamma)$ is isomorphic to its function field $\mathbb{C}(X_\Gamma)$.

In fact every compact Riemann surface S corresponds to a smooth projective curve over $X/\mathbb{C}$ with function field $\mathbb{C}(X) \simeq \mathbb{C}(S)$, and given a smooth projective curve $X/\mathbb{C}$ we can endow the set $X(\mathbb{C})$ with a topology and a complex structure that makes it a Riemann surface S with $\mathbb{C}(S) \simeq \mathbb{C}(X)$.

If $\Gamma' \subseteq \Gamma$ are congruence subgroups, every modular function for Γ is also a modular function for Γ', and this induces an inclusion $\mathbb{C}(\Gamma) \subseteq \mathbb{C}(\Gamma')$ of their function fields that induces a corresponding morphism $X_{\Gamma'} \to X_\Gamma$ of modular curves.

The q-expansion of the j-function.

Lemma

Let $\sigma_k(n) = \sum_{d|n} d^k$, *and let* $q = e^{2\pi i\tau}$. *We have*

$$g_2(\tau) = \frac{4\pi^4}{3}\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right), \qquad g_3(\tau) = \frac{8\pi^6}{27}\left(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n\right),$$

$$\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2 = (2\pi)^{12}q\prod_{n=1}^{\infty}(1-q^n)^{24}.$$

Corollary

The q*-expansion of the* j*-function is* $j(\tau) = q^{-1} + 744 + \sum_{n\geq 1} a_n q^n$ *with* $a_n \in \mathbb{Z}$. *In particular, the* j*-function is meromorphic at the cusps.*

Proof: To the board!

Modular functions for $\Gamma(1)$

The corollary implies that the j-function is a modular function for $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$.

Recall that the j-function defines a holomorphic bijection $Y(1) \xrightarrow{\sim} \mathbb{C}$.
If we put $j(\infty) := \infty$ then it defines a meromorphic bijection $X(1) \xrightarrow{\sim} \mathcal{S} := \mathbb{P}^1(\mathbb{C})$ that has only a simple pole at ∞ (if we put $j(\rho) := 0$, $j(i) := 1728$ this determines j).

Theorem

Every modular function for $\Gamma(1)$ is a rational function of $j(\tau)$, that is, $\mathbb{C}(\Gamma(1)) = \mathbb{C}(j)$.
Proof: We have $\mathbb{C}(j) \subseteq \mathbb{C}(\Gamma(1))$ and the lemma below gives the reverse inclusion.

Lemma

Every meromorphic $f : \mathcal{S} \to \mathbb{C}$ is a rational function.

Corollary

The $\mathbb{C}[j]$ is precisely the subring of $\mathbb{C}(j) = \mathbb{C}(\Gamma(1))$ that is holomorphic on $\mathcal{H}$.

Modular functions for $\Gamma_0(N)$

Theorem

Let Γ *be a congruence subgroup.* $[\mathbb{C}(\Gamma) : \mathbb{C}(j)]$ *has degree at most* $[\mathrm{SL2}(\mathbb{Z}) : \Gamma]$.
Proof: To the board!

Remark

If $-I \in \Gamma$ then $[\mathbb{C}(\Gamma) : \mathbb{C}(j)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ (we will prove this for $\Gamma = \Gamma_0(N)$).

Theorem

The function $j_N(\tau) := j(N\tau)$ *is a modular function for* $\Gamma_0(N)$.
Proof: To the board!

Theorem

$\mathbb{C}(\Gamma_0(N)) = \mathbb{C}(j)(j_N)$ *and* $[\mathbb{C}(\Gamma_0(N)) : \mathbb{C}(j)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$.
Proof: To the board!

The modular polynomial $\Phi_N \in \mathbb{C}[X, Y]$

Definition

The modular polynomial Φ_N is the minimal polynomial of j_N over $\mathbb{C}(j)$.

We may write $\Phi_N \in \mathbb{C}(j)[Y]$ as

$$\Phi_N(Y) = \prod_{i=1}^{n} (Y - j_N(\gamma_i \tau)),$$

where $\{\gamma_1, \dots \gamma_n\}$ is a set of right coset representatives for $\Gamma_0(N)$.

The coefficients of $\Phi_N(Y)$ are symmetric polynomials in $j_N(\gamma_i \tau)$, so $\Gamma(1)$-invariant, and holomorphic on $\mathcal{H}$, hence lie in $\mathbb{C}[j]$. Thus $\Phi_N \in \mathbb{C}[j, Y]$.

If we replace every occurrence of j in Φ_N with a new variable X we obtain a polynomial in $\mathbb{C}[X, Y]$ that we write as $\Phi_N(X, Y)$.

The modular polynomial $\Phi_N \in \mathbb{Z}[X, Y]$

Lemma

Let $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ *and* $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. *For* N *prime the right cosets of* $\Gamma_0(N)$ *in* $\Gamma(1)$ *are*

$$\left\{\Gamma_0(N)\right\} \cup \left\{\Gamma_0(N) S T^k : 0 \leq k < N\right\}.$$

Theorem

$\Phi_N \in \mathbb{Z}[X, Y]$.

Proof: To the board!

Lemma (Hasse q-expansion principle)

Let $f(\tau)$ *be a modular function for* $\Gamma(1)$ *that is holomorphic on* $\mathcal{H}$ *and whose* q*-expansion has coefficients that lie in an additive subgroup* A *of* $\mathbb{C}$.
Then $f(\tau) = P(j(\tau))$, *for some polynomial* $P \in A[X]$.