Review of Modular Forms and Introduction to Modular Curves

Yifan Wu

12131236

28th Sep, 2023

References I

[DS05] Fred Diamond and Jerry Michael Shurman, *A first course in modular forms*, vol. 228, Springer, 2005.

[KM85] Nicholas M Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, no. 108, Princeton University Press, 1985.

[Mil90] James S Milne, *Modular functions and modular forms*, Course Notes of the University of Michigan (1990).

Contents

Let $\Lambda = \alpha\mathbb{Z} + \beta\mathbb{Z} \subset \mathbb{C}$ be a lattice. $E = \mathbb{C}/\Lambda$ is an elliptic curve.

$$\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda^{'}$$

iff $\Lambda = \gamma\Lambda^{'}$ for some $\gamma \in \mathbb{C}$.

How can we classify these elliptic curves up to isomorphism?

That is for what $\tau, \tau' \in \mathbb{H}$ we have

$$\Lambda_{\tau} = \mathbb{Z}\tau + \mathbb{Z} \cong \mathbb{Z}\tau' + \mathbb{Z} = \Lambda_{\tau'} \text{ ?}$$

$$\tau' = \gamma a\tau + \gamma b,$$
$$1 = \gamma c\tau + \gamma d.$$

for some $a, b, c, d \in \mathbb{Z}$ such that,

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

Hence each point on $\Gamma(1)\backslash\mathbb{H}$ represents an class of elliptic curves.

$\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ is generated by

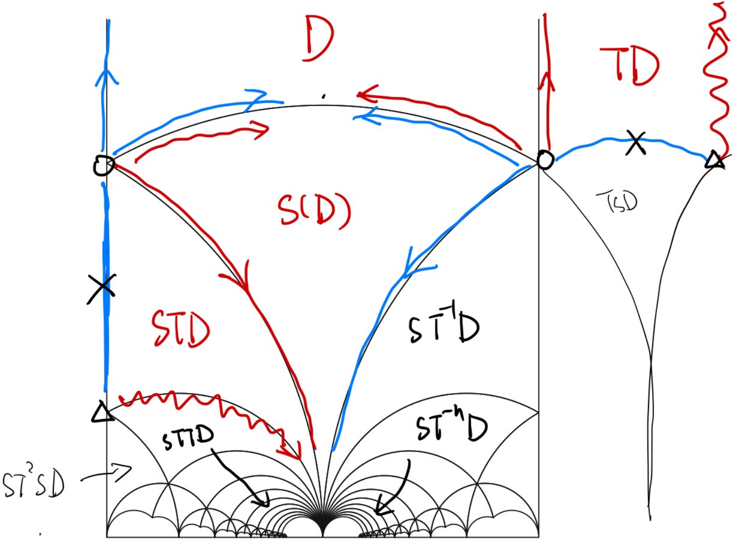
$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \text{ and } \ T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

with action on $\mathbb{H}$:

$$Sz = -\frac{1}{z}, \quad Tz = z + 1.$$

Let $D = \{z \in \mathbb{H} \mid |z| \geq 1, \ |\mathrm{Re}(z)| \leq \frac{1}{2}\}$, which is called the **fundamental domain** for $\Gamma(1)$, we have the following picture.

Fundamental Domain for Γ(1)



How to classify an elliptic curve E with a point C of exact order N ?

$$(\mathbb{C}/\Lambda_\tau, 1/N) \xrightarrow{m} (\mathbb{C}/\Lambda_{\tau'}, 1/N)$$

This means that first $\tau \sim \tau'$ under $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.
$m = c\tau' + d$, and we have

$$\frac{c\tau' + d}{N} - \frac{1}{N} \in \Lambda_{\tau'}.$$

Hence $(c, d, a) = (0, 1, 1)$ mod N. Thus we define

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

Modular Curves over $\mathbb{C}$

$$\begin{aligned} Y_1(N) &:= \Gamma_1(N)\backslash\mathbb{H} \rightsquigarrow (\mathbb{C}/\Lambda, C) \\ Y_0(N) &:= \Gamma_0(N)\backslash\mathbb{H} \rightsquigarrow (\mathbb{C}/\Lambda, \langle C\rangle) \\ Y(N) &:= \Gamma(N)\backslash\mathbb{H} \rightsquigarrow (\mathbb{C}/\Lambda, (P, Q)) \end{aligned}$$

where

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

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

Compactification and Cusps

Compactification:

$$Y_*(N) \xrightarrow{\text{Adding points}} X_*(N)$$

Those additional points are called **cusps**.

$\Gamma(1)$ has only one cusp, namely $i\infty$, and the resulting compact Riemann surface $X(1) \cong S^2$, which has genus 0.

The first $X_0(p)$ with nonzero genus is $X_0(11)$ with has $g = 1$.

Genus Formulas

For each congruence subgroup $\Gamma \subset \Gamma(1)$, we have a natural map

$$\pi : X(\Gamma) = \Gamma \backslash \mathbb{H} \Rightarrow \Gamma(1) \backslash \mathbb{H} = X(1).$$

By Hurwitz formula, we have

$$g(X(\Gamma)) = 1 + \frac{d}{12} - \frac{e_2}{4} - \frac{e_3}{3} - \frac{v_\infty}{2},$$

where $d = \deg \pi$, e_2, e_3 corresponds to number of elliptic points for Γ of order 2, 3 respectively, and v_∞ is the number of cusps for Γ.

Moduli Schemes

Let C/S be an elliptic curve over a scheme S. In particular, over a field k, we have the Weierstrass equation

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

$$W = \mathrm{Spec}\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, \Delta^{-1}]$$

$\mathrm{Spec}k \to W$ gives isomorphism class of elliptic curves over k?

$\mathcal{M}_{ell} := [W/H]$ is called the **moduli stack** of elliptic curves, and $\mathcal{M}_{ell}(S)$ does indeed give the groupoid of elliptic curves over S!

A **moduli problem** over S is a contravariant functor

$$\phi : Ell/S \Rightarrow Sets$$

Over $\mathbb{Z}[1/N]$ the problem $[\Gamma_1(N)]$ and $[\Gamma(N)]$ are representable, while $[\Gamma_0(N)]$ only be relative representable.

Remark: There is a local model around the supersingular locus for the moduli scheme $\mathcal{M}_{N,p}$ of moduli problem $[\Gamma_1(N) \times \Gamma_0(p)]$ over $\mathbb{Z}[1/N]$ provided by Zhu, in [Zhu18, Semi-stable].

A meromorphic function on $X(\Gamma)$ is equivalent to

$$f \text{ meromorphic on } \mathbb{H}^*, f(\gamma z) = f(z), \gamma \in \Gamma$$

such functions are called **modular functions**.

There are some h with $T^h \in \Gamma$, hence $f(z+h) = f(z)$ is periodic.

At cusp $i\infty$, $f^*(q)$ meromorphic at $q = 0$, $q = e^{2\pi i z/h}$.
At cusp $\tau \neq i\infty$, there is $\theta \in \Gamma(1)$, with $\tau = \theta(i\infty)$. $f(\theta z)$ is invariant under $\theta\Gamma\theta^{-1}$, we require $f(\theta z)$ meromorphic at $i\infty$.

Modular Forms

Let f be a holomorphic function on $\mathbb{H}$ with

- $f(\gamma z) = (cz+d)^{2k} f(z)$ for $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$;
- f holomorphic on $\mathbb{H}$;
- f holomorphic at cusps for Γ.

These functions are called **modular forms of weight** $2k$.

Such a modular form vanishing at all cusps are called **cusp form**.

Here are some important examples.

- **Eisenstein series** $G_k(\Lambda) := \sum_{\omega\in\Lambda,\omega\neq 0} \omega^{-2k}$. And

$$G_k(z) := G_k(z\mathbb{Z}+\mathbb{Z}) = \sum_{(m,n)\neq(0,0)} 1/(mz+n)^{2k}$$

It is a modular form of weight $2k$ for $\Gamma(1)$, with value $2\xi(2k)$ at the cusp.

- $\Delta := g_2^3 - 27g_3^2$, $g_2 = 60G_2$ and $g_3 = 140G_3$.

  Modular form for $\Gamma(1)$, weight: 12. Cusp form.

- $j := 1728g_2^3/\Delta$

  Modular function for $\Gamma(1)$, with a simple pole at cusp $i\infty$, and $j(i) = 1728$, $j(\rho) = 0$.

Relation with Elliptic Curves

Recall that over $\mathbb{C}$, any elliptic curve can be written as

$$E : y^2 = 4x^3 - ax - b.$$

And we require $\Delta \stackrel{def}{=} a^3 - 27b^2 \neq 0$. $j(E) \stackrel{def}{=} 1728a^3/\Delta$.

There is a Weierstrass $\wp$ function defined by

$$\wp'(z; \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

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

For any lattice Λ, we define $E(\Lambda)$ to be

$$y^2 = 4x^3 - g_2 x - g_3$$

Then there is an isomorphism

$$\mathbb{C}/\Lambda \to E(\Lambda), \begin{cases} z & \mapsto (\wp(z) : \wp'(z) : 1), \; z \neq 0 \\ 0 & \mapsto (0 : 1 : 0) \end{cases}$$

Dimension Formulas

Consider $\omega = f(z)dz$ a differential form on $X(\Gamma)$, then we must have

$$\gamma^*\omega = f(\gamma z) \cdot d\frac{az+b}{cz+d} = \omega$$

this is equivalent to f is a meromorphic modular form of weight 2.

Hence we can identity such a modular form with a section of $\Omega_{X(\Gamma)}$

$$f \text{ weight } 2k \rightsquigarrow \text{section of } \Omega_{X(\Gamma)}^{\otimes n}$$

By Riemann-Roch, we can compute the dimension of $\mathcal{M}_k(\Gamma)$.

$$\dim \mathcal{M}_k(\Gamma) = \begin{cases} 0 & k \leq -1 \\ 1 & k = 0 \\ (2k-1)(g-1) + v_\infty k + \sum_P [k(1 - \frac{1}{e_P})] & k \geq 1 \end{cases}$$

k	=	1	2	3	4	5	6	7	...
$\dim \mathcal{M}_k$	=	0	1	1	1	1	2	1	...

Table: Dimension of $\mathcal{M}_k$ for $\Gamma(1)$

$$\dim \mathcal{M}_k(\Gamma(1)) = 1 - k + [k/2] + [2k/3], \quad k > 1.$$

Proposition 2.1

- $\Delta : \mathcal{M}_{k-6} \to \mathcal{S}_k$ *is isomorphic.*
- $\mathcal{M}(\Gamma(1)) = \bigoplus \mathcal{M}_k = \mathbb{C}[G_2, G_3]$.

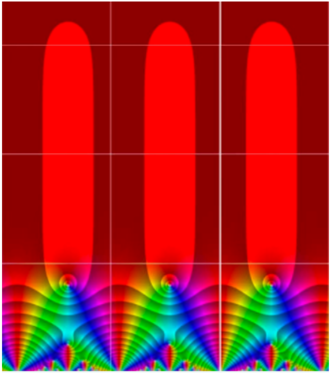
The inverse of Δ is $f \mapsto f/\Delta$. For f and Δ both have zeros at $i\infty \Rightarrow f/\Delta \in \mathcal{M}_{k-6}$.

Expansion of Δ and j

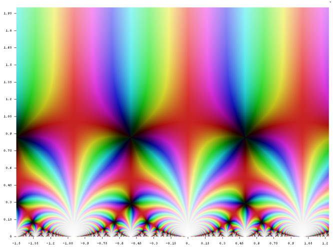
- $\Delta = (2\pi)^{12} q \prod_{n=1}^{\infty}(1-q^n)^{24}$, $q = e^{2\pi iz}$

  Verify $f(-1/z) = z^{12} f(z)$, and $\dim \mathcal{S}_{12} = 1$.
- $q \prod_{n=1}^{\infty}(1-q^n)^{24} = \sum \tau(n) q^n$, τ is called the **Ramanujan** $\tau-$**function**.
- $j = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots$, with all coefficients **integral**.

Remark: The coefficients of j have a closed relation with monster groups. Moonshine...



(a) Weight 4 Eisenstein



(b) Graph of j

Figure: Graph of two functions

Ramanujan's Conjecture

Recall that we have a cusp form of weight 12:

$$f = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

$$\begin{cases} \tau(m)\tau(n) & = \tau(mn) \ \text{ if } \gcd(m,n)=1 \\ \tau(p)\tau(p^n) & = \tau(p^{n+1}) + p^{11}\tau(p^{n-1}), \ p \text{ prime}, \ n \geq 1. \end{cases}$$

Hecke Operators

There are such linear operators

$$T(n) : \mathcal{M}_k(\Gamma(1)) \to \mathcal{M}_k(\Gamma(1))$$

for each $n \geq 1$, with relations

$$\begin{cases} T(m)T(n) & = T(mn) \ \text{ if } \ \gcd(m,n) = 1 \\ T(p)T(p^n) & = T(p^{n+1}) + p^{2k-1}T(p^{n-1}), \ \ p \text{ prime}, \ \ n \geq 1 \end{cases}$$

and preserve $\mathcal{S}_k(\Gamma(1))$.

Suppose $f = \sum c(m)q^m$, then let $T(n)f = \sum \gamma(m)q^m$, we have

$$\gamma(m) = \sum_{a|\gcd(m,n)} a^{2k-1} \cdot c(\frac{mn}{a^2}).$$

In particular, $\gamma(1) = c(n)$.

Proposition 3.1

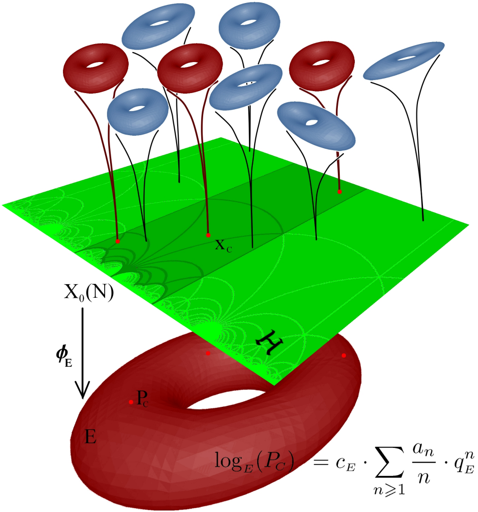
If $f \neq 0$ is an eigenform, i.e. $T(n)f = \lambda(n)f$ for all n, then $c(1) \neq 0$. Moreover, if f is nolmalized, i.e. $c(1) = 1$, then $\lambda(n) = c(n)$.

$\gamma(1) = c(n) = \lambda(n)c(1)$, $c(1) = 0$ implies $f = 0$.

- $\dim \mathcal{S}_{12}(\Gamma(1)) = 1 \Rightarrow f$ is an normalized eigenform.
- $\tau(n)$ satisfies those formulas for $\tau(n) = \lambda(n)$

What's Beyond

- Double coset operators: $\langle n \rangle$, $T(n) : \mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$.
- Peterson inner product: $\mathcal{S}_k(\Gamma_1(N))$ a Hilbert space.
- $\mathcal{S}_k(\Gamma_1(N))$ has orthogonal basis consists of eigenforms of $\{\langle n \rangle, T(n) : \gcd(n, N) = 1\}$.
- $\mathcal{S}_k(\Gamma_1(N))$ can decomposed into 'old forms' and 'new forms'.


X_c
$X_0(N)$
ϕ_E
$\mathcal{H}$
P_c
E
$\log_E(P_C) = c_E \cdot \sum_{n \geqslant 1} \frac{a_n}{n} \cdot q_E^n$