Modular Forms and Hecke Operators

Wei Wenqing

May 2023

Contents

1 Motivations for modular forms

Let $\mathbb{H}$ be the upper half plane, i.e. $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Roughly speaking, modular forms are holomorphic functions on $\mathbb{H}$ satisfying certain conditions under group actions. These conditions may be difficult to understand at fist. In this section, we will give four motivations for the definition of modular forms.

1.1 Motivation from elliptic curves over $\mathbb{C}$

To start with, Let's state the fundamental result for complex elliptic curve:

Theorem 1.1. *Let Λ be a lattice in $\mathbb{C}$, then the quotient $\mathbb{C}/\Lambda$ is an complex elliptic curve. Let*

$$\varphi_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda,\omega\neq 0} \frac{1}{(z-w)^2} - \frac{1}{\omega^2}$$

$\wp_\Lambda(z)$ and $\wp'_\Lambda(z)$ are rational function on $\mathbb{C}/\Lambda$. They satisfy the equation

$$\wp_\Lambda'^{\,2} = 4\wp_\Lambda^3 - 60G_4(\Lambda)\wp_\Lambda - 140G_6(\Lambda) \tag{1.1}$$

where the definition of $G_4(\Lambda)$ and $G_6(\Lambda)$ will be given in this section. The function field of $\mathbb{C}/\Lambda$ is $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$. Furthermore, the map defined by

$$\mathbb{C}/\Lambda \longrightarrow \mathbb{P}^2(\mathbb{C}) \qquad z \longmapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1)$$

gives an isomorphism between $\mathbb{C}/\lambda$ and $E(\mathbb{C})$, where E is an nonsingular projective curve defined by equation $y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$. Above all, there is an equivalence between the following two categories through the map we construct above

$$\boxed{\begin{array}{c}\textit{Lattices in } \mathbb{C}/\textit{homothety}\\ \textit{morphism: complex multiplications}\end{array}} \Longleftrightarrow \boxed{\begin{array}{c}\textit{Elliptic curve over } \mathbb{C}\\ \textit{morphism: Isogenies}\end{array}}$$

Every lattice Λ in $\mathbb{C}$ is homothety to a lattice $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathbb{H}$. Thus, every point in $\mathbb{H}$ can be viewed as a complex elliptic curve. To find out the moduli space for complex elliptic curves, we need to which points in $\mathbb{H}$ give rise to same elliptic curve. For $\tau, \tau' \in \mathbb{H}$, Λ_τ and $\Lambda_{\tau'}$ are homothety if and only if there exists a complex number z, such that $z\Lambda_\tau = \Lambda_{\tau'}$. This is equivalent to exist a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau' = \frac{a\tau+b}{c\tau+d}$. Defines an action of $\mathrm{GL}_2^+(\mathbb{R})$ on $\mathbb{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{a\tau + b}{c\tau + d}$$

Then τ and τ' are homothety if and only if there exists a $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau' = g \cdot \tau$. Therefore, the moduli space of complex elliptic curves is the quotient space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$.

It is nature to consider "functions" on the moduli space of complex elliptic curves. For example, the j-invariant characterizes the elliptic curves up to isomorphism, i.e. two complex elliptic curves are isomorphic if and only if they have equal j-invariant. In this case, j-invariant defines a complex valued function on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. This function can also be viewed as complex valued function on $\mathbb{H}$ which is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$, denoted by $j(\tau)$. Finally we will know that this function is holomorphic and in fact is a weight zero automorphic form. It has Fourier expansion

$$j(\tau) = 1/q + 744 + 196884q + 21493760q^2 + \cdots$$

Denote $G_i(\Lambda_\tau) = G_i(\tau)$ for $i = 4, 6$. By the theory of elliptic curves, two equations $y^2 = 4x^3 + ax + b$ and $y^2 = 4x^3 + a'x + b'$ defines isomorphic elliptic curves over $\mathbb{C}$ if and only if there exists a $u \in \mathbb{C}$ such that $a' = u^4 a$ and $b' = u^6 b$. Therefore, there exists a function $\gamma : \mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H} \to \mathbb{C}$, such that for any $g \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$

$$G_4(g\tau) = \gamma(g, \tau)^4 G_4(\tau) \qquad G_6(g\tau) = \gamma(g, \tau)^6 G_6(\tau)$$

By writing down equations for $G_4(g_1g_2, \tau)$ and $G_6(g_1g_2, \tau)$ for any $g_1, g_2 \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$\gamma(g_1g_2, \tau)^2 = \gamma(g_1, g_2\tau)^2\gamma(g_2, \tau)^2$$

In fact, as we will see below, the relation is simpler:

$$\gamma(g_1g_2,\tau)=\gamma(g_1,g_2\tau)\gamma(g_2,\tau)$$

Moreover, the discriminant of elliptic curve defined by $y^2=4x^3+ax+b$ is $\Delta=-a^3-27b^2$. The discriminant function $\Delta(\tau)=(60G_4(\tau))^3-27(140G_6(\tau))^2$ hence satisfies

$$\Delta(g\tau)=\gamma(g,\tau)^{12}\Delta(\tau)$$

Now, it is time to uncover the what G_4 and G_6 truly is. For each $k\in\mathbb{Z}$, and lattice Λ, define function G_k by

$$G_k(\Lambda)=\sum_{\omega\in\Lambda\setminus\{0\}}\frac{1}{\omega^k}$$

In particular, we denote

$$G_k(\tau)=\sum_{\omega\in\Lambda_\tau\setminus\{0\}}\frac{1}{\omega^k}=\sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}}\frac{1}{(m\tau+n)^k}$$

$G_k(\Lambda)$ is uniformly convergent for $k\geq 4$. The Taylor expansions of $\wp_\Lambda(z)$ and $\wp'_\Lambda(z)$ at $z=0$, is given by

$$\wp_\Lambda(z)=\frac{1}{z^2}+\sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\Lambda)z^{2n}$$
$$\wp'_\Lambda(z)=-\frac{1}{z^3}+\sum_{n=1}^{\infty}2n(2n+1)G_{2n+2}(\Lambda)z^{2n-1}$$

by comparing the coefficients in equation 1.1, we can verify that $G_4(\tau),G_6(\tau)$ defined above are exactly $G_4(\Lambda_\tau)$ and $G_6(\Lambda_\tau)$. Moreover, we can prove that for any $g=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in$ $\mathrm{SL}_2(\mathbb{Z})$ and $\tau\in\mathbb{H}$,

$$G_k(g\tau)=(c\tau+d)^kG_k(\tau)$$

Therefore, the function $\gamma(g,\tau)$ we define above can be taken as $c\tau+d$, if $g=\begin{pmatrix}a&b\\c&d\end{pmatrix}$.

Definition A function $f:\mathbb{H}\longrightarrow\mathbb{C}$ is call a weakly modular function of weight k with respect to $\mathrm{SL}_2(\mathbb{Z})$ if for any $g=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$,

$$f\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^kf(\tau)$$

To rigorously define modular forms, additional conditions on cusps ought to be stated. We will give the formal definition in the next chapter.

1.2 Motivation from homogeneous functions on lattices

As we can see in last section, modular forms should not be viewed as functions on the moduli space of elliptic curves. Instead, they should be viewed as homogeneous functions on lattices.

Let $\mathcal{L}$ be the $\mathbb{Q}$-vector space generated by the set of all lattices in $\mathbb{C}$ i.e.

$$\mathcal{L} = \{a_1\Lambda_1 + \cdots a_k\Lambda_k \big| a_i \in \mathbb{Q}, \Lambda_i \text{ is a lattice}, i = 1, ..., k\}$$

A linear function $F : \mathcal{L} \longrightarrow \mathbb{C}$ is called homogeneous with degree k if for any $z \in \mathbb{C}$,

$$F(z\Lambda) = z^{-k}F(\Lambda)$$

We can dehomogenize F to a function f on $\mathbb{H}$ by

$$f(\tau) = F(\Lambda_\tau)$$

Lemma 1.2. *The function $f : \mathbb{H} \longrightarrow \mathbb{C}$ defined above is a weakly modular function of weight k with respect to $SL_2(\mathbb{Z})$.*

Proof. For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$,

$$f(g\tau) = F(\Lambda_{g\tau}) = F\left(\mathbb{Z} + \mathbb{Z}\frac{a\tau + b}{c\tau + d}\right) = F((c\tau + d)^{-1}(\mathbb{Z} + \mathbb{Z}\tau)) = (c\tau + d)^k f(\tau)$$

□

Conversely, if f is a weakly modular function of weight k, then we can define a homogeneous function $F : \mathcal{L} \longrightarrow \mathbb{C}$ by

$$F(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = \omega_1^{-k} f\left(\frac{\omega_2}{\omega_1}\right) \qquad \mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right) > 0$$

Lemma 1.3. *The function $F : \mathcal{L} \longrightarrow \mathbb{C}$ defined above is a homogeneous function of weight k.*

Proof. Firstly, we should prove that the function F is well-defined. Suppose a lattice Λ has two basis ω_1, ω_2 and ω_1', ω_2'. Then their exists a $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, such that $\begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_2' \\ \omega_1' \end{pmatrix}$. Then

$$\begin{aligned} F(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = \omega_1^{-k} f\left(\frac{\omega_2}{\omega_1}\right) &= (c\omega_2' + \omega_1')^{-k} f\left(\frac{a\omega_2 + b\omega_1}{c\omega_2 + d\omega_1}\right) \\ &= (c\omega_2' + \omega_1')^{-k}\left(c\frac{\omega_2'}{\omega_1'} + d\right)^k f\left(\frac{\omega_2'}{\omega_1'}\right) \\ &= {\omega_1'}^{-k} f\left(\frac{\omega_2'}{\omega_1'}\right) = F(\mathbb{Z}\omega_1' + \mathbb{Z}\omega_2') \end{aligned}$$

Now for any $z \in \mathbb{C}$,

$$F(z(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)) = (z\omega_1)^{-k} f\left(\frac{\omega_2}{\omega_1}\right) = z^{-k}F(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$$

Therefore, F is a homogeneous function of degree k. □

In conclusion, there is a one to one correspondence between weakly modular functions of weight k with respect to $\mathrm{SL}_2(\mathbb{Z})$ and homogeneous functions on lattices of degree k.

Note that a homogeneous function only depends on its value at each lattices. It is certainly fine to merely define homogeneous functions on the set of lattices, instead of the vector space they span. However, we need the vector space structure when defining Hecke operators. That's why we define a vector space here.

1.3 Motivation from analytic continuation of L-function

Now we have a rough understanding about modular forms. It is a kind of functions satisfy certain "automorphic" property (some kinds of invariant under group actions). Actually, "automorphic" property is not a stranger to us. It has secretly show up in number theory. Specifically, in the proof of analytic continuation of Riemann zeta function. Recall that in the proof, we pay a special attention to the Jacobin theta function

$$\theta(z) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 z} \qquad \mathrm{Re}(z) > 0$$

It can be written as $\theta(z) = \widehat{\theta}(iz)$, where

$$\widehat{\theta}(\omega) = 1 + \sum_{n=1}^{\infty} q^{\frac{n^2}{2}} \qquad q = e^{2\pi i\omega} \text{ and } \omega \in \mathbb{H}$$

By Poisson summation formula, we have equation

$$\theta(z) = \frac{1}{\sqrt{z}}\theta\left(\frac{1}{z}\right) \qquad \text{and} \qquad \widehat{\theta}(\omega) = \frac{1}{\sqrt{-i\omega}}\widehat{\theta}\left(-\frac{1}{\omega}\right)$$

This relation between the value of $\widehat{\theta}(\omega)$ and $\widehat{\theta}(-\frac{1}{\omega})$ is exactly a prototype of automorphic property. The Jacobin theta function is sometimes called modular form of weight $\frac{1}{2}$.

Here is more comments about the technique used in the analytic continuation of Riemann zeta function. Let's recall the technique. First, we find that $\theta(x) \to 1$ as $x \to 0$ and $\theta(x) \to \frac{1}{\sqrt{x}}$ as $x \to \infty$ (here we consider θ takes values on $\mathbb{R}$). Next, we construct a function:

$$\phi(s) = \int_0^1 (\theta(x) - \frac{1}{\sqrt{x}})x^{s-1}dx + \int_1^{+\infty} (\theta(x) - 1)x^{s-1}dx$$

This function can be viewed as the variation of mellin transform on theta function. The automorphic property implies that $\phi(s) = \phi(1-s)$ and by computing this integral term by term we can derive the functional equation for Riemann zeta function.

Actually, the above method to get analytic continuation and functional equation is under a general procedure, demonstrated by the diagram below

$$\begin{tikzcd}
\boxed{\text{Modular form}} \arrow[r] \arrow[rr, bend right, "\text{Mellin transform}"'] & \boxed{\text{Fourier series}} \arrow[r] & \boxed{\text{L-function}}
\end{tikzcd}$$

For example, Let f be a cuspital modular form of weight k with respect to $\mathrm{SL}_2(\mathbb{Z})$ and Let the L series associated to f be

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

consider the mellin transform of the function $f(ix)$:

$$\begin{aligned}
\widehat{L}(s,f) &= \int_0^\infty f(ix)x^{s-1}dx \\
&= \sum_{n=1}^\infty \int_0^\infty a_n e^{-2\pi i x} x^{s-1} dx \\
&= \sum_{n=1}^\infty \frac{a_n}{(2\pi n)^s} \int_0^\infty e^{-x} x^{s-1} dx \\
&= \frac{\Gamma(s)}{(2\pi)^s} L(s,f)
\end{aligned}$$

Consider $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ acting on f, we have $f(\frac{i}{x}) = (ix)^k f(ix)$. Therefore,

$$\begin{aligned}
\int_0^\infty f(ix)x^{s-1}dx &= \int_0^\infty (ix)^{-k} f(\frac{i}{x}) x^{s-1} dx \\
&= i^{-k} \cdot \int_0^\infty f(ix) x^{k-s-1} dx \\
&= i^{-k} \widehat{L}(k-s,f)
\end{aligned}$$

Therefore, we have functional equation

$$\widehat{L}(s,f) = (-1)^{\frac{k}{2}} \widehat{L}(k-s,f)$$

This method also work for $S_k(\Gamma_0(N))$.

1.4 Motivation from the four square problem

It is known that every positive integer can be written as the sum of four square. The question is for a given integer n, find the number of ways to express n as the sum of four square. More generally, we wish to compute the number

$$r(n,k) = \#\{(n_1, ..., n_k) \in \mathbb{Z} : n = n_1^2 + ... + n_k^2\}$$

Note that if $i + j = k$, then $r(n,k) = \sum_{l=0}^n r(l,i) r(n-l,j)$. Let

$$\theta(z,k) = \sum_{n=0}^\infty r(n,k) q^n q = e^{2\pi i z}$$

then $\theta(z,k) = \theta(z,i)\theta(z,j)$. In particular,

$$\theta(z,1) = 1 + \sum_{n=1}^\infty 2q^{n^2} = \widehat{\theta}(2z) \qquad z \in \mathbb{H}$$

where $\widehat{\theta}(\omega)$ is the theta function we defined in last section. Therefore, $\theta(z,1)$ satisfies

$$\theta(z,1) = \frac{1}{\sqrt{-2iz}} \theta\left(-\frac{1}{4z}, 1\right)$$

Now, since $\theta(z,4) = \theta(z,1)^4$, we have

$$\theta(z,4) = -\frac{1}{4z^2}\theta\left(-\frac{1}{4z},4\right)$$

Together we the property $\theta(z+1,4) = \theta(z,4)$, we can derive

$$\theta\left(\frac{z}{4z+1},4\right) = (4z+1)^2\theta\left(z,4\right) \qquad z \in \mathbb{H}$$

the above equations mean that

$$\theta(gz,4) = \gamma(g,z)^2\theta(z,4) \tag{1.2}$$

for $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$, where $\gamma(g,z)$ is defined in section 1.1. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be the subgroup generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$. Then the equation 1.2 holds for all $g \in \Gamma$. We say $\theta(z,4)$ is a modular form of weight 2 with respect to the group Γ. It is easy to prove that Γ is equal to $\Gamma_1(4)$, which we define in the next chapter. This example motivates us to study modular forms with respect to not only $\mathrm{SL}_2(\mathbb{Z})$, but also its (congruence) subgroups.

More generally, we are interested in counting the integer solution for a arbitrary quadratic form

$$f(x_1,...,x_k) = \sum_{1\leq i,j\leq k} a_ijx_ix_j \qquad (a_ij \in \mathbb{Z})$$

Consider the generating series

$$\theta_f(z) = \sum_{x_1,...,x_k\in\mathbb{Z}} q^{f(x_1,...,x_k)} = \sum_{n=0}^{\infty} N_f(n)q^n \qquad q = e^{2\pi iz}$$

For many quadratic form, θ_f is a modular form of weight $\frac{k}{2}$ with respect to some group G. If we know a basis of the space $M_{\frac{k}{2}}(G)$, i.e. we know all coefficients of a basis:

$$f_i(z) = \sum_{n=0}^{\infty} c_{i,n}q^n \qquad i = 1,...,m$$

where $m = \dim(M_{\frac{k}{2}}(G))$. Then we can express $\theta_f = \alpha_1 f_1 + \cdots + \alpha_m f_m$, $\alpha_i \in \mathbb{C}$. Thus, for $n \in \mathbb{Z}_{\geq 0}$

$$N_f(n) = \alpha_1 c_{1,n} + \cdots \alpha_m c_{m,n}$$

to obtain coefficients $\alpha_1,...,\alpha_m$. we only need to compute $N_f(n)$ for small n and solve a linear equation. Then we can obtain a formula of $N_f(n)$ for arbitrary n.

1.5 Motivation from Ramanujan's study

The third motivation for modular form arises from Ramanujan's remarkable study on the Fourier expansion of series

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n \qquad q = e^{2\pi iz}$$

It seems confusing to pay special attention to this series. However, Δ and $\tau(n)$ indeed possess several incredible relations. Here is a list:

1.
$$\Delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12}\Delta(z) \text{ for any } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

2. The coefficients satisfy
   (a) $a_{mn} = a_m a_n$ for any $gcd(m,n) = 1$,
   (b) $a_{p^n} = a_p a_{p^{n-1}} - p^{11} a_{p^{n-2}}$ for any prime p and $n \geq 2$
   (c) $a_1 = 1$.

3. Let $L(s,\Delta) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$, then
   (a)
   $$L(s,\Delta) = \prod_p (1 - \tau(p)p^{-s} + p^{11-2s})^{-1}$$
   (b) $L(s,\Delta)$ can be analytic continuated to the whole complex plane.
   (c) Let $\widehat{L}(s,\Delta) = (2\pi)^{-s}\Gamma(s)L(s,\Delta)$, then
   $$\widehat{L}(s,\Delta) = \widehat{L}(12-s,\Delta)$$

The first property means $\Delta(z)$ is a modular form of weight 12 with respect to $\mathrm{SL}_2(\mathbb{Z})$. To prove the second property, mathematicians introduce a set of operators, called Hecke operators, on spaces of modular forms. $\Delta(z)$'s coefficients satisfying these property is exactly because it is a Hecke eigenform, i.e. the eigenvector for all Hecke operators. Personally, I believe it is this equation that motivate the origin definition of Hecke operator to satisfy

$$T_{p^{n+1}} = T_p T_{p^n} - p^{n-1}{<}p{>}T_{p^{n-1}} \qquad \text{for any prime } p \text{ and } n \geq 0$$

To prove the third property, we only need to take the procedure we have introduced in section 1.3.

2 Modular forms

2.1 Modular curves

Let $\mathbb{H}$ be the upper half plane and $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. The action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ can extend to $\mathbb{H}^*$. Note that for every $q \in \mathbb{Q}$, there exists a $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $g \cdot q = \infty$.

$\mathbb{H}^*$ is a subset of $\mathbb{CP}^1$. However, we should equip $\mathbb{H}^*$ with a topology different from the subspace topology from $\mathbb{CP}^1$. This is because in the following discussion, we will study the quotient space $\Gamma\backslash\mathbb{H}^*$ for some subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with finite index. Thus, it would be convenient for $\mathbb{H}^*$ to equip with a topology such that for any $z \in \mathbb{H}^*$ and $g \in \mathrm{SL}_2(\mathbb{Z})$, z and $g \cdot z$ have same neighborhood. Naturally, we choose

$$\mathcal{A}_\infty = \{B_r = \{z \in \mathbb{H} : \ \mathrm{Im}(z) > r\} \cup \{\infty\} | r > 0\}$$

to be the basis of neighborhood of ∞. Then for any $q \in \mathbb{Q}$, there exists $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $g \cdot q = \infty$. Thus, the neighborhood of q should has a basis:

$$\mathcal{A}_q = \{g^{-1}(B_r) | B_r \in \mathcal{A}_\infty\}$$

These sets are exactly all disks lying in $\mathbb{H}^*$ which are tangent to $\mathbb{R}$ at q.

Therefore, the topology on $\mathbb{H}^*$ is generated by the usual topology on $\mathbb{H}$ and $\mathcal{A}_q$ for all $q \in \mathbb{Q} \cup \{\infty\}$.

Definition Let

- $\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$
- $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$
- $\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}$

A subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup if there exists a integer N such that $\Gamma(N) \subset \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$. N is called the level of Γ.

Let Γ be congruence group. Let $Y(\Gamma) = \Gamma\backslash\mathbb{H}$ and $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$, both equipped with quotient topology.

Theorem 2.1. *$Y(\Gamma)$ is a Riemann surface and $X(\Gamma)$ is a compact Riemann surface.*

2.2 Modular forms

We finally arrive at the formal definition of modular forms.

Definition a modular form of weight $k \in \mathbb{Z}$ with respect to a congruence subgroup Γ is a function $f : \mathbb{H}^* \longrightarrow \mathbb{C}$ such that

1. f is holomorphic on $\mathbb{H}^*$,
2. for any $g \in \Gamma$ and $z \in \mathbb{H}^*$,

$$f(g \cdot z) = \gamma(g, z)^k f(z)$$

   where $\gamma(g, z) = cz + d$ if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Definition A cusp form is a modular form that vanishes at all cusp points($\mathbb{Q} \cup \{\infty\}$).

In the definition, the holomorphic condition at cusp points seem to be vague. Let's explain it.

Definition A function $f : \mathbb{H} \longrightarrow \mathbb{C}$ is said to be holomorphic at ∞ if $f(z) \to C$ for a constant C when $\mathrm{Im}(z) \to \infty$.

Now suppose f is a modular form of weight k with respect to a congruence subgroup Γ. There exists a integer N such that $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$. Thus, $f(z + N) = f(z)$, f defines a holomorphic function $\widehat{f}$ on the puncture disk $\mathbb{D}$ satisfying $f(z) = \widehat{f}(e^{\frac{2\pi i}{N} z})$. The Taylor expansion of $\widehat{f}(q)$ at the origin gives us:

$$f(z) = \sum_{n \geq k} a_n q^n \qquad q = e^{\frac{2\pi i}{N} z}$$

Then f is holomorphic at ∞ if and only if $k = 0$, i.e. $\widehat{f}$ can be analytically continuated to the origin.

Define an action of $\mathrm{GL}_2^+(\mathbb{R})$ on a modular form f of weight k by

$$f \cdot [g]_k(z) = \det(g)^{k-1}\gamma(g,z)^{-k}f(gz) \qquad \text{for any } g \in \mathrm{GL}_2^+(\mathbb{R})$$

The necessity of coefficient $\det(g)^{k-1}$ would be clear in the next chapter. It is easy to verify that this is a right action. f is a weakly modular function of weight k with respect to Γ if and only if for any $g \in \Gamma$, $f \cdot [g]_k = f$.

Definition For $p \in \mathbb{Q}$, f is said to be holomorphic at cusp p if for any $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $g(\infty) = p$, $f \cdot [g]_k$ is holomorphic at ∞.

Example 2.1. *The Eisenstein series*

$$G_k(\tau) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(m\tau+n)^k}$$

is a modular form of weight k with respect to $SL_2(\mathbb{Z})$. The Fourier expansion of $G_k(\tau)$ is given by

2.3 Modular curves as moduli spaces

In this section, N is a fixed positive integer and Γ always refers to $\Gamma(N)$, $\Gamma_1(N)$, and $\Gamma_0(N)$. In the first chapter, we show that $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ can be viewed as the moduli space of all isomorphic elliptic curves over $\mathbb{C}$. In this section, we will demonstrate that $\Gamma\backslash\mathbb{H}$ are also moduli spaces of certain datum.

Consider following moduli spaces:

1. An enhanced elliptic curve with respect to $\Gamma_0(N)$ is a pair (E, C), where E is an elliptic curve and $C \subset E$ is a cyclic group of order N. We say (E, C) and (E', C') are equivalent if and only if there exists an isomorphism $\varphi : E \to E'$ such that $\varphi(C) = C'$. The moduli space is defined by

$$S_0(N) = \{\text{Enhanced elliptic curves with respect to } \Gamma_0(N)\}/\sim$$

2. An enhanced elliptic curve with respect to $\Gamma_1(N)$ is a pair (E, P), where E is an elliptic curve and $P \in E$ is a point of order N. We say (E, P) and (E', P') are equivalent if and only if there exists an isomorphism $\varphi : E \to E'$ such that $\varphi(P) = P'$. The moduli space is defined by

$$S_0(N) = \{\text{Enhanced elliptic curves with respect to } \Gamma_1(N)\}/\sim$$

3. An enhanced elliptic curve with respect to $\Gamma_1(N)$ is a pair (E, P, Q), where E is an elliptic curve and $P, Q \in E$ are points of order N such that $e(P, Q) = \mu_N$. We say (E, P, Q) and (E', P', Q') are equivalent if and only if there exists an isomorphism $\varphi : E \to E'$ such that $\varphi(P) = P'$ and $\varphi(Q) = Q'$. The moduli space is defined by

$$S(N) = \{\text{Enhanced elliptic curves with respect to } \Gamma(N)\}/\sim$$

Proposition 2.2. *There are bijections:*

1.

$$\Gamma_0(N)\backslash\mathbb{H} \longrightarrow S_0(N) \qquad \Gamma_0(N)\tau \longmapsto \left(E_\tau, \langle\frac{1}{N}\rangle\right)$$

2.

$$\Gamma_1(N)\backslash\mathbb{H} \longrightarrow S_1(N) \qquad \Gamma_1(N)\tau \longmapsto \left(E_\tau, \frac{1}{N}\right)$$

3.

$$\Gamma(N)\backslash\mathbb{H} \longrightarrow S(N) \qquad \Gamma(N)\tau \longmapsto \left(E_\tau, \frac{\tau}{N}, \frac{1}{N}\right)$$

where E_τ, $\tau \in \mathbb{H}$, is the elliptic curve corresponding to lattice $\mathbb{Z} + \mathbb{Z}\tau$.

Proof. We present a proof for the last statement as other two can be proved in the same way. Apparently, every pair can be equivalent to a pair $(E_\tau, \frac{m_1\tau+k_1}{N}, \frac{m_2\tau+k_2}{N})$ and $\det\begin{pmatrix} m_1 & k_1 \\ m_2 & k_2 \end{pmatrix} \equiv 1 \mod N$. Then there exists a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} m_1 & k_1 \\ m_2 & k_2 \end{pmatrix} \equiv I_2 \mod N$. Let $\tau' \in \mathbb{H}$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau' = \tau$, then their exists an isomorphism $E_\tau \longrightarrow E_{\tau'}$. From the lattices' viewpoint, this map sends τ to $a\tau' + b$ and sends 1 to $c\tau' + d$. Thus, for any integer $m.k$

$$\frac{m\tau + k}{N} \longmapsto \frac{m(a\tau' + b) + k(c\tau' + d)}{N} = \frac{(ma + kc)\tau' + (mb + kd)}{N}$$

then $(E'_\tau, \frac{m_1\tau+k_1}{N}, \frac{m_2\tau+k_2}{N})$ is equivalent to $(E_\tau, \frac{\tau}{N}, \frac{1}{N})$, the map $\mathbb{H} \longrightarrow S(N)$ is surjective.

Suppose $(E_\tau, \frac{\tau}{N}, \frac{1}{N})$ and $(E'_\tau, \frac{\tau'}{N}, \frac{1}{N})$ are equivalent, then there exists $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau'$. then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N$. Thus, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N$. The converse also holds. Therefore, $\Gamma(N)\backslash\mathbb{H} \longrightarrow S(N)$ is a bijection. $\square$

Recall that in the first chapter, we construct a one to one correspondence between weakly modular functions with respect to $\mathrm{SL}_2(\mathbb{Z})$ and homogeneous functions on lattices. We can also establish such kind of correspondence for weakly modular functions with respect to Γ.

Let $\mathcal{L}_0^N$ be the $\mathbb{Q}$-vector space generated by the set of all pairs (Λ, C), where Λ is a lattices in $\mathbb{C}$ and C is a cyclic group of order N in Λ.

Let $\mathcal{L}_1^N$ be the $\mathbb{Q}$-vector space generated by the set of all pairs (Λ, P), where Λ is a lattices in $\mathbb{C}$ and P is a N torsion point in Λ.

Let $\mathcal{L}^N$ be the $\mathbb{Q}$-vector space generated by the set of all pairs (Λ, P, Q), where Λ is a lattices in $\mathbb{C}$ and P, Q are N torsion points in Λ with $e(P, Q) = \mu_N$

Definition Let $F : \mathcal{L}_*^N \longmapsto \mathbb{C}$ be a complex valued function . We say F is homogeneous with degree k if for any complex number z

1. $F(z\Lambda, zC) = z^{-k}F(\Lambda, C) \qquad$ for $\mathcal{L}_*^N = \mathcal{L}_0^N$
2. $F(z\Lambda, zP) = z^{-k}F(\Lambda, P) \qquad$ for $\mathcal{L}_*^N = \mathcal{L}_1^N$
3. $F(z\Lambda, zP, zQ) = z^{-k}F(\Lambda, P, Q) \qquad$ for $\mathcal{L}_*^N = \mathcal{L}^N$

Define $f : \mathbb{H} \longrightarrow \mathbb{C}$ by

$$f(\tau) = \begin{cases} F(\Lambda_\tau, \langle\frac{1}{N}\rangle) & \mathcal{L}_*^N = \mathcal{L}_0^N \\ F(\Lambda_\tau, \frac{1}{N}) & \mathcal{L}_*^N = \mathcal{L}_1^N \\ F(\Lambda_\tau, \frac{\tau}{N}, \frac{1}{N}) & \mathcal{L}_*^N = \mathcal{L}^N \end{cases}$$

It is easy to verify that f is a modular function of weight k with respect to Γ.

The reason for introducing these correspondences is because it is more easier to define homogeneous functions on $\mathcal{L}_*^N$ and in this way can we obtain massive modular functions. Recall that the Weierstrass $\wp$ function does not play any role in the construction of homogeneous functions over lattices. That's because in order to get a value, one should input both a lattice and a point to the Weierstrass $\wp$ function. In this case, this method becomes feasible. For example, we can construct following homogeneous functions of weight 2:

$$\begin{array}{lll} \Gamma(N): & F_2^{(m,n)}(\Lambda, P, Q) = \wp_\Lambda(mP + nQ) & (m,n) \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \Gamma_1(N): & F_2^d(\Lambda, P) = \wp_\Lambda(dP) & d \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\} \\ \Gamma_0(N): & F_2(\Lambda, C) = \sum_{P \in C \setminus \{0\}} \wp_\Lambda(P) & \end{array}$$

They correspond to weight 2 modular functions:

$$\begin{aligned} f_2^{(m,n)}(\tau) &= \wp_\tau\left(\frac{m\tau + n}{N}\right) \\ f_2^d(\tau) &= f_0^{(0,d)}(\tau) = \wp_\tau\left(\frac{d}{N}\right) \\ f_2(\tau) &= \sum_{d=1}^{N-1} f_0^d(\tau) = \sum_{d=1}^{N-1} \wp_\tau\left(\frac{d}{N}\right) \end{aligned}$$

Thereby, we can construct weight 0 modular functions with respect to Γ:

$$\begin{aligned} f_0^{(m,n)}(\tau) &= \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau\left(\frac{m\tau + n}{N}\right) \\ f_0^d(\tau) &= \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau\left(\frac{d}{N}\right) \\ f_0(\tau) &= \frac{g_2(\tau)}{g_3(\tau)} \sum_{d=1}^{N-1} \wp_\tau\left(\frac{d}{N}\right) \end{aligned}$$

Lemma 2.3. *Let $g \in SL_2(\mathbb{Z})$, then $f^{(m,n)} \circ g = f^{(m,n)g}$.*

Proposition 2.4. *Weight 0 modular functions defined above are meromorphic functions on their corresponding modular curves.*

Proof. We only need to prove that $f^{(m,n)}$ is a meromorphic function on $\mathbb{H}^*$ for all $(m,n) \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{0\}$. It's easy to see that $f^{(m,n)}$ is meromorphic on $\mathbb{H}$. So, we only need to verify that $f^{(m,n)}$ is meromorphic at all cusps. By lemma, it suffices to prove that $f^{(m,n)}$ is meromorphic at ∞. Without loss of generality, assume $0 \le m \le N-1$

$$\begin{aligned}\wp_\tau\left(\frac{m\tau+n}{N}\right) &= \frac{1}{\left(\frac{m\tau+n}{N}\right)^2} + \sum_{(k,l)\neq(0,0)} \frac{1}{\left(\frac{m\tau+n}{N}-k\tau-l\right)^2} - \frac{1}{(k\tau+l)^2} \\ &= \sum_{k\ge 1}\sum_{l} \frac{1}{\left(\left(k-\frac{m}{N}\right)\tau - \frac{n}{N}+l\right)^2} - \frac{1}{(k\tau+l)^2} \\ &+ \sum_{k\le -1}\sum_{l} \frac{1}{\left(\left(\frac{m}{N}-k\right)\tau + \frac{n}{N}-l\right)^2} - \frac{1}{(k\tau+l)^2} + \sum_{l} \frac{1}{\left(\frac{m\tau+n}{N}-l\right)^2} - \frac{1}{l^2}\end{aligned}$$

For $z \in \mathbb{H}$, we have formula:

$$\sum_{d\in\mathbb{Z}} \frac{1}{(\tau+d)^2} = C_2 \sum_{d=1}^{\infty} dq^d$$

where $C_2 = -4\pi^2$ and $q = e^{2\pi i z}$. Thus,

$$\sum_{k\ge 1}\sum_{l} \frac{1}{\left(\left(k-\frac{m}{N}\right)\tau - \frac{n}{N}+l\right)^2} - \frac{1}{(k\tau+l)^2} = C_2 \sum_{k\ge 1}\sum_{d=1}^{\infty} d\left(e^{2\pi i d\left(\left(k-\frac{m}{N}\right)\tau - \frac{n}{N}\right)} - e^{2\pi i d k\tau}\right)$$

when $\mathrm{Im}(\tau)\to\infty$, this term vanishes. By similar argument, one can show that the second term vanishes as $\mathrm{Im}(\tau)\to\infty$. If $m=0$, then

$$\sum_{l} \frac{1}{\left(\frac{m\tau+n}{N}-l\right)^2} - \frac{1}{l^2} = -\xi(2) + N^2 \sum_{d\equiv n \mod N} \frac{1}{d^2}$$

If $m \neq 0$, then

$$\sum_{l} \frac{1}{\left(\frac{m\tau+n}{N}-l\right)^2} - \frac{1}{l^2} = -2\xi(2) + \sum_{d=1}^{\infty} de^{2\pi i d\frac{m\tau+n}{N}}$$

when $\mathrm{Im}(\tau)\to\infty$, this term converge to $-\xi(2)$. In summary,

$$\wp_\tau\left(\frac{m\tau+n}{N}\right) \to \begin{cases} -\xi(2) & m \not\equiv 0 \mod N \\ -\xi(2) + \sum_{d\equiv n \mod N} \frac{1}{d^2} & m\equiv 0 \mod N \end{cases}$$

Thus $\wp_\tau\left(\frac{m\tau+n}{N}\right)$ and $f_0^{(m,n)}$ is holomorphic at cusp ∞.

□

Therefore, we conclude that

$$f_0^{(m,n)} \in \mathbb{C}(X(N)) \qquad f_0^d \in \mathbb{C}(X_1(N)) \qquad f_0 \in \mathbb{C}(X_0(N))$$

for any $(m,n) \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{0\}$ and $d \in \mathbb{Z}/N\mathbb{Z}\setminus\{0\}$. We will show in the next section that these functions in fact generated whole function fields.

2.4 Modular curves as algebraic curves

The modular curve associated to $\mathrm{SL}_2(\mathbb{Z})$ is has genus 0 and its function field is generated by the j-invariant, i.e.

$$\mathbb{C}(X(1)) = \mathbb{C}(j)$$

In last section, we have prove that:

$$f_0^{(m,n)} \in \mathbb{C}(X(N)) \qquad f_0^d \in \mathbb{C}(X_1(N)) \qquad f_0 \in \mathbb{C}(X_0(N))$$

The theorem below tells us that these functions generate whole function fields.

Theorem 2.5.

$$\begin{aligned}
\mathbb{C}(X(N)) =& \mathbb{C}\left(j, f_0^{(m,n)} \middle| (m,n) \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{0\}\right) \\
=& \mathbb{C}(j, f_0^{(0,1)}, f_0^{(1,0)}) \\
\mathbb{C}(X_1(N)) =& \mathbb{C}\left(j, f_0^d \middle| d \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\}\right) \\
=& \mathbb{C}(j, f_0^1) \\
\mathbb{C}(X_0(N)) =& \mathbb{C}(j, f_0) = \mathbb{C}(j, j_N) \ \textit{where } j_N(\tau) = j(N\tau)
\end{aligned}$$

Proof. Since $\wp_\tau(z) = \wp_\tau(z')$ if and only if $z \equiv z' \mod \Lambda_\tau$, we conclude that $f_0^{(m,n)}$ and $f_0^{(m',n')}$ are equal if and only if $(m,n) \equiv \pm(m',n')$. Since $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$, we have morphisms of curves:

$$X(N) \to X_1(N) \to X_0(N) \to X(1)$$

which is induced by

$$\Gamma(N)\backslash\mathbb{H} \to \Gamma_1(N)\backslash\mathbb{H} \to \Gamma_0(N)\backslash\mathbb{H} \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$$

Since $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$, $g \in \mathrm{SL}_2(\mathbb{Z})$ can act on $X(N) = \Gamma(N)\backslash\mathbb{H}^*$ by

$$\Gamma(N)\backslash\mathbb{H}^* \longrightarrow \Gamma(N)\backslash\mathbb{H}^* \qquad \Gamma(N)\tau \longmapsto \Gamma(N)g\tau$$

This action induces an action on the fucntion field $\mathbb{C}(X(N))$:

$$\mathbb{C}(X(N)) \longrightarrow \mathbb{C}(X(N)) \qquad f \longmapsto f \circ g$$

It defines a map

$$\Phi : \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{Aut}(\mathbb{C}(X(N)))$$

Apparently, $\{\pm I_2\}\Gamma(N)$ lies in the kernel of Φ. On the other hand, if $g \in \ker\Phi$, then for any $(m,n) \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{0\}$,

$$g \cdot f_0^{(m,n)} = f_0^{(m,n)g} = f_0^{(m,n)}$$

This implies $g \in \{\pm I_2\}\Gamma(N)$. Thus, the kernel of Φ is exactly $\{\pm I_2\}\Gamma(N)$. Denote the image of Φ as H, then

$$H \cong \mathrm{SL}_2(\mathbb{Z})/\{\pm I_2\}\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$$

The fixed field of H is exactly the function field of $X(1)$, which is $\mathbb{C}(j)$. Hence, $\mathbb{C}(X(N))$ is Galois over $\mathbb{C}(j)$. It is easy to see that the only subgroup of H that fix $f_0^{(1,0)}$ and $f_0^{(0,1)}$ is the trivial subgroup, thus they generate $\mathbb{C}(X(N))$ over $\mathbb{C}(j)$.

The subgroup of $\mathrm{SL}_2(\mathbb{Z})$ which fixes $\mathbb{C}(j, f_0^1)$ is $\{\pm I_2\}\Gamma_1(N)$. Thus,

$$[\mathbb{C}(X(N)) : \mathbb{C}(j, f^1)] = [\mathrm{SL}_2(\mathbb{Z}) : \{\pm I_2\}\Gamma_1(N)] = [\mathbb{C}(X(N)) : \mathbb{C}(X_1(N)]$$

Therefore, $\mathbb{C}(X_1(N)) = \mathbb{C}(j, f_0^1)$.

If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, then $g' = \begin{pmatrix} a & Nb \\ \frac{c}{N} & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Thus

$$j(Ng\tau) = j\left(\frac{aN\tau + Nb}{\frac{c}{N}N\tau + d}\right) = j(g'(N\tau)) = j(N\tau)$$

Note that $j(\tau) = j(\tau')$ if and only if there exists $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau = g\tau'$. If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ satisfies $j(Ng\tau) = j(N\tau)$ for any $\tau\mathbb{H}$, then there exists a $g' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ such that $g'(Ng\tau) = N\tau$. We would obtain $g \in \{\pm I_2\}\Gamma_0(N)$. Thus, $j_N \circ g = j_N$ if and only if $g \in \{\pm I_2\}\Gamma_0(N)$. Therefore, $\mathbb{C}(X_0(N)) = \mathbb{C}(j, j_N)$ □

Since we have learned that j and $f^{(m,n)}$ should be algebraically dependent over $\mathbb{C}$, we'd like to study the algebraic relation between them. Since we have the lattices-elliptic curves correspondence,

$$\mathbb{C}/\Lambda \longrightarrow \mathbb{P}^2(\mathbb{C}) \qquad z \longmapsto (\varphi_\Lambda(z) : \varphi'_\Lambda(z) : 1)$$

the function $f_0^{(m,n)}(\tau) = \frac{g_2(\tau)}{g_3(\tau)}\wp_\tau(\frac{m\tau+n}{N})$ can be viewed as the x-coordinate of a N torsion point on an elliptic curve, multiplying by a scalar. We wish $f_0^{(m,n)}$ is exactly the x-coordinate of this N torsion point. Thus, we need to modify our lattices-elliptic curves correspondence to

$$\mathbb{C}/\Lambda \longrightarrow \mathbb{P}^2(\mathbb{C}) \qquad z \longmapsto \left(\frac{g_2(\tau)}{g_3(\tau)}\wp_\Lambda(z) : \left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{\frac{3}{2}} \wp'_\Lambda(z) : 1\right)$$

This map is defined by coordinate change $(x, y) \longmapsto (u^2x, u^3y)$, where $u = \left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{\frac{1}{2}}$. The corresponding elliptic curve now has equation:

$$y^2 = 4x^3 - \frac{g_2(\tau)^3}{g_3(\tau)^2}x - \frac{g_2(\tau)^3}{g_3(\tau)^2}$$

The j-invariant does not change under this transform. Note that $j(\tau) = \frac{1728g_2^3(\tau)}{g_2^3(\tau)-27g_3^2(\tau)}$. If $g_3(\tau) \neq 0$, then $\frac{g_2(\tau)^3}{g_3(\tau)^2} = \frac{27j}{j-1728}$. Thus, the corresponding elliptic curve satisfies equation:

$$y^2 = 4x^3 - \frac{27j}{j-1728}x - \frac{27j}{j-1728} \tag{2.1}$$

Lemma 2.6. *There exists a polynomial $\phi(x, y, z) \in \mathbb{Z}[x, y, z]$ such that for any elliptic curve $y^2 = 4x^3 - g_2x - g_3$ over field k, $char(k) = 0$, the x coordinate of a N torsion point satisfies*

$$\phi(g_2, g_3, x) = 0$$

Now $f_0^{(m,n)}$ is the x coordinate of the curve 2.1. By lemma, it should satisfies the equation

$$\phi(g(\tau), g(\tau), f_0^{(m,n)}) = 0 \qquad g(\tau) = \frac{27j(\tau)}{j(\tau) - 1728}$$

The left hand side is a meromorphic function on $\mathbb{H}^*$ and vanishes for all but finite many points. So, it is constantly zero. Thus, in the function field, we have

$$\phi(g, g, f_0^{(m,n)}) = 0 \qquad g = \frac{27j}{j - 1728}$$

In other words, $f_0^{(m,n)}$ is algebraic over $\mathbb{Q}(j)$ for all $(m,n) \in \mathbb{Z}/N\mathbb{Z})^2 \setminus \{0\}$. Therefore, $\mathbb{Q}(j, f_0^{(1,0)}, f_0^{(0,1)})$, $\mathbb{Q}(j, f_0^1)$, $\mathbb{Q}(j, f_0)$ are extension fields of $\mathbb{Q}$ with transcendental degree 1. Let $X(N)_{alg}$, $X_1(N)_{alg}$, and $X_0(N)_{alg}$ be smooth projective curves with function field $\mathbb{Q}(j, f_0^{(1,0)}, f_0^{(0,1)})$, $\mathbb{Q}(j, f_0^1)$, and $\mathbb{Q}(j, f_0)$.

Theorem 2.7. *$X_1(N)_{alg}$ and $X_0(N)_{alg}$ are curves defined over $\mathbb{Q}$. $X(N)$ is a curve defined over $\mathbb{Q}(\mu_N)$.*

3 Hecke operators

3.1 Hecke correspondence

Let Γ_1 and Γ_2 be two congruence subgroups and $\alpha \in \mathrm{GL}_2^+(\mathbb{R})$. α induces a map

$$\alpha : \mathbb{H} \longrightarrow \mathbb{H} \qquad z \longmapsto \alpha z$$

It is natural to consider the reduction of this map:

$$\alpha : \Gamma_1 \backslash \mathbb{H} \longrightarrow \Gamma_2 \backslash \mathbb{H} \qquad \Gamma_1 z \longmapsto \Gamma_2 \alpha z$$

However, this map is not well defined in most cases. For example, take $\tau \in \mathbb{H}$ and $\gamma \in \Gamma_1$, then $\Gamma_1 \tau$ maps to $\Gamma_2 \alpha \tau$ and $\Gamma_1 \gamma \tau$ maps to $\Gamma_2 \alpha \gamma \tau$. In most cases, $\Gamma_2 \alpha \tau$ and $\Gamma_2 \alpha \gamma \tau$ do not represent a same coset. One way to make sense this map is to consider a multi-value map:

$$\alpha : \Gamma_1 \backslash \mathbb{H} \longrightarrow \Gamma_2 \backslash \mathbb{H} \qquad \Gamma_1 z \longmapsto \{\Gamma_2 \alpha \gamma z \big| \gamma \in \Gamma_1\} \tag{3.1}$$

To write multi values as disjoint cosets, consider the left action of Γ_2 on $\Gamma_2 \alpha \Gamma_1$. Assume

$$\Gamma_2 \alpha \Gamma_1 = \bigcup_{i \in I} \Gamma_2 \alpha_i$$

Note that I is a finite set. Then the multi-value map 3.1 can be written as

$$\alpha : \Gamma_1 \backslash \mathbb{H} \longrightarrow \Gamma_2 \backslash \mathbb{H} \qquad \Gamma_1 z \longmapsto \{\Gamma_2 \alpha_i z \big| i \in I\}$$

Lemma 3.1. *Let $\Gamma_3 = \alpha^{-1} \Gamma_2 \alpha \cap \Gamma_1$. Assume $\Gamma_3 \backslash \Gamma_1 = \bigcup_{i \in I} \Gamma_3 \gamma_i$, then*

$$\Gamma_2 \alpha \Gamma_1 = \bigcup_{i \in I} \Gamma_2 \alpha \gamma_i$$

However, multi-value functions are definitely something we do not wish to study. Instead of union of cosets, we can write it as sum, making it a map between divisor group.

$$\Phi_\alpha : \mathrm{Div}(X(\Gamma_1)) \longrightarrow \mathrm{Div}(X(\Gamma_2)) \qquad \Gamma_1 z \longmapsto \sum_{i\in I} \Gamma_2 \alpha_i z$$

A map between divisor groups always derives from push forward and pull back of morphisms between curves. The map we defined above also comes in this way. Consider maps:

$$\begin{tikzcd}
 & \Gamma_1 \cap \alpha^{-1}\Gamma_2\alpha\backslash\mathbb{H} \arrow[dl, "\mathrm{Id}"'] \arrow[dr, "\alpha"] & \\
\Gamma_1\backslash\mathbb{H} & & \Gamma_2\backslash\mathbb{H}
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \Gamma_1 \cap \alpha^{-1}\Gamma_2\alpha z \arrow[dl, mapsto] \arrow[dr, mapsto] & \\
\Gamma_1 z & & \Gamma_2\alpha z
\end{tikzcd}$$

Proposition 3.2. *Let α_* be the push forward map of divisor groups and Id^* be the pull back of divisor groups. Then*

$$\Phi_\alpha = \alpha_* \circ Id^*$$

The map Φ_α then induces a map between $M_k(\Gamma_2)$ and $M_k(\Gamma_1)$:

$$[\Gamma_2\alpha\Gamma_1] : M_k(\Gamma_2) \longrightarrow M_k(\Gamma_1) \qquad f \longmapsto \sum_{i\in I} f\cdot[\alpha_i]_k$$

It is easy to verify that this map is well-defined. Since f can almost be "viewed" as a section of tensor product of the differential sheaf, one can interpret the map defined above as pull back of the section compositing with push forward.

The Hecke operator T_p on $M_k(\Gamma)$ is defined by $[\Gamma\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma]$. Let

$$\Gamma_p = \left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix}a & b\\ c & d\end{pmatrix} \equiv \begin{pmatrix}* & 0\\ * & *\end{pmatrix} \mod p\right\}$$

Then $\begin{pmatrix}1 & 0\\ 0 & p^{-1}\end{pmatrix}\Gamma\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix} = \Gamma_p\cap\Gamma$. The cosets representation of $\Gamma_p\cap\Gamma\backslash\Gamma$ is given by:

1. $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, $\left\{\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}\middle| k=1,...,p\right\} \cup \left\{\begin{pmatrix}p & p-1\\ 1 & 1\end{pmatrix}\right\}$
2. $\Gamma = \Gamma_0(N)$ and $p\nmid N$, $\left\{\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}\middle| k=1,...,p\right\} \cup \left\{\begin{pmatrix}p & N\\ k & l\end{pmatrix} \in \Gamma_0(N)\right\}$
3. $\Gamma = \Gamma_0(N)$ and $p\nmid N$, $\left\{\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}\middle| k=1,...,p\right\}$
4. $\Gamma = \Gamma_1(N)$ and $p\nmid N$, $\left\{\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}\middle| k=1,...,p\right\} \cup \left\{\begin{pmatrix}pm & k\\ N & l\end{pmatrix} \in \Gamma_1(N)\right\}$
5. $\Gamma = \Gamma_1(N)$ and $p\mid N$, $\left\{\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}\middle| k=1,...,p\right\}$

Therefore, the Hecke operator is given by

1. $\Gamma = \mathrm{SL}_2(\mathbb{Z})$,

$$T_p(f)(z) = p^{-1}\sum_{k=1}^{p} f\left(\frac{z+k}{p}\right) + p^{k-1}f(pz)$$

2. $\Gamma = \Gamma_0(N)$,

$$T_pf(z) = \begin{cases} p^{-1}\sum_{k=1}^{p} f\left(\frac{z+k}{p}\right) + p^{k-1}f(pz) & \text{if } p \nmid N \\ p^{-1}\sum_{k=1}^{p} f\left(\frac{z+k}{p}\right) & \text{if } p \mid N \end{cases}$$

3. $\Gamma = \Gamma_1(N)$,

$$T_pf(z) = \begin{cases} p^{-1}\sum_{k=1}^{p} f\left(\frac{z+k}{p}\right) + p^{k-1}(\langle p\rangle f)(pz) & \text{if } p \nmid N \\ p^{-1}\sum_{k=1}^{p} f\left(\frac{z+k}{p}\right) & \text{if } p \mid N \end{cases}$$

However, by defining Hecke operators T_p following this method, there is no intuitive way to generalize it to general T_n. In the next section, we will give a more intuitive method to define Hecke operator T_n for arbitrary integer $n > 0$.

3.2 Hecke operators for $\mathrm{SL}_2(\mathbb{Z})$

In last section, we construct the Hecke operators by the method of correspondences. In this section, we take a different approach, which give arises to Hecke operators T_n for arbitrary positive integer n.

We start by defining general Hecke operators for $\mathrm{SL}_2(\mathbb{Z})$. Recall that $\mathcal{L}$ is the $\mathbb{Q}$-vector space generated by the set of all lattices in $\mathbb{C}$.

Definition The n^{th} Hecke operator $T_n : \mathcal{L} \longrightarrow \mathcal{L}$ is defined by

$$T_n(\Lambda) = \frac{1}{n}\sum_{[\Lambda':\Lambda]=n} \Lambda'$$

Here the sum is taken over all lattices Λ' in $\mathbb{C}$ containing Λ such that Λ'/Λ is a group of order n.

Definition The operator $R(n) : \mathcal{L} \longrightarrow \mathcal{L}$ is defined by

$$R(n)(\Lambda) = \frac{1}{n^2}(n^{-1}\Lambda)$$

We will see later that coefficients $\frac{1}{n}$ and $\frac{1}{n^2}$ here is used to normalize the action of Hecke operators on modular forms.

Proposition 3.3. *1. T_n and $R(m)$ commute for any positive integer n, m.*

2. $T_nT_m = T_{mn}$, if $(m, n) = 1$.

3. Let p be a prime, then

$$T_{p^{n+1}} = T_{p^n} T_p - pR(p) T_{p^{n-1}}$$

4. $\{T_n : n \in \mathbb{Z}_{>0}\}$ *commute with each other.*

Proof. 1. For any lattice Λ,

$$nT_n \circ m^2 R(m)(\Lambda) = \sum_{[\Lambda' : m^{-1}\Lambda]=n} \Lambda' = \sum_{[m\Lambda' : \Lambda]=n} \Lambda' = \sum_{[\Lambda' : \Lambda]=n} m^{-1}\Lambda' = m^2 R(m) \circ nT_n(\Lambda)$$

2. This is because of a lemma: if G is an abelian group of order mn, m, n coprime, then their exists a unique subgroup H in G order m.

3. It suffices to prove

$$p^n T_{p^n} \circ pT_p(\Lambda) = p^{n+1} T_{p^{n+1}}(\Lambda) + p \cdot p^2 R(p) \circ p^{n-1} T_{p^{n-1}}(\Lambda) \tag{3.2}$$

Note that the left hand side equals to the sum of

$$\{(\Lambda'', \Lambda') | [\Lambda'' : \Lambda'] = p^n \text{ and } [\Lambda' : \Lambda] = p\}$$

$p^2 R(p) \circ p^{n-1} T_{p^{n-1}}(\Lambda)$ is equal to the sum of

$$\left\{\Lambda' | [\Lambda' : p^{-1}\Lambda] = p^{n-2}\right\}$$

For lattice Λ'' satisfying $[\Lambda'' : \Lambda] = p^{n+1}$, assume that α_1, α_2 is a basis of Λ'' such that $p^i \alpha_1$ and $p^j \alpha_2$ is a basis of Λ, where $i \leq j$ are non negative integers and $i + j = n$.

(a) If $p^{-1}\Lambda \not\subset \Lambda''$, then i equals to 0. In this case, there exists a unique lattice Λ', generated by α_1 and $p^{j-1}\alpha_2$, such that $[\Lambda' : \Lambda] = p$.

(b) If $p^{-1}\Lambda \subset \Lambda''$, then $i, j \geq 1$. In this case, by lemma 3.5, there exists exactly $p + 1$ lattices Λ' contained in Λ'' such that $[\Lambda' : \Lambda] = p$.

Therefore, the number of appearance of each lattice on the both sides of the equation 3.2 equal.

□

Let $F : \mathcal{L} \longrightarrow \mathbb{C}$ be a linear function . Hecke operators act on F by

$$T_n(F)(\Lambda) = F(T_n(F)(\Lambda)) = \frac{1}{n} \sum_{[\Lambda' : \Lambda]=n} F(\Lambda')$$

$$R(m)F(\Lambda) = F(R(m)(\Lambda)) = \frac{1}{m^2} F(m^{-1}\Lambda)$$

A linear function $F : \mathcal{L} \longrightarrow \mathbb{C}$ is called homogeneous with degree k if $F(m\Lambda) = m^{-k}F(\Lambda)$. If F is homogeneous with degree k, then so are $T_n(F)$ and $R(m)(F)$. We can dehomogenize F to a function f on $\mathbb{H}$ by

$$f(\tau) = F(\Lambda_\tau)$$

then f is a weakly modular function of weight k. Conversely, if f is a weakly modular function of weight k, then we can define a homogeneous function $F : \mathcal{L} \longrightarrow \mathbb{C}$ by

$$F(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = \omega_2^{-k} f\left(\frac{\omega_2}{\omega_1}\right) \qquad \mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right) > 0$$

One important consequence is that Hecke operators are linear maps on the space $M_k(\mathrm{SL}_2(\mathbb{Z}))$ i.e. they transform a modular form of weight k to a modular form of weight k.

Proposition 3.4. *If we consider Hecke operators as operators on $M_k(SL_2(\mathbb{Z}))$, then*

1. *$R(n)$ is multiplying by n^{k-2}*
2. *$T_nT_m = T_{mn}$, if $(m,n) = 1$.*
3. *Let p be a prime, then*
$$T_{p^{n+1}} = T_{p^n}T_p - p^{k-1}T_{p^{n-1}}$$
4. *$\{T_n : n \in \mathbb{Z}_{>0}\}$ commute with each other.*

Let's figure out how Hecke operators act on f explicitly.

Lemma 3.5. *Let Λ be a lattice in $\mathbb{C}$ generated by ω_1 and ω_2. Then the set of all lattices Λ' in $\mathbb{C}$ containing Λ such that $[\Lambda' : \Lambda] = n$ is given by*

$$\left\{\mathbb{Z}\frac{1}{a}\omega_1 + \mathbb{Z}(\frac{b}{n}\omega_1 + \frac{1}{d}\omega_2) : a, b, d \in \mathbb{Z}_{>0}, ad = n, \text{ and } 1 \le b \le d\right\}$$

In particular, if $n = p$ is a prime then the set of all lattices Λ' in $\mathbb{C}$ containing Λ such that $[\Lambda' : \Lambda] = p$ is given by

$$\left\{\mathbb{Z}\omega_1 + \mathbb{Z}\frac{\omega_2 + b\omega_1}{p} : 1 \le b \le p\right\} \cup \{\mathbb{Z}\frac{\omega_1}{p} + \mathbb{Z}\omega_2\}$$

Proof. Let $\mathrm{M}(n)$ be the subset of all matrices in $\mathrm{M}_2(\mathbb{Z})$ that have determinant n. Assume lattice Λ' in $\mathbb{C}$ contains Λ such that $[\Lambda' : \Lambda] = n$, Let $\{\omega_1', \omega_2'\}$ be a basis of Λ'. Then there exists a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z})$ such that

$$(\omega_1', \omega_2')A = (\omega_1, \omega_2)$$

Since $[\Lambda' : \Lambda] = n$, the absolute value of $\det A$ is n and hence $A \in \{\pm I_2\}\mathrm{M}(n)$ Conversely, if $A \in \{\pm I_2\}\mathrm{M}(n)$, then $(\omega_1, \omega_2)A^{-1}$ generates a lattice that has order n over Λ. Two matrices A, B define same lattice if and only if there exists a matrix $C \in \{\pm I_2\}\mathrm{SL}_2(\mathbb{Z})$, such that $A = CB$. Therefore, there is a one to one correspondence between the set of all lattices Λ' in $\mathbb{C}$ containing Λ such that $[\Lambda' : \Lambda] = n$ and the quotient space

$$\{\pm I_2\}\mathrm{SL}_2(\mathbb{Z})\backslash\{\pm I_2\}\mathrm{M}(n) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{M}(n)$$

For any $A \in M(n)$, one can apply row operations (multiply elements in $\mathrm{SL}_2(\mathbb{Z})$) to A and get a matrix of form

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

where a, b, d are positive integers, $ad = n$, and $1 \le b \le d$. We can show that:

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{M}(n) = \coprod_{\substack{ad=n \\ 1\le b\le d}} \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

For each $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, the corresponding lattice has a basis $(\omega_1, \omega_2)\begin{pmatrix} a^{-1} & -bn^{-1} \\ 0 & d^{-1} \end{pmatrix} = (\frac{1}{a}\omega_1, -\frac{b}{n}\omega_1 + \frac{1}{d}\omega_2)$. Thus, we have proved the lemma. $\square$

Proposition 3.6. *if f is a modular form of weight k with respect to $SL_2(\mathbb{Z})$, then*

$$T_n(f)(\tau) = n^{-1} \cdot \sum_{\substack{ad=n \\ 1 \le b \le d}} a^k f(\frac{a\tau + b}{d})$$

Proof. Assume f can be lifted to a homogeneous function F, then

$$\begin{aligned} T_n(f)(\tau) &= n^{-1} \cdot \sum_{\substack{ad=n \\ 1 \le b \le d}} F\left(\mathbb{Z}\frac{1}{a} + \mathbb{Z}(\frac{b}{n} + \frac{1}{d}\tau)\right) \\ &= n^{-1} \cdot \sum_{\substack{ad=n \\ 1 \le b \le d}} a^k F\left(\mathbb{Z} + \mathbb{Z}(\frac{a\tau + b}{d})\right) \\ &= n^{-1} \cdot \sum_{\substack{ad=n \\ 1 \le b \le d}} a^k f\left(\frac{a\tau + b}{d}\right) \end{aligned}$$

□

Proposition 3.7. *Let*

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n$$

be the Fourier expansion of a modular form of weight k. Then

$$T_m(f)(\tau) = \sum_{n=0}^{\infty} a_n(T_m f) q^n$$

where

$$a_n(T_m f) = \sum_{d|(n,m)} d^{k-1} a_{\frac{mn}{d^2}} \qquad n \ge 1 \qquad a_0(T_m f) = \sigma_{k-1}(m) a_0$$

In particular, $a_1(T_m f) = a_m$.

Proof.

$$\begin{aligned} T_m\left(\sum_{n=0}^{\infty} a_n q^n\right) &= m^{-1} \sum_{\substack{ad=m \\ 1 \le b \le d}} a^k \sum_{n=0}^{\infty} a_n e^{2\pi i \frac{a}{d}\tau n} \cdot e^{2\pi i \frac{b}{d} n} \\ &= m^{-1} \sum_{ad=m} a^k \sum_{n=0}^{\infty} a_n q^{\frac{a}{d} n} \sum_{b=1}^{d} e^{2\pi i \frac{b}{d} n} \\ &= \sum_{ad=m} a^{k-1} \sum_{n=0}^{\infty} a_{nd} q^{an} \\ &= \sigma_{k-1}(m) a_0 + \sum_{n=1}^{\infty} \sum_{a|(m,n)} a^{k-1} a_{\frac{mn}{a^2}} q^n \end{aligned}$$

□

Corollary 3.8. *Hecke operators map cusp forms to cusp forms. In other words, Hecke operators act on space $S_k(SL_2(\mathbb{Z}))$.*

3.3 Hecke operators for $\Gamma_1(N)$ and $\Gamma_0(N)$

In last section,

Definition The n^{th} Hecke operator $T_n : \mathcal{L}_*^N \longrightarrow \mathcal{L}_*^N$ is defined by

$$T_n((\Lambda, P)) = \frac{1}{n} \sum_{\substack{[\Lambda':\Lambda]=n \\ P \text{ is order } N \text{ in } \Lambda'}} (\Lambda', P)$$

$$T_n((\Lambda, C)) = \frac{1}{n} \sum_{\substack{[\Lambda':\Lambda]=n \\ C \text{ is order } N \text{ in } \Lambda'}} (\Lambda', C)$$

Definition For positive integer n, $(n, N) = 1$, the operator $R(n) : \mathcal{L}_1 \longrightarrow \mathcal{L}_1$ and $R(n) : \mathcal{L}_0 \longrightarrow \mathcal{L}_0$ are defined by

$$R(n)((\Lambda, P)) = \frac{1}{n^2}(n^{-1}\Lambda, P)$$

$$R(n)((\Lambda, C)) = \frac{1}{n^2}(n^{-1}\Lambda, C)$$

Proposition 3.9. *1. T_n and $R(m)$ commute for any positive integer n, m.*

2. $T_n T_m = T_{mn}$, if $(m, n) = 1$.

3. Let p be a prime, then if $p|N$, then $T_p^n = (T_p)^n$. If $p \nmid N$, then

$$T_{p^{n+1}} = T_{p^n} T_p - pR(p)T_{p^{n-1}}$$

4. $\{T_n : n \in \mathbb{Z}_{>0}\}$ commute with each other.

Proof. Let (Λ, P) be a lattice with a N torsion point. Let ω_1, ω_2 be a basis of Λ such that $P = \frac{\omega_1}{N}$.

If $p \mid N$, then the set of all lattices Λ' in $\mathbb{C}$ containing Λ such that $[\Lambda' : \Lambda] = p^n$ and P is still a N torsion point is given by

$$\left\{ \mathbb{Z}\omega_1 + \mathbb{Z}\frac{\omega_2 + b\omega_1}{p^n} : 1 \leq b \leq p^n \right\}$$

they are in one to one correspondence with $(pT_p)^n(\Lambda)$. Thus, $T_{p^n} = (T_p)^n$.

If $p \nmid N$, then we can simply ignore the torsion point. In other word, their is a diagram

$$\begin{tikzcd} \mathcal{L}_1 \arrow[r, "T_{p^n}"] \arrow[d, "\pi"'] & \mathcal{L}_1 \arrow[d, "\pi"'] \\ \mathcal{L} \arrow[r, "T_{p^n}"] & \mathcal{L} \end{tikzcd}$$

where $\pi : \mathcal{L}_1 \longrightarrow \mathcal{L}$ is given by $(\Lambda, P) \longmapsto \Lambda$. Thus, the equation for Hecke operators does not change. We can prove these results for Hecke operators on $\mathcal{L}_0$ similarly. $\square$

As we stated in section 2.3, homogeneous functions can dehomogenize to modular functions. Thus, we obtain actions of Hecke operators on modular forms with respect to $\Gamma_0(N)$ and $\Gamma_1(N)$.

To begin with, Let's consider actions of Hecke operators on $M_k(\Gamma_0(N))$. All results are similar to results for $\mathrm{SL}_2(\mathbb{Z})$:

Proposition 3.10. *If we consider Hecke operators as operators on $M_k(SL_2(\mathbb{Z}))$, then*

1. *$R(n)$ is multiplying by n^{k-2}, if $(n,N)=1$.*
2. *$T_nT_m = T_{mn}$, if $(m,n)=1$.*
3. *Let p be a prime, If $p \mid N$, then $T_{p^n} = (T_p)^n$. If $p \nmid N$, then*
$$T_{p^{n+1}} = T_{p^n}T_p - p^{k+1}R(p)T_{p^{n-1}}$$
4. *$\{T_n : n \in \mathbb{Z}_{>0}\}$ commute with each other.*

Proposition 3.11. *if f is a modular form of weight k with respect to $\Gamma_0(N)$, then*

$$T_n(f)(\tau) = n^{-1} \cdot \sum_{\substack{ad=n,(a,N)=1 \\ 1\le b\le d}} a^k f(\frac{a\tau+b}{d})$$

Proposition 3.12. *Let*

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n$$

be the Fourier expansion of a modular form of weight k with respect to $\Gamma_0(N)$. Then

$$T_m(f)(\tau) = \sum_{n=0}^{\infty} a_n(T_m f)q^n$$

where

$$a_n(T_m f) = \sum_{\substack{d\mid(n,m) \\ (d,N)=1}} d^{k-1} a_{\frac{mn}{d^2}} \qquad n \ge 1 \qquad a_0(T_m f) = \left(\sum_{\substack{d\mid m \\ (d,N)=1}} d^{k-1}\right) a_0$$

In particular, $a_1(T_m f) = a_m$.

Corollary 3.13. *Hecke operators map cusp forms to cusp forms. In other words, Hecke operators act on the space $S_k(\Gamma_0(N))$.*

Actions of Hecke operators on $M_k(\Gamma_1(N))$ are not so simple as the $\Gamma_0(N)$ case, mostly due to the proposition:

Proposition 3.14. *For positive integer n such that $(n,N)=1$, Let $g_n \in SL_2(\mathbb{Z})$ such that $g_n \equiv \begin{pmatrix} n^{-1} & * \\ 0 & n \end{pmatrix} \mod N$. Then for $f \in \Gamma_1(N)$*

$$R(n)f = n^{k-2} f \cdot [g_n]_k$$

Proof. Let F be the homogeneous function corresponds to f. Then

$$R(n)f = n^{-2}F(n^{-1}\Lambda_\tau, \frac{1}{N}) = n^{k-2}F(\Lambda_\tau, \frac{n}{N})$$

Let $\tau' = g_n\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau$, then $\tau = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\tau'$

$$F(\Lambda_\tau, \frac{n}{N}) = (-c\tau' + a)^k F(\Lambda_{\tau'}, \frac{1}{N}) = (c\tau+d)^{-k} f(g\tau) = f \cdot [g_n]_k$$

Therefore, $R(n)f = n^{k-2} f \cdot [g_n]_k$ □

Note that the action of $n^{2-k} \cdot R(n)$ only depends on $n \mod N$. This gives rise to an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $M_k(\Gamma_1(N))$:

$$(\mathbb{Z}/N\mathbb{Z})^\times \times M_k(\Gamma_1(N)) \longmapsto M_k(\Gamma_1(N)) \qquad \langle n\rangle \cdot f = f \cdot [g_n]_k$$

By decomposing $M_k(\Gamma_1(N))$ into irreducible representations, we have

$$M_k(\Gamma_1(N)) = \oplus M_k(\Gamma_1(N), \chi)$$

where $(\mathbb{Z}/N\mathbb{Z})^\times$ acts on $M_k(\Gamma_1(N), \chi)$ by character χ, i.e. for $f \in M_k(\Gamma_1(N), \chi)$, $R(n)f = n^{k-2}\chi(n)f$. Moreover, if we define

$$M_{k,\chi}(\Gamma_0(N)) = \left\{ f \in M_k(\Gamma_1(N)) \middle| f\left(\frac{a\tau+b}{c\tau+d}\right) = \chi(d)(c\tau+d)^k f(\tau) \text{ for any } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right\}$$

Then $M_{k,\chi}(\Gamma_0(N)) = M_k(\Gamma_1(N), \chi)$.

Proposition 3.15. *If we consider Hecke operators as operators on $M_k(\Gamma_1(N))$, then*

1. *$T_n T_m = T_{mn}$, if $(m, n) = 1$.*

2. *Let p be a prime. If $p \mid N$, then $T_{p^n} = (T_p)^n$. If $p \nmid N$, then*

$$T_{p^{n+1}} = T_{p^n} T_p - p^{k+1} R(p) T_{p^{n-1}}$$

In particular, if $f \in M_k(\Gamma_1(N), \chi)$, then

$$T_{p^{n+1}} f = T_{p^n} T_p f - p^{k-1} \chi(p) T_{p^{n-1}} f$$

3. *$\{T_n : n \in \mathbb{Z}_{>0}\}$ commute with each other.*

Proposition 3.16. *if f is a modular form of weight k with respect to $\Gamma_1(N)$, then*

$$T_n(f)(\tau) = n^{-1} \cdot \sum_{\substack{ad=n,(a,N)=1 \\ 1\le b\le d}} a^k(\langle a\rangle \cdot f)\left(\frac{a\tau+b}{d}\right)$$

Proof. Assume f can be lifted to a homogeneous function F, then

$$\begin{aligned} T_n(f)(\tau) &= n^{-1} \cdot \sum_{\substack{ad=n,(a,N)=1 \\ 1\le b\le d}} F\left(\mathbb{Z}\frac{1}{a} + \mathbb{Z}(\frac{b}{n} + \frac{1}{d}\tau), \frac{1}{N}\right) \\ &= n^{-1} \cdot \sum_{\substack{ad=n,(a,N)=1 \\ 1\le b\le d}} a^k F\left(\mathbb{Z} + \mathbb{Z}(\frac{a\tau+b}{d}), \frac{a}{N}\right) \end{aligned}$$

Assume $g_a = \begin{pmatrix} l & m \\ p & q \end{pmatrix}$, Let $\tau' = \frac{a\tau+b}{d}$ and $\tau'' = g_a\tau'$, then

$$\begin{aligned} F\left(\mathbb{Z} + \mathbb{Z}\tau', \frac{a}{N}\right) &= (-p\tau'' + m)^k F\left(\mathbb{Z} + \mathbb{Z}\tau'', \frac{1}{N}\right) \\ &= (p\tau' + q)^{-k} f(\tau'') \\ &= (p\tau' + q)^{-k} f(g_a\tau') \\ &= f \cdot [g_a]_k(\tau') \\ &= (\langle a\rangle \cdot f)(\tau') \end{aligned}$$

Thus,

$$T_n(f)(\tau) = n^{-1} \cdot \sum_{\substack{ad=n,(a,N)=1 \\ 1\le b\le d}} a^k(\langle a\rangle \cdot f)\left(\frac{a\tau+b}{d}\right)$$

□

Proposition 3.17. *Let*

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n$$

be the Fourier expansion of a modular form of weight k with respect to $\Gamma_1(N)$. Then

$$T_m(f)(\tau) = \sum_{n=0}^{\infty} a_n(T_m f) q^n$$

where

$$a_n(T_m f) = \sum_{\substack{d\mid(n,m) \\ (d,N)=1}} d^{k-1} a_{\frac{mn}{d^2}}(\langle d\rangle f) \qquad n \ge 1 \qquad a_0(T_m f) = \sum_{\substack{d\mid m \\ (d,N)=1}} d^{k-1} a_0(\langle d\rangle f)$$

In particular, $a_1(T_m f) = a_m$.

Proof.

$$\begin{aligned}
T_m\left(\sum_{n=0}^{\infty} a_n q^n\right) &= m^{-1} \sum_{\substack{ad=m,(a,N)=1 \\ 1\le b\le d}} a^k \sum_{n=0}^{\infty} a_n(\langle a\rangle f) e^{2\pi i \frac{a}{d}\tau n} \cdot e^{2\pi i \frac{b}{d} n} \\
&= m^{-1} \sum_{ad=m,(a,N)=1} a^k \sum_{n=0}^{\infty} a_n(\langle a\rangle f) q^{\frac{a}{d}n} \sum_{b=1}^{d} e^{2\pi i \frac{b}{d} n} \\
&= \sum_{ad=m,(a,N)=1} a^{k-1} \sum_{n=0}^{\infty} a_{nd}(\langle a\rangle f) q^{an} \\
&= \sum_{\substack{a\mid m \\ (a,N)=1}} a^{k-1} a_0(\langle a\rangle f) + \sum_{n=1}^{\infty} \sum_{\substack{a\mid(m,n) \\ (a,N)=1}} a^{k-1} a_{\frac{mn}{a^2}}(\langle a\rangle f) q^n
\end{aligned}$$

□

Corollary 3.18. *Hecke operators map cusp forms to cusp forms. In other words, Hecke operators act on the space $S_k(\Gamma_1(N),\chi) = S_k(\Gamma_1(N)) \cap M_k(\Gamma_1(N),\chi)$.*

3.4 Hecke eigenforms

Recall that in Ramanujan's study, he claims that coefficients of $\Delta(z)$ satisfy relations similar to that of Hecke operators. Roughly speaking, this is because $\Delta(z)$ is a Hecke eigenform.

Definition An nonzero modular form $f \in S_k(\Gamma)$ is called a Hecke eigenform or simply eigenform with respect to Γ if it is an eigenvector for all Hecke operators T_n and $R(n)$, $n \in \mathbb{Z}_{>0}$. A Hecke eigenform is normalized if $a_1(f) = 1$.

In last section, we have prove that Hecke operators act on $S_k(\mathrm{SL}_2(\mathbb{Z}))$, $S_k(\Gamma_0(N))$ and $S_k(\Gamma_1(N),\chi)$. We claim that all most all Hecke operators are diagonalizable. The main idea to show this result is to prove that Hecke operators are normal operator on these spaces with inner products. So, our first step is to construct inner product on the space $S_k(\Gamma)$.

The invariant differential on $\mathbb{H}$ with respect to the action of $\mathrm{GL}_2^+(\mathbb{R})$ is given by

$$\frac{dx\wedge dy}{y^2}=\frac{i}{2}\frac{dz\wedge d\overline{z}}{y^2}$$

i.e. for $g\in \mathrm{GL}_2^+(\mathbb{R})$

$$\frac{dx\wedge dy}{y^2}\circ g=\frac{dx\wedge dy}{y^2}$$

Lemma 3.19. *Let D be a fundamental domain for Γ. If $f,h\in S_k(\Gamma)$, then the integral*

$$\langle f,h\rangle=\int_D f(z)\cdot\overline{h(z)}y^k dxdy$$

converges.

Note that this lemma does not hold for modular forms that are not cusp forms. That's why we only consider cusp forms. The Petersson inner product on $S_k(\Gamma)$ is defined by

$$\langle f,h\rangle=\int_D f(z)\cdot\overline{h(z)}y^k dxdy$$

$S_k(\Gamma)$ with $\langle\cdot,\cdot\rangle$ is a finite dimensional Hilbert space.

Proposition 3.20. *Hecke operators are self-adjoint operators on $S_k(SL_2(\mathbb{Z}))$, i.e.*

$$\langle T_n f,h\rangle=\langle f,T_n h\rangle$$

Since Hecke operators mutually commute and are normal operators, we conclude that all Hecke operators on $S_k(\mathrm{SL}_2(\mathbb{Z}))$ can be diagonalize simultaneously. Assume $f\in S_k(\mathrm{SL}_2(\mathbb{Z}))$ is an eigenvector for all Hecke operators, then $T_n(f)=\lambda_n f$ for some $\lambda_n\in\mathbb{R}$. In last section, we show that $a_1(T_n(f))=a_n$, so $\lambda_n\cdot a_1=a_n$. Specially, if $a_1=1$, then $\lambda_n=a_n$. Therefore,

Theorem 3.21. *If $f\in S_k(SL_2(\mathbb{Z}))$ is a normalized Hecke eigenform, its Fourier coefficients satisfies*

1. $a_0=1$
2. $a_n a_m=a_{mn}$, *if* $(m,n)=1$.
3. *Let p be a prime, then for any $n\geq 1$*

$$a_{p^{n+1}}=a_{p^n}a_p-p^{k-1}a_{p^{n-1}}$$

The Hecke operators on $S_k(\Gamma_1(N))$ is more subtle.

Proposition 3.22. *If $(n,N)=1$, then Hecke operators T_n and $R(n)$ are normal operators on $S_k(\Gamma_1(N))$.*

Let M be a positive integer, $M|N$, $N = Ml$. There are many modular forms in $S_k(N)$ which in fact derive from $S_k(M)$. For example, if $f(z) \in S_k(M)$, then $f(z) \in S_k(N)$. Moreover, $i_d(f)(z) = f(lz) \in S_k(N)$, because for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S_k(N)$, $\begin{pmatrix} a & bl \\ \frac{c}{l} & d \end{pmatrix} \in \Gamma_1(M)$

$$f\left(l\frac{az+b}{cz+d}\right) = f\left(\frac{azl+bl}{\frac{c}{l}zl+d}\right) = f(lz)$$

Images of inclusion and i_d generate a subspace of $S_k(\Gamma_1(N))$. If we sum over these subspace for all $M|N$, then we obtain a subspace of $S_k(N)$ which consists of modular forms that are not "new" to $S_k(N)$.

Definition The space of old forms in $S_k(\Gamma_1(N))$ is defined by

$$S_k^{\text{old}}(\Gamma_1(N)) = \bigoplus_{N=Md} i(S_k(M)) \oplus i_d(S_k(M))$$

The space of new forms is the orthogonal complement of the space of old form, i.e.

$$S^{\text{new}}(\Gamma_1(N)) = \left(S^{\text{old}}(\Gamma_1(N))\right)^{\perp}$$

Proposition 3.23. *1.*

$$S_k^{old}(\Gamma_1(N)) = \bigoplus_{\substack{p|N \\ p \text{ is a prime}}} i(S_k(Np^{-1})) \oplus i_p(S_k(Np^{-1}))$$

2. $S_k^{new}(\Gamma_1(N))$ and $S_k^{old}(\Gamma_1(N))$ are invariant spaces under the action of Hecke operator $T(n)$ and $R(m)$ for all $n, m \in \mathbb{Z}_{>0}$, $(m, N) = 1$.

Now assume $N = Md$, $f \in S_k(M)$, $f = \sum_{n=1}^{\infty} a_n q^n$, then the Fourier expansion of $i_d(f)$ is given by

$$i_d(f)(z) = \sum_{n=0}^{\infty} a_n q^{dn}$$

This shows that if $f \in S_k(\Gamma_1(N))$ takes the form $f = \sum_{p|N} i_p(f_p)$ with $f_p \in S_k(\Gamma_1(Np^{-1}))$, then $a_n(f) = 0$ for all $(n, N) = 1$. The converse also holds.

Theorem 3.24 (**Main lemma**). *If $f \in S_k(\Gamma_1(N))$ such that $a_n(f) = 0$ for all $(n, N) = 1$, then there exists $f_p \in S_k(\Gamma_1(Np^{-1}))$ for each prime $p|N$, such that*

$$f = \sum_{p|N} i_p(f_p)$$

Let $f \in S(\Gamma_1(N))$ be a non zero newform. By the main lemma, $a_n(f) \neq 0$ for all $(n, N) = 1$. In particular, $a_1(f) \neq 0$. Now assume f is an eigenvector for all T_n and $R(n)$, $(n, N) = 1$. For any positive integer m, $T_m(f)$ and $a_m \cdot f$ are newforms. Then $g_m = T_m f - a_m f$ is also a newform, $a_1(g_m) = 0$. Thus, $g_m = 0$, $T_m f = a_m f$. This implies f is a Hecke eigenform.

Theorem 3.25. *$S_k^{new}(N)$ has an orthogonal basis consisting of Hecke eigenforms.*

Let $f_1^N, ..., f_{n_N}^N$ be a basis of $S_k^{\text{new}}(\Gamma_1(N))$ consisting of Hecke eigenforms. Then we can construct a basis of $S_k(\Gamma_1(N))$.

Theorem 3.26. *The set below forms a basis of $S_k(\Gamma_1(N))$:*

$$\left\{ f_i^M(nz) \middle| Mn|N \text{ and } 1 \leq i \leq n_M \right\}$$

At last, we state the result for Fourier coefficients:

Theorem 3.27. *If $f \in S_k(\Gamma_1(N), \chi)$ is a normalized Hecke eigenform, its Fourier coefficients satisfies*

1. $a_0 = 1$
2. $a_n a_m = a_{mn}$, *if* $(m, n) = 1$.
3. *Let p be a prime, then for any $n \geq 1$*

$$a_{p^{n+1}} = a_{p^n} a_p - p^{k-1} \chi(p) a_{p^{n-1}}$$

References

[1]

[2]