Introduction to Modular Forms

Lectures by
Dipendra Prasad

Written by Sagar Shrivastava

School and Workshop on Modular Forms and Black Holes
(January 5-14, 2017)
National Institute of Science Education and Research

Langlands program identifies relations between Number theory, Representation theory, Harmonic analysis and Algebraic geometry. In modern terminology, we use the collective term of Automorphic Forms. Typically, modular forms (automorphic forms) are a certain class of functions on spaces of the form $\mathrm{SL}_2(\mathbb{Z})\backslash\mathrm{SL}_2(\mathbb{R})$. (General automorphic forms are functions on spaces of the form $G(\mathbb{Z})\backslash G(\mathbb{R})$ where $G(\mathbb{Z})$ is the group of 'integral' points and $G(\mathbb{R})$, the group of real points of G.)

Poincaré Upper Half Plane

Recall the Poincaré upper half plane $\mathbb{H} = \{z \in \mathbb{C} | \, \mathfrak{Im}(z) > 0\}$, which is a complex manifold of dimension 1 on which we can talk of holomorphic functions.

The group $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{H}$ by linear fractional transformations:

$$gz \overset{def}{=} \frac{az+b}{cz+d}; \qquad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

It can be checked that the above defines an action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$, in other words: $g_1(g_2z) = (g_1g_2)z$ for all $g_1, g_2 \in \mathrm{SL}_2(\mathbb{R}), z \in \mathbb{H}$.

This action is transitive on $\mathbb{H}$, as given $z = x + iy \in \mathbb{H}$, consider the matrix:

$$g_z = \begin{pmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2} \end{pmatrix} x, y \in \mathbb{R}, y > 0 \Rightarrow g_z \in \mathrm{SL}_2(\mathbb{R}), \qquad g_z i = x + iy.$$

Also, if $g \in \mathrm{SL}_2(\mathbb{R})$ with $gi = i$, then we can see that $g \in \mathrm{SO}(2)$, the subgroup of $\mathrm{SL}_2(\mathbb{R})$ consisting of the matrices:

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix};$$

thus we have an isomorphism of spaces: $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2) \cong \mathbb{H}$

For a point $z \in \mathbb{H}$, let $\mathfrak{Im}(z)$ be its imaginary part. For several calculations below, the relationship between $\mathfrak{Im}(z)$ and $\mathfrak{Im}(gz)$ will be very useful. This will also prove that $\mathrm{SL}_2(\mathbb{R})$ preserves $\mathbb{H}$. Note that:

$$\mathfrak{Im}(gz) = \mathfrak{Im}\left(\frac{az+b}{cz+d}\right) = \mathfrak{Im}\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right) = |cz+d|^{-2}\mathfrak{Im}(adz+bc\bar{z}).$$

But $\mathfrak{Im}(adz + bc\bar{z}) = (ad - bc)\mathfrak{Im}(z) = \mathfrak{Im}(z)$, since $\det(g) = 1$. Hence

$$\mathfrak{Im}(gz) = |cz+d|^{-2}\mathfrak{Im}(z) \quad \text{for } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

So $\mathfrak{Im}(z) > 0 \Rightarrow \mathfrak{Im}(gz) > 0$. Thus the group $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{H}$ (by linear fractional transformations).

The subgroup of $\mathrm{SL}_2(\mathbb{R})$ consisting of matrices with integer coefficients is by definition $\mathrm{SL}_2(\mathbb{Z})$. It is called the "Full modular group". Besides $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, certain of its subgroups have special significance. Let N be a positive integer, we define

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

In other words, $\Gamma(N)$ consists of 2×2 integral matrices of determinant 1 which are congruent modulo N to the identity matrix. $\Gamma(N)$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$, actually a normal subgroup, because it is the kernel of the homomorphism from $\mathrm{SL}_2(\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing entries modulo N. (This also implies that $\Gamma(N)$ has finite index in $\mathrm{SL}_2(\mathbb{Z})$). A subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is called a "congruence subgroup of level N" if it contains $\Gamma(N)$. Notice that a congruence subgroup of level N also has level N' (if $N \mid N'$), so we choose the N to be the smallest such number. (Any congruence subgroup has finite index in $\mathrm{SL}_2(\mathbb{Z})$, and hence its fundamental domain will have finite volume.)

Similarly we define the following subgroups of $\mathrm{SL}_2(\mathbb{Z})$ which play very prominent roles in the theory of modular forms:

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

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

Modular forms for $\mathrm{SL}_2(\mathbb{Z})$

A modular form $f : \mathbb{H} \longrightarrow \mathbb{C}$ of weight k for $\mathrm{SL}_2(\mathbb{Z})$ is a function on $\mathbb{H}$ with the following properties:

1. $f : \mathbb{H} \longrightarrow \mathbb{C}$ is a holomorphic function (meromorphic function in case of a modular function).

2. $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \forall z \in \mathbb{H}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

   Note that $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, so $f(z+1) = f(z)$. Hence these functions will have a Fourier expansion:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n z}.$$

3. $a_n = 0,\ \forall n < 0$ i.e. $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z} = \sum_{n=0}^{\infty} a_n q^n, \quad q = e^{2\pi i z}$.

If further, $a_0 = 0$, then f is called a cusp form.

Remark: Condition 3 is equivalent to say that f remains bounded at $i\infty$, i.e. $\lim_{t\to\infty} f(it) < \infty$, and the cuspidality condition is equivalent to say that $f(i\infty) = 0$.

Observe that $z \mapsto e^{2\pi i z} = q$ gives rise to the identification:

$$\mathbb{H}/\mathbb{Z} \cong D^* = \{q \mid |q| < 1, q \neq 0\}.$$

So if f is a modular form, f considered as a function on D^* can be extended to a holomorphic function on D. It is a cusp form if it extends to D holomorphically and vanishes at $q = 0$.

Since $\mathrm{SL}_2(\mathbb{Z}) = \langle S, T\rangle$ (as we will see later) where

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

for the modularity of a function f on $\mathbb{H}$, we "just" need to check that,

$$f(z+1) = f(z) \quad \text{and} \quad f(\frac{-1}{z}) = z^k f(z).$$

Modular forms are an interplay between continuous and discrete as they are continuous functions with discrete symmetries.

The set of all modular forms of weight k for $\mathrm{SL}_2(\mathbb{Z})$ is a finite dimensional vector space, and is denoted by $M_k(\mathrm{SL}_2(\mathbb{Z}))$. Similarly, the set of all cusp forms of weight k for $\mathrm{SL}_2(\mathbb{Z})$ is also a vector space, and is denoted by $S_k(\mathrm{SL}_2(\mathbb{Z}))$.

Fundamental Domain ($\mathfrak{F}$)

A fundamental domain is a set of equivalence classes on $\mathbb{H}$ under the action of $\mathrm{SL}_2(\mathbb{Z})$, thus with the property:

$$\mathbb{H} = \bigcup_{\gamma \in \mathrm{SL}_2(\mathbb{Z})} \gamma \mathfrak{F}$$

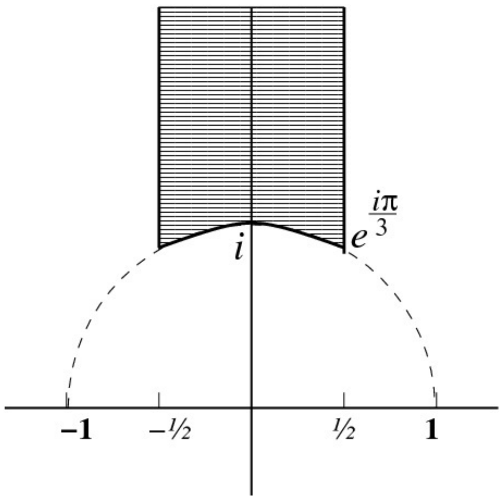
with intersections allowed only on the boundary points of $\gamma\mathfrak{F}$, i.e.

$$(\gamma_1\mathfrak{F})^\circ \bigcap (\gamma_2\mathfrak{F})^\circ = \phi \quad \text{if} \quad \gamma_1 \neq \gamma_2,\ \gamma_1, \gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$$

where $(\gamma_1\mathfrak{F})^\circ$ is the interior of $\gamma_1\mathfrak{F}$

Theorem. *A fundamental domain for the action of* $\mathrm{SL}_2(\mathbb{Z})$ *in* $\mathbb{H}$ *is*

$$\mathfrak{F} = \left\{ z \mid |z| \geq 1, |\mathfrak{Re}(z)| \leq \frac{1}{2} \right\}$$



Proof. We begin by proving that given $z \in \mathbb{H}$, there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma z \in \mathfrak{F}$. This will follow from the following claim.

Claim : Given $z \in \mathbb{H}$, there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\mathfrak{Im}(\gamma z)$ is maximum possible and for such a γ, $|\gamma z| \geq 1$.

The existence of $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\mathfrak{Im}(\gamma z)$ is maximum possible follows from the fact that

$$\mathfrak{Im}(\gamma z) = |cz + d|^{-2}\mathfrak{Im}(z),$$

and the fact that for a given $z \in \mathbb{H}$, $|cz + d|$ tends to infinity as (c, d) (which are pair of coprime integers) tends to infinity, i.e., when $|c| + |d|$ tends to infinity. Note that the set of coprime integers (c, d) is a single orbit for the action of $\mathrm{SL}_2(\mathbb{Z})$ with the isotropy subgroup of the point $(1, 0)$ being the group of upper triangular integral unipotent matrices.

Assume that $\gamma_\circ \in \Gamma$ is such that $\mathfrak{Im}(\gamma_\circ z)$ is the maximum possible, and assume without loss of generality that $|\mathfrak{Re}(\gamma_\circ z)| \leq \frac{1}{2}$. If $\gamma_\circ z \notin \mathfrak{F} \Rightarrow |\gamma_\circ z| < 1$. In this case $\mathfrak{Im}(S\gamma_\circ z) = \frac{\mathfrak{Im}(\gamma_\circ z)}{|\gamma_\circ z|^2} > \mathfrak{Im}(\gamma_\circ z)$, a contradiction, hence we have that $\gamma_\circ z \in \mathfrak{F}$. ∎

Corollary. $\Gamma = \mathrm{SL}_2(\mathbb{Z}) = \langle S, T \rangle$.

Proof. The proof above shows that any element of $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\pm 1$ is a product of S, T, since for any $\gamma \in \Gamma$, z_0 an interior point of $\mathfrak{F}$, $\gamma \cdot z_0$ can be brought back to $\mathfrak{F}$ using the group generated by S, T. (To prove this, we will need to use the easy fact that $\mathrm{SL}_2(\mathbb{Z})$ has no stabilizer in the interior of $\mathfrak{F}$.)

□

Eisenstien Series

For f a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$, considering the action of $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ on f, we get $f(z) = (-1)^k f(z)$, hence for f to be non-zero, k should be an even positive integer.

Let k be an even positive integer greater than 2. For $z \in \mathbb{H}$, we define

$$G_k(z) \underset{def}{=} \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k}.$$

It can be seen that this double sum is absolutely convergent (for $k \geq 4$), and is uniformly convergent in any compact subset of $\mathbb{H}$, hence $G_k(z)$ is a holomorphic function on $\mathbb{H}$. Clearly, $G_k(z) = G_k(z+1)$, and the Fourier expansion of G_k has no-non negative terms as the limit of $G_k(z)$ is finite as $z \to i\infty$:

$$\lim_{z\to i\infty} G_k(z) = \sum_{n\neq 0} n^{-k} = 2\zeta(k).$$

Finally, we have that

$$G_k(-1/z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(n-m/z)^k} = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{z^k}{(nz-m)^k} = z^k G_k(z).$$

Hence $G_k(z)$ satisfies the criterion for being a modular form, giving us first example of modular forms $G_k(z) \in M_k(\Gamma)$.

With some computation, one shows that $G_k(z)$ has the following q-expansion:

$$G_k(z) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n\right),$$

where B_k is the k^{th} Bernoulli coefficient obtained as an expansion of

$$\frac{x}{e^x - 1} = \sum_{l=0}^{\infty} B_k \frac{x^k}{k!}$$

and $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$.

We define the Eisenstein Series $E_k(z)$ as the normalized version of $G_k(z)$:

$$E_k(z) = \frac{1}{2\zeta(k)} G_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

The Eisenstein series $E_k(z)$ have rational q-expansion coefficients. The first few $E_k(z)$ are:

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n,$$

$$E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n,$$

$$E_8(z) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n,$$

$$E_{10}(z) = 1 - 264 \sum_{n=1}^{\infty} \sigma_9(n) q^n.$$

It can be seen that for the Eisenstien series $E_k(z)$, the Fourier coefficients have the bound $|a_n| = O(n^{k-1})$.

Theorem. *The space of modular forms* (M_*) *is a graded algebra,* $M_* = \langle E_4, E_6 \rangle$*, i.e.* M_k *is generated by* $E_4^a E_6^b$*, where* $4a + 6b = k$*.*

Definition. $j(z) = \frac{1728 E_4^3}{E_4^3 - E_6^2}$ *is a modular function of weight* 0

Theorem. *The space of modular functions of weight 0 is isomorphic to* $\mathbb{C}(j)$*.*

Another way of defining modular forms

Given $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}), z \in \mathbb{H}$, define a **factor of automorphy** $j(g, z)$ to be $j(g, z) = (cz + d)$. For a modular form $f : \mathbb{H} \to \mathbb{C}$ of weight k,

$$f(\gamma z) = j(\gamma, z)^k f(z), \quad \forall \gamma \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

A factor of automorphy satisfies the following defining condition, called the *cocycle condition*:

$$j(g_1 g_2, z) = j(g_1, g_2 z) j(g_2, z) \quad \forall g_1, g_2 \in \mathrm{SL}_2(\mathbb{R}), z \in \mathbb{H}$$

Another way of defining modular forms is to consider functions of the following type:

$$\phi_f : \mathrm{SL}_2(\mathbb{R}) \to \mathbb{C},$$

with the property:

$$\phi_f(\gamma g m) = \phi_f(g)\chi_k(m), \quad \gamma \in \mathrm{SL}_2(\mathbb{Z}), \quad \chi_k(m) = e^{ik\theta},$$

where

$$m = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \in \mathrm{SO}(2).$$

For a modular form $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$, define

$$\phi_f(g) = f(gi)j(g,i)^{-k}, \quad g \in \mathrm{SL}_2(\mathbb{R}).$$

Claim. *For* $\gamma \in \mathrm{SL}_2(\mathbb{Z}), \phi_f(\gamma g) = \phi_f(g)$.

Proof. By the cocycle condition satisfied by $j(g,z)$ we have:

$$\begin{aligned} \phi_f(\gamma g) &= f(\gamma g i)j(\gamma g, i)^{-k} \\ &= f(\gamma(gi))j(\gamma,(gi))^{-k} j(g,i)^{-k}, \end{aligned}$$

but since f is a modular form of weight k, $f(\gamma z) = j(\gamma,z)^k f(z)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Therefore:

$$\phi_f(\gamma g) = f(gi)j(g,i)^{-k} = \phi_f(g),$$

completing the proof of the claim. □

Claim. *For* $m \in \mathrm{SO}(2), \phi_f(gm) = \phi_f(g)\chi_k(m)$. *(Recall that* $\mathrm{SO}(2)$ *is the stabilizer of* i*.)*

Proof. Once again, using the cocycle condition satisfied by $j(g,z)$, we have:

$$\begin{aligned} \phi_f(gm) &= f(gmi)j(gm,i)^{-k} \\ &= f(g(mi))j(g,(mi))^{-k} j(m,i)^{-k} \\ &= f(g,i)j(g,i)^{-k} j(m,i)^{-k} \quad \text{(since } mi = i\text{)} \\ &= \phi_f(g)(-i\sin\theta + \cos\theta)^{-k} \\ &= \phi_f(g)(e^{-i\theta})^{-k} \\ &= \phi_f(g)e^{ik\theta} \\ &= \phi_f(g)\chi_k(m). \end{aligned}$$

□

Shimura's Slash Notation

We introduce what's called Shimura's slash notation which is very useful for the theory of modular forms.

Let $\mathrm{GL}_2^+(\mathbb{Q})$ denote the subgroup of $\mathrm{GL}_2(\mathbb{Q})$ consisting of matrices with positive determinant. Define

$$f(z)|[\gamma]_k \underset{def}{=} (\det(\gamma))^{k/2}(cz+d)^{-k}f(\gamma z), \quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}).$$

(The determinant factor is added so that diagonal matrices act trivially.) It can be seen that:

$$f(z)|[\gamma_1\gamma_2]_k = (f(z)|[\gamma_1]_k)|[\gamma_2]_k,$$

and that f is a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$ if and only if

$$f(z)|[\gamma]_k = f, \quad \forall \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

(besides holomorphy conditions at infinity).

Modular forms for congruence subgroups

Suppose that $\Gamma \supset \Gamma(N)$ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of level N. We say that $f \in M_k(\Gamma)$ if f is a holomorphic function on $\mathbb{H}$ and it satisfies:

1. $f(z)|[\gamma]_k = f, \quad \forall \gamma \in \Gamma$
2. $\forall \gamma \in \mathrm{SL}_2(\mathbb{Z}), f|[\gamma]_k(q) = \sum_{n\geq 0} a_n q^{\frac{n}{N}}$.

The second condition comes into picture as $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma(N) \subset \Gamma$. Therefore, $f(z+N) = f(z)$, hence by condition (1), $f|[\gamma]_k(z+N) = f|[\gamma]_k(z)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Hecke Operators

Let $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$, $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, a congruence subgroup. Then it can be seen that the double coset $\Gamma\gamma\Gamma$ is a finite union of cosets: $\Gamma\gamma\Gamma = \bigsqcup_{i=1}^{l} \Gamma\gamma_i$. We define certain operators on the space of modular forms, called the Hecke operators, as:

$$T_\gamma(f) = f|[\Gamma\gamma\Gamma]_k \stackrel{def}{=} \sum_{i=1}^{l} f|[\gamma_i]_k.$$

The most conventional Hecke operators are

$$T_n = \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \mathrm{SL}_2(\mathbb{Z}),$$

acting on the space of modular forms of weight k; these are a commuting set of operators.

As a specific example, note that:

$$T_p = \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i=0}^{p-1} \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} \bigsqcup \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

It is known that

$$T_m T_n = T_{mn},$$

if $(m, n) = 1$.

The space of cusp forms $S_k(\mathrm{SL}_2(\mathbb{Z}))$, carries a hermitian form, called the Petersson inner product:

$$\langle f_1, f_2 \rangle = \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}} y^k f_1(z) \bar{f}_2(z) \frac{dxdy}{y^2} = \int_{\mathfrak{F}} y^k f_1(z) \bar{f}_2(z) \frac{dxdy}{y^2}.$$

with respect to which the Hecke operators are hermitian:

$$\langle T_m f_1, f_2 \rangle = \langle f_1, T_m f_2 \rangle.$$

Thus we have a commuting set of hermitian operators on a finite dimensional space of modular forms, which can then be simultaneously diagonalized for all the Hecke operators T_m, i.e., there exists a basis of modular forms f_n such that:

$$T_m(f_n) = \lambda_m(n) f_n, \quad \forall m.$$

It can be seen that $a_1(f_n) \neq 0$, which we can then normalize to be 1, in which case,

$$\lambda_m(n) = a_m(f_n).$$

As the Hecke operators are hermitian, their eigenvalues are real, thus the Fourier coefficients of Hecke eigenforms are real (assuming $a_1 = 1$). In fact, the space of cusp forms $S_k(\mathrm{SL}_2(\mathbb{Z}))$ is a vector space defined over $\mathbb{Q}$ (since the space of all modular forms is generated by $E_4^a E_6^b$, there is a natural $\mathbb{Q}$ structure on the space of modular forms through the basis consisting of $E_4^a E_6^b$, or through modular forms with q-expansion in $\mathbb{Q}$.) This $\mathbb{Q}$-structure on the space of modular forms, or on cusp forms, is invariant under the Hecke operators. Therefore the eigenvalues of Hecke operators are totally real algebraic numbers.

Theorem. *(Hecke) If* $f = \sum a_n q^n$ *is a cusp form of weight* k*, then* $|a_n| = O(n^{k/2})$*, i.e. there exists* $c > 0$ *such that* $|a_n| \leq cn^{k/2}$ *for all* $n > 0$*.*

Proof. Observe that $\psi_f(z) = f(z)y^{k/2}$ is a modular function, i.e. $\mathrm{SL}_2(\mathbb{Z})$ invariant. Since f is a cusp form, so it vanishes at $i\infty$ exponentially, therefore:

$$|\psi_f(z)| \leq M \quad \text{for some } M > 0,$$

for all $z \in \mathbb{H}$. (To elaborate, ψ_f being a modular function, one needs to prove the above only inside the fundamental domain $\mathfrak{F}$. The part of the fundamental domain below any horizontal line is compact, so ψ_f in this part of the fundamental domain is bounded; it needs to be checked that ψ_f is bounded on the part of the fundamental domain above any horizontal line too. Under the mapping $z \to e^{2\pi iz}$, the function $\psi_f(z) = f(z)y^{k/2}$ becomes the function $F_f(e^{-2\pi y})y^{k/2}$ where F_f is the associated function on D and $y \to \infty$ which by the cuspidality of f tends to zero, completing the proof of boundedness of ψ_f on the part of the fundamental domain above any horizontal line.)

For any point $y > 0$, and any integer $n > 0$, we have:

$$|a_n|e^{-2\pi ny} = \frac{1}{2\pi}\left|\int_0^1 f(x+iy)e^{-2\pi inx}dx\right| \leq \frac{1}{2\pi}\int_0^1 |f(x+iy)|dx \leq \frac{1}{2\pi}y^{-k/2}M.$$

Therefore,

$$|a_n| \leq \frac{M}{2\pi}y^{-k/2}e^{2\pi ny},$$

for any $n > 0$ and any $y > 0$. Taking $y = \frac{1}{n}$, gives

$$|a_n| \leq \frac{M}{2\pi}n^{k/2}e^{2\pi} = cn^{k/2},$$

which is the desired conclusion. □

Corollary. *Cusp forms give rise to the "Error terms" in the Fourier expansion of noncuspidal modular forms, i.e., given any modular form* $g \in M_k(\mathrm{SL}_2(\mathbb{Z}))$, $g = \lambda E_k + f$*, where* f *is a cusp form. Hence* $a_n(g) = \lambda a_n(E_k) + a_n(f)$ *with* $|a_n(E_k)| = O(n^{k-1})$ *whereas* $|a_n(f)| = O(n^{k/2})$*.*

Remark: The relatively simple proof of Hecke's theorem should be contrasted with the much deeper theorem of Deligne on Ramanujan bound — proved as a consequence of his proof of the Weil conjectures — which gives a bound of $|a_n(f)| = O(n^{(k-1+\epsilon)/2})$ for any $\epsilon > 0$, for f any holomorphic cusp form of integral weight k. The Hecke bound is valid for half integral weight modular forms, and although Ramanujan bound is expected for half integral weight modular forms too, it is far from being a theorem.

L-functions

For $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$, $f(z) = \sum_{n=1}^{\infty} a_n q^n$, define the following function of the complex variable s:

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

called the L-function associated to the cusp form.

By Hecke's estimate on Fourier coefficients, these functions $L(f,s)$ are analytic functions of s in the half-region of the complex plane $Re(s) > k/2+1$. Hecke proved that they have analytic continuation to the whole complex plane as an entire function, and satisfy a functional equation.

If f is an eigenform for all the Hecke operators T_p, and $a_1 = 1$, then it is known that the coefficients are multiplicative, i.e., $a_{mn} = a_n a_m$, whenever $(m,n) = 1$. In fact, we have the following Euler product formula

$$L(f,s) = \prod_p \frac{1}{(1 - \frac{a_p}{p^s} + \frac{p^{k-1}}{p^{2s}})}.$$

For a cusp form f of weight k, we define

$$\Lambda_f(s) \stackrel{def}{=} (2\pi)^{-s}\Gamma(s)L(f,s)$$

Theorem. $\Lambda_f(s)$ *has analytic continuation on the whole complex plane, and it satisfies the following functional equation:*

$$\Lambda_f(s) = (-1)^{k/2}\Lambda_f(k-s)$$

Remark : In our lectures, we have not emphasized L-functions so much, but for many people, these give the most important aspect of modular forms. There are many L-functions associated to modular forms, for example the so-called symmetric power L-functions, whose analytic continuation and functional equation are important open problems. It is a theorem of Hecke that the theorem above has a converse: any L-function with analytic continuation, and the above functional equation, and some estimates on growth properties arises from modular forms for $\mathrm{SL}_2(\mathbb{Z})$.

Elliptic Curves

An elliptic curve over a field K is a projective non-singular curve of genus one over K with a specific base point. If the $\mathrm{Char}(K) \neq 2, 3$, then we have the *short Weierstrass form* of the elliptic curve as

$$y^2 = x^3 + Ax + B$$

which has discriminant $= -16(4A^3 + 27B^2)$. The above curve is non singular if the discriminant is nonzero.

Definition. *A lattice in the complex plane* $\mathbb{C}$ *is a discrete subgroup of the form* $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$*, where* ω_1 *and* ω_2 *are linearly independent over real numbers. Two lattices* Λ *and* Λ' *are said to be equivalent if there exists* $\lambda \in \mathbb{C} - \{0\}$*, with* $\lambda\Lambda = \Lambda'$*. A complex torus* $\mathbb{T}$ *is a quotient* $\mathbb{C}/\Lambda$ *of the complex plane with the lattice* Λ

It can be shown that any complex analytic isomorphism between two tori actually corresponds to an equivalence between the associated lattices.

Any complex torus $\mathbb{T} = \mathbb{C}/\Lambda$ can be given an algebraic structure using the Weierstrass $\wp$ and $\wp'$ functions:

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3,$$

where

$$g_2 = 60 \sum_{\lambda \in \Lambda \backslash 0} \frac{1}{\lambda^4}, \quad g_3 = 140 \sum_{\lambda \in \Lambda \backslash 0} \frac{1}{\lambda^6}.$$

This allows one to identify the set of complex tori and elliptic curves over $\mathbb{C}$.

The following lemma brings out the *first relationship* between elliptic curves and 'modular varieties' which are the 'homes' for modular forms. There is a similar relationship in much greater generality for abelian varieties with level structures and a given endomorphism rings, and points on certain 'Shimura varieties'.

Lemma. *Points in* $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ *are in bijective correspondence with the isomorphism classes of Elliptic curves over* $\mathbb{C}$*. The correspondence is given by* $\tau \in \mathbb{H} \to E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$*.*

Given an Elliptic curve E over $\mathbb{Q}$, we can reduce it mod p. If the reduced curve $\overline{E}$ is non-singular, then we call p a prime of good reduction for E, otherwise we call p a prime of bad reduction.

For a prime p, if E has a good reduction mod p, define an integer

$$a_p(E) = p + 1 - \#\overline{E}(\mathbb{F}_p).$$

One can define $a_p(E)$ even for primes of bad reduction, but we shall not do so here.

The number of points of E over $\mathbb{F}_p$ as p varies, can be packaged in what's called the *Hasse-Weil L-function* of E, as

$$L(E, s) = \prod_p L_p(E, s) = \prod_p \frac{1}{(1 - \frac{a_p(E)}{p^s} + \frac{p}{p^{2s}})}.$$

The following conjecture (now a theorem of Wiles) brings out the *second relationship* — a much deeper one than the first one above — between elliptic curves and modular forms.

Conjecture (Shimura-Taniyama-Weil)**.** *$L(E, s)$ is the L-function of a modular form on $\Gamma_0(N)$ of weight 2, and as a consequence, there exists a bijective correspondence between cusp forms on $\Gamma_0(N)$ (for some integer N) of weight 2 with integral Fourier coefficients, and Elliptic curves (up to isogeny) over $\mathbb{Q}$.*

As is well-known, the Shimura-Taniyama-Weil conjecture was proved by A. Wiles and others in the mid 90's, and as a consequence Fermat's Last Theorem was proved.

References

[1] Jean-Pierre Serre, *A course in arithmetic*, Springer Science & Business Media, Volume 7, 2012.

[2] Neal Koblitz, *Introduction to elliptic curves and modular forms*, Springer Science & Business Media, Volume 97, 2012.

[3] Daniel Bump, *Automorphic forms and representations*, Cambridge university press, Volume 55, 1998.

[4] Joseph H Silverman *The arithmetic of elliptic curves*, Springer Science & Business Media, Volume 106, 2009.