Modular Forms III

Shiv Yajnik

October 2024

These notes are based on Sections 5.5-5.9 from *Invitation to the Mathematics of Fermat-Wiles* by Yves Hellegouarch.

1 Review from Modular Forms II (Sections 5.3-5.4)

Zach L.'s lecture began by introducing a subgroup of the *Möbius transformations* on the Poincaré upper half plane $\mathcal{H} := \{\mathrm{Im}(z) > 0\} \subset \mathbb{C}$. These look like:

$$z \mapsto \frac{az+b}{cz+d}$$

with constants $a, b, c, d \in \mathbb{C}$ Möbius transformations are special. If we require $a, b, c, d \in \mathbb{R}$ such that $ab - cd = 1$, such transformations are *all* of the biholomorphic maps from the upper half plane to itself! Furthermore, if upon the upper half plane we bestow the hyperbolic metric–which yields a certain definition of distance[1]–these transformations become *isometries*–or maps that preserve angles and distance on $\mathcal{H}$ with respect to the metric. Finally, Möbius transformations on the complex plane also ascend to transformations on $\mathbb{P}^1_{\mathbb{C}} \cong \mathbb{S}^2$; if we look at the class of transformations where $a, b, c, d \in \mathbb{C}$ such that $d = \bar{a}$, $c = -\bar{b}$, and $|a|^2 + |b|^2 = 1$, these become the group of rotations isomorphic to $SO(3)$ on the sphere.

Equivalently, we can define this as a left group action of $SL(2, \mathbb{Z}) \times \mathcal{H} \to \mathcal{H}$, where we say

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \frac{az+b}{cz+d}$$

But notice that the group action is invariant under scaling the matrix:

$$\lambda \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \frac{\lambda az+\lambda b}{\lambda cz+\lambda d} = \frac{az+b}{cz+d}$$

This makes the group action non-transitive; in other words, for every z_0, there may be more than one matrix A such that $A \cdot z = z_0$. To remedy this, we take the group quotient $SL(2, \mathbb{Z})/\{I, -I\} = PSL(2, \mathbb{Z})$ (this is legal, as $-I$ and I generate a normal subgroup of $SL(2, \mathbb{Z})$). Now, $PSL(2, \mathbb{Z})$ is guaranteed to act transitively on $\mathcal{H}$. We call $PSL(2, \mathbb{Z})$ *the modular group*.

For the purposes of studying modular forms, we require $a, b, c, d \in \mathbb{Z}$. We introduced these transformations for the following reason:

Recall that we had from earlier that if $Y^2 = 4X^3 - g_4 X - g_6$ is the Weierstrass cubic associated to $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$, we have for $k \geq 2$, we have defined

$$G_{2k}(\tau) := G_{2k}(\Lambda_\tau)$$
$$\Delta(\tau) := \Delta(\Lambda_\tau) = g_4(\Lambda_\tau)^3 - 27 g_6(\Lambda_\tau)^2$$
$$j(\tau) = j(\Lambda_\tau) = 1728 \frac{g_4(\Lambda_\tau)^3}{\Delta(\Lambda_\tau)}$$

These followed the rules

$$G_{2k}\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{2k} G_{2k}(\tau)$$

[1] Curves of minimal on the hyperbolic metric are given by semicircles whose endpoints are on the real axis, so you can find the distance between two points by finding said semicircle that those two points lie on.

$$\Delta\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^{12}\Delta(\tau)$$

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

This happened because of the transformation rules

$$G_{2k}(\alpha\Lambda)=\alpha^{-2k}G_{2k}(\Lambda)$$

$$\Delta(\alpha\Lambda)=\alpha^{-12}\Delta(\Lambda)$$

$$j(\alpha\Lambda)=j(\Lambda)$$

some of which we had discussed in previous lectures.

$G_{2k},\ \Delta$, and j turned out to be examples of functions that satisfied requirements of *modularity* for modular forms.

It turns out that the modular group is generated by the following two matrices:

$$S=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}\quad T=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$$

Now, we have some definitions:

Definition 1.1. Let H be a subgroup of $PSL(2,\mathbb{Z})$ and let $k\in\mathbb{Z}$. A *weakly modular form of weight* k for $SL(2,\mathbb{Z})$ is a meromorphic function $f:\mathcal{H}\to\mathcal{H}$ satisfying

$$f\left(A\cdot\tau\right)=(A_{21}\tau+A_{22})^{k}f(\tau)$$

For every automorphism $A\in H$ A function is *weakly modular* if it is a weakly modular form of weight 0.

Definition 1.2. A *fundamental domain* of $\mathcal{H}$ for the group H is an open subset U of $\mathcal{H}$ where

- $|U\cap(H\cdot z)|=1$ for every $z\in\mathcal{H}$
- $|\bar{U}\cap(H\cdot z)|\geq 1$ for every $z\in\mathcal{H}$.

An example of such a domain is $D=\{\tau\in\mathcal{H}:|\operatorname{Re}(\tau)|<\frac{1}{2},\ |\tau|>1\}$; two equivalent elements of $\bar{D}$ must lie on ∂D.[2]

Then, we introduced *congruence subgroups*: Define $\pi_N: SL(2,\mathbb{Z})\to SL(2,\mathbb{Z}/N\mathbb{Z})$ by

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\longmapsto\begin{bmatrix}\bar{a} & \bar{b}\\ \bar{c} & \bar{d}\end{bmatrix}$$

Definition 1.3. The *principal congruence subgroup of level* N, denoted $\Gamma(N)$, is the kernel of π_N. Equivalently,

$$\Gamma(N):=\{A\in SL(2,\mathbb{Z}):A\equiv I\mod N\}$$

The *Hecke subgroups* of level n are given by:

$$\Gamma_0(N):=\{A\in SL(2,\mathbb{Z}):A_{21}\equiv 0\mod N\}$$

$$\Gamma^0(N):=\{A\in SL(2,\mathbb{Z}):A_{12}\equiv 0\mod N$$

$\Gamma\leq SL(2,\mathbb{Z})$ is a *congruence subgroup* if $\Gamma\supset\Gamma(N)$ for some $N\geq 1$.

It turns out that $\Gamma(N)$ is a normal subgroup Γ_θ of $PSL(2,\mathbb{Z})$, whereas the subgroup generated by S and T^2, which were the symmetries of the function θ^8 from Jacobi theta-function theory (see Zach K.'s lecture), is not a normal subgroup of $PSL(2,\mathbb{Z})$. Furthermore, $SL(2,\mathbb{Z})/\Gamma(N)\cong SL(2,\mathbb{Z}/N\mathbb{Z})$.

[2] ∂D is notation for the boundary of D.

Definition 1.4. A weakly modular form of weight k[3] becomes *meromorphic of weight k relative to* $H \supset \Gamma(N)$ if in addition we have the *condition of meromorphy at the cusps*, meaning that for all $B \in SL(2,\mathbb{Z})$, the function

$$(B_{21}\tau + B_{22})^{-k} f(B \cdot \tau)$$

is the limit of a Fourier series expansion in powers of $q^{1/N}$ (with $q = e^{2\pi i\tau}$ converging in $C = \{0 < |q| < 1\}$, where only a finite number of terms have strictly negative exponents.

A meromorphic modular form f becomes a *modular form* if f is entire (including at ∞). The Eisenstein series $G_{2k}(\tau)$ is an example of a modular form with weight $2k$ for $SL(2,\mathbb{Z})$.

A modular form is a *cusp* form[4] if it vanishes at the *cusps*, which are the sets $\{(H \cdot z)/H\}$ with $z \in \mathbb{Q} \cup \{i\infty\}$. $\varphi(\tau) = \theta_2^8(0,\tau)\theta_3^8(0,\tau)\theta_4^8(0,\tau)$ is an example of a cusp form of weight 12 for $SL(2,\mathbb{Z})$.

A meromorphic modular form of weight 0 is a *modular function.* $\theta^8(\tau)$ is an example of a modular form of weight 4 for $\Gamma_\theta \supset \Gamma(2)$.

Then, we introduced some notation: Let $H \leq SL(2,\mathbb{Z})$, $M_k(H)$ (resp. $S_k(H)$) be the complex vector space of meromorphic modular forms (resp. cusp forms) of weight k relative to H.

Let $f \in M_k(H)$, $\gamma \in GL(2,\mathbb{R})$. We write

$$f|_k\gamma(\tau) = (\det\gamma)^{k/2}(\gamma_{21}\tau + \gamma_{22})^{-k} f(\gamma(\tau))$$

The modularity condition can be rewritten as

$$f|_k\gamma = f \quad \forall \gamma \in H$$

We can check that

$$f|_k\gamma_1\gamma_2 = (f|_k\gamma_1)|_k\gamma_2$$

2 Section 5.5: The Fifth Operation of Arithmetic

The rest of Zach L.'s lecture described the space of modular forms of weight k for $SL(2,\mathbb{Z})$. Some big results were that the compactification of $\mathcal{H}/PSL(2,\mathbb{Z})$, denoted $\widehat{\mathcal{H}/PSL(2},\mathbb{Z})$, is a Riemann surface of genus zero, meaning that it is isomorphic to the Riemann sphere. We know precisely what this isomorphism is, and furthermore, every Weierstrass cubic defined over $\mathbb{C}$ can be parametrized by elliptic functions. Furthermore, the functions on $\widehat{\mathcal{H}/PSL(2},\mathbb{Z})$ are modular functions.

Recall that in Zach K.'s lecture, we proved the formula

$$\left(\sum_{-\infty}^{\infty} z^{n^2}\right)^4 = 1 + 8\sum_{m=1}^{\infty}\left(\sum_{d|m\ 4\nmid d} d\right) z^m$$

by Jacobi. We will show that the results from Zach L.'s lecture will lead to identities such as this.

Let M_k (resp. S_k) denote the complex vector space of modular forms (rep. cusp forms) of weight k for the modular group $PSL(2,\mathbb{Z})$. The map $M_k \to \mathbb{C}$ given by $f \mapsto f(\infty)$ is a $\mathbb{C}$-linear form. Since cusp forms vanish at ∞ by definition, the kernel of this map is S_k. We also have the theorem from section 5.3 (Theorem 5.3.1) which states that for $k \geq 2$,

$$G_{2k}(\tau) = 2\zeta(2k) + \frac{2(2i\pi)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n \quad \sigma_h(n) = \sum_{d>0\ d|n} d^h \quad q = e^{2\pi i\tau}$$

[3]This is referred to as the *modularity condition*

[4]such a form is also known as *parabolic.*

Which means that in particular, means that $G_{2k}(i\infty) = 2\zeta(2k) \neq 0$. By linearity, we now know that the aforementioned map $M_k \to \mathbb{C}$ is onto and that therefore G_{2k} generates the rest of M_k. So we can write

$$M_{2k} = S_{2k} \oplus \mathbb{C}G_{2k} \quad k \geq 2$$

We had defined the order of f at $\tau_0 \in \mathcal{H}$ to be the integer n such that $\frac{f}{(\tau-\tau_0)^n}$ is an invertible holomorphic function in some neighborhood of τ_0; we denote this by $\nu_{\tau_0}(f)$. Equivalently, around each $\tau_0 \in \mathcal{H}$, we can write $f = (\tau - \tau_0)^n h(\tau)$ where h is a holomorphic function, and $n = \nu_{\tau_0}(f)$. It follows from the modularity of f that if $\gamma \in G$, then $\nu_{\tau_0}(f) = \nu_{\gamma(\tau_0)}(f)$; so we can write this as $\nu_P(f)$, where P is the projection of τ_0 to $\mathcal{H}/G$.

We proved that a non-zero meromorphic modular form f of weight k relative to $SL(2,\mathbb{Z})$ must satisfy

$$\nu_\infty(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_\rho(f) + \sum_{P\in\mathcal{H}/PSL(2,\mathbb{Z})}^{*} \nu_P(f) = \frac{k}{12}$$

Where the astrisk indicates that we take the sum over $(\mathcal{H}/G) \setminus \{i, \rho\}$, and i and ρ are the projections of i and $e^{2\pi i/3}$ to $\mathcal{H}/PSL(2,\mathbb{Z})$. (This is Theorem 5.4.1 from the Hellegouarch.)

Proposition 2.1. *We have the following*

(i) $M_k = \{0\}$ *if* k *is odd, negative, or equal to* 2.

(ii) If $k = 0, 4, 6, 8, 10$, *then* $\dim_{\mathbb{C}} M_k = 1$ *with basis* 1, G_4, G_6, G_8, *and* G_{10}, *respectively; furthermore,* $S_k = \{0\}$.

(iii) Multiplication by Δ *is an isomorphism* $M_k \to S_{k+12}$.

Proof. Parts (i) and (ii) follow from Theorem 5.4.1.

(i) The possible values on the LHS of Theorem 5.4.1 are $0, \frac{1}{3}, \frac{1}{2}, \frac{5}{6}, 1, 1\frac{1}{3}, 1\frac{1}{2}, 1\frac{5}{6}, 2$, and so on; if k were odd, the RHS could never match the LHS.

By Theorem 5.4.1, if $k = 2$, then for $f \in M_2 \setminus \{0\}$, f satisfies

$$\nu_\infty(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_\rho(f) + \sum_{P\in\mathcal{H}/PSL(2,\mathbb{Z})}^{*} \nu_P(f) = \frac{1}{6}$$

All of $\nu_\infty(f)$, $\nu_i(f)$, $\nu_\rho(f)$, and $\nu_P(f)$ have to be nonnegative integers because modular forms are by definition entire. Therefore, the smallest value other than 0 that the LHS can take is $\frac{1}{3} > \frac{1}{6}$. Therefore, f has order 0 at all points. But the only way that f can satisfy the modularity condition $f(A \cdot \tau) = (A_{21}\tau + A_{22})^2 f(\tau)$ for all $A \in SL(2,\mathbb{Z})$ is if $f \equiv 0$. Therefore, $M_2 = \{0\}$

If k is negative, since $\nu_\infty(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_\rho(f) + \sum^{*}_{P\in\mathcal{H}/PSL(2,\mathbb{Z})} \nu_P(f)$ cannot be a negative number, we get by similar reasoning that $f \equiv 0$, which means $M_k = \{0\}$ for $k \in \mathbb{Z}^-$.

(ii) For $k = 0$, it follows by reasoning similar to that from before that f must be a constant function, but this time, the modularity condition becomes $f(A \cdot \tau) = f(\tau)$, which means that f can be any constant function. So $M_0 \cong \mathbb{C}$. Then, observe that if $\nu_\infty(f) \geq 1$, then

$$\nu_\infty(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_\rho(f) + \sum_{P\in\mathcal{H}/PSL(2,\mathbb{Z})}^{*} \nu_P(f) \geq 1 > \frac{k}{12}$$

For $k = 4, 6, 8, 10$, contradicting Theorem 5.4.1. Therefore, in these cases, we conclude that $S_k = \{0\}$ and, from the decomposition $M_k = S_k \oplus G_k$, $M_k = \mathbb{C}G_k$.

(iii) Since Δ is associated with a smooth elliptic curve, it does not vanish on $\mathcal{H}$, so we can conclude that multiplication by Δ defines an isomorphism $M_k \to S_{k+12}$.

□

Remark. For those who know about divisors on algebraic curves: An alternative approach may involve using the Riemann-Roch theorem, which states that for any divisor D on a Riemann surface, we have

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1$$

where K_C is the canonical divisor that contains the zeroes and poles of a meromorphic differential 1-form, and $\ell(D)$ is the dimension of the space of meromorphic f where $\operatorname{div}(f) + D \geq 0$. In our context, the Riemann surface is isomorphic to $\mathbb{P}^1_{\mathbb{C}}$, and the functions on it are modular functions, which means $g = 0$. So we can use divisors to place bounds on the $\ell(D)$ in different cases, where D contains the points where the modular form is required to vanish.

Corollary 2.1.1. *The dimension for general M_k for $k \geq 0$ is given by*

$$\dim_{\mathbb{C}} M_k = \begin{cases} \lfloor \frac{k}{12} \rfloor & k \equiv 2 \mod 12 \\ \lfloor \frac{k}{12} \rfloor + 1 & \textit{else} \end{cases}$$

Proof. It follows from (ii) in Proposition 2.1 that the formula holds for $1 \leq k \leq 11$. Then, to get the result, we apply (iii) from 2.1 to get that

$$M_k \cong M_{k-12} \oplus \mathbb{C}G_k \Longrightarrow \dim_{\mathbb{C}} M_k = \dim_{\mathbb{C}} M_{k-12} + 1$$

which gives us the result. □

Corollary 2.1.2. *A basis of the space M_k is given by $\{G_4^\alpha G_6^\beta : \alpha, \beta \in \mathbb{Z}_{\geq 0},\ 4\alpha + 6\beta = k\}$.*

Proof. It follows from Proposition 2.1 that the statement holds for $k \leq 6$. Then, we can use induction.

Suppose the statement holds for all cases up to $2k$. Note that for $n \geq 1$ and even, we can write $4\alpha + 6\beta = n$ for some $\alpha, \beta \in \mathbb{Z}_{\geq 0}$. To complete the inductive step, we now assume $n = 2k + 2$. G_4^α and G_6^β do not vanish at infinity, so $G_4^\alpha G_6^\beta \notin S_{2k+2}$; by the decomposition $M_{2k+2} = S_{2k+2} \oplus \mathbb{C}G_{2k+2}$, we can write for any $f \in M_{2k+2}$,

$$f = \lambda G_4^\alpha G_6^\beta + g \quad g \in S_{2k+2} \quad \lambda \in \mathbb{C}$$

By (iii) of Proposition 2.1, $g = \Delta h$ for some $h \in M_{2k-10}$. But by the induction hypothesis, h itself is a linear combination of monomials of the form $G_4^\alpha G_6^\beta$, and recall that for $\Delta = g_4^3 - 26g_6^2$, g_4 is a multiple of G_4 and g_6 is a multiple of G_6. So M_{2k+2} mus be spanned by monomials of the form $G_4^\alpha G_6^\beta$.

It remains to show linear independence. Note that it follows from Theorem 5.4.1 that G_4 vanishes only at ρ and G_6 vanishes only at i. This means that $G_4^\alpha G_6^\beta$ has a zero of order α at ρ and a zero of order β at i. Functions with different order zeros cannot be constant multiples of each other; this demonstrates linear independence. □

Now, we introduce a few applications: Recall that we defined $E_{2k}(\tau)$ by

$$G_{2k}(\tau) = \frac{2(2i\pi)^{2k}}{(2k-1)!} E_{2k}(\tau)$$

Since $\dim_{\mathbb{C}} M_8 = 1$, seeing that $E_4^2, E_8 \in M_8$, we can write

$$E_8 = \lambda E_4^2 \quad \lambda \in \mathbb{C}$$

We also saw that the series expansions of these forms look like

$$E_4(\tau) = \frac{1}{240} + q + 9q^2 + 28q^3 + 73q^4 + 126q^5 + 252q^6 + \ldots$$

$$E_8(\tau) = \frac{1}{480} + q + 129q^2 + 2188q^3 + \ldots$$

with $q = e^{2\pi i\tau}$

Looking at the constant terms, we can deduce

$$\lambda = \frac{240^2}{480} = \frac{240}{2} = 120$$

Recall from earlier that

$$G_4(\tau) = 2\zeta(\tau) + \frac{2(2i\pi)^4}{3!}\sum_{n=1}^{\infty}\sigma_3(n)q^n$$

$$G_8(\tau) = 2\zeta(\tau) + \frac{2(2i\pi)^8}{7!}\sum_{n=1}^{\infty}\sigma_7(n)q^n$$

So from observing the coefficients of q, we find

$$\sigma_7(n) = \sigma_3(n) + 120\sum_{m=1}^{n-1}\sigma_3(m)\sigma_3(n-m)$$

Also, since we know $\dim_{\mathbb{C}} M_10 = 1$ and $E_4E_6, E_{10} \in M_{10}$, we can similarly deduce that $\frac{5040}{11}E_4E_6 = E_{10}$ and the identity

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040\sum_{m=1}^{n-1}\sigma_3(m)\sigma_5(n-m)$$

The rest of the section discusses the magnitude of the coefficients a_n in the Fourier series expansion of elements of M_k. The section proves that if $f \in S_k$, then $a_n = O(n^{k/2})$. Tihs leads to a corollary: If $f \in M_k \setminus S_k$, then $|a_n| = O(n^{k-1})$.

Deligne also proved in 1969, that for $f \in S_k$, $|a(n)| = O(n^{(k-1/2+\varepsilon)})$.

Recall that we defined the Ramanujan function:

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

These are the coefficients of Δ. It follows that

$$|\tau(n)| = O(n^{11/2+\varepsilon})$$

Deligne proved the *Ramanujan-Petersson Conjecture*: for p prime,

$$|\tau(p)| \leq 2p^{11/2}$$

3 Section 5.6: The Petersson Hermitian Product

For a given group of transformations, the space of cusp forms forms a Hermitian inner product space; this will lead to the core of our discussion for this half of the lecture, which is Hecke theory. Now, require the following:

- $H \leq PSL(2, \mathbb{Z})$ is a congruence subgroup.
- D_H is a fundamental domain for the action of H on $\mathcal{H}$.
- $S_{2k}(H)$ be the space of cusp forms for the group H–modular forms which vanishe at the cusps of D_H–of weight $2k > 0$.
- Define an invariant measure $d\mu$ on $\mathcal{H}$ by[5]

$$d\mu(t) := y^{-2}dx \wedge dy = \frac{y^{-2}}{-2i}(d\tau \wedge d\bar{\tau})$$

[5]It is a demonstrable fact that this measure is invariant; the proof is a rather messy computation in differential geometry. The definition of this form is based on the hyperbolic metric, and from Section 1 that the Mobius transformations preserve the hyperbolic metric.

Now, we define for $f,\, g \in S_{2k}(H)$ a measure:

$$(f,g)(\tau) := f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^{2k} d\mu(\tau)$$

Proposition 3.1. *The exterior form (f,g) satisfies the relations*

(i) $(f,g) = \overline{(g,f)}$

(ii) $(f,f) \geq 0,\ (f,f) = 0 \Longrightarrow f = 0$

(iii) $(f,g)(\gamma\tau) = (f,g)(\tau)\ \forall \gamma \in H$

Proof. The first two properties are clear by definition. To demonstrate (iii), we observe that for $\gamma \in H$,

$$\begin{aligned}
\mathrm{Im}(\gamma(\tau)) &= \mathrm{Im}\left(\frac{\gamma_{11}\tau + \gamma_{12}}{\gamma_{21}\tau + \gamma_{22}}\right) \\
&= \mathrm{Im}\left(\frac{(\gamma_{11}\tau + \gamma_{12})(\gamma_{21}\bar{\tau} + \gamma_{22})}{|\gamma_{21}\tau + \gamma_{22}|^2}\right) \\
&= \frac{\mathrm{Im}(\gamma_{11}\gamma_{22}|\tau|^2 + \gamma_{12}\gamma_{21}\bar{\tau} + \gamma_{11}\gamma_{22}\tau + \gamma_{12}\gamma_{22})}{|\gamma_{21}\tau + \gamma_{22}|^2} \\
&= \frac{\mathrm{Im}(\tau)(-\gamma_{12}\gamma_{21} + \gamma_{11}\gamma_{22})}{|\gamma_{21}\tau + \gamma_{22}|^2} \\
&= \frac{\mathrm{Im}(\tau)}{|\gamma_{21}\tau + \gamma_{22}|^2}
\end{aligned}$$

Since $\gamma \in H$ and $f, g \in S_{2k}(H)$,

$$\begin{aligned}
f(\gamma\tau) &= (\gamma_{12}\tau + \gamma_{22})^{2k} f(\tau) \\
g(\gamma\tau) &= (\gamma_{12}\tau + \gamma_{22})^{2k} g(\tau)
\end{aligned}$$

$$\begin{aligned}
\Longrightarrow f(\gamma\tau)\overline{g(\gamma\tau)}\,\mathrm{Im}(\gamma(\tau))^{2k} d\mu(\gamma\tau) &= \frac{(\gamma_{12}\tau + \gamma_{22})^{2k} f(\tau)\overline{(\gamma_{12}\tau + \gamma_{22})^{2k} g(\tau)}\,\mathrm{Im}(\tau)^{2k} d\mu(\tau)}{|\gamma_{21}\tau + \gamma_{22}|^{4k}} \\
&= f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^{2k} d\mu(\tau) \\
&= (f,g)(\tau)
\end{aligned}$$

□

Definition 3.2. A *Hilbert space* is an inner product space where the distance metric induced by the norm is complete.

Theorem 3.3. *The space $S_{2k}(H)$ of modular forms of weight $2k > 0$ for H is a Hilbert space of finite dimension for the Petersson Hermitian product:*

$$(f,g) = \int_{D_H} (f,g)(\tau) = \int_{D_H} f(\tau)\overline{g(\tau)} y^{2(k-1)} dx \wedge dy$$

Proof. It suffices to show that the integral converges.

(Step 1) Let $T(\tau) = \tau + N$ be a small translation of H. Choose $D_H = \{0 \leq \mathrm{Re}\{\tau\} \leq N\}$; we partition D_H into D'_H and D''_H so that $D_H = D'_H \cup D''_H$:

$$D'_H := \{\tau \in D : 0 \leq \mathrm{Re}\{\tau\} \leq N;\ y \geq 1\}$$

$$D''_H := \{\tau \in D : 0 \leq \mathrm{Re}\{\tau\} \leq N;\ y \leq 1\}$$

(Step 2) Because of the condition of meromorphy at the cusps, we have

$$f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n\tau/N}$$

$$g(\tau) = \sum_{n=1}^{\infty} b_n e^{2\pi i n\tau/N}$$

These series converge uniformly in D'_H. Identifying $y = \mathrm{Im}(\tau)$, we have

$$\begin{aligned}
|f(\tau)\overline{g(\tau)}y^{2k-1}| &\leq \sum_{m,n=1}^{\infty} |a_m \bar{b_n} e^{2\pi i m\tau/N - 2i\pi n\bar{\tau}/N} y^{2(k-1)} \\
&\leq \sum_{m,n=1}^{\infty} |a_m \bar{b}_n| e^{-2\pi y(m+n)/N} y^{2(k-1)} \\
&= \sum_{\nu=2}^{\infty} c_\nu e^{-2\pi\nu y/N} y^{2(k-1)} \qquad\qquad c_\nu = \sum_{m+n=\nu} |a_m \bar{b}_n|
\end{aligned}$$

The last series converges uniformly on D'_H, which means that

$$\left|\int_{D'} f(\tau)\overline{(g(\tau)}y^{2(k-1)}dxdy\right| \leq N \int_{y=1}^{\infty} \left(c_\nu e^{-2\pi\nu y/N} y^{2(k-1)}\right) dy$$

For $\nu \geq 1$,

$$\begin{aligned}
\int_{y=1}^{\infty} e^{-2\pi\nu y/N} y^{2(k-1)} dy &= e^{-2\pi\nu/N} \int_0^{\infty} e^{-2\pi\nu(y-1)/N} y^{2(k-1)} dy \\
&\leq e^{-2\pi\nu/N} \int_0^{\infty} e^{-2\pi(y-1)/N} y^{2(k-1)} dy \\
&= K e^{-2\pi\nu/N}
\end{aligned}$$

We deduce that

$$\left|\int_{D'} f(\tau)\overline{(g(\tau)}y^{2(k-1)}dxdy\right| \leq N \sum_{\nu=2}^{\infty} K c_\nu e^{-2\pi\nu/N}$$

This is a convergent series because

$$\sum_{\nu=2}^{\infty} c_\nu e^{-2\pi\nu y/N} y^{2(k-1)}$$

is a convergent series, and $\sum_{\nu=2}^{\infty} K c_\nu e^{-2\pi\nu/N}$ is this series with $y = 1$ multiplied by a constant K.

(Step 3) Now, we just need to make sure the integral converges in D'_H, because D''_H minus small neighborhoods containing the cusps is a compact set, and integrals of continuous functions over compact sets exist.

Because there are only finitely many cusps, it suffices to study the integral in a neighborhood V of just *one* cusp P. Let $S \in PSL(2,\mathbb{Z}) : S(P) = \infty$, let $f_0 = f|_S$ and $g_0 = g|_S$.[6]

$$f(S^{-1}\tau) = (S^{21}\tau + S^{22})^{2k} f_0(\tau)$$

$$g(S^{-1}\tau) = (S^{21}\tau + S^{22})^{2k} g_0(\tau)$$

$$\Longrightarrow \int_V f(\tau)\overline{g(\tau)}y^{2(k-1)}dx \wedge dy = \int_{SV} f_0(\tau)\overline{g_0(\tau)}y^{2(k-1)}dx \wedge dy$$

$$(\tau \to P \Rightarrow f, g \to 0) \Longrightarrow (\tau \to \infty \Rightarrow f_0, g_0 \to 0)$$

This reduces to the case in Step 2.

In summary, the series expansion was defined near $i\infty$, so Step 2 ensured convergence in D''_H, a neighborhood around $i\infty$, and Step 3 allowed us to make sure the integral does not blow up around cusps outside of D''_H by using the transformation law to reduce the problem back to convergence in D''_H. This last step is needed especially for subgroups H that are not necessarily $SL(2,\mathbb{Z})$. □

[6] Raised indices indicate the entries of the inverse matrix.

4 Section 5.7: Hecke Forms

One interesting property of modular forms is that their Fourier coefficients $a(n)$ of their expansion in powers of $q = e^{2\pi i\tau}$ are multiplicative functions or linear combinations of multiplicative functions. For example, the Ramanujan function satisfies $\tau(mn) = \tau(m)\tau(n)$ for m, n relatively prime.

Let $m \in \mathbb{Z}^+$, and $f(\tau) = \sum_{n=0}^{\infty} a(n)q^n$ be a modular form of weight k for $\Gamma_0(N)$. Recall that

$$\Gamma_0(N) := \{A \in SL(2,\mathbb{Z}) : A_{21} \equiv 0 \mod N\}$$

Define V_m, U_m so that

$$V_m f(\tau) = m^{-\frac{k}{2}} f|_k \begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix} (\tau) = f(m\tau) = \sum_{n=0}^{\infty} a(n)q^{mn}$$

$$U_m f(\tau) = m^{-\frac{k}{2}-1} f|_k \begin{bmatrix} 1 & j \\ 0 & m \end{bmatrix} (\tau) = \sum_{n=0}^{\infty} a(mn)q^n$$

V_m and U_m are linear maps $M_k(\Gamma_0(N)) \to M_k(\Gamma_0(mN))$. If $m \mid N$, then $U_m \in \text{End}(M_k(\Gamma_0(N)))$.

The following is not actually true, but pretend that $U_m \in \text{End}(S_{12}(SL_2(\mathbb{Z}))$ for every $m > 0$. Then since $S_{12} \cong M_0$, by multiplication by Δ, we would have $U_m\Delta = \lambda_m\Delta$ with $\lambda_m \in \mathbb{C}$. Then, if τ is the Ramanujan-tau function, we would get for $m \in \mathbb{Z}^+$

$$\tau(m) = \lambda_m\tau(1) = \lambda_m \Longrightarrow \tau(mn) = \lambda_m\tau(n) = \tau(m)\tau(n)$$

Which would prove τ is multiplicative.

Though we arrived here on a false assumption, we could try to make this work by trying to average U_m and V_m somehow. We need to find the endomorphisms of M_k and S_k.

Let $n \in \mathbb{Z}_{\geq 1}$.

$$\mathbb{M}_n := \{A \in \mathbb{M}_2(\mathbb{Z}) : \det A = n\}$$

$SL(2,\mathbb{Z})$ acts on $\mathbb{M}_n$ on the left (since the determinant function is multiplicative). So we consider $\mathbb{M}_n/SL(2,\mathbb{Z})$, the finite collection of representatives of the orbits.[7]

The sum $\sum_{\mu\in\mathbb{M}_n/SL(2,\mathbb{Z})} f|_k\mu$ does not depend on the choice of representatives because if $\gamma \in \Gamma_1$, then by the modularity condition $f|_k\gamma = f$,

$$f|_k\gamma\mu = (f|_k\gamma)|_k\mu = f|_k\mu$$

Let the operator T_n be defined by

$$T_n f(z) = n^{\frac{k}{2}-1} \sum_{\mu\in\mathbb{M}_n/SL(2,\mathbb{Z})} f|_k\mu$$

If f is holomorphic on H and invariant under $\gamma \in SL(2,\mathbb{Z})$, then T_nf is as well:

$$\begin{aligned} T_n f|_k\gamma &= n^{\frac{k}{2}-1} \sum_{\mu\in\mathbb{M}_n/SL(2,\mathbb{Z})} (f|_k\mu)|_k\gamma \\ &= n^{\frac{k}{2}-1} \sum_{\mu\in\mathbb{M}_n/SL(2,\mathbb{Z})} (f|_k\mu\gamma) = T_nf \Longrightarrow T_n \in \text{End}(M_k) \cap \text{End}(S_k) \end{aligned}$$

This happens by a re-indexing argument; $\mu\gamma$ for another system of orbits of $\mathbb{M}_n$. T_n is known as the *Hecke operator* of index n.

Theorem 4.1. *The Hecke operator has the following properties.*

[7] The reason that this collection is finite will be explained in the upcoming proof.

(i) Let $n \in \mathbb{Z}^+$, $f(\tau) = \sum_{h=0}^{\infty} \alpha(h) q^h \in M_k$. Then

$$T_n f(\tau) = \sum_{h=0}^{\infty} \left(\sum_{d|(n,h)} d^{k-1} \alpha\left(\frac{nh}{d^2}\right) \right) q^h$$

This means that M_k and S_k are stable for T_n.

(ii) If m and n are two integers ≥ 1, then

$$T_n T_m = \sum_{d|(n,m)} d^{k-1} T_{nm/d^2} = T_m T_n$$

In particular, $T_n T_m = T_{mn}$ if n, m are coprime.

Proof. Through elementary row operations, we can transform a matrix $\mu \in \mathbb{M}_n$ into an upper triangular matrix. So we can left multiply $\mu = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ by $\pm \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \in SL(2, \mathbb{Z})$, which yields the matrix $\begin{bmatrix} a & b + dr \\ 0 & d \end{bmatrix}$. This operation does not change the equivalence class in $\mathbb{M}_n / PSL(2, \mathbb{Z})$. Then, we can assume $r = 1$. Since $ad = n$, we can asssume WLOG that $a > 0$ and $0 \leq b < d$.[8] So we have

$$T_n f(\tau) = n^{k-1} \sum_{a,d>0} \sum_{ad=n} \sum_{b=0}^{d-1} d^{-k} f\left(\frac{a\tau + b}{d}\right)$$

Then by the modularity condition on f, we get

$$T_n f(\tau) = \sum_{b=0}^{d-1} f\left(\frac{a\tau + b}{d}\right) = \sum_{m=0}^{\infty} d\alpha(md) q^{ma}$$

Then upon reindexing, we get the result. We can apply this formula to get (ii). □

This theorem is nice because we can obtain a formal expression for T_n for every n. If p, is a prime number, we can use this to get

$$T_p = U_p + p^{k-1} V_p$$

This allows us to conclude the following:

- If p is a factor of n of order 1, then
$$T_n = T_{n/p} T_p$$
- If p is a factor of n of order 2, then
$$T_n = T_{n/p} T_p - p^{k-1} T_{n/p^2}$$

It is useful to define T_0. For $h > 0$, the formula from (i) of Theorem 4.1 tells us that the coefficients $\alpha(h)$ are given by $\sigma_{k-1}(h)\alpha(0)$. So recalling our discussion of Eisenstein series, we expect $T_0 f(\tau)$ to behave like $E_k(\tau)$. But if $T_0 f(\tau) \in M_k$, based on the structure of M_k as a vector space, we can conclude that the constant term must be $\alpha(0) E_k(z)$, so we define

$$T_0 f(\tau) = \alpha(0) E_k(\tau)$$

We proved earlier that for $k = 4, 6, 8, 10$ and 14 that $\dim_{\mathbb{C}} M_k = 1$, which means that every nonzero modular form in M_k is an eigenvector of every T_n. Because T_n is an endomorphism, using (ii) from Theorem 4.1, we get

$$\alpha(n) = \lambda_n \alpha(1)$$

If $a(1) = 0$, then $f = 0$, but f is an eigenvector so this is not true; then $\alpha(1) \neq 0$.

Definition 4.2. A *Hecke form* of M_k (for $k > 0$) is an eigenfunction of all the Hecke operators of T_n such that $\alpha(1) = 1$ (normalization).

[8]This shows that there are only finitely many equivalence classes in $\mathbb{M}_n / PSL(2, \mathbb{Z})$

Then we get that the Fourier coefficients $\alpha(n)$ of f are eigenvalues of T_n, and (ii) from Theorem 4.1 gives us

$$\alpha(n)\alpha(m) = \sum_{d|(m,n)} d^{k-1} a\left(\frac{mn}{d^2}\right)$$

So $n \mapsto \alpha(n)$ is multiplicative. We can apply our considerations to S_k when it is of dimension 1 (i.e. $k = 12, 16, 18, 20, 22, 26$.)

Lemma 4.3. *The Eisenstein series of even index*

$$E_{2k}(z) = -\frac{B_{2k}}{4k} + \sum_{m=1}^{\infty} \sigma_{2k-1}(m) q^m$$

are eigenfunctions of all the Hecke operators.

Proof. By (i) from 4.1 as well as our earlier observations which set up $T_0 f(\tau) = \alpha(0) E_k(\tau)$, it suffices to verify the multiplicative property for the Fourier coefficients described by

$$\alpha(n)\alpha(m) = \sum_{d|(m,n)} d^{k-1} a\left(\frac{mn}{d^2}\right)$$

If n or m is zero or 1, then this is fine.

When $nm > 0$, since σ_k is a variant of the Euler-φ function from number theory, we can deduce that σ_{k-1} exhibits the multiplicativity. Hence, we reduce to the case where $m = p^\mu$ and $n = p^\nu$. Then,

$$\alpha(m)\alpha(n) = \sigma_{k-1}(p^\mu)\sigma_{k-1}(p^\nu) = \frac{k^{(k-1)(\mu+1)} - 1}{p^{k-1} - 1} \cdot \frac{p^{(k-1)(\nu+1)} - 1}{p^{k-1} - 1}$$

So WLOG if $\mu \leq \nu$, then we can check that

$$\sum_{d|(p^\mu, p^\nu)} d^{k-1} \alpha\left(\frac{mn}{d^2}\right) = \alpha(p^{\mu+\nu}) + p^{k-1} a(p^{\mu+\nu-2}) + \ldots + p^{(k-1)\mu} \alpha(p^{\mu+\nu-2\mu})$$

Setting $r = p^{k-1}$, we check that

$$\frac{(r^{\mu+1} - 1)(r^{\mu+1} - 1)}{(r-1)^2} = \frac{(r^{\mu+\nu+1} - 1) + r(r^{\mu+\nu-1} - 1) + \ldots + r^\mu (r^{\nu-\mu+1} - 1}{r - 1}$$

This gives us the result.

∎

Theorem 4.4. *(Hecke) For $k > 0$, the Hecke forms form a basis for M_k.*

Proof. E_{2k} are eigenfunction of T_n. From our earlier observations, if $\alpha(0) \neq 0$ and f is an eigenfunction of T_0, then f is some constant multiple of E_{2k}.

Since $M_{2k} = \langle E_{2k} \rangle \oplus S_{2k}$, it suffices to check that the Hecke forms are a basis of S_{2k}.

For this, we need the Petersson Hermitian product. It is demonstrable that T_n are self-adjoint operators on the inner product, meaning

$$(T_n f, g) = (f, T_n g)$$

for all f and $g \in S_{2k}$ for every $n > 0$. (This is an Exercise in the Hellegouarch).

It follows from a spectral theorem in linear algebra that T_n are diagonalizable. This in particular proves that the Hecke forms span S_{2k}.

The coefficients $\alpha(n)$ of the eigenfunctions are real:

$$a(n)(f,f) = (a(n)f, f) = (T_n(f), f) = f(T_n(f)) = (f, a(n)f) = \overline{a(n)}(f,f)$$

Suppose Hecke forms f, g are such that f is not a constant multiple of g. So if $\alpha(n)$ are the Fourier coefficients of f and $\beta(n)$ are the Fourier coefficients of g, there must be an n where $\alpha(n) \neq \beta(n)$. This means that

$$a(n)(f,g) = (T_n f, g) = (f, T_n g) = (T_n f, g) = (f, T_n g) = (f, \beta(n) g) = \overline{b(n)}(f,g) = \beta(n)(f,g)$$

So $(f,g) = 0$, proving linear independence. □

Theorem 4.5. *The Fourier coefficients of the Hecke forms $f \in S_k$ are real algebraic integers of degree $\leq \dim_{\mathbb{C}} S_k$.*

Proof. By the theorems from Section 2, S_k are generated by forms with integer Fourier coefficients (these are the σ_n). Therefore, the $\mathbb{Z}$-module generated by the forms is closed (or stable) under T_n.

Therefore, the matrices have integer coefficients; since the formula for eigenvalues is a polynomial, we can conclude that the eigenvalues are algebraic integers, and the previous proof gives us that these are real. □

I will end by defining what an L-function is.

Definition 4.6. Let $f(\tau) = \sum_{m=0}^{\infty} \alpha(m) q^m \in M_k$ be a modular form for $SL(2,\mathbb{Z})$. Then the L-function of $f(z)$ is

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

Some may recognize this as the associated Dirichlet series, and it follows from $a(n) = O(n^{k-1})$ that $L(f,s)$ converges in the half-plane $\mathrm{Re}(s) > k$. This has many nice properties–for example, it can be expressed as an Euler product

$$L(f,s) = \prod_{p \text{ prime}} \left(1 + \sum_k \frac{\alpha(p^k)}{p^{ks}}\right)$$

It turns out that can associate to an eigenform f an elliptic curve E whose L-function agrees with that of f, and we can use this to say something about modularity in the context of what role it plays in the proof of FLT.