A Brief Introduction to Modular Forms

Catherine M. Hsu

Department of Mathematics
University of Oregon

Coding Theory, Cryptography, and Number Theory Seminar
Clemson University

September 18, 2017

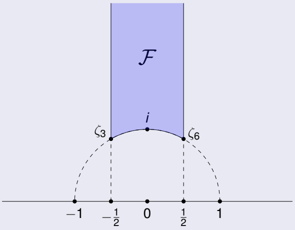
Let $N > 1$ be an integer.

- $\Gamma(N) \;\; = \{\gamma \in \mathrm{SL}(2,\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}\}$
- $\Gamma_1(N) = \{\gamma \in \mathrm{SL}(2,\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}\}$
- $\Gamma_0(N) = \{\gamma \in \mathrm{SL}(2,\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{N}\}$

$\mathrm{SL}(2,\mathbb{Z})$ acts on $\mathfrak{h}$ via Möbius transformations:

$$z \in \mathfrak{h}, \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z}),$$

$$\gamma z := \frac{az+b}{cz+d}.$$



Modular forms: Definition

A **modular form of weight** k **and level** N is a complex function

$$f : \mathfrak{h} \to \mathbb{C}$$

satisfying the following properties:

1. f is holomorphic on $\mathfrak{h}$;
2. $f(\gamma z) = (cz + d)^k f(z), \quad \forall \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$;
3. f is holomorphic at the cusps.

---

4. f vanishes at the cusps.

Modular forms with Nebentypus

Consider the following spaces of modular forms:

- $M_k(\Gamma_1(N))$, $S_k(\Gamma_1(N))$
- $M_k(\Gamma_0(N))$, $S_k(\Gamma_0(N))$

For a Dirichlet character

$$\varepsilon : (\mathbb{Z}/N\mathbb{Z})^{\times} \to \mathbb{C}^{\times},$$

we say a modular form $f \in M_k(\Gamma_1(N))$ has **Nebentypus** ε if

$$f(\gamma z) = \varepsilon(d)(cz+d)^k f(z), \quad \forall \gamma \in \Gamma_0(N).$$

We denote this space of modular forms by $M_k(N, \varepsilon)$.

Fourier expansions of modular forms

For $f \in M_k(\Gamma_0(N))$, we have

$$f(z) = f(z+1),$$

and hence, there is a Fourier expansion for f at ∞:

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

The coefficients $\{a_n\}$ are called the **Fourier coefficients** of f.

Decomposition and Dimension of $M_k(\Gamma_1(N))$

For each $N > 1$, we have a decomposition

$$M_k(\Gamma_1(N)) = \bigoplus_{\varepsilon} M_k(N, \varepsilon),$$

where ε runs over all Dirichlet characters mod N such that

$$\varepsilon(-1) = (-1)^k.$$

We can also compute the dimension of $M_k(\mathrm{SL}(2,\mathbb{Z}))$:

$$\dim M_k(\mathrm{SL}(2,\mathbb{Z})) = \begin{cases} 0, & \text{if } k < 0 \text{ or } k \text{ is odd}, \\ \lfloor k/12 \rfloor + 1, & \text{if } k \not\equiv 2 \pmod{12}, \\ \lfloor k/12 \rfloor, & \text{if } k \equiv 2 \pmod{12}. \end{cases}$$

First Example: Eisenstein Series

Let $k > 2$ be an even integer and define for each $z \in \mathfrak{h}$

$$G_k(z) = \sum_{(m,n) \neq (0,0)} \frac{1}{(mz+n)^k}.$$

Then, $G_k(z) \in M_k(\mathrm{SL}(2,\mathbb{Z}))$ with Fourier expansion

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

Identities involving sums of powers of divisors

For $k = 4, 6, 8, 10$, and 14, the dimension of $M_k(\mathrm{SL}(2, \mathbb{Z}))$ is 1.

Each of these spaces is spanned by the Eisenstein series $E_k(z)$, and so, we have the following equalities:

$$E_4(z)^2 = E_8(z)$$
$$E_4(z)E_6(z) = E_{10}(z)$$
$$E_6(z)E_8(z) = E_4(z)E_{10}(z) = E_{14}(z)$$

Identities involving sums of powers of divisors (cont.)

Comparing Fourier coefficients then yields identities such as

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

$$\sum_{m=1}^{n-1} \sigma_3(m)\sigma_9(n-m) = \frac{\sigma_{13}(n) - 11\sigma_9(n) + 10\sigma_3(n)}{2640}$$

Proof of identity with $E_4(z)^2 = E_8(z)$

- $E_4(z) = 1 + 240q + 2160q^2 + \cdots = 1 + 240\sum_{n=1}^{\infty} \sigma_3(n)q^n$
- $E_8(z) = 1 + 480q + 61920q^2 + \cdots = 1 + 480\sum_{n=1}^{\infty} \sigma_7(n)q^n2$

Since $E_4(z)^2 = E_8(z)$, for each $n \geq 1$, we have

$$480 \cdot \sigma_3(n) + 240^2 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m)2 = 480 \cdot \sigma_7(n)$$

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

Congruences between modular forms

For a prime $p \in \mathbb{Z}$, we say that two modular forms

$$f_1 = \sum_{n=0}^{\infty} a_n q^n, \quad f_2 = \sum_{n=0}^{\infty} b_n q^n$$

are **congruent mod** p if

$$a_n \equiv b_n \pmod{\mathfrak{p}}, \quad \forall n \geq 0,$$

where $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ is a prime ideal lying over p.

Let $p \in \mathbb{Z}$ be prime. If k, k' are two even integers satisfying

$$k \equiv k' \pmod{p-1},$$

then Fermat's Little Theorem implies

$$\sigma_{k-1}(n) \equiv \sigma_{k'-1}(n) \pmod{p}, \quad \forall n \geq 1.$$

Thus,

$$a_n(E_k) \equiv a_n(E_{k'}) \pmod{p}, \quad \forall n \geq 1.$$

We also have a congruence between $a_0(E_k)$ and $a_0(E_{k'})$ so that

$$E_k \equiv E_{k'} \pmod{p}.$$

The Discriminant Function

For $z \in \mathfrak{h}$, define

$$\Delta(z) = \frac{1}{1728}\left(E_4(z)^3 - E_6(z)^2\right).$$

Since Δ vanishes at ∞, we have $\Delta \in S_{12}(\mathrm{SL}(2,\mathbb{Z}))$. Moreover,

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

where $\tau(n)$ is the Ramanujan tau function.

A Congruence of Ramanujan

The first few values of $\tau(n)$ are given below:

n	1	2	3	4	5	6	7	$\cdots$
$\tau(n)$	1	-24	252	-1472	4830	-6048	-16744	$\cdots$

In particular, we note that $\tau(n)$ is multiplicative and satisfies

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}, \quad \forall n \geq 1.$$

Hecke theory: Definitions

For each integer $m \geq 1$, there is a linear operator T_m, called the m^{th} Hecke operator, acting on $M_k(\mathrm{SL}(2,\mathbb{Z}))$.

If $\mathcal{M}_m$ denotes the set of 2×2 integral matrices with determinant m, then for a modular form $f(z) \in M_k(\mathrm{SL}(2,\mathbb{Z}))$ and $z \in \mathfrak{h}$,

$$T_m f(z) = m^{k-1} \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z}) \backslash \mathcal{M}_m} (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right).$$

Hecke theory: Equivalent definitions

Hecke operators also arise in the context of:

- abstract Hecke rings such as $R(\Gamma_0(N), \Delta_0(N))$
- modular correspondences on $(\Gamma_0(N)\backslash\mathfrak{h}) \times (\Gamma_0(N)\backslash\mathfrak{h})$
- certain moduli spaces such as $S_1(N)$

Hecke theory: Fourier expansions

Let $f(z)$ have Fourier expansion $f(z) = \sum_{n=0}^{\infty} a_n q^n$. Then

$$T_m f(z) = \sum_{n \geq 0} \left(\sum_{\substack{r|(m,n) \\ r>0}} r^{k-1} a_{mn/r^2} \right) q^n.$$

Important observation: The Hecke operators T_m all commute!

Hecke action on the discriminant function

Consider the action of T_m on $\Delta \in S_{12}(\mathrm{SL}(2,\mathbb{Z}))$. Since

$$\dim(S_{12}(\mathrm{SL}(2,\mathbb{Z}))) = 1,$$

$T_m\Delta$ must be a multiple of Δ for each $m \geq 1$.

In particular, since

$$T_m\Delta = \tau(m)q + \cdots,$$
$$\Delta = q + \cdots,$$

we must have

$$T_m\Delta = \tau(m)\Delta, \quad \forall m \geq 1.$$

Hecke action on eigenforms

More generally, if $f(z)$ is a normalized Hecke eigenform, then

$$\begin{aligned} T_m f(z) &= \lambda_m a_0 + \lambda_m q + \cdots , \\ &= \sigma_{k-1}(m) a_0 + a_m q + \cdots . \end{aligned}$$

Hence, for each $m \geq 1$, we have an equality

$$\lambda_m = a_m.$$

Applying this with the formula for the action of T_m on f yields

$$a_m a_n = \sum_{\substack{r|(m,n) \\ r>0}} r^{k-1} a_{mn/r^2}.$$

Old and new spaces of $S_k(\Gamma_0(N))$

Let $d, M, N > 0$ be integers such that $dM \mid N$, and define

$$\begin{aligned} \iota^*_{d,M,N} : S_k(\Gamma_0(M)) &\to S_k(\Gamma_0(N)), \\ f(z) &\mapsto d^{k-1} f(dz). \end{aligned}$$

For a fixed N, we define the **old subspace of** $S_k(\Gamma_0(N))$ by

$$S_k(\Gamma_0(N))^{\text{old}} = \bigoplus \iota^*_{d,M,N}\left(S_k(\Gamma_0(M))\right),$$

where the sum is taken over all d, M with $dM \mid N$ and $M \neq N$.

Old and new spaces of $S_k(\Gamma_0(N))$ (cont.)

Moreover, there is a Hecke-equivariant decomposition

$$S_k(\Gamma_0(N)) = \underbrace{S_k(\Gamma_0(N))^{\text{old}}}_{\substack{\text{images of}\\ \text{level-raising}}} \bigoplus \underbrace{S_k(\Gamma_0(N))^{\text{new}}}_{\substack{\text{spanned by}\\ \text{newforms}}}.$$

Old and new spaces of $S_2(\Gamma_0(33))$

Using various dimension formulas, we find that

$$\dim(S_2(\Gamma_0(33))) = 3.$$

Since $S_2(\Gamma_0(3)) = 0$, we have a decomposition

$$S_2(\Gamma_0(33))^{\text{old}} = \iota^*_{1,11,33}(S_2(\Gamma_0(11))) \oplus \iota^*_{3,11,33}(S_2(\Gamma_0(11))).$$

Thus,

$$S_2(\Gamma_0(33)) = \underbrace{S_2(\Gamma_0(33))^{\text{old}}}_{\dim 2} \bigoplus \underbrace{S_2(\Gamma_0(33))^{\text{new}}}_{\dim 1}.$$

Importance of Hecke theory

There are many deep connections between Hecke theory and the theory of modular forms including:

- The strong multiplicity one theorem
- Duality between spaces of cusp forms and Hecke algebras
- Galois representations attached to Hecke eigenforms