

# JUNIOR NUMBER THEORY TALK: INTRODUCTION TO MODULAR FORMS

KIMBERLY HOPKINS  
(BASED ON NOTES BY DON ZAGIER)

ABSTRACT. Though modular forms are perhaps most important to number theorists, they appear as well in topology, physics, and nature, and their theory uses topology, complex analysis, and both the analytic and algebraic sides of number theory. In this talk we will give an introduction to modular forms. We will begin with their definitions, and cover the central elements of the theory up to and including Hecke operators. There will be key motivating examples throughout. This talk is self contained and is intended to be an introduction.

This talk is based on and contains parts directly from lecture notes by Don Zagier for a course given in Utrecht in the spring of 1991. I would like to thank Professor Zagier for writing such a clear and concise set of notes on this subject.

## 1. INTRODUCTION

The word “modular” refers to the moduli space (i.e. classification) of Riemann surfaces of genus 1.

A Riemann surface can be written as

$$\mathbb{C}/\Lambda$$

where  $\Lambda \subset \mathbb{C}$  is a lattice.

Recall  $\Lambda \subset \mathbb{C}$  is a lattice if there is an  $\mathbb{R}$ -basis  $\{\omega_1, \omega_2\}$  of  $\mathbb{C}$  (i.e.  $\mathbb{C} = \mathbb{R}\omega_1 + \mathbb{R}\omega_2$ ) which is a  $\mathbb{Z}$ -basis for  $\Lambda$  (i.e.  $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ ).

Two lattices  $\Lambda_1$  and  $\Lambda_2$  give the same curve (i.e. Riemann surface) if

$$\Lambda_2 = \lambda\Lambda_1$$

for some  $\lambda \neq 0 \in \mathbb{C}$ .

A **Modular Function**  $F$  assigns a lattice to a complex number  $F(\Lambda)$ , and ( to be consistent with the equivalence of curves above ) should satisfy

$$F(\Lambda_1) = F(\Lambda_2) \quad \text{for } \Lambda_1 = \lambda\Lambda_2.$$

Since any lattice

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

is equivalent to a lattice of the form

$$\mathbb{Z}\tau + \mathbb{Z}$$

(take  $\lambda = \omega_2$ ,  $\tau = \omega_1/\omega_2 \in \mathbb{H}$  and note that we can always choose so that  $\Im(\omega_1/\omega_2) > 0$ ), we see that  $F$  is completely determined by

$$f(\tau) := F(\mathbb{Z}\tau + \mathbb{Z}) \quad \tau \in \mathbb{H}.$$

How does changing the basis for this lattice affect  $f$ ? If  $\omega_1, \omega_2$  are a basis for  $\Lambda$  then any other basis of  $\Lambda$  is of the form

$$a\omega_1 + b\omega_2, \quad c\omega_1 + d\omega_2$$

for some matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ . Therefore the lattices,

$$\mathbb{Z}\tau + \mathbb{Z}, \quad \mathbb{Z}\frac{a\tau + b}{c\tau + d} + \mathbb{Z}$$

are homothetic (give the same curve) and so since  $F$  preserves this property so must  $f$ , that is,

$$f(\tau) = f\left(\frac{a\tau + b}{c\tau + d}\right) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

called the “modular invariance property”.

From here on out let  $\Gamma_1 := \mathrm{SL}_2(\mathbb{Z})$  denote the **full modular group**.

**Definition 1.1.** A **Modular Function** is a holomorphic complex valued function  $f : \mathbb{H} \rightarrow \mathbb{C}$  which is invariant under the action,

$$\gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1.$$

*Example 1.2.* The “modular invariant” or “ $j$ -invariant”

$$j(\tau) = e^{-2\pi i\tau} + 744 + 196884e^{2\pi i\tau} + \dots$$

However, it turns out that for many purposes, this condition of (complete) modular invariance is too restrictive. Instead consider complex valued functions  $F$  on lattices such that

$$F(\Lambda_1) = \lambda^k F(\Lambda_2) \quad \text{for } \Lambda_1 = \lambda\Lambda_2,$$

$\lambda \neq 0 \in \mathbb{C}$  and for some integer  $k$  called the **weight**.

Again we get a corresponding  $f : \mathbb{H} \rightarrow \mathbb{C}$  by

$$f(\tau) := F(\mathbb{Z}\tau + \mathbb{Z}) \quad \text{for } \Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \tau = \omega_1/\omega_2.$$

But now, instead of the modular invariance property, we get

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

called the “modular transformation property”.

With this definition we can construct functions that are “holomorphic at infinity”. Take  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ , then the modular transformation property implies

$$f(\tau + 1) = f(\tau)$$

which implies  $f$  is periodic with period 1 and so has a Fourier expansion,

$$f(\tau) = \sum a(n)e^{2\pi in\tau}.$$

Define  $q = e^{2\pi in\tau}$ . Then this can be thought of as an expansion around  $q = 0$  since

$$f = \sum a(n)q^n.$$

But  $q = 0 \Leftrightarrow \tau = i\infty$  (the point at infinity) so if we want  $f$  to be “nice” at infinity it makes sense to require that the Fourier expansion is holomorphic near  $q = 0$ , so...

**Definition 1.3.**  $f$  is **holomorphic at infinity** if  $a(n) = 0$  for  $n < 0$ .

We can now define the objects that will be the subject of this talk,

**Definition 1.4.** Holomorphic functions  $f : \mathbb{H} \rightarrow \mathbb{C}$  that satisfy

$$(1.1) \quad f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1$$

are called

(1) **Modular Forms of weight  $k$**  if  $a(n) = 0$  for all  $n < 0$ . (The set of such denoted  $M_k$ ).

(2) **Cusp Forms of weight  $k$**  if  $a(n) = 0$  for all  $n \leq 0$ . (The set of such denoted  $S_k$ ).

Note the requirement for cusp forms is that  $f$  “vanishes at infinity”.

These forms,  $M_k$  (respectively  $S_k$ ) (clearly) form a vector space over  $\mathbb{C}$ . We are interested in studying them because

(i) They arise naturally in math and physics and often encode the arithmetically interesting information about a problem.

(ii)  $M_k$  (respectively  $S_k$ ) is a *finite dimensional* vector space for each  $k$ .

The point of this is that if  $\dim M_k = d$  and we have more than  $d$  situations giving rise to modular forms in  $M_k$ , then we automatically get a linear relation among these functions and get “for free” information—highly non trivial—relating these different situations.

Nature often produces situations which turn out to be the Fourier coefficients of a modular form. Examples include but are certainly not limited to multiplicities of energy levels, sums over the divisors of integers, special values of zeta functions, or the number of solutions of Diophantine equations.

*Example 1.5. Eisenstein Series*

Suppose  $k$  is even,  $k > 2$  and define the **Eisenstein series of weight  $k$**  by

$$G_k(\tau) = \frac{(k-1)!}{2(2\pi i)^k} \sum_{\substack{(m,n) \in \mathbb{Z}^2 \\ (m,n) \neq (0,0)}} \frac{1}{(m\tau + n)^k}.$$

This satisfies the transformation property (1.1) because replacing  $G_k(\tau)$  with  $(c\tau + d)^{-k} G_k\left(\frac{a\tau + b}{c\tau + d}\right)$  simply replaces  $(m, n)$  by  $(am + cn, bm + dn)$  and hence just permutes the terms of the sum.

Using some analysis (Lipschitz Formula and “Hecke’s trick”) we can compute the Fourier expansion of  $G_k$ ,

$$G_k(\tau) = \frac{1}{2} \zeta(1-k) + \sum_{n \geq 1} \sigma_{k-1}(n) q^n$$

where  $\sigma_{k-1}(n) := \sum_{r|n} r^{k-1}$  (sum over all positive divisors  $r$  of  $n$ ). (Note: using this it turns out we can also define  $G_k$  for  $k = 2$ ).

A couple examples for different weights...

$$G_2(\tau) = -\frac{1}{24} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + 12q^6 + 8q^7 + 15q^8 + \dots$$

$$G_4(\tau) = \frac{1}{240} + q + 9q^2 + 28q^3 + 73q^4 + 126q^5 + 252q^6 + \dots$$

$$G_6(\tau) = -\frac{1}{504} + q + 33q^2 + 244q^3 + 1057q^4 + \dots$$

$$G_8(\tau) = \frac{1}{480} + q + 129q^2 + 2188q^3 + \dots$$

Since it satisfies the transformation property and is holomorphic on  $\mathbb{H}$  and at infinity,  $G_k$  is a modular form of weight  $k$  for each  $k$ .

Arithmetic Interest of  $G_k$

It turns out, for example, that  $\dim M_8 = 1$ . Both  $120G_4(\tau)^2$  and  $G_8(\tau)$  are weight 8 and have constant term  $1/480$ , hence must be equal. Thus we get the identity,

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m), \quad n > 0.$$

This is a nontrivial number-theoretical relation.

We also get new proof and insight into the values of the Riemann zeta function, for example we see

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}.$$

*Example 1.6. The discriminant function*

$$\Delta(\tau) = q \prod_{n \geq 1} (1 - q^n)^{24} = q - 24q^2 + 252q^3 + \dots$$

It can be shown that  $\Delta(\tau)$  is a cusp form of weight 12.

$\Delta$  can be written in terms of the Eisenstein series,

$$1728\Delta = (240G_4)^3 - (504G_6)^2$$

which gives the coefficients of  $\Delta$  in terms of the elementary number theoretic functions  $\sigma_{k-1}(n)$ .

Even more important, observe

$$\begin{aligned} \text{coefficient of } q^2 \times \text{coefficient of } q^3 &= \text{coefficient of } q^6 \\ -24 \times 252 &= -6048 \end{aligned}$$

It turns out that indeed the coefficients of  $\Delta$  are multiplicative! This was originally observed by Ramanujan in 1916 and proved by Mordell a year later).

This observation was developed into a theory for all modular forms by Hecke and is the center of the whole theory of modular forms, which we'll discuss about in a moment.

*Example 1.7. Jacobi Theta Function*

$$\theta(\tau) = \sum_{m \in \mathbb{Z}} q^{m^2} = 1 + 2q + 2q^4 + 2q^9 + \dots$$

This turns out to be a modular form of weight  $1/2$ , which we will discuss in the next talk.

The powers of  $\theta(\tau)$  tell us the number of ways of representing an integer as a sum of a given number of squares.

For example,

$$\begin{aligned}\theta(\tau)^4 &= \sum_{m_1, m_2, m_3, m_4} q^{m_1^2 + m_2^2 + m_3^2 + m_4^2} \\ &= 1 + \sum_{n \geq 1} r_4(n) q^n\end{aligned}$$

where  $r_4(n)$  is the number of ways of representing  $n$  as  $m_1^2 + m_2^2 + m_3^2 + m_4^2$ ,  $m_i \in \mathbb{Z}$ . For example,

$$r_4(1) = 8, r_4(2) = 24, r_4(3) = 24.$$

Since  $\theta(\tau)$  is a modular form of weight  $1/2$ ,  $\theta(\tau)^4$  is a modular form of weight  $2$ , and one can show is spanned by

$$G_2(\tau) - 2G_2(2\tau)$$

and

$$G_2(\tau) - 4G_2(4\tau),$$

which implies  $\theta(\tau)^4$  is a linear combination of the two, and by comparing coefficients we see

$$\theta(\tau)^4 = 8(G_2(\tau) - 4G_2(4\tau)).$$

Hence

$$r_4(n) = 8 \sum_{\substack{d|nd, \\ d \neq 0(4)}} (n > 0)$$

a famous formula of Jacobi.

In particular,  $r_4(n) \geq 8$  for all  $n$  so we get an immediate proof of

**Theorem 1.8.** (*Lagrange 4 square theorem*)

*Every positive integer is a sum of 4 squares.*

## 2. HECKE THEORY

The key to the theory of modular forms is the existence of a commutative algebra of operators  $T_n$  ( $n \in \mathbb{N}$ ) acting on the space  $M_k$  of modular forms of weight  $k$ . An outline of the key facts are,

- $M_k$  has a canonical basis of simultaneous eigenvectors (modular forms) of all the  $T_n$ .
- These “eigenvector” modular forms  $\sum a(n)q^n$  are very special:
  - Their Fourier coefficients  $a(n)$  are all algebraic integers.
  - Their coefficients are multiplicative, i.e.  $a(nm) = a(n)a(m)$  for all  $(n, m) = 1$ .
- Their associated Dirichlet series  $\sum a(n)n^{-s} \dots$ 
  - have Euler products
  - have analytic continuations to the whole complex plane, which satisfy functional equations analogous to that of the Riemann zeta function

Recall the bijection

$$\begin{aligned}F(\Lambda) &\mapsto f(\tau) := F(\mathbb{Z}\tau + \mathbb{Z}) \\ f(\tau) &\mapsto F(\Lambda) := \omega_2^{-k} f(\omega_1/\omega_2), \quad (\Lambda := Z\omega_1 + \mathbb{Z}\omega_2, \Im(\omega_1/\omega_2) > 0).\end{aligned}$$

More concisely this is a bijection between functions  $f : \mathbb{H} \rightarrow \mathbb{C}$  with transformations like modular forms of weight  $k$  and functions  $F : \{\text{lattices } \Lambda \subset \mathbb{C}\} \rightarrow \mathbb{C}$  which are homogenous of weight  $k$ ,

$$\begin{aligned} & \left\{ \text{functions } f : \mathbb{H} \rightarrow \mathbb{C} : f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{-k} f(\tau) \right\} \\ \leftrightarrow & \left\{ \text{functions } F : \{\text{lattices } \Lambda \subset \mathbb{C}\} \rightarrow \mathbb{C} : F(\lambda\Lambda) = \lambda^{-k} F(\Lambda) \right\}. \end{aligned}$$

For fixed  $n \in \mathbb{N}$ , define the function (pointwise on  $\Lambda$ )

$$T_n F(\Lambda) := n^{k-1} \sum_{\substack{\Lambda' \subseteq \Lambda \\ [\Lambda : \Lambda'] = n}} F(\Lambda').$$

This is a finite sum since there are only finitely many sublattices  $\Lambda' \subseteq \Lambda$  of index  $n$ . ( $|\Lambda/\Lambda'| = n$  so  $n\omega_i \equiv 0 \pmod{\Lambda'}$  hence  $n\Lambda \subseteq \Lambda'$  which means  $\Lambda'$  corresponds to a subgroup of  $\Lambda/n\Lambda \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ ).

$T_n F(\Lambda)$  is (clearly) homogeneous of degree  $k$  so this corresponds to an operator on the set of functions  $\{f\}$  from the bijection above. The above definition thus gives

**Definition 2.1.** The  $n$ th Hecke operator  $T_n$  in weight  $k$  is defined by

$$T_n f(\tau) = n^{k-1} \sum_{\gamma \in \Gamma_1 \backslash \mathcal{M}_n} (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right)$$

for  $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  and where  $\mathcal{M}_n = \{2 \times 2 \text{ integral matrices with determinant } n\}$ .  $\Gamma_1 \backslash \mathcal{M}_n$  is the set of orbits of  $\mathcal{M}_n$  under (the action of) left multiplication by  $\Gamma_1 = \text{SL}_2(\mathbb{Z})$ .

We now show  $T_n f \in M_k$  for all  $f \in M_k$  (and  $T_n f \in S_k$  for all  $f \in S_k$ ).

**Theorem 2.2.** (i) If  $f(\tau) \in M_k$ ,  $f(\tau) = \sum_{m \geq 0} a(m)q^m$  ( $q = e^{2\pi iz}$ ), then the Fourier expansion of  $T_n f$  is

$$T_n f(\tau) = \sum_{m \geq 0} \left( \sum_{d|n, m} d^{k-1} a\left(\frac{nm}{d^2}\right) \right) q^m,$$

where  $\sum_{d|n, m}$  is a sum over the positive common divisors of  $m$  and  $n$ .

(ii)  $T_n f \in M_k$  for all  $f \in M_k$  and  $T_n f \in S_k$  for all  $f \in S_k$ .

(iii) The Hecke operators of weight  $k$  satisfy the multiplicative rule,

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

In particular,  $T_n T_m = T_m T_n$  for all  $n, m$  and  $T_n T_m = T_{nm}$  for all  $(n, m) = 1$ .

*Proof.* Proof of (i):

We just need to describe the orbits of  $\Gamma_1 \backslash \mathcal{M}_n$ . If  $\mu = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  with  $\det \mu = n$ , and  $c \neq 0$ , then choose

$$\gamma = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$$

with  $\frac{a'}{c'} = \frac{a}{c}$ . Then

$$\gamma^{-1}\mu = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Therefore we may assume that the coset representatives  $\mu$  of  $\Gamma_1 \backslash \mathcal{M}_n$  have the form

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

with  $ad = n$ ,  $b \in \mathbb{Z}$ .

Any different choice of representative for the coset containing  $\mu$  is of the form

$$\begin{aligned} & \gamma \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad \gamma \in \mathrm{SL}_2(\mathbb{Z}) \\ &= \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \Leftrightarrow \gamma = \pm \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, \quad r \in \mathbb{Z} \end{aligned}$$

which implies

$$\gamma \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \pm \begin{pmatrix} a & b + dr \\ 0 & d \end{pmatrix}.$$

So we can make the choice of representative  $\mu$  *unique* by requiring  $a, d > 0$  and  $0 \leq b < d$ . With this parametrization of  $\Gamma_1 \backslash \mathcal{M}_n$  we have

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

Plugging in the definition  $f(\tau) = \sum a(m)q^m$  of  $f(\tau)$  and letting  $a = n/d$  we get

$$\begin{aligned} &= n^{k-1} \sum_{\substack{d > 0 \\ d|n}} d^{-k} \sum_{b=0}^{d-1} \sum_{m \geq 0} a(m) e^{2\pi i m \left(\frac{n\tau + b}{d}\right)} \\ &= \sum_{m \geq 0} \sum_{\substack{d > 0 \\ d|n}} \left(\frac{n}{d}\right)^{k-1} a(m) e^{2\pi i m n \tau / d^2} \frac{1}{d} \sum_{b=0}^{d-1} e^{2\pi i m \frac{b}{d}} \end{aligned}$$

If  $d|m$  then the sum over  $b$  is the sum of 1 over  $d$  terms so equals  $d$ , and otherwise it is a geometric sum equal to 0. So we get

$$= \sum_{m \geq 0} \sum_{\substack{d > 0 \\ d|n, d|m}} \left(\frac{n}{d}\right)^{k-1} a(m) e^{2\pi i m n \tau / d^2}$$

then let  $m = ld$ ,

$$= \sum_{l \geq 0} \sum_{\substack{d > 0 \\ d|n}} \left(\frac{n}{d}\right)^{k-1} a(ld) e^{2\pi i l n \tau / d},$$

replace  $d$  by  $n/d$ ,

$$\begin{aligned} &= \sum_{l \geq 0} \sum_{\substack{d > 0 \\ d|n}} d^{k-1} a\left(\frac{ln}{d}\right) e^{2\pi i l d \tau} \\ &= \sum_{l \geq 0} \sum_{\substack{d > 0 \\ d|n}} d^{k-1} a\left(\frac{ln}{d}\right) q^{ld}. \end{aligned}$$

Now for fixed  $m$  we collect all terms with exponent  $ld = m$ , (so  $l = m/d$  and  $d|m$ )

$$= \sum_{m \geq 0} \sum_{\substack{d > 0 \\ d|n, d|m}} d^{k-1} a\left(\frac{mn}{d^2}\right) q^m.$$

*Proof of (ii):*

Part (ii) follows because the exponents of  $q$  on the right hand side of (i) are  $> 0$  ( $\geq 0$  respectively), because  $T_n f$  is holomorphic (from its original definition, it is the composition of holomorphic functions), and we know the modular transformation property holds since  $T_n f$  came from  $T_n F$  so by our bijection.

A short computation on the coefficients proves (iii). □

**2.1. Eigenforms.** We have seen that the  $T_n$  are linear operators on  $M_k$  (respectively  $S_k$ ).

Suppose  $f(\tau) = \sum_{m \geq 0} a(m)q^m$  is an eigenvector of all the  $T_n$  i.e.

$$(2.1) \quad T_n f = \lambda_n f \quad \forall n, \text{ some } \lambda_n \in \mathbb{C}.$$

*Example 2.3.* If  $k = 4, 6, 8, 10$ , or  $14$ , then  $\dim M_k = 1$  and is spanned by  $G_k$ , so it must be the case that

$$T_n G_k = \lambda_n G_k$$

for all  $n$ .

Comparing the Fourier coefficients of  $T_n$  from the Theorem (i) with the coefficients of (2.1) gives

$$(2.2) \quad \lambda_n a(m) = \sum_{d|n, m} d^{k-1} a\left(\frac{nm}{d^2}\right)$$

for  $f$ .

In particular (plug in  $m = 1$ ),

$$\lambda_n a(1) = a(n) \quad \forall n.$$

If  $f$  is not identically 0, then  $a(1) \neq 0$  by above, so we can normalize  $f$  by assuming  $a(1) = 1$ .

**Definition 2.4.** If  $f \in M_k$  such that  $T_n f = \lambda_n f$  for all  $n$ , and  $a(1) = 1$ ,  $f$  is called a **Hecke eigenform** (or “normalized Hecke eigenform”).

Since  $a(1) = 1$  and  $\lambda_n a(1) = a(n)$  this implies

$$\lambda_n = a(n) \quad \text{for all } n,$$

i.e. the Fourier coefficients of  $f$  are equal to its eigenvalues under the Hecke operators.

By (2.2) we get

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

in particular  $a(nm) = a(n)a(m)$  for all  $(n, m) = 1$  (for  $f$  a Hecke eigenform).

In particular this implies

$$a(p_1^{r_1} \cdots p_l^{r_l}) = a(p_1^{r_1}) \cdots a(p_l^{r_l})$$

and in fact, for  $n = p^r$  and  $m = p$  we get,

$$a(p^{r+1}) = a(p)a(p^r) - p^{k-1}a(p^{r-1}), \quad (r \geq 1)$$

so  $a(n)$  is determined if we know  $a(p)$  for all  $p$ .

*Example 2.5.*  $G_k \in M_k$  is a Hecke form for all  $k \geq 4$  with  $\lambda_n = a(n) = \sigma_{k-1}(n)$ .

*Example 2.6.*  $\Delta \in S_{12}$  is a Hecke form.

**Theorem 2.7.** *The Hecke forms in  $S_k$  form a basis of  $S_k$  for every  $k$ .*

Note: In fact this is also true for  $M_k$  but we will just prove the  $S_k$  case here.

*Proof.* It suffices to show that  $S_k$  is spanned by the Hecke forms and that they are all linearly independent.

**Petersson Scalar Product**

$$(f, g) := \int_{\mathbb{H}/\Gamma_1} \int y^k f(\tau) \overline{g(\tau)} d\mu$$

$f, g \in S_k$ ,  $\tau = x + iy$ ,  $d\mu = y^{-2} dx dy$  measure on  $\mathbb{H}$  (hyperbolic space).

This gives  $S_k$  the structure of a finite dimensional Hilbert space.

Using the definition of the  $T_n$  one can check that they are self adjoint with respect to  $(, )$ , i.e.

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

and from the first theorem we proved, we know they commute. Hence from the spectral theorem, the vector space  $S_k$  is spanned by simultaneous eigenvectors for all the  $T_n$ .

It remains to show the Hecke forms are linearly independent, but

(2.3)

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

by the self adjointness of  $T_n$  and the sesquilinearity of the scalar product. Therefore  $a(n) = \overline{a(n)}$  so the Fourier coefficients of  $f$  are real.

We use this to show linear independence. Let  $g = \sum b(n)q^n$  be a second eigenform in  $S_k$ , then the same computation shows

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

where the last line used that the  $b(n)$  are real. This implies  $(f, g) = 0$  for  $f \neq g$  so the Hecke forms in  $S_k$  are mutually orthogonal and hence linearly independent.  $\square$

In fact we can say more about the coefficients of a Hecke form in  $S_k$ . Using the Eisenstein series and the discriminant function one can prove the space  $S_k$  has a basis of forms all of whose Fourier coefficients are integral. The lattice of all such forms is preserved by  $T_n$ , hence the action of  $T_n$  on this space with respect to this basis is given by a  $d \times d$  matrix ( $d := \dim S_k$ ) with coefficients in  $\mathbb{Z}$ . In particular the eigenvalues of  $T_n$  are algebraic integers of degree  $\leq d$ , which implies

**Theorem 2.8.** *The Fourier coefficients of a Hecke form  $f \in S_k$  are real algebraic integers of degree  $\leq \dim S_k$ .*

## 3. FORMS OF HIGHER LEVEL

We have restricted our study to the “full modular group”  $\Gamma_1 = \mathrm{SL}_2(\mathbb{Z})$ . However, for my work (and many others!) I am primarily interested in modular (specifically cusp) forms for a specific subgroup of  $\Gamma_1$ ,

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1 : c \equiv 0 \pmod{N} \right\}$$

(fixed  $N \in \mathbb{N}$ ).

Much of the theory above is the same for  $\Gamma_0(N)$  as  $\Gamma_1$  but there are some important differences with the Hecke theory. We will now discuss some of these differences.

For forms of level  $N = 1$  (i.e.  $\Gamma_1$ ) the Theorem above is apparently *sharp* (in all cases which have been calculated), that is,

$$\mathrm{degree}(\mathbb{Q}(\{a(n)\})) = \dim S_k.$$

That is, the degree of the number field generated by the Fourier coefficients of a Hecke cusp form of weight  $k$  is equal to the dimension of  $S_k$ . So  $S_k$  is spanned by a single form and all its algebraic conjugates.

For forms of higher level, however, there are in general further splittings. In general for level  $N$ ,

$$S_k(\Gamma_0(N))^{\mathrm{new}} = \bigoplus_{i=1}^r W_{d_i}$$

splits as the sum of eigenspaces  $W_{d_i}$  of some dimensions  $d_1, \dots, d_r \geq 1$ , each of which is spanned by some Hecke form and the algebraic conjugates of this form,

$$W_{d_i} = \mathrm{span}(f_{d_i}^\sigma) \quad (\text{distinct}) \sigma \in \mathrm{Gal}(K_i/\mathbb{Q}).$$

(Note the Fourier coefficients of each Hecke form are in a totally real field  $K_i$  of degree  $d_i$  over  $\mathbb{Q}$ .) In general the number  $r$  and the dimensions  $d_i$  are unknown.

**Examples**

*Example 3.1.*  $k = 2, N = 11$ .  $\dim M_k(\Gamma_0(N)) = 2$  (nontrivial).

One “old form”:

$$G_2^*(\tau) - 11G_2^*(11\tau) = \frac{5}{12} + \sum_{n \geq 1} \left( \sum_{d|n, 11 \nmid d} d \right) q^n$$

One “new form”:

$$f(\tau) = (\Delta(\tau)\Delta(11\tau))^{1/12} = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \dots$$

with Fourier coefficients in  $\mathbb{Z}$ .

The famous Taniyama-Shimura-Weil Theorem (which, by Ribet, implied Fermat’s Last Theorem) proved by Wiles and others essentially states

**Theorem 3.2.** (*Taniyama-Shimura-Weil Theorem*)

*Any elliptic curve can be obtained via a rational map with integer coefficients from the classical modular curve  $X_0(N) := \Gamma_0(N) \backslash \mathbb{H}$ .*

Equivalently, for any elliptic curve  $E$  over  $\mathbb{Q}$  there exists a modular form  $f$  of weight 2 such that

$$L(E, s) = L(f, s)$$

where  $L(E, s) := \sum a_n n^{-s}$ ,  $L(f, s) = \sum a(n) n^{-s}$  are the corresponding  $L$ -functions of  $E, f$  respectively. (The converse, by Shimura, also holds for weight 2 Hecke newforms  $f$ ).

By this theorem, our weight 2  $f$  corresponds to an elliptic curve,

$$E : y^2 - y = x^3 - x^2.$$

Equivalent again to the above theorem is that the number of solutions to  $y^2 - y = x^3 - x^2$  in the integers mod  $p$  is given by  $p - a(p)$  for every prime  $p$ .

*Example 3.3.*  $k = 2$ ,  $N = 23$ .  $\dim M_k(\Gamma_0(N)) = 3$ .

One old form:

$$G_2^*(\tau) - NG_2^*(N\tau)$$

Two new forms:

$$f_1 = q - \frac{1 - \sqrt{5}}{2}q^2 + \sqrt{5}q^3 - \frac{1 + \sqrt{5}}{2}q^4 - (1 - \sqrt{5})q^5 - \frac{5 - \sqrt{5}}{2}q^6 + \dots$$

with coefficients in  $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{5}}{2}$ , and the conjugate form,

$$f_2 = q - \frac{1 + \sqrt{5}}{2}q^2 - \sqrt{5}q^3 - \frac{1 - \sqrt{5}}{2}q^4 - (1 + \sqrt{5})q^5 - \frac{5 + \sqrt{5}}{2}q^6 + \dots$$

obtained by replacing  $\sqrt{5}$  by  $-\sqrt{5}$  everywhere in  $f_1$ .

*Example 3.4.*  $k = 2$ ,  $N = 37$ .  $\dim M_k(\Gamma_0(N)) = 3$ .

One old form: Same one as before.

Two new forms:

$$f_1 = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + \dots$$

and

$$f_2 = q + 0q^2 + q^3 - 2q^4 + 0q^5 + 0q^6 - q^7 + \dots$$

both have coefficients in  $\mathbb{Z}$  (so are not conjugate). By the TSW Theorem, they each correspond to an elliptic curve,

$$\begin{aligned} E : y^2 - y &= x^3 - x \\ E : y^2 - y &= x^3 + x^2 - 3x + 1 \end{aligned}$$

respectively.

*Example 3.5.*  $k = 4$ ,  $N = 13$ .  $\dim M_k(\Gamma_0(N)) = 5$ .

Two old forms:

$$G_4(\tau), G_4(N\tau).$$

Three new forms:

$$f_1, f_2 = q + \frac{1 \pm \sqrt{17}}{2}q^2 + \frac{5 \mp 3\sqrt{17}}{2}q^3 - \frac{7 \mp \sqrt{17}}{2}q^4 + \dots$$

with coefficients in the real quadratic field  $\mathbb{Q}(\sqrt{17})$ , and the form

$$f_3 = q - 5q^2 - 7q^3 + 17q^4 - 7q^5 + 35q^6 - 13q^7 - \dots$$

with coefficients in  $\mathbb{Q}$ .

## REFERENCES

- D. Zagier, *Introduction to Modular Forms in One Variable*, lecture notes 1-46 (1991)  
*E-mail address:* `khopkins@math.utexas.edu`