April 14, 2:00 pm

1 First Facts About Spaces of Modular Forms

The set of modular forms of weight k for $SL(2,\mathbb{Z})$ form a complex vector space, as is clear from the definition of a modular form. We'll let $\mathcal{M}_{2k}(SL(2,\mathbb{Z}))$ denote the space of modular forms of weight $2k$. For brevity, when no confusion can arise, we may just write $\mathcal{M}_{2k}$. Further, let $\mathcal{S}_{2k} = \mathcal{S}_{2k}(SL(2,\mathbb{Z}))$ denote the subspace of $\mathcal{M}_{2k}$ consisting of cusp forms (those forms whose q-series expansion have constant term 0, which is clearly preserved under addition and scalar multiplication).

Note there is a natural homomorphism $\pi : \mathcal{M}_{2k} \to \mathbb{C}$ given by

$$\pi : f \mapsto f(\infty), \quad f(\infty) := c_0 \text{ , the constant term in the } q\text{-series expansion at infinity}$$

whose kernel is $\mathcal{S}_{2k}$. Moreover, for $2k \geq 4$, we have an Eisenstein series G_k in $\mathcal{M}_{2k}$ whose constant term $G_k(\infty) = 2\zeta(2k) \neq 0$. Since the map π is linear, then π is surjective for $2k \geq 4$, so we may write

$$\mathcal{M}_{2k} = \mathcal{S}_{2k} \oplus \mathbb{C}G_k,$$

a direct sum of vector spaces. In a subsequent section, we'll prove the following result:

Theorem 1 *The vector space $\mathcal{M}_{2k}$ has the following basis*

$$\mathcal{M}_{2k}(SL(2,\mathbb{Z})) = \langle G_2^a G_3^b \mid 4a + 6b = k \rangle,$$

where G_2, G_3 are Eisenstein series of weights 4 and 6, respectively.

This shows, in particular, that the dimension of these vector spaces is finite.

We've seen throughout the semester that Eisenstein series of low weight (Berndt labels them P, Q, R) played a role in Ramanujan's solutions to representations by sums of squares. As we noted then, those questions were easier when they related to modular forms of low weight because (as this theorem shows) modular forms of weight 4, 6, and 8 are one dimensional vector spaces. When the dimension of the space is larger than 1, how can we select modular forms with interesting coefficients? After all, since any complex-valued linear combination of basis elements is allowed, you'd like to somehow select a canonical basis. There are many ways to do this – the basis above in terms of Eisenstein series is one such way – but by far the most important for number theoretic applications is via the use of Hecke operators.

2 Hecke Operators: The Basic Idea

We'll again rely on Serre's exposition of this topic. We start by defining a natural map (technically a "correspondence" – an action on the free abelian group generated by a set) denoted $T(n)$ for any integer $n \geq 1$. For us, the set is the space of all complex lattices $\mathcal{R}$, so the free abelian group contains a basis element for each lattice. T(n) takes any lattice $\Gamma \in \mathcal{R}$ to a sum over all sublattices of index n. Formally, we write

$$T(n)\Gamma = \sum_{[\Gamma:\Gamma']=n} \Gamma' \quad \text{for any } \Gamma \in \mathcal{R}.$$

Recall that a sublattice $\Gamma' \subseteq \Gamma$ has index n if the quotient group Γ/Γ' has order n. In particular, all the lattices Γ' must contain $n\Gamma$, the lattice of all n multiples of elements in Γ. This implies that the number of sublattices of index n is equal to the number of subgroups of order n in $\Gamma/n\Gamma = (\mathbb{Z}/n\mathbb{Z})^2$. For those who know a bit of group theory, it is fairly elementary to check that if n is prime, the number of such lattices is $n+1$.

It is also useful to define "homothety operators" R_λ for $\lambda \in \mathbb{C}^\times$ by

$$R_\lambda(\Gamma) = \lambda\Gamma.$$

Regarded as an endomorphism of the free abelian group of $\mathcal{R}$, we may compose them with the $T(n)$.

Proposition 1 *We have the following identities among the correspondences $T(n)$ and R_λ:*

1. $R_\lambda R_\mu = R_{\lambda\mu}$ *for all* $\lambda, \mu \in \mathbb{C}^\times$.
2. $R_\lambda T(n) = T(n) R_\lambda$ *for any* $n \geq 1$, $\lambda \in \mathbb{C}^\times$.
3. $T(m)T(n) = T(mn)$ *for* $\gcd(m,n) = 1$.
4. $T(p^n)T(p) = T(p^{n+1}) + pT(p^{n-1})R_p$, *for* p *prime,* $n \geq 1$.

Proof The first two properties follow immediately from the definitions above. As for (3), if m, n are relatively prime, it suffices to show that to each sublattice Γ'' of Γ of index mn, there exists a unique sublattice Γ' with $\Gamma'' \subseteq \Gamma' \subseteq \Gamma$ with $[\Gamma : \Gamma'] = n$ and $[\Gamma' : \Gamma''] = m$. This, in turn, follows from the fact that the group Γ/Γ'', of order mn decomposes uniquely into a direct sum of a group of order m and a group of order n. (Serre calls this "Bezout's Theorem" which is a statement about how two algebraic curves of degree m and n intersect in at most mn points (counting correctly), where his curves are now defined over finite fields. My initial reaction is to use the structure theorem for finite abelian groups.)

Finally, to prove (4), we note that all three correspondences in the identity – $T(p^n)T(p), T(p^{n+1})$, and $T(p^{n-1})R_p$ produce sums of lattices of index p^{n+1} in Γ. Suppose Γ'' is a lattice appearing in these correspondences for Γ. Then it appears for $T(p^n)T(p)$ with integer coefficient a, with coefficient 1 in $T(p^{n+1})$ (which is just the sum of ALL lattices of index p^{n+1}) and coefficient c in $T(p^{n-1})R_p$. So to prove the relation, we must show that for any such lattice Γ'', $a = 1 + pc$. We consider two cases (and drawing a picture of these cases can be quite helpful as their just lattices in $\mathbb{C}$):

First, suppose $\Gamma'' \nsubseteq p\Gamma$. Then it will not appear in R_p and hence $c = 0$. Further, a is the number of lattices between Γ and Γ'' of index p in Γ. Any such lattice Γ' (as we remarked earlier) must contain $p\Gamma$ and is characterized by its image as a subgroup of index p in $\Gamma/p\Gamma$. Since Γ' must contain the image of Γ'' which must be of order p (and hence index p) in the quotient group, this uniquely characterizes Γ', so $a = 1$ as desired.

Finally, if $\Gamma'' \subseteq p\Gamma$, then $c = 1$. In this case, the intermediate lattices Γ' of index p in Γ will again contain $p\Gamma$ and thus automatically Γ''. As remarked above, there are $p + 1$ such subgroups of index p in $p\Gamma$, so $a = p + 1$, again satisfying the relation $a = 1 + pc$. □

Corollary 1 *The correspondences $T(p^n)$, $n \geq 1$ can be expressed as polynomials in $T(p)$ and R_p.*

This follows by induction using part (4) of the proposition repeatedly to reduce the powers of p.

Corollary 2 *The algebra generated by the correspondences R_λ and $T(p)$ for p prime is commutative and contains all the $T(n)$.*

This is clear from (1), (2), (3) and the above corollary.

These correspondences can also be extended to functions F on the space of lattices, by

$$R_\lambda(F(\Gamma)) = F(R_\lambda(\Gamma)), \quad T(n)(F(\Gamma)) = F(T(n)\Gamma).$$

In particular, if F is a function on $\mathcal{R}$ of weight 2k, then

$$R_\lambda(F) = \lambda^{-2k} F \quad \text{for all } \lambda \in \mathbb{C}^\times.$$

Since the $T(n)$ commute with the R_λ,

$$R_\lambda(T(n)F) = T(n)(R_\lambda F) = \lambda^{-2k}T(n)F$$

which shows that $T(n)F$ is again a weight $2k$ function. Moreover, the actions in the above proposition can be rewritten for weight 2k functions as

$$T(m)T(n)F = T(mn)F, \ \gcd(m,n) = 1$$

$$T(p)T(p^n)F = T(p^{n+1})F + p^{1-2k}T(p^{n-1})F, \text{ for } p \text{ prime}, \ n \geq 1$$

This can be translated into an action on the space of modular forms of weight $2k$. In the next section, we will translate the action of Hecke operators $T(n)$ into the language of matrices, which give a much more concrete and computationally beneficial way of understanding the correspondences. Then we'll use some facts from linear algebra, including the spectral theorem, to show that the space of cusp forms (which has an inner product to be defined) has an orthonormal basis which can be simultaneously diagonalized by the $T(p)$ with p prime. As we might expect, these so-called Hecke eigenforms are quite special, and are conjectured (and in some cases proven) to have deep connections with number theory and arithmetic geometry.

3 Using matrices to define Hecke operators

Given a lattice Γ with basis $\{\omega_1, \omega_2\}$ and an integer $n \geq 1$, the following result explains how to obtain all sublattices of Γ of index n.

Proposition 2 *Let B_n be the set of integer matrices of form*

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \qquad ad = n, a \geq 1, 0 \leq b < d$$

To each matrix $b \in B_n$, let Γ_b be the sublattice of Γ having basis

$$\omega_1' = a\omega_1 + b\omega_2, \quad \omega_2 = d\omega_2'.$$

Then the map $b \mapsto \Gamma_b$ is a bijection of B_n with the set of sublattices $\Gamma(n)$ of index n in Γ.

Proof First, note Γ_b belongs to $\Gamma(n)$ since $\det(b) = n$. Given any $\Gamma' \in \Gamma(n)$, let

$$Y_1 = \Gamma/(\Gamma' + \mathbb{Z}\omega_2), \quad Y_2 = \mathbb{Z}\omega_2/(\Gamma' \cap \mathbb{Z}\omega_2).$$

These are finite cyclic groups generated by the images of ω_1 and ω_2, respectively, in the quotient group Γ/Γ'. Let their orders be a and d. The exact sequence

$$0 \to Y_2 \to \Gamma/\Gamma' \to Y_1 \to 0$$

implies that $ad = n$ (counting cardinalities). If $\omega_2' = d\omega_2$ then $\omega_2' \in \Gamma'$. Moreover, there exists an $\omega_1' \in \Gamma'$ such that $\omega_1' \equiv a\omega_1$ $(\mathbb{Z}\omega_2)$. (That is, the two elements differ by an element of $\mathbb{Z}\omega_2$.) Then ω_1' and ω_2' give a basis of Γ' and

$$\omega_1' = a\omega_1 + b\omega_2 \text{ for some } b \in \mathbb{Z}$$

with b uniquely determined mod d. Thus, picking b such that $0 \le b < d$ uniquely determines b. Of course, the map we have just constructed is the inverse of that described in the proposition, giving the bijection. □

As an example, let p be a prime. Then the elements of B_p, in bijection with $\Gamma(p)$ are the $p+1$ matrices:

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \cup \left\{ \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} \mid 0 \le b < p \right\}$$

4 Hecke operators acting on modular functions

Recall that weakly modular functions f of weight $2k$ are associated to functions F of weight $2k$ on the space of lattices $\mathcal{R}$ by the equality

$$F(\Gamma(\omega_1, \omega_2)) = \omega_2^{-2k} f(\omega_1/\omega_2).$$

So we can immediately give an action of $T(n)$ on f via this equality. Let $T(n)f$ be the function on $\mathcal{H}$ associated to the function $n^{2k-1}T(n)F$. (The coefficient n^{2k-1} ends up giving a convenient normalization, but is otherwise inconsequential.) More precisely,

$$T(n)f(z) = n^{2k-1}T(n)F(\Gamma(z,1)).$$

Using the result of proposition in the last section, describing sublattices according to change of basis matrices with determinant n, we have

$$T(n)f(z) = n^{2k-1} \sum_{a \ge 1, ad=n, 0 \le b < d} d^{-2k} f\left(\frac{az+b}{d}\right). \tag{1}$$

Proposition 3 *If f is a weakly modular function of weight $2k$, so is $T(n)f$. If f is holomorphic, so is $T(n)f$. Additionally,*

$$T(m)T(n)f = T(mn)f \ \ \gcd(m,n) = 1$$

$$T(p)T(p^n)f = T(p^{n+1})f + p^{2k-1}T(p^{n-1})f, \text{ for } p \text{ prime}, \ n \geq 1$$

This follows immediately from the explicit definition of $T(n)f$ in terms of matrices above, which verifies that $T(n)f$ is meromorphic or holomorphic if f is meromorphic or holomorphic. The transformation formulas follow from our normalized definition for $T(n)f$ using n^{2k-1} and are based on similar transformation formulas given above for $T(n)F$.

Finally, we want to describe the effect of Hecke operators on f as a q-series expansion at infinity.

Theorem 2 *Given a modular function*

$$f(z) = \sum_{m \in \mathbb{Z}} c(m) q^m \quad q = e^{2\pi i z},$$

then the modular function $T(n)f$ has q-series

$$T(n)f(z) = \sum_{m \in \mathbb{Z}} \gamma(m) q^m \quad \text{with} \quad \gamma(m) = \sum_{a | \gcd(m,n), a \geq 1} a^{2k-1} c\left(\frac{mn}{a^2}\right)$$

Proof By the matrix action given in (1) above,

$$T(n)f(z) = n^{2k-1} \sum_{a \geq 1, ad=n, 0 \leq b < d} d^{-2k} \sum_{m \in \mathbb{Z}} c(m)\, e\left(\frac{m(az+b)}{d}\right)$$

where we've used the usual convention that $e(z) := e^{2\pi i z}$. This double sum simplifies by noting that

$$\sum_{0 \leq b < d} e(mb/d) = \begin{cases} d & d|m \\ 0 & \text{otherwise.} \end{cases}$$

since the exponential is trivial if $d|m$ and otherwise we're summing over a complete set of roots of unity modulo a divisor of d. Hence we may assume $d|m$ and make the change of variables $m = dm'$ in the above sum, giving

$$T(n)f(z) = n^{2k-1} \sum_{a \geq 1, ad=n, m' \in \mathbb{Z}} d^{-2k+1} c(dm')\, q^{am'}.$$

Collecting powers of q by taking $am' = \mu$, we have

$$T(n)f(z) = \sum_{\mu \in \mathbb{Z}} q^{\mu} \sum_{a \geq 1, a | \gcd(n,\mu)} a^{2k-1} c\left(\frac{\mu d}{a}\right).$$

Note that since f is meromorphic at infinity, so by definition there is an $N \geq 0$ such that $c(m) = 0$ for all $mleq - N$, then $c(\mu d/a)$ must be 0 for $\mu \leq -nN$, and hence $T(n)f$ is likewise meromorphic at infinity. Recalling that $ad = n$, the above formula gives the desired result as well. □

As a consequence, we have

$$\gamma(0) = \sigma_{2k-1}(n)c(0), \quad \gamma(1) = c(n)$$

Moreover, if $n = p$, p prime, then

$$\gamma(m) = \begin{cases} c(pm), & m \not\equiv 0 \pmod{p} \\ c(pm) + p^{2k-1}c(m/p) & m \equiv 0 \pmod{p} \end{cases}$$

Corollary 3 *If $f \in \mathcal{M}_{2k}$, then $T(n)f \in \mathcal{M}_{2k}$. If $f \in \mathcal{S}_{2k}$, then $T(n)f \in \mathcal{S}_{2k}$. (I.e. the operators $T(n)$ act on these spaces.)*

This follows immediately from our formula for the q-series at infinity for $T(n)f$, which shows that if $c(m) = 0$ for m negative, then $\gamma(m) = 0$ for these integers as well. The constant term computation verifies the $T(n)$ act on $\mathcal{S}_{2k}$.

5 Eigenfunctions of the $T(n)$

Given two cusp forms $f, g \in \mathcal{S}_{2k}$, then we may define a measure on $\mathcal{S}_{2k}$ by

$$\mu(f,g) = f(z)\overline{g(z)}y^{2k}\frac{dxdy}{y^2}, \quad z = x + iy.$$

One can check that this measure is invariant under action of G (Try it!) and that it is a bounded measure on the quotient space $\mathcal{H}/G$ (because f, g are cusp forms, and with regard to the q-expansion, $q \to \infty$ very quickly as $z \to i\infty$). Hence,

$$\langle f, g\rangle = \int_{H/G} \mu(f,g) = \int_D f(z)\overline{g(z)}y^{2k-2}dxdy$$

defines a positive definite Hermitian inner product on $\mathcal{S}_{2k}$. By Hermitian (or "self-adjoint") we mean that

$$\langle T(n)f, g\rangle = \langle f, T(n)g\rangle.$$

Then, because the $T(n)$ commute with each other, by the spectral theorem (assuming the finite dimensionality of the space $\mathcal{S}_{2k}$ yet to be proved), there exists an orthogonal basis of $\mathcal{S}_{2k}$ consisting of simultaneous eigenvectors of $T(n)$. Further, the eigenvalues of the $T(n)$ are real numbers.

As we will show later, $\mathcal{S}_{12}$ has dimension 1, and contains the cusp form $\Delta(z)$. Hence $\Delta(z)$ must be an eigenfunction of the Hecke operators $T(n)$ of weight 12 for all n. In what follows, suppose that

$$f(z) = \sum_{n=0}^{\infty} c(n)q^n$$

is a non-zero modular form of weight $2k$ (not necessarily a cusp form) and that f is an eigenfunction of all the $T(n)$. That is, there exist complex numbers $\lambda(n)$ such that

$$T(n)f = \lambda(n)f \quad \text{for all } n \geq 1.$$

(So far, we have only asserted the existence of such eigenforms for $\mathcal{S}_{2k}$ but we'll see other examples in $\mathcal{M}_{2k}$ shortly.)

Proposition 4 *Given f as above, the coefficient $c(1)$ of q^1 is non-zero. Moreover, if we normalize f by multiplying by a constant so that $c(1) = 1$, then*

$$c(n) = \lambda(n) \quad \textit{for all } n > 1.$$

Proof In the previous section we saw that $\gamma(1)$, the coefficient of q^1 in $T(n)f$ is $c(n)$. On the other hand, by assuming f is an eigenfunction, we have that $T(n)f = \lambda(n)f$ so $\gamma(1) = \lambda(n)c(1)$. Putting these together, we have $c(n) = \lambda(n)c(1)$. If $c(1) = 0$, then the equality implies that $c(n)$ is zero for all n, hence f is a constant, which is a contradiction. The second statement of the proposition now follows immediately from the previous equality upon normalizing. □

Corollary 4 *Two modular forms of weight $2k$, $k > 0$, which are eigenfunctions of the $T(n)$ with matching eigenvalues $\lambda(n)$ for all n and which are normalized, are in fact equal.*

Use the same proof as the proposition, applied to the difference of the two modular forms.

Corollary 5 *Given a normalized eigenform f as above, with q-series coefficients $c(m)$, then*

$$c(m)c(n) = c(mn) \quad \gcd(m,n) = 1$$
$$c(p)c(p^n) = c(p^{n+1}) + p^{2k-1}c(p^{n-1})$$

This follows because the eigenvalues $\lambda(n)$ (which equal $c(n)$ for a normalized form) satisfy the same identities as the $T(n)$ presented in Proposition 3. In short, the coefficients of an eigenfunction of Hecke operators are multiplicative (on relatively prime pairs of integers – this is typically what is meant by "multiplicative" in the analytic number theory literature).

6 Dirichlet series made from modular forms

A Dirichlet series is an infinite series of the form

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

where the coefficients $a(n)$ should be bounded as a function of n, say $O(n^{m-1})$ for some positive integer m. (This notation means that $a(n) < Cn^{m-1}$ for some constant C.) In this case, the Dirichlet series converges for $\mathrm{Re}(s) > m$. Our prototype example is the Riemann zeta function, where $a(n) = 1$ for all n, so we may take $m = 1$, as is well known. The zeta function possesses a functional equation as $s \to 1 - s$ and has connections to number theory owing to its product representation as a product over primes – an "Euler product":

$$\zeta(s) = \prod_p \left(1 - p^{-s}\right)^{-1}, \quad \mathrm{Re}(s) > 1$$

This allows one to prove, for example, the prime number theorem (which counts the number of primes up to x asymptotically as $x \to \infty$) via analytic properties of the Dirichlet series, like location of poles. You may have seen other variants of zeta function, where $a(n) = \chi_d(n)$, where

$$\chi_d : \mathbb{Z} \to (\mathbb{Z}/d\mathbb{Z})^\times \to \mathbb{C}.$$

That is, χ_d is a homomorphism from the multiplicative group $(\mathbb{Z}/d\mathbb{Z})^\times$ extended to the integers. To be a homomorphism, it's image in $\mathbb{C}^\times$ must be a finite multiplicative group, and hence lie on the complex unit circle. Again, a Dirichlet series made with

$\chi_d(n)$ will converge for $\text{Re}(s) > 1$, and since $\chi_d(n)$ is multiplicative, we again have an Euler product

$$\sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s} = \prod_p \left(1 - \chi_d(p)p^{-s}\right)^{-1}, \quad \text{Re}(s) > 1.$$

Analytic properties of this series (namely that it's value at 1 upon analytic continuation is non-zero) were used to show there are infinitely many primes congruent to c mod d for any c relatively prime to d.

Here, we construct a Dirichlet series from the Fourier coefficients (i.e. q-series coefficients) of a modular form:

$$f(z) = \sum_{n=0}^{\infty} c(n)q^n \mapsto \Phi(s, f) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s}$$

Note that we omit the constant term in passing to the Dirichlet series. Again, we'll need growth estimates on the size of the Fourier coefficients to conclude that the Dirichlet series converges in a right half plane of the complex plane. We'll obtain these very shortly, but first we note an important property.

Proposition 5 *Let $f \in \mathcal{M}_{2k}$ be an eigenfunction of the Hecke operators $T(n)$. Then $\Phi(s, f)$ has an Euler product (for s in the region of absolute convergence):*

$$\Phi(s, f) = \prod_{p:prime} \left(1 - c(p)p^{-s} + p^{2k-1-2s}\right)^{-1}$$

Proof The coefficients $c(n)$ are multiplicative, since f is an eigenfunction of the Hecke operators. In the region of absolute convergence, we may thus write

$$\sum_{n=1}^{\infty} \frac{c(n)}{n^s} = \prod_{p:\text{prime}} \left(\sum_{m=0}^{\infty} c(p^m)p^{-ms} \right).$$

Typically, this is rigorously justified by taking S to be a finite set of primes, and thus asserting the equality between the sum over $n \in N(S)$ ($N(S)$ are integers with prime factors in S) and the product over $p \in S$. We then take the limit as S increases, and note the sum tends to the left-hand side above. Hence the infinite product converges and equals the left-hand side.

Hence, to finish the proposition, it suffices to prove a generating function identity:

$$\sum_{m=0}^{\infty} c(p^m)T^m = \frac{1}{1 - c(p)T + p^{2k-1}T^2}$$

This follows immediately from the recursion asserted in corollary 5:

$$c(p)c(p^n) = c(p^{n+1}) + p^{2k-1}c(p^{n-1})$$

by standard generating function techniques. Or, simpler but less motivated, we may consider

$$\psi(T) = \left(\sum_{m=0}^{\infty} c(p^m)T^m\right)(1 - c(p)T + p^{2k-1}T^2)$$

and try to prove $\psi(T) = 1$. We verify the coefficient of T^m is 0 for $m > 0$ by again resorting to the recursion for prime powers, leaving only the constant term as desired. □

Note, we've talked about products a lot in class, and even used the letter q, often used to denote primes. But there, q was the parameter in the Fourier series, $q = e^{2\pi iz}$, and here we're taking a product over primes. At this point, it is not at all clear how we'll use the Euler product to any effect.

7 Examples of L-functions

Series that satisfy nice analytic properties like those of the Riemann zeta function, Dirichlet L-functions, and Dirichlet series associated to modular forms are typically all referred to as L-series, after Dirichlet. (It's not clear what L is meant to stand for. Some believe Dirichlet was paying tribute in his notation to Legendre, but maybe sometimes an L is just an L.) More specifically, L-functions should possess the following properties:

- They are initially defined for complex s sufficiently large, and possess analytic continuation to a meromorphic function on $\mathbb{C}$.
- They satisfy an "Euler product" – a product over an infinite set of primes
- They satisfy a functional equation (akin to that of the Riemann zeta function, which relates $\zeta(s)$ to $\zeta(1-s)$ up to Gamma factors)

In this section, we'll discuss these properties for $\Phi(s, f)$, thus asserting it is an L-function associated to a modular form f.

Proposition 6 *Let G_k be the weight $2k$ Eisenstein series with Fourier coefficients $a(n)$. There exist positive constants A, B such that*

$$An^{2k-1} \leq |a(n)| \leq Bn^{2k-1}$$

We leave the proof as an exercise to the reader. (Hint: use the explicit Fourier expansion derived earlier in terms of the divisor function.)

Corollary 6 *The Dirichlet series $\Phi(s, G_k)$ formed with the Fourier coefficients of G_k converges for Re$(s) > 2k$.*

This follows immediately from the previous proposition and the well-known convergence of $\sum_n n^{-\alpha}$ for $\alpha > 1$. Similar facts will follow for all modular forms, once we prove they're generated by Eisenstein series. For cusp forms, however, we can do much better.

Theorem 3 (Hecke) *If $f \in \mathcal{S}_{2k}$, the space of cusp forms of weight $2k$, then*

$$a(n) = O(n^k).$$

That is, the quotient $a(n)/n^k$ remains bounded as $n \to \infty$.

Proof Consider the function $\phi(z) = |f(z)|y^k$ where $z = x + iy$. Remembering how the imaginary part y transforms under action by G, we see ϕ is invariant under G. Since ϕ is continuous on the fundamental domain, and $|f(z)| = O(q) = O(e^{-2\pi y})$ implies $\phi \to 0$ as $y \to \infty$, then ϕ is bounded on $\mathcal{H}$. That is, there exists an M such that

$$|f(z)| \leq My^{-k} \quad \text{for all } z \in \mathcal{H}. \tag{2}$$

How can we use this information to extract info about the Fourier coefficients? Now the sneaky idea: For fixed y, letting x vary from 0 to 1 gives $q = e^{2\pi i(x+iy)}$ running along a circle of radius $e^{-2\pi y}$ centered at the origin. Call this circle C_y and consider the contour integral:

$$\frac{1}{2\pi i}\int_{C_y} f(z)q^{-n-1}dq = \int_0^1 f(x+iy)q^{-n}dx.$$

By residue theorem, this is just $a(n)$. On the other hand, using (2), this integral is bounded above by $My^{-k}e^{-2\pi ny}$, valid for any $y > 0$. Choosing $y = 1/n$ gives the desired bound. □

In fact, one can do a bit better than this result. Deligne has shown that for cusp forms that

$$a(n) = O(n^{k-1/2}\sigma_0(n)) = O(n^{k-1/2+\epsilon}) \quad \text{for any } \epsilon > 0.$$

where $\sigma_0(n)$ is just the sum of positive divisors of n. So we basically save 1/2. This might not seem like a big deal, but it is extremely deep and follows from what is known as the "Riemann hypothesis for curves" which Deligne won a Fields Medal for proving in the early '70's.

Proposition 7 *The Eisenstein series G_k is an eigenfunction of the $T(n)$. The corresponding eigenvalue is $\sigma_{2k-1}(n)$ and the normalized eigenfunction then has q-series*

$$(-1)^k \frac{B_k}{4k} E_k := (-1)^k \frac{B_k}{4k} + \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

where we've normalized so that $T(1) = 1$. Hence, the corresponding Dirichlet series is $\zeta(s)\zeta(s-2k+1)$, a product of Riemann zeta functions.

Proof To prove G_k is an eigenfunction, it suffices to prove this on a generating set $T(p)$, p prime. Recalling the lattice definition, we have (as a function on $\mathcal{R}$, the space of lattices)

$$G_k(\Gamma) = \sum_{\gamma \neq (0,0) \in \Gamma} \frac{1}{\gamma^{2k}}$$

and hence

$$T(p) G_k(\Gamma) = \sum_{[\Gamma:\Gamma']=p} \sum_{\gamma \neq (0,0) \in \Gamma'} \frac{1}{\gamma^{2k}}$$

Given $\gamma \in \Gamma$, if $\gamma \in p\Gamma$ then it lies in all $(p+1)$ sublattices of index p, and thus contributes $(p+1)/\gamma^{2k}$ to $T(p)G_k$. If $\gamma \in \Gamma \backslash p\Gamma$, then as we saw before, γ belongs to a unique sublattice of index p, so contributes $1/\gamma^{2k}$. Hence,

$$T(p) G_k(\Gamma) = G_k(\Gamma) + p \sum_{\gamma \neq (0,0) \in p\Gamma} \frac{1}{\gamma^{2k}} = G_k(\Gamma) + p G_k(p\Gamma) = (1 + p^{1-2k}) G_k(\Gamma).$$

This says G_k, as a function on the space of lattices, is an eigenfunction of the $T(p)$ with eigenvalue $1 + p^{1-2k}$. Recalling how to translate to modular forms, this implies $G_k(z)$ is an eigenfunction with eigenvalue $p^{2k-1}(1 + p^{1-2k}) = \sigma_{2k-1}(p)$ as desired. Hence, it is an eigenfunction of all the $T(n)$, and recalling that $a(n) = T(n)$ for a normalized form, we have $T(n) = \sigma_{2k-1}(n)$ for general n from our earlier formulas for the q-series. We leave the final identity for the Dirichlet series as a product of zeta functions as an exercise to the reader. □

Even if we hadn't known the description in terms of zeta functions, which instantly gives an Euler product, we would obtain one from results in the last section which give such a product for any Hecke eigenform. (Check that the Euler product from the two zeta functions matches the form of the one given for Hecke eigenfunctions in the previous section.)

We've now addressed many of the bullet points. It remains to say something about analytic continuation and functional equations. Just like in the proof of the continuation and functional equation for the Riemann zeta function, we often handle both properties in one fell swoop. Let

$$\Phi^*(s, f) = (2\pi)^{-s}\Gamma(s)\Phi(s, f)$$

(almost exactly the same as we do for $\zeta(s)$. Can you see what is different?) Then Hecke proved that

$$\Phi^*(s, f) = (-1)^k \Phi^*(2k - s, f)$$

using the Mellin transform of f defined by

$$\int_0^\infty (f(iy) - f(\infty)) y^s \frac{dy}{y} = \Phi^*(s, f).$$

One checks this equality simply by expanding f as a q-series, reversing the order of summation and integration, and performing a change of variables in the resulting integral. To prove a functional equation, we simply note that $f(-1/z) = z^{2k} f(z)$. Substituting this into the integral gives the functional equation. (Noting that the integral gives a meromorphic function on $\mathbb{C}$ provides the analytic continuation.)

So we have obtained L-functions from modular forms, including the examples G_k, $k \geq 2$, and Δ, the cusp form of weight 12. We don't exactly know what they're good for yet, but here's a hint that they're important. Suppose that you have a Dirichlet series formed from a q-series for a function f with good growth properties and a functional equation as $s \mapsto 2k - s$. Then Hecke proves your function is a modular form of weight $2k$ – a sort of converse theorem to this set of analytic properties.

References

[1] T. M. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, Second Edition, Graduate Texts in Mathematics, vol. 41, Springer-Verlag (1990).

[2] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer-Verlag (1973).