Part III — Modular Forms and L-functions
Theorems with proof

Based on lectures by A. J. Scholl
Notes taken by Dexter Chua

Lent 2017

Modular Forms are classical objects that appear in many areas of mathematics, from number theory to representation theory and mathematical physics. Most famous is, of course, the role they played in the proof of Fermat's Last Theorem, through the conjecture of Shimura-Taniyama-Weil that elliptic curves are modular. One connection between modular forms and arithmetic is through the medium of L-functions, the basic example of which is the Riemann ζ-function. We will discuss various types of L-function in this course and give arithmetic applications.

Pre-requisites

Prerequisites for the course are fairly modest; from number theory, apart from basic elementary notions, some knowledge of quadratic fields is desirable. A fair chunk of the course will involve (fairly 19th-century) analysis, so we will assume the basic theory of holomorphic functions in one complex variable, such as are found in a first course on complex analysis (e.g. the 2nd year Complex Analysis course of the Tripos).

Contents

0 Introduction

1 Some preliminary analysis

1.1 Characters of abelian groups

Theorem (Pontryagin duality)**.** *Pontryagin duality* If G is locally compact, then $G \to \hat{\hat{G}}$ is an isomorphism.

Proposition. Let G be a finite abelian group. Then $|\hat{G}| = |G|$, and G and $\hat{G}$ are in fact isomorphic, but not canonically.

Proof. By the classification of finite abelian groups, we know G is a product of cyclic groups. So it suffices to prove the result for cyclic groups $\mathbb{Z}/N\mathbb{Z}$, and the result is clear since

$$\widehat{\mathbb{Z}/N\mathbb{Z}} = \mu_N \cong \mathbb{Z}/N\mathbb{Z}.$$

□

1.2 Fourier transforms

Proposition. If $f \in \mathcal{S}(\mathbb{R})$, then $\hat{f} \in \mathcal{S}(\mathbb{R})$, and the *Fourier inversion formula*

$$\hat{\hat{f}} = f(-x)$$

holds.

Proposition.

$$f(x) = \sum_{n \in \mathbb{Z}} c_n(f) e^{2\pi i n x} = \sum_{n \in \mathbb{Z} \cong \hat{G}} c_n(f) \chi_n(x).$$

Proposition. For a function $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, we have

$$f(x) = \frac{1}{N} \sum_{\zeta \in \mu_N} \zeta^x \hat{f}(\zeta).$$

Proof. We see that both sides are linear in f, and we can write each function f as

$$f = \sum_{a \in \mathbb{Z}/N\mathbb{Z}} f(a)\delta_a,$$

where

$$\delta_a(x) = \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases}.$$

So we wlog $f = \delta_a$. Thus we have

$$\hat{f}(\zeta) = \zeta^{-a},$$

and the RHS is

$$\frac{1}{N} \sum_{\zeta \in \mu_N} \zeta^{x-a}.$$

We now note the fact that

$$\sum_{\zeta \in \mu_N} \zeta^k = \begin{cases} N & k \equiv 0 \pmod N \\ 0 & \text{otherwise} \end{cases}.$$

So we know that the RHS is equal to δ_a, as desired. □

Theorem. Let G be a locally compact abelian group G. Then there is a Haar measure on G, unique up to scaling.

Theorem (Fourier inversion theorem)**.** Given a locally compact abelian group G with a fixed Haar measure, there is some constant C such that for "suitable" $f : G \to \mathbb{C}$, we have

$$\hat{\hat{f}}(g) = Cf(-g),$$

using the canonical isomorphism $G \to \hat{\hat{G}}$.

Theorem (Poisson summation formula)**.** Let $f \in \mathcal{S}(\mathbb{R}^n)$. Then

$$\sum_{a \in \mathbb{Z}^n} f(a) = \sum_{b \in \mathbb{Z}^n} \hat{f}(b).$$

Proof. Let

$$g(x) = \sum_{a \in \mathbb{Z}^n} f(x + a).$$

This is now a function that is invariant under translation of $\mathbb{Z}^n$. It is easy to check this is a well-defined C^∞ function on $\mathbb{R}^n/\mathbb{Z}^n$, and so has a Fourier series. We write

$$g(x) = \sum_{b \in \mathbb{Z}^n} c_b(g) e^{2\pi i b \cdot x},$$

with

$$c_b(g) = \int_{\mathbb{R}^n/\mathbb{Z}^n} e^{-2\pi i b \cdot x} g(x)\,\mathrm{d}x = \sum_{a \in \mathbb{Z}^n} \int_{[0,1]^n} e^{-2\pi i b \cdot x} f(x + a)\,\mathrm{d}x.$$

We can then do a change of variables $x \mapsto x - a$, which does not change the exponential term, and get that

$$c_b(g) = \int_{\mathbb{R}^n} e^{-2\pi i b \cdot x} f(x)\,\mathrm{d}x = \hat{f}(b).$$

Finally, we have

$$\sum_{a \in \mathbb{Z}^n} f(a) = g(0) = \sum_{b \in \mathbb{Z}^n} c_b(x) = \sum_{b \in \mathbb{Z}^n} \hat{f}(b). \qquad \square$$

1.3 Mellin transform and Γ-function

Lemma. Suppose $f : \mathbb{R}_{>0} \to \mathbb{C}$ is such that

- $y^N f(y) \to 0$ as $y \to \infty$ for all $N \in \mathbb{Z}$
- there exists m such that $|y^m y(f)|$ is bounded as $y \to 0$

Then $M(f, s)$ converges and is an analytic function of s for $\mathrm{Re}(s) > m$.

Proof. We know that for any $0 < r < R < \infty$, the integral

$$\int_r^R y^s f(y)\,\frac{\mathrm{d}y}{y}$$

is analytic for all s since f is continuous.

By assumption, we know $\int_R^\infty \to 0$ as $R \to \infty$ uniformly on compact subsets of $\mathbb{C}$. So we know

$$\int_r^\infty y^s f(y)\,\frac{\mathrm{d}y}{y}$$

converges uniformly on compact subsets of $\mathbb{C}$.

On the other hand, the integral $\int_0^r$ as $r \to 0$ converges uniformly on compact subsets of $\{s \in \mathbb{C} : \mathrm{Re}(s) > m\}$ by the other assumption. So the result follows. □

Proposition.

$$M(f(\alpha y), s) = \alpha^{-s} M(f, s)$$

for $\alpha > 0$.

Proposition.

$$s\Gamma(s) = \Gamma(s+1).$$

Proposition. For an integer $n \geq 1$, we have

$$\Gamma(n) = (n-1)!.$$

Proposition.

(i) The *Weierstrass product*: We have

$$\Gamma(s)^{-1} = e^{\gamma s} s \prod_{n \geq 1} \left(1 + \frac{s}{n}\right) e^{-s/n}$$

for all $s \in \mathbb{C}$. In particular, $\Gamma(s)$ is never zero. Here γ is the *Euler-Mascheroni constant*, given by

$$\gamma = \lim_{n \to \infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right).$$

(ii) *Duplication and reflection formulae*:

$$\pi^{\frac{1}{2}} \Gamma(2s) = 2^{2s-1} \Gamma(s) \Gamma\left(s + \frac{1}{2}\right)$$

and

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi z}.$$

2 Riemann ζ-function

Proposition (Euler product formula)**.** We have

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

Proof. Euler's proof was purely formal, without worrying about convergence. We simply note that

$$\prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} = \prod_p (1 + p^{-s} + (p^2)^{-s} + \cdots) = \sum_{n \geq 1} n^{-s},$$

where the last equality follows by unique factorization in $\mathbb{Z}$. However, to prove this properly, we need to be a bit more careful and make sure things converge.

Saying the infinite product $\prod_p$ convergence is the same as saying $\sum p^{-s}$ converges, by basic analysis, which is okay since we know $\zeta(s)$ converges absolutely when $\mathrm{Re}(s) > 1$. Then we can look at the difference

$$\begin{aligned}\zeta(s) - \prod_{p \leq X} \frac{1}{1 - p^{-s}} &= \zeta(s) - \prod_{p \leq X} (1 + p^{-s} + p^{-2s} + \cdots) \\ &= \prod_{n \in \mathcal{N}_X} n^{-s},\end{aligned}$$

where $\mathcal{N}_X$ is the set of all $n \geq 1$ such that at least one prime factor is $\geq X$. In particular, we know

$$\left| \zeta(s) - \prod_{p \leq X} \frac{1}{1 - p^{-s}} \right| \leq \sum_{n \geq X} |n^{-s}| \to 0$$

as $X \to \infty$. So the result follows. □

Theorem. If $\mathrm{Re}(s) > 1$, then

$$(2\pi)^{-s} \Gamma(s) \zeta(s) = \int_0^\infty \frac{y^s}{e^{2\pi y} - 1} \frac{\mathrm{d}y}{y} = M(f, s),$$

where

$$f(y) = \frac{1}{e^{2\pi y} - 1}.$$

Proof. We can write

$$f(y) = \frac{e^{-2\pi y}}{1 - e^{-2\pi y}} = \sum_{n \geq 1} e^{-2\pi n y}$$

for $y > 0$.

As $y \to 0$, we find

$$f(y) \sim \frac{1}{2\pi y}.$$

So when $\mathrm{Re}(s) > 1$, the Mellin transform converges, and equals

$$\sum_{n \geq 1} M(e^{-2\pi n y}, s) = \sum_{n \geq 1} (2\pi n)^{-s} M(e^{-y}, s) = (2\pi)^{-s} \Gamma(s) \zeta(s). \qquad \square$$

Corollary. $\zeta(s)$ has a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$ as its only singularity, and

$$\operatorname*{res}_{s=1} \zeta(s) = 1.$$

Proof. We can write

$$M(f, s) = M_0 + M_\infty = \left(\int_0^1 + \int_1^\infty\right) \frac{y^s}{e^{2\pi y} - 1} \frac{\mathrm{d}y}{y}.$$

The second integral M_∞ is convergent for all $s \in \mathbb{C}$, hence defines a holomorphic function.

For any fixed N, we can expand

$$f(y) = \sum_{n=-1}^{N-1} c_n y^n + y^N g_N(y)$$

for some $g \in C^\infty(\mathbb{R})$, as f has a simple pole at $y = 0$, and

$$c_{-1} = \frac{1}{2\pi}.$$

So for $\mathrm{Re}(s) > 1$, we have

$$\begin{aligned} M_0 &= \sum_{n=-1}^{N-1} c_n \int_0^1 y^{n+s-1} \,\mathrm{d}y + \int_0^N y^{N+s-1} g_N(y) \,\mathrm{d}y \\ &= \sum_{n=-1}^{N-1} \frac{c_n}{s+n} y^{s+n} + \int_0^1 g_N(y) y^{s+N-1} \,\mathrm{d}y. \end{aligned}$$

We now notice that this formula makes sense for $\mathrm{Re}(s) > -N$. Thus we have found a meromorphic continuation of

$$(2\pi)^{-s}\Gamma(s)\zeta(s)$$

to $\{\mathrm{Re}(s) > N\}$, with at worst simple poles at $s = 1 - N, 2 - N, \cdots, 0, 1$. Also, we know $\Gamma(s)$ has a simple pole at $s = 0, -1, -2, \cdots$. So $\zeta(s)$ is analytic at $s = 0, -1, -2, \cdots$. Since $c_{-1} = \frac{1}{2\pi}$ and $\Gamma(1) = 1$, we get

$$\operatorname*{res}_{s=1} \zeta(s) = 1.$$ □

Corollary. There are infinitely many primes.

Proposition. $B_n = 0$ if n is odd and $n \geq 3$.

Proof. Consider

$$f(t) = \frac{t}{e^t - 1} + \frac{t}{2} = \sum_{n \geq 0, n \neq 1} B_n \frac{t^n}{n!}.$$

We find that

$$f(t) = \frac{t}{2} \frac{e^t + 1}{e^t - 1} = f(-t).$$

So all the odd coefficients must vanish. □

Corollary. We have

$$\zeta(0) = B_1 = -\frac{1}{2}, \quad \zeta(1-n) = -\frac{B_n}{n}$$

for $n > 1$. In particular, for all $n \geq 1$ integer, we know $\zeta(1-n) \in \mathbb{Q}$ and vanishes if $n > 1$ is odd.

Proof. We know

$$(2\pi)^{-s}\Gamma(s)\zeta(s)$$

has a simple pole at $s = 1-n$, and the residue is c_{n-1}, where

$$\frac{1}{e^{2\pi y} - 1} = \sum_{n \geq -1} c_n y^n.$$

So we know

$$c_{n-1} = (2\pi)^{n-1}\frac{B_n}{n!}.$$

We also know that

$$\operatorname*{res}_{s=1-n} \Gamma(s) = \frac{(-1)^{n-1}}{(n-1)!},$$

we get that

$$\zeta(1-n) = (-1)^{n-1}\frac{B_n}{n}.$$

If $n = 1$, then this gives $-\frac{1}{2}$. If n is odd but > 1, then this vanishes. If n is even, then this is $-\frac{B_n}{n}$, as desired. □

Proposition.

$$M\left(\frac{\Theta(y) - 1}{2}, \frac{s}{2}\right) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

Proof. The left hand side is

$$\sum_{n \geq 1} M\left(e^{-\pi n^2 y}, \frac{s}{2}\right) = \sum_{n \geq 1} (\pi n^2)^{-s/2} M\left(e^{-y}, \frac{s}{2}\right) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s). \quad \square$$

Theorem (Functional equation for Θ-function)**.** If $y > 0$, then

$$\Theta\left(\frac{1}{y}\right) = y^{1/2}\Theta(y), \tag{$*$}$$

where we take the positive square root. More generally, taking the branch of $\sqrt{\ }$ which is positive real on the positive real axis, we have

$$\vartheta\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{1/2}\vartheta(z).$$

Proof. By analytic continuation, it suffices to prove $(*)$. Let

$$g_t(x) = e^{-\pi t x^2} = g_1(t^{1/2}x).$$

In particular,

$$g_1(x) = e^{-\pi x^2}.$$

Now recall that $\hat{g}_1 = g_1$. Moreover, the Fourier transform of $f(\alpha x)$ is $\frac{1}{\alpha}\hat{f}(y/\alpha)$. So

$$\hat{g}_t(y) = t^{-1/2}\hat{g}_1(t^{-1/2}y) = t^{-1/2}g_1(t^{-1/2}y) = t^{-1/2}e^{-\pi y^2/t}.$$

We now apply the Poisson summation formula:

$$\Theta(t) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t} = \sum_{n\in\mathbb{Z}} g_t(n) = \sum_{n\in\mathbb{Z}} \hat{g}_t(n) = t^{-1/2}\Theta(1/t). \qquad \square$$

Theorem (Functional equation for ζ-function)**.**

$$Z(s) = Z(1-s).$$

Moreover, $Z(s)$ is meromorphic, with only poles at $s = 1$ and 0.

Proof. For $\mathrm{Re}(s) > 1$, we have

$$\begin{aligned} 2Z(s) &= M\left(\Theta(y) - 1, \frac{s}{2}\right) \\ &= \int_0^\infty [\Theta(y) - 1] y^{s/2}\frac{\mathrm{d}y}{y} \\ &= \left(\int_0^1 + \int_1^\infty\right) [\Theta(y) - 1] y^{s/2}\frac{\mathrm{d}y}{y} \end{aligned}$$

The idea is that using the functional equation for the Θ-function, we can relate the $\int_0^1$ part and the $\int_1^\infty$ part. We have

$$\begin{aligned} \int_0^1 (\Theta(y) - 1)y^{s/2}\frac{\mathrm{d}y}{y} &= \int_0^1 (\Theta(y) - y^{-1/2})y^{s/2}\frac{\mathrm{d}y}{y} + \int_0^1 \left(y^{\frac{s-1}{2}} - y^{1/2}\right)\frac{\mathrm{d}y}{y} \\ &= \int_0^1 (y^{-1/2}\Theta(1/y) - y^{-1/2})\frac{\mathrm{d}y}{y} + \frac{2}{s-1} - \frac{2}{s}. \end{aligned}$$

In the first term, we change variables $y \leftrightarrow 1/y$, and get

$$= \int_1^\infty y^{1/2}(\Theta(y) - 1)y^{-s/2}\frac{\mathrm{d}y}{y} + \frac{2}{s-1} - \frac{2}{s}.$$

So we find that

$$2Z(s) = \int_1^\infty (\Theta(y) - 1)(y^{s/2} + y^{\frac{1-s}{2}})\frac{\mathrm{d}y}{y} + \frac{2}{s-1} - \frac{2}{s} = 2Z(1-s).$$

Note that what we've done by separating out the $y^{\frac{s-1}{2}} - y^{s/2}$ term is that we separated out the two poles of our function. $\square$

3 Dirichlet L-functions

Proposition. If $\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}$, then there exists a unique $M \mid N$ and a *primitive* $\chi_* \in \widehat{(\mathbb{Z}/M\mathbb{Z})^\times}$ that is equivalent to χ.

Proposition.

$$L(\chi, s) = \prod_{\text{prime } p \nmid N} \frac{1}{1 - \chi(p) p^{-s}}.$$

Proposition. Suppose $M \mid N$ and $\chi_M \in \widehat{(\mathbb{Z}/M\mathbb{Z})^\times}$ and $\chi_N \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}$ are equivalent. Then

$$L(\chi_M, s) = \prod_{\substack{p \nmid M \\ p \mid N}} \frac{1}{1 - \chi_M(p) p^{-s}} L(\chi_N, s).$$

In particular,

$$\frac{L(\chi_M, s)}{L(\chi_N, s)} = \prod_{\substack{p \nmid M \\ p \mid N}} \frac{1}{1 - \chi_M(p) p^{-s}}$$

is analytic and non-zero for $\mathrm{Re}(s) > 0$.

Theorem.

(i) $L(\chi, s)$ has a meromorphic continuation to $\mathbb{C}$, which is analytic except for at worst a simple pole at $s = 1$.

(ii) If $\chi \neq \chi_0$ (the trivial character), then $L(\chi, s)$ is analytic everywhere. On the other hand, $L(\chi_0, s)$ has a simple pole with residue

$$\frac{\varphi(N)}{N} = \prod_{p \mid N} \left(1 - \frac{1}{p}\right),$$

where φ is the Euler function.

Proof. More generally, let $\phi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ be any N-periodic function, and let

$$L(\phi, s) = \sum_{n=1}^{\infty} \phi(n) n^{-s}.$$

Then

$$(2\pi)^{-s} \Gamma(s) L(\phi, s) = \sum_{n=1}^{\infty} \phi(n) M(e^{-2\pi n y}, s) = M(f(y), s),$$

where

$$f(y) = \sum_{n \geq 1} \phi(n) e^{-2\pi n y}.$$

We can then write

$$f(y) = \sum_{n=1}^{N} \sum_{r=0}^{\infty} \phi(n) e^{-2\pi(n + rN)y} = \sum_{n=1}^{N} \phi(n) \frac{e^{-2\pi n y}}{1 - e^{-2\pi N y}} = \sum_{n=1}^{N} \phi(n) \frac{e^{2\pi(N-n)y}}{e^{2\pi N y} - 1}.$$

As $0 \leq N - n < N$, this is $O(e^{-2\pi y})$ as $y \to \infty$. Copying for $\zeta(s)$, we write

$$M(f, s) = \left(\int_0^1 + \int_1^\infty\right) f(y) y^s \frac{\mathrm{d}y}{y} \equiv M_0(s) + M_\infty(s).$$

The second term is analytic for all $s \in \mathbb{C}$, and the first term can be written as

$$M_0(s) = \sum_{n=1}^N \phi(n) \int_0^1 \frac{e^{2\pi(N-n)y}}{e^{2\pi N y} - 1} y^s \frac{\mathrm{d}y}{y}.$$

Now for any L, we can write

$$\frac{e^{2\pi(N-n)y}}{e^{2\pi N y} - 1} = \frac{1}{2\pi N y} + \sum_{r=0}^{L-1} c_{r,n} y^r + y^L g_{L,n}(y)$$

for some $g_{L,n}(y) \in C^\infty[0, 1]$. Hence we have

$$M_0(s) = \sum_{n=1}^N \phi(n) \left(\int_0^1 \frac{1}{2\pi N y} y^s \frac{\mathrm{d}y}{y} + \int_0^1 \sum_{r=0}^{L-1} c_{r,n} y^{r+s-1}\,\mathrm{d}y\right) + G(s),$$

where $G(s)$ is some function analytic for $\mathrm{Re}(s) > -L$. So we see that

$$(2\pi)^{-s}\Gamma(s) L(\phi, s) = \sum_{n=1}^N \phi(n) \left(\frac{1}{2\pi N(s-1)} + \frac{c_{0,n}}{s} + \cdots + \frac{c_{L-1,n}}{s + L - 1}\right) + G(s).$$

As $\Gamma(s)$ has poles at $s = 0, -1, \cdots$, this cancels with all the poles apart from the one at $s = 1$.

The first part then follows from taking

$$\phi(n) = \begin{cases} \chi(n) & (n, N) = 1 \\ 0 & (n, N) \geq 1 \end{cases}.$$

By reading off the formula, since $\Gamma(1) = 1$, we know

$$\operatorname*{res}_{s=1} L(\chi, s) = \frac{1}{N} \sum_{n=1}^N \phi(n).$$

If $\chi \neq \chi_0$, then this vanishes by the orthogonality of characters. Otherwise, it is $|(\mathbb{Z}/N\mathbb{Z})^\times|/N = \varphi(N)/N$. □

Theorem. If $\chi \neq \chi_0$, then $L(\chi, 1) \neq 0$.

Proof. The trick is the consider all characters together. We let

$$\zeta_N(s) = \prod_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} L(\chi, s) = \prod_{p \nmid N} \prod_\chi (1 - \chi(p) p^{-s})^{-1}$$

for $\mathrm{Re}(s) > 1$. Now we know $L(\chi_0, s)$ has a pole at $s = 1$, and is analytic everywhere else. So if any other $L(\chi, 1) = 0$, then $\zeta_N(s)$ is analytic on $\mathrm{Re}(s) > 0$. We will show that this cannot be the case.

We begin by finding a nice formula for the product of $(1 - \chi(p)p^{-s})^{-1}$ over all characters.

Claim. If $p \nmid N$, and T is any complex number, then
$$\prod_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} (1 - \chi(p)T) = (1 - T^{f_p})^{\varphi(N)/f_p},$$
where f_p is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$.

So
$$\zeta_N(s) = \prod_{p \nmid N} (1 - p^{-f_p s})^{-\varphi(N)/f_p}.$$

To see this, we write $f = f_p$, and, for convenience, write
$$G = (\mathbb{Z}/N\mathbb{Z})^\times$$
$$H = \langle p \rangle \subseteq G.$$

We note that $\hat{G}$ naturally contains $\widehat{G/H} = \{\chi \in \hat{G} : \chi(p) = 1\}$ as a subgroup. Also, we know that
$$|\widehat{G/H}| = |G/H| = \varphi(N)/f.$$

Also, the restriction map
$$\frac{\hat{G}}{\widehat{G/H}} \to \hat{H}$$
is obviously injective, hence an isomorphism by counting orders. So
$$\prod_{\chi \in \hat{G}} (1 - \chi(p)T) = \prod_{\chi \in \hat{H}} (1 - \chi(p)T)^{\varphi(N)/f} = \prod_{\zeta \in \mu_f} (1 - \zeta T)^{\varphi(N)/f} = (1 - T^f)^{\varphi(N)/f}.$$

We now notice that when we expand the product of ζ_N, at least formally, then we get a Dirichlet series with non-negative coefficients. We now prove the following peculiar property of such Dirichlet series:

Claim. Let
$$D(s) = \sum_{n \geq 1} a_n n^{-s}$$
be a Dirichlet series with real $a_n \geq 0$, and suppose this is absolutely convergent for $\mathrm{Re}(s) > \sigma > 0$. Then if $D(s)$ can be analytically continued to an analytic function $\tilde{D}$ on $\{\mathrm{Re}(s) > 0\}$, then the series converges for all real $s > 0$.

Let $\rho > \sigma$. Then by the analytic continuation, we have a convergent Taylor series on $\{|s - \rho| < \rho\}$
$$D(s) = \sum_{k \geq 0} \frac{1}{k!} D^{(k)}(\rho)(s - \rho)^k.$$

Moreover, since $\rho > \sigma$, we can directly differentiate the Dirichlet series to obtain the derivatives:
$$D^{(k)}(\rho) = \sum_{n \geq 1} a_n (-\log n)^k n^{-\rho}.$$

So if $0 < x < \rho$, then
$$D(x) = \sum_{k \geq 0} \frac{1}{k!} (p - x)^k \left(\sum_{n \geq 1} a_n (\log n)^k n^{-\rho} \right).$$

Now note that all terms in this sum are all non-negative. So the double series has to converge absolutely as well, and thus we are free to rearrange the sum as we wish. So we find

$$\begin{aligned} D(x) &= \sum_{n\geq 1} a_n n^{-\rho} \sum_{k\geq 0} \frac{1}{k!}(\rho - x)^k (\log n)^l \\ &= \sum_{n\geq 1} a_n n^{-\rho} e^{(\rho-x)\log n} \\ &= \sum_{n\geq 1} a_n n^{-\rho} n^{\rho - x} \\ &= \sum_{n\geq 1} a_n n^{-x}, \end{aligned}$$

as desired.

Now we are almost done, as

$$\zeta_N(s) = L(\chi_0, s) \prod_{\chi\neq\chi_0} L(\chi, s).$$

We saw that $L(\chi_0, s)$ has a simple pole at $s = 1$, and the other terms are all holomorphic at $s = 1$. So if some $L(\chi, 1) = 0$, then $\zeta_N(s)$ is holomorphic for $\text{Re}(s) > 0$ (and in fact everywhere). Since the Dirichlet series of η_N has ≥ 0 coefficients, by the lemma, it suffices to find some point on $\mathbb{R}_{>0}$ where the Dirichlet series for ζ_N doesn't converge.

We notice

$$\zeta_N(x) = \prod_{p\nmid N}(1 + p^{-f_p x} + p^{-2f_p x} + \cdots)^{\varphi(N)/f_p} \geq \sum_{p\nmid N} p^{-\varphi(N)x}.$$

It now suffices to show that $\sum p^{-1} = \infty$, and thus the series for $\zeta_N(x)$ is not convergent for $x = \frac{1}{\varphi(N)}$.

Claim. We have

$$\sum_{p \text{ prime}} p^{-x} \sim -\log(x-1)$$

as $x \to 1^+$. On the other hand, if $\chi \neq \chi_0$ is a Dirichlet character mod N, then

$$\sum_{p\nmid N} \chi(p) p^{-x}$$

is bounded as $x \to 1^+$.

Of course (and crucially, as we will see), the second part is not needed for the proof, but it is still nice to know.

To see this, we note that for any χ, we have

$$\log L(\chi, x) = \sum_{p\nmid N} -\log(1 - \chi(p)p^{-x}) = \sum_{p\nmid N}\sum_{r\geq 1} \frac{\chi(p)^r p^{-rx}}{r}.$$

So

$$\left|\log L(\chi, x) - \sum_{p\nmid N} \chi(p) p^{-x}\right| < \sum_{p\nmid N} \sum_{r\geq 2} p^{-rx}$$
$$= \sum_{p\nmid N} \frac{p^{-2x}}{1-p^{-x}}$$
$$\leq \sum_{n\geq 1} \frac{n^{-2}}{1/2},$$

which is a (finite) constant for $C < \infty$. When $\chi = \chi_0, N = 1$, then

$$\left|\log \zeta(x) - \sum_p p^{-x}\right|$$

is bounded as $x \to 1^+$. But we know

$$\zeta(s) = \frac{1}{s-1} + O(s).$$

So we have

$$\sum_p p^{-x} \sim \log(x-1).$$

When $\chi \neq \chi_0$, then $L(\chi, 1) \neq 0$, as we have just proved! So $\log L(\chi, x)$ is bounded as $x \to 1^+$. and so we are done. □

Theorem (Dirichlet's theorem on primes in arithmetic progressions)**.** Let $a \in \mathbb{Z}$ be such that $(a, N) = 1$. Then there exists infinitely many primes $p \equiv a \pmod{N}$.

Proof. We want to show that the series

$$\sum_{\substack{p \text{ prime} \\ p \equiv a \bmod N}} p^{-x}$$

is unbounded as $x \to 1^+$, and in particular must be infinite. We note that for $(x, N) = 1$, we have

$$\sum_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} \chi(x) = \begin{cases} \varphi(N) & x \equiv 1 \pmod{N} \\ 0 & \text{otherwise} \end{cases},$$

since the sum of roots of unity vanishes. We also know that χ is a character, so $\chi(a)^{-1}\chi(p) = \chi(a^{-1}p)$. So we can write

$$\sum_{\substack{p \text{ prime} \\ p \equiv a \bmod N}} p^{-x} = \frac{1}{\varphi(N)} \sum_{\chi \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(a)^{-1} \sum_{\text{all } p} \chi(p) p^{-x},$$

Now if $\chi = \chi_0$, then the sum is just

$$\sum_{p\nmid N} p^{-x} \sim -\log(x-1)$$

as $x \to 1^+$. Moreover, all the other sums are bounded as $x \to 1^+$. So

$$\sum_{p \equiv a \bmod N} p^{-x} \sim -\frac{1}{\varphi(N)} \log(x-1).$$

So the whole sum must be unbounded as $x \to 1^+$. So in particular, the sum must be infinite. □

Theorem (Cebotarev density theorem)**.** *Cebotarev density theorem* Let L/K be a Galois extension. Then for any conjugacy class $C \subseteq \mathrm{Gal}(L/K)$, there exists infinitely many $\mathfrak{p}$ with $[\sigma_{\mathfrak{p}}] = C$.

4 The modular group

Theorem. The group $\mathrm{SL}_2(\mathbb{R})$ admits the *Iwasawa decomposition*

$$\mathrm{SL}_2(\mathbb{R}) = KAN = NAK,$$

where

$$K = \mathrm{SO}(2), \quad A = \left\{\begin{pmatrix} r & 0 \\ 0 & \frac{1}{r}\end{pmatrix}\right\}, \quad N = \left\{\begin{pmatrix} 1 & x \\ 0 & 1\end{pmatrix}\right\}$$

Proof. This is just Gram–Schmidt orthogonalization. Given $g \in \mathrm{GL}_2(\mathbb{R})$, we write

$$ge_1 = e_1', \quad ge_2 = e_2',$$

By Gram-Schmidt, we can write

$$\begin{aligned} f_1 &= \lambda_1 e_1' \\ f_2 &= \lambda_2 e_1' + \mu e_2' \end{aligned}$$

such that

$$\|f_1\| = \|f_2\| = 1, \quad (f_1, f_2) = 0.$$

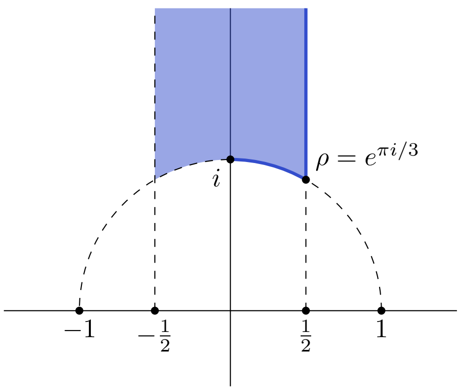
So we can write

$$\begin{pmatrix} f_1 & f_2 \end{pmatrix} = \begin{pmatrix} e_1' & e_2' \end{pmatrix} \begin{pmatrix} \lambda_1 & \lambda_2 \\ 0 & \mu \end{pmatrix}$$

Now the left-hand matrix is orthogonal, and by decomposing the inverse of $\begin{pmatrix} \lambda_1 & \lambda_2 \\ 0 & \mu \end{pmatrix}$, we can write $g = \begin{pmatrix} e_1' & e_2' \end{pmatrix}$ as a product in KAN. □

Theorem. Let

$$\mathcal{D} = \left\{z \in \mathcal{H} : -\frac{1}{2} \leq \operatorname{Re} z \leq \frac{1}{2}, |z| > 1\right\} \cup \{z \in \mathcal{H} : |z| = 1, \operatorname{Re}(z) \geq 0\}.$$



Then $\mathcal{D}$ is a *fundamental domain* for the action of $\bar{\Gamma}$ on $\mathcal{H}$, i.e. every orbit contains exactly one element of $\mathcal{D}$.

The stabilizer of $z \in \mathcal{D}$ in Γ is trivial if $z \neq i, \rho$, and the stabilizers of i and ρ are

$$\bar{\Gamma}_i = \langle S \rangle \cong \frac{\mathbb{Z}}{2Z}, \quad \bar{\Gamma}_\rho = \langle TS \rangle \cong \frac{\mathbb{Z}}{3\mathbb{Z}}.$$

Finally, we have $\bar{\Gamma} = \langle S, T \rangle = \langle S, TS \rangle$.

Proof. Let $\bar{\Gamma}^* = \langle S, T\rangle \subseteq \bar{\Gamma}$. We will show that if $z \in \mathcal{H}$, then there exists $\gamma \in \bar{\Gamma}^*$ such that $\gamma(z) \in \mathcal{D}$.

Since $z \notin \mathbb{R}$, we know $\mathbb{Z} + \mathbb{Z}z = \{cz + d : c, d \in \mathbb{Z}\}$ is a discrete subgroup of $\mathbb{C}$. So we know

$$\{|cz + d| : c, d \in \mathbb{Z}\}$$

is a discrete subset of $\mathbb{R}$, and is in particular bounded away from 0. Thus, we know

$$\left\{\operatorname{Im}\gamma(z) = \frac{\operatorname{Im}(z)}{|cz+d|^2} : \gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \bar{\Gamma}^*\right\}$$

is a discrete subset of $\mathbb{R}_{>0}$ and is bounded above. Thus there is some $\gamma \in \bar{\Gamma}^*$ with $\operatorname{Im}\gamma(z)$ maximal. Replacing γ by $T^n\gamma$ for suitable n, we may assume $|\operatorname{Re}\gamma(z)| \leq \frac{1}{2}$.

We consider the different possible cases.

- If $|\gamma(z)| < 1$, then

$$\operatorname{Im} S\gamma(z) = \operatorname{Im}\frac{-1}{\gamma(z)} = \frac{\operatorname{Im}\gamma(z)}{|\gamma(z)|^2} > \operatorname{Im}\gamma(z),$$

  which is impossible. So we know $|\gamma(z)| \geq 1$. So we know $\gamma(z)$ lives in the closure of $\mathcal{D}$.

- If $\operatorname{Re}(\gamma(z)) = -\frac{1}{2}$, then $T\gamma(z)$ has real part $+\frac{1}{2}$, and so $T(\gamma(z)) \in \mathcal{D}$.

- If $-\frac{1}{2} < \operatorname{Re}(z) < 0$ and $|\gamma(z)| = 1$, then $|S\gamma(z)| = 1$ and $0 < \operatorname{Re} S\gamma(z) < \frac{1}{2}$, i.e. $S\gamma(z) \in \mathcal{D}$.

So we can move it to somewhere in $\mathcal{D}$.

We shall next show that if $z, z' \in \mathcal{D}$, and $z' = \gamma(z)$ for $\gamma \in \bar{\Gamma}$, then $z = z'$. Moreover, either

- $\gamma = 1$; or
- $z = i$ and $\gamma = S$; or
- $z = \rho$ and $\gamma = TS$ or $(TS)^2$.

It is clear that this proves everything.

To show this, we wlog

$$\operatorname{Im}(z') = \frac{\operatorname{Im} z}{|cz+d|^2} \geq \operatorname{Im} z$$

where

$$\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix},$$

and we also wlog $c \geq 0$.

Therefore we know that $|cz + d| \leq 1$. In particular, we know

$$1 \geq \operatorname{Im}(cz+d) = c\operatorname{Im}(z) \geq c\frac{\sqrt{3}}{2}$$

since $z \in \mathcal{D}$. So $c = 0$ or 1.

- If $c = 0$, then
$$\gamma = \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$$
for some $m \in \mathbb{Z}$, and this $z' = z + m$. But this is clearly impossible. So we must have $m = 0$, $z = z'$, $\gamma = 1 \in \mathrm{PSL}_2(\mathbb{Z})$.
- If $c = 1$, then we know $|z + d| \leq 1$. So z is at distance 1 from an integer. As $z \in \mathcal{D}$, the only possibilities are $d = 0$ or -1.
  - If $d = 0$, then we know $|z| = 1$. So
$$\gamma = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$$
for some $a \in \mathbb{Z}$. Then $z' = a - \frac{1}{z}$. Then
    * either $a = 0$, which forces $z = i$, $\gamma = S$; or
    * $a = 1$, and $z' = 1 - \frac{1}{z}$, which implies $z = z' = \rho$ and $\gamma = TS$.
  - If $d = -1$, then by looking at the picture, we see that $z = \rho$. Then
$$|cz + d| = |z - 1| = 1,$$
and so
$$\operatorname{Im} z' = \operatorname{Im} z = \frac{\sqrt{3}}{2}.$$
So we have $z' = \rho$ as well. So
$$\frac{a\rho + b}{\rho - 1} = \rho,$$
which implies
$$\rho^2 - (a+1)\rho - b = 0$$
So $\rho = -1, a = 0$, and $\gamma = (TS)^2$. □

Proposition. The measure
$$\mathrm{d}\mu = \frac{\mathrm{d}x\,\mathrm{d}y}{y^2}$$
is invariant under $\mathrm{PSL}_2(\mathbb{R})$. If $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ is of finite index, then $\mu(\Gamma\backslash\mathcal{H}) < \infty$.

Proof. Consider the 2-form associated to μ, given by
$$\eta = \frac{\mathrm{d}x \wedge \mathrm{d}y}{y^2} = \frac{i\mathrm{d}z \wedge \mathrm{d}\bar{z}}{2(\operatorname{Im} z)^2}.$$
We now let
$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$
Then we have
$$\operatorname{Im} \gamma(z) = \frac{\operatorname{Im} z}{|cz + d|^2}.$$

Moreover, we have

$$\frac{\mathrm{d}\gamma(z)}{\mathrm{d}z} = \frac{a(cz+d) - c(az+b)}{(cz+d)^2} = \frac{1}{(cz+d)^2}.$$

Plugging these into the formula, we see that η is invariant under γ.

Now if $\bar{\Gamma} \leq \mathrm{PSL}_2(\mathbb{Z})$ has finite index, then we can write $\mathrm{PSL}_2(\mathbb{Z})$ as a union of cosets

$$\mathrm{PSL}_2(\mathbb{Z}) = \coprod_{i=1}^{n} \bar{\gamma}\gamma_i,$$

where $n = (\mathrm{PSL}_2(\mathbb{Z}) : \bar{\Gamma})$. Then a fundamental domain for $\bar{\Gamma}$ is just

$$\bigcup_{i=1}^{n} \gamma_i(\mathcal{D}),$$

and so

$$\mu(\bar{\Gamma} \setminus H) = \sum \mu(\gamma_i \mathcal{D}) = n\mu(\mathcal{D}).$$

So it suffices to show that $\mu(\mathcal{D})$ is finite, and we simply compute

$$\mu(\mathcal{D}) = \int_{\mathcal{D}} \frac{\mathrm{d}x\ \mathrm{d}y}{y^2} \leq \int_{x=-\frac{1}{2}}^{x=\frac{1}{2}} \int_{y=\sqrt{2}/2}^{y=\infty} \frac{\mathrm{d}x\ \mathrm{d}y}{y^2} < \infty. \qquad \square$$

5 Modular forms of level 1

5.1 Basic definitions

Theorem. G_k is a modular form of weight k and level 1. Moreover, its q-expansion is

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

where

$$\sigma_r(n) = \sum_{1\leq d\mid n} d^r.$$

Proposition. Let $(e_1, \cdots, e_d)$ be some basis for $\mathbb{R}^d$. Then if $r \in \mathbb{R}$, the series

$$\sum_{\mathbf{m}\in\mathbb{Z}^d}{}' \|m_1e_1 + \cdots + m_de_d\|^{-r}$$

converges iff $r > d$.

Proof. The function

$$(x_i) \in \mathbb{R}^d \mapsto \left\|\sum_{i=1} x_ie_i\right\|$$

is a norm on $\mathbb{R}^d$. As any 2 norms on $\mathbb{R}^d$ are equivalent, we know this is equivalent to the sup norm $\|\cdot\|_\infty$. So the series converges iff the corresponding series

$$\sum_{\mathbf{m}\in\mathbb{Z}^d}{}' \|\mathbf{m}\|_\infty^{-r}$$

converges. But if $1 \leq N \leq Z$, then the number of $\mathbf{m} \in \mathbb{Z}^d$ such that $\|\mathbf{m}\|_\infty = N$ is $(2N+1)^d - (2N-1)^d \sim 2^d dN^{d-1}$. So the series converges iff

$$\sum_{N\geq 1} N^{-r}N^{d-1}$$

converges, which is true iff $r > d$. □

Proof of theorem. Then convergence of the Eisenstein series by applying this to $\mathbb{R}^2 \cong \mathbb{C}$. So the series is absolutely convergent. Therefore we can simply compute

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

Also we can compute

$$G_k\left(-\frac{1}{z}\right) = \sum_{m,n}{}' = \frac{z^k}{(-m+nz)^k} = z^kG_k(z).$$

So G_k satisfies the invariance property. To show that G_k is holomorphic, and holomorphic at infinity, we'll derive the q-expansion (1). □

Lemma.
$$\sum_{n=\infty}^{\infty} \frac{1}{(n+w)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{d=1}^{\infty} d^{k-1} e^{2\pi i d w}$$
for any $w \in \mathcal{H}$ and $k \geq 2$.

Proof. Let
$$f(x) = \frac{1}{(x+w)^k}.$$
We compute
$$\hat{f}(y) = \int_{-\infty}^{\infty} \frac{e^{-2\pi i x y}}{(x+w)^k}\;\mathrm{d}x.$$
We replace this with a contour integral. We see that this has a pole at $-w$. If $y > 0$, then we close the contour downwards, and we have
$$\hat{f}(y) = -2\pi i \operatorname{Res}_{z=-w} \frac{e^{-2\pi i y z}}{(z+w)^k} = -2\pi i \frac{(-2\pi i y)^{k-1}}{(k-1)!} e^{2\pi i y w}.$$
If $y \leq 0$, then we close in the upper half plane, and since there is no pole, we have $\hat{f}(y) = 0$. So we have
$$\sum_{n=-\infty}^{\infty} \frac{1}{(n+w)^k} = \sum_{n \in \mathbb{Z}} f(n) = \sum_{d \in \mathbb{Z}} \hat{f}(d) = \frac{(-2\pi i)^k}{(k-1)!} \sum_{d \geq 1} d^{k-1} e^{2\pi i d w}$$
by Poisson summation formula. □

Proposition.

(i) $j(\gamma\delta, z) = j(\gamma, \delta(z)) j(\delta, z)$ (in fancy language, we say j is a 1-cocycle).

(ii) $j(\gamma^{-1}, z) = j(\gamma, \gamma^{-1}(z))^{-1}$.

(iii) $\gamma : \varphi \mapsto f\underset{k}{|}\gamma$ is a (right) action of $G = \mathrm{GL}_2(\mathbb{R})^+$ on functions on $\mathcal{H}$. In other words,
$$f\underset{k}{|}\gamma\underset{k}{|}\delta = f\underset{k}{|}(\gamma\delta).$$

Proof.

(i) We have
$$j(\gamma\delta, z)\begin{pmatrix} \gamma\delta(z) \\ 1 \end{pmatrix} = \gamma\delta \begin{pmatrix} z \\ 1 \end{pmatrix} = j(\delta, z)\gamma \begin{pmatrix} \delta(z) \\ 1 \end{pmatrix} = j(\delta, z) j(\gamma, \delta(z)) \begin{pmatrix} z \\ 1 \end{pmatrix}$$

(ii) Take $\delta = \gamma^{-1}$.

(iii) We have
$$\begin{aligned}((f\underset{k}{|}\gamma)\underset{k}{|}\delta)(z) &= (\det \delta)^{k/2} j(\delta, z)^{-k} (f\underset{k}{|}\gamma)(\delta(z)) \\ &= (\det \delta)^{k/2} j(\delta, z)^{-k} (\det \gamma)^{k/2} j(\gamma, \delta(z))^{-k} f(\gamma\delta(z)) \\ &= (\det \gamma\delta)^{k/2} j(\gamma\delta, z)^{-k} f(\gamma\delta(z)) \\ &= (f\underset{k}{|}\gamma\delta)(z).\end{aligned}$$
□

5.2 The space of modular forms

Proposition. Let f be a weak modular form (i.e. it can be meromorphic at ∞) of weight k and level 1. If f is not identically zero, then

$$\left(\sum_{z_0 \in \mathcal{D}\setminus\{i,\rho\}} \operatorname{ord}_{z_0}(f)\right) + \frac{1}{2}\operatorname{ord}_i(f) + \frac{1}{3}\operatorname{ord}_\rho f + \operatorname{ord}_\infty(f) = \frac{k}{12},$$

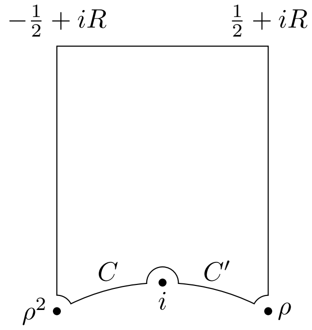
where $\operatorname{ord}_\infty f$ is the least $r \in \mathbb{Z}$ such that $a_r(f) \neq 0$.

Proof. Note that the function $\tilde{f}(q)$ is non-zero for $0 < |q| < \varepsilon$ for some small ε by the principle of isolated zeroes. Setting

$$\varepsilon = e^{-2\pi R},$$

we know $f(z) \neq 0$ if $\operatorname{Im} z \geq R$.

In particular, the number of zeroes of f in $\mathcal{D}$ is finite. We consider the integral along the following contour, counterclockwise.



We assume f has no zeroes along the contour. Otherwise, we need to go around the poles, which is a rather standard complex analytic maneuver we will not go through.

For ε sufficiently small, we have

$$\int_\Gamma \frac{f'(z)}{f(z)}\,\mathrm{d}z = 2\pi i \sum_{z_0 \in \mathcal{D}\setminus\{i,\rho\}} \operatorname{ord}_{z_0 f}$$

by the argument principle. Now the top integral is

$$\int_{\frac{1}{2}+iR}^{-\frac{1}{2}iR} \frac{f'}{f}\,\mathrm{d}z = -\int_{|q|=\varepsilon} \frac{\frac{\mathrm{d}\tilde{f}}{\mathrm{d}q}}{\tilde{f}(q)}\,\mathrm{d}q = -2\pi i \operatorname{ord}_\infty f.$$

As $\frac{f'}{f}$ has at worst a simple pole at $z = i$, the residue is $\operatorname{ord}_i f$. Since we are integrating along only half the circle, as $\varepsilon \to 0$, we pick up

$$-\pi i \operatorname{res} = -\pi i \operatorname{ord}_i f.$$

Similarly, we get $-\frac{2}{3}\pi i \operatorname{ord}_\rho f$ coming from ρ and ρ^2.

So it remains to integrate along the bottom circular arcs. Now note that $S : z \mapsto -\frac{1}{z}$ maps C to C' with opposite orientation, and

$$\frac{\mathrm{d}f(Sz)}{f(Sz)} = k\frac{\mathrm{d}z}{z} + \frac{\mathrm{d}f(z)}{f(z)}$$

as

$$f(Sz) = z^k f(z).$$

So we have

$$\begin{aligned}\int_C + \int_{C'} \frac{f'}{f}\,\mathrm{d}z &= \int_{C'} \frac{f'}{f}\,\mathrm{d}z - \left(\frac{k}{z}\,\mathrm{d}z + \frac{f'}{f}\,\mathrm{d}z\right) - -k\int_{C'} \frac{\mathrm{d}z}{z}\\ &\to k\int_\rho^i \frac{\mathrm{d}z}{z}\\ &= \frac{\pi i k}{6}.\end{aligned}$$

So taking the limit $\varepsilon \to 0$ gives the right result. □

Corollary. If $k < 0$, then $M_k = \{0\}$.

Corollary. If $k = 0$, then $M_0 = \mathbb{C}$, the constants, and $S_0 = \{0\}$.

Proof. If $f \in M_0$, then $g = f - f(1)$. If f is not constant, then $\operatorname{ord}_i g \geq 1$, so the LHS is > 0, but the RHS is $= 0$. So $f \in \mathbb{C}$.

Of course, $a_0(f) = f$. So $S_0 = \{0\}$. □

Corollary.

$$\dim M_k \leq 1 + \frac{k}{12}.$$

In particular, they are finite dimensional.

Proof. We let $f_0, \cdots, f_d$ be $d + 1$ elements of M_k, and we choose distinct points $z_1, \cdots, z_d \in \mathcal{D} \setminus \{i, \rho\}$. Then there exists $\lambda_0, \cdots, \lambda_d \in \mathbb{C}$, not all 0, such that

$$f = \sum_{i=0}^d \lambda_i f_i$$

vanishes at all these points. Now if $d > \frac{k}{12}$, then LHS is $> \frac{k}{12}$. So $f \equiv 0$. So (f_i) are linearly dependent, i.e. $\dim M_k < d + 1$. □

Corollary. $M_2 = \{0\}$ and $M_k = \mathbb{C}E_k$ for $4 \leq k \leq 10$ (k even). We also have $E_8 = E_4^2$ and $E_{10} = E_4 E_6$.

Proof. Only $M_2 = \{0\}$ requires proof. If $0 \neq f \in M_2$, then this implies

$$a + \frac{b}{2} + \frac{c}{3} = \frac{1}{6}$$

for integers $a, b, c \geq 0$, which is not possible.

Alternatively, if $f \in M_2$, then $f^2 \in M_4$ and $f^3 \in M_6$. This implies $E_4^3 = E_6^2$, which is not the case as we will soon see.

Note that we know $E_8 = E_4^2$, and is not just a multiple of it, by checking the leading coefficient (namely 1). □

Corollary. The cusp form of weight 12 is

$$E_4^3 - E_6^2 = (1 + 240q + \cdots)^3 - (1 - 504q + \cdots)^2 = 1728q + \cdots .$$

Proposition. $\Delta(z) \neq 0$ for all $z \in \mathcal{H}$.

Proof. We have

$$\sum_{z_0 \neq i, \rho} \operatorname{ord}_{z_0} \Delta + \frac{1}{2} \operatorname{ord}_i \Delta + \frac{1}{3} \operatorname{ord}_\rho \Delta + \operatorname{ord}_\infty \Delta = \frac{k}{12} = 1.$$

Since $\operatorname{ord}_\rho \Delta = 1$, it follows that there can't be any other zeroes. □

Proposition. The map $f \mapsto \Delta f$ is an isomorphism $M_{k-12}(\Gamma(1)) \to S_k(\Gamma(1))$ for all $k > 12$.

Proof. Since $\Delta \in S_{12}$, it follows that if $f \in M_{k-1}$, then $\Delta f \in S_k$. So the map is well-defined, and we certainly get an injection $M_{k-12} \to S_k$. Now if $g \in S_k$, since $\operatorname{ord}_\infty \Delta = 1 \leq \operatorname{ord}_\infty g$ and $\Delta \neq \mathcal{H}$. So $\frac{g}{\Delta}$ is a modular form of weight $k - 12$. □

Theorem.

(i) We have

$$\dim M_k(\Gamma(1)) = \begin{cases} 0 & k < 0 \text{ or } k \text{ odd} \\ \lfloor \frac{k}{12} \rfloor & k > 0, k \equiv 2 \pmod{12} \\ 1 + \lfloor \frac{k}{12} \rfloor & \text{otherwise} \end{cases}$$

(ii) If $k > 4$ and even, then

$$M_k = S_k \oplus \mathbb{C}E_k.$$

(iii) Every element of M_k is a polynomial in E_4 and E_6.

(iv) Let

$$b = \begin{cases} 0 & k \equiv 0 \pmod 4 \\ 1 & k \equiv 2 \pmod 4 \end{cases}.$$

Then

$$\{h_j = \Delta^j E_6^b E_4^{(k-12j-6b)/4} : 0 \leq j < \dim M_k\}.$$

is a basis for M_k, and

$$\{h_j : 1 \leq j < \dim M_k\}$$

is a basis for S_k.

Proof.

(ii) S_k is the kernel of the homomorphism $M_k \to \mathbb{C}$ sending $f \mapsto a_0(f)$. So the complement of S_k has dimension at most 1, and we know E_k is an element of it. So we are done.

(i) For $k < 12$, this agrees with what we have already proved. By the proposition, we have
$$\dim M_{k-12} = \dim S_k.$$
So we are done by induction and (ii).

(iii) This is true for $k < 12$. If $k \geq 12$ is even, then we can find $a, b \geq 0$ with $4a + 6b = k$. Then $E_4^a E_6^b \in M_k$, and is not a cusp form. So
$$M_k = \mathbb{C} E_4^a E_6^b \oplus \Delta M_{k-12}.$$
But Δ is a polynomial in E_4, E_6, So we are done by induction on k.

(iv) By (i), we know $k - 12j - 6k \geq 0$ for $j < \dim M_k$, and is a multiple of 4. So $h_j \in M_k$. Next note that the q-expansion of h_j begins with q^j. So they are all linearly independent. □

5.3 Arithmetic of Δ

Proposition.

(i) $\tau(n) \in \mathbb{Z}$ for all $n \geq 1$.

(ii) $\tau(n) = \sigma_{11}(n) \pmod{691}$

Proof.

(i) We have
$$1728\Delta = (1 + 240 A_3(q))^3 - (1 - 504 A_5(q))^2,$$
where
$$A_r = \sum_{n \geq 1} \sigma_r(n) q^n.$$
We can write this as
$$1728\Delta = 3 \cdot 240 A_3 + 3 \cdot 240^2 A_3^2 + 240^3 A_3^3 + 2 \cdot 504 A_5 - 504^2 A_5^2.$$
Now recall the deep fact that $1728 = 12^3$ and $504 = 21 \cdot 24$.
Modulo 1728, this is equal to
$$720 A_3 + 1008 A_5.$$
So it suffices to show that
$$5\sigma_3 + 7\sigma_5(n) \equiv 0 \pmod{12}.$$
In other words, we need
$$5d^3 + 7d^5 \equiv 0 \pmod{12},$$
and we can just check this manually for all d.

(ii) Consider

$$E_4^3 = 1 + \sum_{n\geq 1} b_n q^n$$

with $b_n \in \mathbb{Z}$. We also have

$$E_{12} = 1 + \frac{65520}{691}\sum_{n\geq 1} \sigma_{11}(n) q^n.$$

Also, we know

$$E_{12} - E_4^3 \in S_{12}.$$

So it is equal to $\lambda\Delta$ for some $\lambda \in \mathbb{Q}$. So we find that for all $n \geq 1$, we have

$$\frac{665520}{691}\sigma_{11}(n) - b_n = \lambda\tau(n).$$

In other words,

$$65520\sigma_{11}(n) - 691 b_n = \mu\tau(n)$$

for some $\tau \in \mathbb{Q}$.

Putting $n = 1$, we know $\tau(1) = 1$, $\sigma_{11}(1) = 1$, and $b_1 \in \mathbb{Z}$. So $\mu \in \mathbb{Z}$ and $\mu \equiv 65520 \pmod{691}$. So for all $n \geq 1$, we have

$$65520\sigma_{11}(n) \equiv 65520\tau(n) \pmod{691}.$$

Since 691 and 65520 are coprime, we are done. □

Lemma.

(i) Suppose $\dim M_k = d + 1 \geq 1$. Then there exists a basis $\{g_j : 0 \leq j \leq d\}$ for M_k such that

- $g_j \in M_k(\mathbb{Z})$ for all $j \in \{0, \cdots, d\}$.
- $a_n(g_j) = \delta_{nj}$ for all $j, n \in \{0, \cdots, d\}$.

(ii) For any R, $M_k(R) \cong R^{d+1}$ generated by $\{g_j\}$.

Proof.

(i) We take our previous basis $h_j = \Delta^j E_6^b E_4^{(k-12j-6b)/4} \in M_k(\mathbb{Z})$. Then we have $a_n(h_n) = 1$, and $a_j(h_n) = 0$ for all $j < n$. Then we just row reduce.

(ii) The isomorphism is given by

$$\begin{aligned} M_k(R) &\longleftrightarrow R^{d+1} \\ f &\longmapsto (a_n(f)) \\ \sum_{j=0}^d c_j g_j &\longleftarrow\!\shortmid (c_n) \end{aligned}$$

□

6 Hecke operators

6.1 Hecke operators and algebras

Theorem. Let $G = \mathrm{GL}_2(\mathbb{Q})$, and $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ a subgroup of finite index. Then (G, Γ) satisfies (H).

Proof. We first consider the case $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. We first suppose

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}),$$

and $\det g = \pm N$, $N \geq 1$. We claim that

$$g^{-1}\Gamma g \cap \Gamma \supseteq \Gamma(N),$$

from which it follows that

$$(\Gamma : \Gamma \cap g^{-1}\Gamma g) < \infty.$$

So given $\gamma \in \Gamma(N)$, we need to show that $g\gamma g^{-1} \in \Gamma$, i.e. it has integer coefficients. We consider

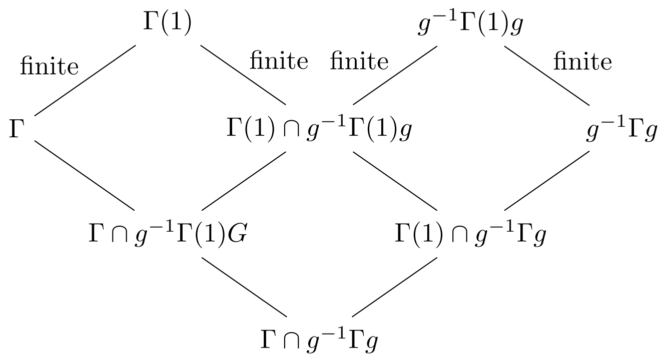
$$\pm N \cdot g\gamma g^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \equiv NI \equiv 0 \pmod{N}.$$

So we know that $g\gamma g^{-1}$ must have integer entries. Now in general, if $g' \in \mathrm{GL}_2(\mathbb{Q})$, then we can write

$$g' = \frac{1}{M} g$$

for g with integer entries, and we know conjugating by g and g' give the same result. So (G, Γ) satisfies (H).

The general result follows by a butterfly. Recall that if $(G : H) < \infty$ and $(G : H') < \infty$, then $(G : H \cap H') < \infty$. Now if $\Gamma \subseteq \Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ is of finite index, then we can draw the diagram



Each group is the intersection of the two above, and so all inclusions are of finite index. □

Proposition.

(i) $m|[\Gamma g \Gamma]$ depends only on $\Gamma g \Gamma$.

(ii) $m|[\Gamma g \Gamma] \in M^\Gamma$.

Proof.

(i) If $g_i' = \gamma_i g_i$ for $\gamma_i \in \Gamma$, then

$$\sum m g_i' = \sum m \gamma_i g_i = \sum m g_i$$

as $m \in M^\Gamma$.

(ii) Just write it out, using the fact that $\{\Gamma g_i\}$ is invariant under Γ. □

Theorem. There is a product on $\mathcal{H}(G, \Gamma)$ making it into an associative ring, the *Hecke algebra* of (G, Γ), with unit $[\Gamma e \Gamma] = [\Gamma]$, such that for every G-module M, we have M^Γ is a right $\mathcal{H}(G, \Gamma)$-module by the operation $(*)$.

Proof. Take $M = \mathbb{Z}[\Gamma \setminus G]$, and let

$$\Gamma g \Gamma = \coprod \Gamma g_i$$
$$\Gamma h \Gamma = \coprod \Gamma h_j.$$

Then

$$\sum_i [\Gamma g_i] \in M^\Gamma,$$

and we have

$$\sum_i [\Gamma g_i] | [\Gamma h \Gamma] = \sum_{i,j} [\Gamma g_i h_j] \in M^\Gamma,$$

and this is well-defined. This gives us a well-defined product on $\mathcal{H}(G, \Gamma)$. Explicitly, we have

$$[\Gamma g \Gamma] \cdot [\Gamma h \Gamma] = \Theta^{-1}\left(\sum_{i,j} [\Gamma g_i h_j]\right).$$

It should be clear that this is associative, as multiplication in G is associative, and $[\Gamma] = [\Gamma e \Gamma]$ is a unit.

Now if M is *any* right G-module, and $m \in M^\Gamma$, we have

$$m|[\Gamma g \Gamma]|[\Gamma h \Gamma] = \left(\sum m g_i\right) |[\Gamma h \Gamma] = \sum m g_i h_j = m([\Gamma g \Gamma] \cdot [\Gamma h \Gamma]).$$

So M^Γ is a right $\mathcal{H}(G, \Gamma)$-module. □

Proposition. We write

$$\Gamma g \Gamma = \coprod_{i=1}^r \Gamma g_i$$
$$\Gamma h \Gamma = \coprod_{j=1}^s \Gamma h_j.$$

Then

$$[\Gamma g \Gamma] \cdot [\Gamma h \Gamma] = \sum_{k \in S} \sigma(k) [\Gamma k \Gamma],$$

where $\sigma(k)$ is the number of pairs (i, j) such that $\Gamma g_i h_j = \Gamma k$.

Proof. This is just a simple counting exercise. □

6.2 Hecke operators on modular forms

Proposition.

(i) Let $\gamma \in \mathrm{Mat}_2(\mathbb{Z})$ and $\det \gamma = n \geq 1$. Then

$$\Gamma\gamma\Gamma = \Gamma \begin{pmatrix} n_1 & 0 \\ 0 & n_2 \end{pmatrix} \Gamma$$

for unique $n_1, n_2 \geq 1$ and $n_2 \mid n_1$, $n_1 n_2 = n$.

(ii)

$$\left\{\gamma \in \mathrm{Mat}_2(\mathbb{Z}) : \det \gamma = n\right\} = \coprod \Gamma \begin{pmatrix} n_1 & 0 \\ 0 & n_2 \end{pmatrix} \Gamma,$$

where we sum over all $1 \leq n_2 \mid n_1$ such that $n = n_1 n_2$.

(iii) Let γ, n_1, n_2 be as above. if $d \geq 1$, then

$$\Gamma(d^{-1}\gamma)\Gamma = \Gamma \begin{pmatrix} n_1/d & 0 \\ 0 & n_2/d \end{pmatrix} \Gamma,$$

Proof. This is the Smith normal form theorem, or, alternatively, the fact that we can row and column reduce. □

Corollary. The set

$$\left\{\left[\Gamma \begin{pmatrix} r_1 & 0 \\ 0 & r_2 \end{pmatrix} \Gamma\right] : r_1, r_2 \in \mathbb{Q}_{>0}, \frac{r_1}{r_2} \in \mathbb{Z}\right\}$$

is a basis for $\mathcal{H}(G, \Gamma)$ over $\mathbb{Z}$.

Theorem.

(i) $R(mn) = R(m)R(n)$ and $R(m)T(n) = T(n)R(m)$ for all $m, n \geq 1$.

(ii) $T(m)T(n) = T(mn)$ whenever $(m, n) = 1$.

(iii) $T(p)T(p^r) = T(p^{r+1}) + pR(p)T(p^{r-1})$ of $r \geq 1$.

Corollary. $\mathcal{H}(G, \Gamma)$ is *commutative*, and is generated by $\{T(p), R(p), R(p)^{-1} : p \text{ prime}\}$.

Proof. We know that $T(n_1, n_2)$, $R(p)$ and $R(p)^{-1}$ generate $\mathcal{H}(G, \Gamma)$, because

$$\left[\Gamma \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \Gamma\right] \left[\Gamma \begin{pmatrix} n_1 & 0 \\ 0 & n_2 \end{pmatrix} \Gamma\right] = \left[\Gamma \begin{pmatrix} pn_1 & 0 \\ 0 & pn_2 \end{pmatrix} \Gamma\right]$$

In particular, when $n_2 \mid n_1$, we can write

$$T(n_1, n_2) = R(n_2) T\left(\frac{n_1}{n_2}, 1\right).$$

So it suffices to show that we can produce any $T(n, 1)$ from the $T(m)$ and $R(m)$. We proceed inductively. The result is immediate when n is square-free, because $T(n, 1) = T(n)$. Otherwise,

$$\begin{aligned} T(n) &= \sum_{\substack{1 \leq n_2 \mid n_1 \\ n_1 n_2 = n}} T(n_1, n_2) \\ &= \sum_{\substack{1 \leq n_2 \mid n_1 \\ n_1 n_2 = n}} R(n_2) T\left(\frac{n_1}{n_2}, 1\right) \\ &= T(n, 1) + \sum_{\substack{1 < n_2 \mid n_1 \\ n_1 n_2 = n}} R(n_2) T\left(\frac{n_1}{n_2}, 1\right). \end{aligned}$$

So $\{T(p), R(p), R(p)^{-1}\}$ does generate $\mathcal{H}(G, \Gamma)$, and by the theorem, we know these generators commute. So $\mathcal{H}(G, \Gamma)$ is commutative. □

Proof of theorem.

(i) We have

$$\left[\Gamma \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \Gamma\right] [\Gamma \gamma \Gamma] = \left[\Gamma \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \gamma \Gamma\right] = [\Gamma \gamma \Gamma] \left[\Gamma \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \Gamma\right]$$

by the formula for the product.

(ii) Recall we had the isomorphism $\Theta : \mathcal{H}(G, \Gamma) \mapsto \mathbb{Z}[\Gamma \setminus G]^\Gamma$, and

$$\Theta(T(n)) = \sum_{\gamma \in \Pi_n} [\Gamma \gamma]$$

for some Π_n. Moreover, $\{\gamma \mathbb{Z}^2 \mid \gamma \in \Pi_n\}$ is exactly the subgroups of $\mathbb{Z}^2$ of index n.

On the other hand,

$$\Theta(T(m) T(n)) = \sum_{\delta \in \Pi_m, \gamma \in \Pi_n} [\Gamma \delta \gamma],$$

and

$$\{\delta \gamma \mathbb{Z}^2 \mid \delta \in \Pi_m\} = \{\text{subgroups of } \gamma \mathbb{Z}^2 \text{ of index } n\}.$$

Since n and m are coprime, every subgroup $\Lambda \subseteq \mathbb{Z}^2$ of index mn is contained in a unique subgroup of index n. So the above sum gives exactly $\Theta(T(mn))$.

(iii) We have

$$\Theta(T(p^r) T(p)) = \sum_{\delta \in \Pi_{p^r}, \gamma \in \Pi_p} [\Gamma \delta \gamma],$$

and for fixed $\gamma \in \Pi_p$, we know $\{\delta \gamma \mathbb{Z}^2 : \delta \in \Pi_{p^r}\}$ are the index p^r subgroups of $\mathbb{Z}^2$.

On the other hand, we have

$$\Theta(T(p^{r+1})) = \sum_{\varepsilon \in \Pi_{p^{r+1}}} [\Gamma \varepsilon],$$

where $\{\varepsilon\mathbb{Z}^2\}$ are the subgroups of $\mathbb{Z}^2$ of index p^{r+1}.

Every $\Lambda = \varepsilon\mathbb{Z}^2$ of index p^{r+1} is a subgroup of some index p subgroup $\Lambda' \in \mathbb{Z}^2$ of index p^r. If $\Lambda \not\subseteq p\mathbb{Z}^2$, then Λ' is unique, and $\Lambda' = \Lambda + p\mathbb{Z}^2$. On the other hand, if $\Lambda \subseteq p\mathbb{Z}^2$, i.e.

$$\varepsilon = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \varepsilon'$$

for some ε' of determinant p^{r-1}, then there are $(p+1)$ such Λ' corresponding to the $(p+1)$ order p subgroups of $\mathbb{Z}^2/p\mathbb{Z}^2$.

So we have

$$\begin{aligned} \Theta(T(p^r)T(p)) &= \sum_{\varepsilon \in \Pi_{p^{r+1}} \setminus (pI\Gamma_{p^{r-1}})} [\Gamma\varepsilon] + (p+1) \sum_{\varepsilon' \in \Pi_{p^{r-1}}} [\Gamma pI\varepsilon'] \\ &= \sum_{\varepsilon \in \Pi_{p^{r+1}}} [\Gamma\varepsilon] + p \sum_{\varepsilon' \in \Pi_{p^{r-1}}} [\Gamma pI\varepsilon'] \\ &= T(p^{r+1}) + pR(p)T(p^{r-1}). \end{aligned}$$

□

Proposition.

(i) $T^k_{mn} T^k_m T^k_n$ if $(m,n) = 1$, and

$$T^k_{p^{r+1}} = T^k_{p^r} T^k_p - p^{k-1} T^k_{p^{r-1}}.$$

(ii) If $f \in M_k$, then $T_n f \in M_k$. Similarly, if $f \in S_k$, then $T_n f \in S_k$.

(iii) We have

$$a_n(T_m f) = \sum_{1 \leq d | (m,n)} d^{k-1} a_{mn/d^2}(f).$$

In particular,

$$a_0(T_m f) = \sigma_{k-1}(m) a_0(f).$$

Proof.

(i) This follows from the analogous relations for $T(n)$, plus $f|R(n) = f$.

(ii) This follows from (iii), since T_n clearly maps holomorphic f to holomorphic f.

(iii) If $r \in \mathbb{Z}$, then

$$q^r \underset{k}{|} T(m) = m^{k/2} \sum_{e|m, 0 \leq b < e} e^{-k} \exp\left(2\pi i \frac{mzr}{e^2} + 2\pi i \frac{br}{e}\right),$$

where we use the fact that the elements of Π_m are those of the form

$$\Pi_m = \left\{ \begin{pmatrix} a & b \\ 0 & e \end{pmatrix} : ae = m, 0 \leq b < e \right\}.$$

Now for each fixed e, the sum over b vanishes when $\frac{r}{e} \notin \mathbb{Z}$, and is e otherwise. So we find

$$q^r \underset{k}{|} T(m) = m^{k/2} \sum_{e|(n,r)} e^{1-k} q^{mr/e^2}.$$

So we have

$$\begin{aligned} T_m(f) &= \sum_{r \geq 0} a_r(f) \sum_{e|(m,r)} \left(\frac{m}{e}\right)^{k-1} q^{mr/e^2} \\ &= \sum_{1 \leq d|m} e^{k-1} \sum a_{ms/d}(f) q^{ds} \\ &= \sum_{n \geq 0} \sum_{d|(m,n)} d^{k-1} a_{mn/d^2} q^n, \end{aligned}$$

where we put $n = ds$. □

Corollary. Let $f \in M_k$ be such that

$$T_n(f) = \lambda f$$

for some $m > 1$ and $\lambda \in \mathbb{C}$. Then

(i) For every n with $(n, m) = 1$, we have

$$a_{mn}(f) = \lambda a_n(f).$$

If $a_0(f) \neq 0$, then $\lambda = \sigma_{k-1}(m)$.

Proof. This just follows from above, since

$$a_n(T_m f) = \lambda a_n(f),$$

and then we just plug in the formula. □

Corollary. Let $0 \neq f \in M_k$, and $k \geq 4$ with $T_m f = \lambda_m f$ for all $m \geq 1$. Then

(i) If $f \in S_k$, then $a_1(f) \neq 0$ and

$$f = a_1(f) \sum_{n \geq 1} \lambda_n q^n.$$

(ii) If $f \notin S_k$, then

$$f = a_0(f) E_k.$$

Proof.

(i) We apply the previous corollary with $n = 1$.

(ii) Since $a_0(f) \neq 0$, we know $a_n(f) = \sigma_{k-1}(m) a_1(f)$ by (both parts of) the corollary. So we have

$$f = a_0(f) + a_1(f) \sum_{n \geq 1} \sigma_{k-1}(n) q^n = A + BE_k.$$

But since F and E_k are modular forms, and $k \neq 0$, we know $A = 0$. □

Theorem. There exists a basis for S_k consisting of normalized Hecke eigenforms.

Partial proof. We know that $\{T_n\}$ are commuting operators on S_k.

Fact. There exists an inner product on S_k for which $\{T_n\}$ are self-adjoint.

Then by linear algebra, the $\{T_n\}$ are simultaneously diagonalized. □

7 L-functions of eigenforms

Proposition. Let $f \in S_k(\Gamma(1))$. Then $L(f, s)$ converges absolutely for $\mathrm{Re}(s) > \frac{k}{2} + 1$.

Lemma. If
$$f = \sum_{n \geq 1} a_n q^n \in S_k(\Gamma(1)),$$
then
$$|a_n| \ll n^{k/2}$$

Proof. Recall from the example sheet that if $f \in S_k$, then $y^{k/2}|f|$ is bounded on the upper half plane. So
$$|a_n(f)| = \left| \frac{1}{2\pi} \int_{|q|=r} q^{-n} \tilde{f}(q) \frac{\mathrm{d}q}{q} \right|$$
for $r \in (0, 1)$. Then for *any* y, we can write this as
$$\left| \int_0^1 e^{-2\pi i n(x+iy)} f(x+iy) \mathrm{d}x \right| \leq e^{2\pi n y} \sup_{0 \leq x \leq 1} |f(x+iy)| \ll e^{2\pi n y} y^{-k/2}.$$
We now pick $y = \frac{1}{n}$, and the result follows. □

Proposition. Suppose f is a normalized eigenform. Then
$$L(f, s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}.$$

Proof. We look at
$$(1 - a_p p^{-s} + p^{k-1-2s})(1 + a_p p^{-s} + a_{p^2} p^{-2s} + \cdots) \\ = 1 + \sum_{r \geq 2} (a_{p^r} + p^{k-1} a_{p^{r-2}} - a_p a_p^{r-1}) p^{-rs}.$$
Since we have an eigenform, all of those coefficients are zero. So this is just 1. Thus, we know
$$1 + a_p p^{-s} + a_{p^2} p^{-2s} + \cdots = \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}.$$
Also, we know that when $(m, n) = 1$, we have
$$a_{mn} = a_m a_n,$$
and also $a_1 = 1$. So we can write
$$L(f, s) = \prod_p (1 + a_p p^{-s} + a_{p^2} p^{-2s} + \cdots) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}.$$ □

Theorem. If $f \in S_k$ then, $L(f, s)$ is entire, i.e. has an analytic continuation to all of C. Define

$$\Lambda(f, s) = (2\pi)^{-s}\Gamma(s)L(f, s) = M(f(iy), s).$$

Then we have

$$\Lambda(f, s) = (-1)^{k/2}\Lambda(f, k - s).$$

Theorem. Suppose we have a function

$$0 \neq f(z) = \sum_{n \geq 1} a_n q^n,$$

with $a_n = O(n^R)$ for some R, and there exists $N > 0$ such that

$$f \underset{k}{|} \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) = cf$$

for some $k \in \mathbb{Z}_{>0}$ and $c \in \mathbb{C}$. Then the function

$$L(s) = \sum_{n \geq 1} a_n n^{-s}$$

is entire. Moreover, $c^2 = (-1)^k$, and if we set

$$\Lambda(s) = (2\pi)^{-s}\Gamma(s)L(s), \quad \varepsilon = c \cdot i^k \in \{\pm 1\},$$

then

$$\Lambda(k - s) = \varepsilon N^{s - k/2}\Lambda(s).$$

Proof. By definition, we have

$$cf(z) = f \underset{k}{|} \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) = N^{-k/2} z^{-k} f\left(-\frac{1}{Nz}\right).$$

Applying the matrix once again gives

$$f \underset{k}{|} \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) \underset{k}{|} \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) = f \underset{k}{|} \left(\begin{smallmatrix} -N & 0 \\ 0 & -N \end{smallmatrix}\right) = (-1)^k f(z),$$

but this is equal to $c^2 f(z)$. So we know

$$c^2 = (-1)^k.$$

We now apply the Mellin transform. We assume $\mathrm{Re}(s) \gg 0$, and then we have

$$\Lambda(f, s) = M(f(iy), s) = \int_0^\infty f(iy) y^s \frac{\mathrm{d}y}{y} = \left(\int_{1/\sqrt{N}}^\infty + \int_0^{1/\sqrt{N}}\right) f(iy) y^s \frac{\mathrm{d}y}{y}.$$

By a change of variables, we have

$$\begin{aligned}\int_0^{1/\sqrt{N}} f(iy) y^s \frac{\mathrm{d}y}{y} &= \int_{1/\sqrt{N}}^\infty f\left(\frac{i}{Ny}\right) N^{-s} y^{-s} \frac{\mathrm{d}y}{y} \\ &= \int_{1/\sqrt{N}}^\infty c i^k N^{k/2 - s} f(iy) y^{k - s} \frac{\mathrm{d}y}{y}.\end{aligned}$$

So

$$\Lambda(f, s) = \int_{1/\sqrt{N}}^{\infty} f(iy)(y^s + \varepsilon N^{k/2-s} y^{k-s}) \frac{\mathrm{d}y}{y},$$

where

$$\varepsilon = i^k c = \pm 1.$$

Since $f \to 0$ rapidly for $y \to \infty$, this integral is an entire function of s, and satisfies the functional equation

$$\Lambda(f, k - s) = \varepsilon N^{s - \frac{k}{2}} \Lambda(f, s). \qquad \square$$

Theorem (Mellin inversion theorem)**.** Let $f : (0, \infty) \to \mathbb{C}$ be a C^∞ function such that

- for all $N, n \geq 0$, the function $y^N f^{(n)}(y)$ is bounded as $y \to \infty$; and
- there exists $k \in \mathbb{Z}$ such that for all $n \geq 0$, we have $y^{n+k} f^{(n)}(y)$ bounded as $y \to 0$.

Let $\Phi(s) = M(f, s)$, analytic for $\mathrm{Re}(s) > k$. Then for all $\sigma > k$, we have

$$f(y) = \frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \Phi(s) y^{-s} \;\mathrm{d}s.$$

Proof. The idea is to reduce this to the inversion of the Fourier transform. Fix a $\sigma > k$, and define

$$g(x) = e^{2\pi\sigma x} f(e^{2\pi x}) \in C^\infty(\mathbb{R}).$$

Then we find that for any $N, n \geq 0$, the function $e^{Nx} g^{(n)}(x)$ is bounded as $x \to +\infty$. On the other hand, as $x \to -\infty$, we have

$$\begin{aligned} g^{(n)}(x) &\ll \sum_{j=0}^{n} e^{2\pi(\sigma + j)x} |f^{(j)}(e^{2\pi x})| \\ &\ll \sum_{j=0}^{n} e^{2\pi(\sigma+j)x} e^{-2\pi(j+k)x} \\ &\ll e^{2\pi(\sigma - k)x}. \end{aligned}$$

So we find that $g \in \mathcal{S}(\mathbb{R})$. This allows us to apply the Fourier inversion formula. By definition, we have

$$\begin{aligned} \hat{g}(-t) &= \int_{-\infty}^{\infty} e^{2\pi\sigma x} f(e^{2\pi x}) e^{2\pi i x t} \;\mathrm{d}x \\ &= \frac{1}{2\pi} \int_0^\infty y^{\sigma + it} f(y) \frac{\mathrm{d}y}{y} = \frac{1}{2\pi} \Phi(\sigma + it). \end{aligned}$$

Applying Fourier inversion, we find

$$\begin{aligned} f(y) &= y^{-\sigma} g\left(\frac{\log y}{2\pi}\right) \\ &= y^{-\sigma} \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{-2\pi i t(\log y / 2\pi)} \Phi(\sigma + it) \;\mathrm{d}t \\ &= \frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \Phi(s) y^{-s} \;\mathrm{d}s. \end{aligned} \qquad \square$$

Theorem. Let

$$L(s) = \sum_{n \geq 1} a_n n^{-s}$$

be a Dirichlet series such that $a_n = O(n^R)$ for some R. Suppose there is some even $k \geq 4$ such that

- $L(s)$ can be analytically continued to $\{\mathrm{Re}(s) > \frac{k}{2} - \varepsilon\}$ for some $\varepsilon > 0$;
- $|L(s)|$ is bounded in vertical strips $\{\sigma_0 \leq \mathrm{Re}\, s \leq \sigma_1\}$ for $\frac{k}{2} \leq \sigma_0 < \sigma_1$.
- The function

  $$\Lambda(s) = (2\pi)^{-s}\Gamma(s)L(s)$$

  satisfies

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

  for $\frac{k}{2} - \varepsilon < \mathrm{Re}\, s < \frac{k}{2} + \varepsilon$.

Then

$$f = \sum_{n \geq 1} a_n q^n \in S_k(\Gamma(1)).$$

Proof. Holomorphicity of f on $\mathcal{H}$ follows from the fact that $a_n = O(n^R)$, and since it is given by a q series, we have $f(z+1) = f(z)$. So it remains to show that

$$f\left(-\frac{1}{z}\right) = z^k f(z).$$

By analytic continuation, it is enough to show this for

$$f\left(\frac{i}{y}\right) = (iy)^k f(iy).$$

Using the inverse Mellin transform (which does apply in this case, even if it might not meet the conditions of the version we proved), we have

$$\begin{aligned}
f(iy) &= \frac{1}{2\pi i}\int_{\sigma - i\infty}^{\sigma + i\infty} \Lambda(s) y^{-s}\;\mathrm{d}s \\
&= \frac{1}{2\pi i}\int_{\frac{k}{2} - i\infty}^{\frac{k}{2} + i\infty} \Lambda(s) y^{-s}\;\mathrm{d}s \\
&= \frac{(-1)^{k/2}}{2\pi i}\int_{\frac{k}{2} - i\infty}^{\frac{k}{2} + i\infty} \Lambda(k - s) y^{-s}\;\mathrm{d}s \\
&= \frac{(-1)^{k/2}}{2\pi i}\int_{\frac{k}{2} - i\infty}^{\frac{k}{2} + i\infty} \Lambda(s) y^{s-k}\;\mathrm{d}s \\
&= (-1)^{k/2} y^{-k} f\left(\frac{i}{y}\right).
\end{aligned}$$

Note that for the change of contour, we need

$$\int_{\frac{k}{2} \pm iT}^{\sigma \pm iT} \Lambda(s) y^{-s}\;\mathrm{d}s \to 0$$

as $T \to \infty$. To do so, we need the fact that $\Gamma(\sigma + iT) \to 0$ rapidly as $T \to \pm\infty$ uniformly for σ in any compact set, which indeed holds in this case. $\square$

Proposition. We have

$$M(f, s) = (2\pi)^{-s}\Gamma(s)\zeta(s)\zeta(s-1).$$

Proof. Doing the usual manipulations, it suffices to show that

$$\sum \sigma_1(m) m^{-s} = \zeta(s)\zeta(s-1).$$

We know if $(m, n) = 1$, then

$$\sigma_1(mn) = \sigma_1(m)\sigma_1(n).$$

So we have

$$\sum_{m \geq 1} \sigma_1(m) m^{-s} = \prod_p (1 + (p+1)p^{-s} + (p^2 + p + 1)p^{-2s} + \cdots).$$

Also, we have

$$(1 - p^{-s})(1 + (p+1)p^{-s} + (p^2 + p + 1)p^{-2s} + \cdots) = 1 + p^{1-s} + p^{2-2s} + \cdots = \frac{1}{1 - p^{1-s}}.$$

Therefore we find

$$\sum \sigma_1(m) m^{-s} = \zeta(s)\zeta(s-1).$$

□

Proposition.

$$M(f, s) = \frac{s-1}{4\pi} Z(s) Z(s-1) = -M(f, 2-s).$$

Theorem. We have

$$f(y) + y^{-2} f\left(\frac{1}{y}\right) = \frac{1}{24} - \frac{1}{4\pi} y^{-1} + \frac{1}{24} y^{-2}.$$

Proof. We will apply the Mellin inversion formula. To justify this application, we need to make sure our f behaves sensibly ass $y \to 0, \infty$. We use the absurdly terrible bound

$$\sigma_1(m) \leq \sum_{1 \leq d \leq m} d \leq m^2.$$

Then we get

$$f^{(n)}(y) \ll \sum_{m \geq 1} m^{2+n} e^{-2\pi m y}$$

This is certainly very well-behaved as $y \to \infty$, and is $\ll y^{-N}$ for all N. As $y \to 0$, this is

$$\ll \frac{1}{(1 - e^{2\pi y})^{n+3}} \ll y^{-n-3}.$$

So f satisfies conditions of our Mellin inversion theorem with $k = 3$.

We pick any $\sigma > 3$. Then the inversion formula says

$$f(y) = \frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} M(f, s) y^{-s} \, \mathrm{d}s.$$

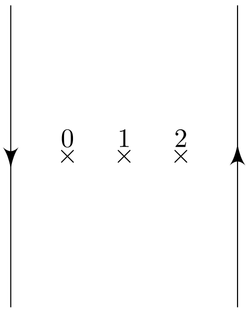
So we have

$$\begin{aligned} f\left(\frac{1}{y}\right) &= \frac{1}{2\pi i}\int_{\sigma - i\infty}^{\sigma + i\infty} -M(f, 2-s) y^s \, \mathrm{d}s \\ &= \frac{-1}{2\pi i}\int_{2-\sigma-i\infty}^{2-\sigma+i\infty} M(f,s) y^{2-s}\, \mathrm{d}s \end{aligned}$$

So we have

$$f(y) + y^{-2} f\left(\frac{1}{y}\right) = \frac{1}{2\pi i}\left(\int_{\sigma - i\infty}^{\sigma + i\infty} - \int_{2-\sigma-i\infty}^{2+\sigma+i\infty}\right) M(f,s) y^{-s}\, \mathrm{d}s.$$

This contour is pretty simple. It just looks like this:



Using the fact that $M(f,s)$ vanishes quickly as $|\operatorname{Im}(s)| \to \infty$, this is just the sum of residues

$$f(y) + y^{-2} f\left(\frac{1}{y}\right) = \sum_{s_0 = 0, 1, 2} \operatorname*{res}_{s = s_0} M(f,s) y^{-s_0}.$$

It remains to compute the residues. At $s = 2$, we have

$$\operatorname*{res}_{s=2} M(f,s) = \frac{1}{4\pi} Z(2) \operatorname*{res}_{s=1} Z(s) = \frac{1}{4\pi}\cdot\frac{\pi}{6}\cdot 1 = \frac{1}{24}.$$

By the functional equation, this implies

$$\operatorname*{res}_{s=0} M(f,s) = \frac{1}{24}.$$

Now it remains to see what happens when $s = 1$. We have

$$\operatorname*{res}_{s=1} M(f,s) = \frac{1}{4\pi}\operatorname*{res}_{s=1} Z(s) \operatorname*{res}_{s=0} Z(s) = -\frac{1}{4\pi}.$$

So we are done. □

Corollary.

$$E_2\left(-\frac{1}{z}\right) = z^2 E_2(z) + \frac{12 z}{2\pi i}.$$

Proof. We have

$$\begin{aligned} E_2(iy) &= 1 - 24f(y) \\ &= 1 - 24y^{-2} f\left(\frac{1}{y}\right) - 1 + \frac{6}{\pi} y^{-1} + y^{-2} \\ &= y^{-2}\left(1 - 24 f\left(\frac{1}{y}\right)\right) + \frac{6}{\pi} y^{-1} \\ &= y^{-2} E\left(\frac{-1}{iy}\right) + \frac{6}{\pi} y^{-1}. \end{aligned}$$

Then the result follows from setting $z = iy$, and then applying analytic continuiation. □

Corollary.

$$\Delta(z) = q \prod_{m \geq 1} (1 - q^m)^{24}.$$

Proof. Let $D(z)$ be the right-hand-side. It suffices to show this is a modular form, since $S_{12}(\Gamma(1))$ is one-dimensional. It is clear that this is holomorphic on $\mathcal{H}$, and $D(z+1) = D(z)$. If we can show that

$$D \underset{12}{|} \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = D,$$

then we are done. In other words, we need to show that

$$D\left(\frac{-1}{z}\right) = z^{12} D(z).$$

But we have

$$\begin{aligned} \frac{D'(z)}{D(z)} &= 2\pi i - 24 \sum_{m \geq 1} \frac{2\pi i m q}{1 - q^m} \\ &= 2\pi i \left(1 - 24 \sum_{m, d \geq 1} m q^{md}\right) \\ &= 2\pi i E_2(z) \end{aligned}$$

So we know

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}z}\left(\log D\left(-\frac{1}{z}\right)\right) &= \frac{1}{z^2} \frac{D'}{D}\left(-\frac{1}{z}\right) \\ &= \frac{1}{z^2} 2\pi i E_2\left(-\frac{1}{z}\right) \\ &= \frac{D'}{D}(z) + 12 \frac{\mathrm{d}}{\mathrm{d}z} \log z. \end{aligned}$$

So we know that

$$\log D\left(-\frac{1}{z}\right) = \log D + 12 \log z + c,$$

for some locally constant function c. So we have

$$D\left(-\frac{1}{z}\right) = z^{12}D(z) \cdot C$$

for some other constant C. By trying $z = i$, we find that $C = 1$ (since $D(i) \neq 0$ by the infinite product). So we are done. □

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

8.1 Definitions

Lemma. Let $\Gamma \leq \Gamma(1)$ be a subgroup of finite index, and $\gamma_1, \cdots, \gamma_i$ be right coset representatives of $\bar{\Gamma}$ in $\overline{\Gamma(1)}$, i.e.

$$\overline{\Gamma(1)} = \coprod_{i=1}^{d} \bar{\Gamma}\gamma_i.$$

Then

$$\coprod_{i=1}^{d} \gamma_i \mathcal{D}$$

is a fundamental domain for Γ.

Proposition. Let Γ have ν cusps of widths $m_1, \cdots, m_\nu$. Then

$$\sum_{i=1}^{\nu} m_i = (\overline{\Gamma(1)} : \bar{\Gamma}).$$

Proof. There is a surjective map

$$\pi : \bar{\Gamma} \setminus \overline{\Gamma(1)} \to \text{cusps}$$

given by sending

$$\bar{\Gamma} \cdot \gamma \mapsto \bar{\Gamma} \cdot \gamma(\infty).$$

It is then an easy group theory exercise that $|\pi^{-1}([\alpha])| = m_\alpha$. □

Proposition. Let $\Gamma \subseteq \Gamma(1)$ be of finite index, and $g \in G = \mathrm{GL}_2(\mathbb{Q})^+$. Then $\Gamma' = g^{-1}\Gamma g \cap \Gamma(1)$ also has finite index in $\Gamma(1)$, and if $f \in M_k(\Gamma)$ or $S_k(\Gamma)$, then $f \underset{k}{|} g \in M_k(\Gamma')$ or $S_k(\Gamma')$ respectively.

Proof. We saw that (G, Γ) has property (H). So this implies the first part. Now if $\gamma \in \Gamma'$, then $g\gamma g^{-1} \in \Gamma$. So

$$f \underset{k}{|} g\gamma g^{-1} = f \Rightarrow f \underset{k}{|} g \underset{k}{|} \gamma = f \underset{k}{|} g.$$

The conditions (ii') and (iii') are clear. □

Theorem. We have

$$M_k(\Gamma) = \begin{cases} 0 & k < 0 \\ \mathbb{C} & k = 0 \end{cases},$$

and

$$\dim_{\mathbb{C}} M_k(\Gamma) \leq 1 + \frac{k}{12}(\Gamma(1) : \Gamma).$$

for all $k > 0$.

Proof. Let
$$\Gamma(1) = \coprod_{i=1}^{d} \Gamma\gamma_i.$$
We let
$$f \in M_k(\Gamma),$$
and define
$$\mathcal{N}_f = \prod_{1 \leq i \leq d} f \underset{k}{|} \gamma_i.$$
We claim that $\mathcal{N}_f \in M_{kd}(\Gamma(1))$, and $\mathcal{N}_f = 0$ iff $f = 0$. The latter is obvious by the principle of isolated zeroes.

Indeed, f is certainly holomorphic on $\mathcal{H}$, and if $\gamma \in \Gamma(1)$, then
$$\mathcal{N}_f \underset{k}{|} \gamma = \prod_i f \underset{k}{|} \gamma_i\gamma = \mathcal{N}_f.$$
As $f \in M_k(\Gamma)$, each $f \underset{k}{|} \gamma_i$ is holomorphic at ∞.

- If $k < 0$, then $\mathcal{N}_f \in M_{kd}(\Gamma(1)) = 0$. So $f = 0$.
- If $k \geq 0$, then suppose $\dim M_k(G) > N$. Pick $z_1, \cdots, z_N \in \mathcal{D} \setminus \{i, \rho\}$ distinct. Then there exists $0 \neq f \in M_k(\Gamma)$ with
$$f(z_1) = \cdots = f(z_N) = 0.$$
So
$$\mathcal{N}_f(z_1) = \cdots = \mathcal{N}_f(z_N) = 0.$$
Then by our previous formula for zeros of modular forms, we know $N \leq \frac{kd}{12}$. So $\dim M_k(\Gamma) \leq 1 + \frac{kd}{12}$.
- If $k = 0$, then $M_0(\Gamma)$ has dimension ≤ 1. So $M_0(\Gamma) = \mathbb{C}$. □

8.2 The Petersson inner product

Proposition.

(i) $\langle \cdot, \cdot \rangle$ is a Hermitian inner product on $S_k(\Gamma)$.

(ii) $\langle \cdot, \cdot \rangle$ is invariant under translations by $GL_2(\mathbb{Q})^+$. In other words, if $\gamma \in GL_2(\mathbb{Q})^+$, then
$$\langle f \underset{k}{|} \gamma, g \underset{k}{|} \gamma \rangle = \langle f, g \rangle.$$

(iii) If $f, g \in S_k(\Gamma(1))$, then
$$\langle T_n f, g \rangle = \langle f, T_n g \rangle.$$

Proof.

(i) We know $\langle f, g\rangle$ is $\mathbb{C}$-linear in f, and $\overline{\langle f, g\rangle} = \langle g, f\rangle$. Also, if $\langle f, f\rangle = 0$, then
$$\int_{\Gamma\backslash\mathcal{H}} y^{k-2}|f|^2 \, \mathrm{d}x\, \mathrm{d}y = 0,$$
but since f is continuous, and y is never zero, this is true iff f is identically zero.

(ii) Let $f' = f\underset{k}{|}\gamma$ and $g' = g\underset{k}{|}\gamma \in S_k(\Gamma')$, where $\Gamma' = \Gamma \cap \gamma^{-1}\Gamma\gamma$. Then
$$y^k f'\bar{g}' = y^k \frac{(\det\gamma)^k}{|cz+d|^{2k}} \cdot f(\gamma(z))\overline{g(\gamma(z))} = (\operatorname{Im}\gamma(z))^k f(\gamma(z))\overline{g(\gamma(z))}.$$
Now $\operatorname{Im}\gamma(z)$ is just the y of $\gamma(z)$. So it follows that Then we have
$$\begin{aligned}\langle f', g'\rangle &= \frac{1}{v(\Gamma')}\int_{\mathcal{D}_{\Gamma'}} y^k f\bar{g}\frac{\mathrm{d}x\,\mathrm{d}y}{y^2}\bigg|_{\gamma(z)}\\ &= \frac{1}{v(\Gamma')}\int_{\gamma(\mathcal{D}_{\Gamma'})} y^k f\bar{g}\frac{\mathrm{d}x\,\mathrm{d}y}{y^2}.\end{aligned}$$
Now $\gamma(\mathcal{D}_{\Gamma'})$ is a fundamental domain for $\gamma\Gamma'\gamma^{-1} = \gamma\Gamma\gamma^{-1}\Gamma$, and note that $v(\Gamma') = v(\gamma\Gamma'\gamma^{-1})$ by invariance of measure. So $\langle f', g'\rangle = \langle f, g\rangle$.

(iii) Note that T_n is a polynomial with integer coefficients in $\{T_p : p \mid n\}$. So it is enough to do it for $n = p$. We claim that
$$\langle T_p f, g\rangle = p^{\frac{k}{2}-1}(p+1)\langle f\underset{k}{|}\delta, g\rangle,$$
where $\delta \in \mathrm{Mat}_2(\mathbb{Z})$ is any matrix with $\det(\delta) = p$.

Assuming this, we let
$$\delta^a = p\delta^{-1} \in \mathrm{Mat}_2(\mathbb{Z}),$$
which also has determinant p. Now as
$$g\underset{k}{|}\left(\begin{smallmatrix} p & 0\\ 0 & p\end{smallmatrix}\right) = g,$$
we know
$$\begin{aligned}\langle T_p f, g\rangle &= p^{\frac{k}{2}-1}(p+1)\langle f\underset{k}{|}\delta, g\rangle\\ &= p^{\frac{k}{2}-1}(p+1)\langle f, g\underset{k}{|}\delta^{-1}\rangle\\ &= p^{\frac{k}{2}-1}(p+1)\langle f, g\underset{k}{|}\delta^{a}\rangle\\ &= \langle f, T_p g\rangle\end{aligned}$$
To prove the claim, we let
$$\Gamma(1)\begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix}\Gamma(1) = \coprod_{0\le j\le p}\Gamma(1)\delta\gamma_i$$

for some $\gamma_i \in \Gamma(1)$. Then we have

$$\begin{aligned}\langle T_p f, g\rangle &= p^{\frac{k}{2}-1}\left\langle \sum_j f\underset{k}{|}\delta\gamma_j, g\right\rangle\\ &= p^{\frac{k}{2}-1}\sum_j \langle f\underset{k}{|}\delta\gamma_j, g\underset{k}{|}\gamma_j\rangle\\ &= p^{\frac{k}{2}-1}(p+1)\langle f\underset{k}{|}\delta, g\rangle,\end{aligned}$$

using the fact that $g\underset{k}{|}\gamma_j = g$. □

8.3 Examples of modular forms

Theorem.

(i) If $\gamma \in \Gamma(1)$, then

$$G_{\mathbf{r},k}\underset{k}{|}\gamma = G_{\mathbf{r}\gamma,k}.$$

(ii) If $N\mathbf{r} \in \mathbb{Z}^2$, then $G_{\mathbf{r},k} \in M_k(\Gamma(N))$.

Proof.

(i) If $g \in \mathrm{GL}_2(\mathbb{R})^+$ and $\mathbf{u} \in \mathbb{R}^2$, then

$$\frac{1}{(u_1 z + u_2)^k}\underset{k}{|}g = \frac{(\det g)^{k/2}}{((au_1 + cu_2)z + (bu_1 + du_2))^k} = \frac{(\det g)^{k/2}}{(v_1 z + v_2)^k},$$

where $\mathbf{v} = \mathbf{n}\cdot g$. So

$$\begin{aligned}G_{\mathbf{r},k}\underset{k}{|}\gamma &= \sum_{\mathbf{m}}{}' \frac{1}{(((\mathbf{m}+\mathbf{r})_1\gamma)z + ((\mathbf{m}+\mathbf{r})\gamma)_2)^k}\\ &= \sum_{\mathbf{m}'} \frac{1}{((m_1' + r_1')z + m_2' + r_2')^k}\\ &= G_{\mathbf{r}\gamma,k}(z),\end{aligned}$$

where $\mathbf{m}' = \mathbf{m}\gamma$ and $\mathbf{r}' = \mathbf{r}\gamma$.

(ii) By absolute convergence, $G_{\mathbf{r},k}$ is holomorphic on the upper half plane. Now if $N\mathbf{r} \in \mathbb{Z}^2$ and $\gamma \in \Gamma(N)$, then $N\mathbf{r}\gamma \equiv N\mathbf{r} \pmod N$. So $\mathbf{r}\gamma \equiv \mathbf{r} \pmod{\mathbb{Z}^2}$. So we have

$$G_{\mathbf{r},k}\underset{k}{|}\gamma = G_{\mathbf{r}\gamma,k} = G_{\mathbf{r},k}.$$

So we get invariance under $\Gamma(N)$. So it is enough to prove $G_{\mathbf{r},k}$ is holomorphic at cusps, i.e. $G_{\mathbf{r},k}\underset{k}{|}\gamma$ is holomorphic at ∞ for all $\gamma \in \Gamma(1)$. So it is enough to prove that for *all* $\mathbf{r}$, $G_{\mathbf{r},k}$ is holomorphic at ∞.

We can write

$$G_{\mathbf{r},k} = \left(\sum_{m_1+r_1>0} + \sum_{m_1+r_1=0} + \sum_{m_1+r_1<0}\right)\frac{1}{((m_1+r_1)z + m_2 + r_2)^k}.$$

The first sum is
$$\sum_{m_1+r_1>0} = \sum_{m_1>-r_1} \sum_{m_2\in\mathbb{Z}} \frac{1}{([(m_1+r_1)z+r_2]+m_2)^k}.$$
We know that $(m_1+r_1)z+r_2 \in \mathcal{H}$. So we can write this as a Fourier series
$$\sum_{m_1>-r_1} \sum_{d\geq 1} \frac{(-2\pi)^k}{(k-1)!} d^{k-1} e^{2\pi r_2 d} q^{(m_1+r_1)d}.$$
We now see that all powers of q are positive. So this is holomorphic.

The sum over $m_1+r_1 = 0$ is just a constant. So it is fine.

For the last term, we have
$$\sum_{m_1+r_1<0} = \sum_{m_1<-r_1} \sum_{m_2\in\mathbb{Z}} \frac{(-1)^k}{((-m_1-r_1)z-r_2-m_2)^k},$$
which is again a series in positive powers of $q^{-m_1-r_1}$. □

Theorem.

(i) $\vartheta_4(z) = \vartheta_3(z\pm 1)$ and $\theta_2(z+1) = e^{\pi i/4}\vartheta_2(z)$.

(ii)
$$\vartheta_3\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{1/2} \vartheta_3(z)$$
$$\vartheta_4\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{1/2} \vartheta_2(z)$$

Proof.

(i) Immediate from definition, e.g. from the fact that $e^{\pi i} = 1$.

(ii) The first part we've seen already. To do the last part, we use the Poisson summation formula. Let
$$h_t(x) = e^{-\pi t(x+1/2)^2} = g_t\left(x+\frac{1}{2}\right),$$
where
$$g_t(x) = e^{-\pi t x^2}.$$
We previously saw
$$\hat{g}_t(y) = t^{-1/2} e^{-\pi y^2/t}.$$
We also have
$$\begin{aligned}\hat{h}_t(y) &= \int e^{-2\pi i x y} g_t\left(x+\frac{1}{2}\right)\,\mathrm{d}x\\ &= \int e^{-2\pi i(x-1/2)y} g_t(x)\,\mathrm{d}x\\ &= e^{\pi i y}\hat{g}_t(y).\end{aligned}$$

So by the Poisson summation formula,

$$\vartheta_2(it) = \sum_{n\in\mathbb{Z}} h_t(n) = \sum_{n\in\mathbb{Z}} \hat{h}_t(n) = \sum_{n\in\mathbb{Z}} (-1)^n t^{-1/2} e^{-\pi n^2/t} = t^{-1/2}\vartheta_4\left(\frac{i}{t}\right).$$

□

Corollary.

(i) Let

$$F = \begin{pmatrix} \vartheta_2^4 \\ \vartheta_3^4 \\ \vartheta_4^4 \end{pmatrix}.$$

Then

$$F(z+1) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} F, \quad z^{-2}F\left(-\frac{1}{z}\right) = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix} F$$

(ii) $\vartheta_j^4 \in M_2(\Gamma)$ for a subgroup $\Gamma \leq \Gamma(1)$ of finite index. In particular, $\vartheta_j^4 \underset{z}{|} \gamma$ is holomorphic at ∞ for any $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$.

Proof.

(i) Immediate from the theorem.

(ii) We know $\overline{\Gamma(1)} = \langle S, T\rangle$, where $T = \pm\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \pm\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. So by (i), there is a homomorphism $\rho : \Gamma(1) \to \mathrm{GL}_3(\mathbb{Z})$ and $\rho(-I) = I$ with

$$F\underset{2}{|}\gamma = \rho(\gamma)F,$$

where $\rho(\gamma)$ is a signed permutation. In particular, the image of ρ is finite, so the kernel $\Gamma = \ker\rho$ has finite index, and this is the Γ we want.

It remains to check holomorphicity. But each ϑ_j is holomorphic at ∞. Since $F\underset{2}{|}\gamma = \rho(\gamma)F$, we know $\vartheta_j^4\underset{2}{|}$ is a sum of things holomorphic at ∞, and is hence holomorphic at ∞. □

Theorem. Let $f(z) = \vartheta(2z)^4$. Then $f(z) \in M_2(\Gamma_0(4))$, and moreover, $f\underset{2}{|}W_4 = -f$.

Lemma. $\Gamma_0(4)$ is generated by

$$-I, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} = W_4 \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} W_4^{-1}.$$

Proof. It suffices to prove that $\overline{\Gamma_0(4)}$ is generated by T and $U = \pm\left(\begin{smallmatrix} 1 & 0 \\ 4 & 1 \end{smallmatrix}\right)$.

Let

$$\gamma = \pm\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \overline{\Gamma_0(4)}.$$

We let

$$s(\gamma) = a^2 + b^2.$$

As c is even, we know $a \equiv 1 \pmod 2$. So $s(\gamma) \geq 1$, and moreover $s(\gamma) = 1$ iff $b = 0, a = \pm 1$, iff $\gamma = T^n$ for some n.

We now claim that if $s(\gamma) \neq 1$, then there exists $\delta \in \{T^{\pm 1}, U^{\pm 1}\}$ such that $s(\gamma\delta) < s(\gamma)$. If this is true, then we are immediately done.

To prove the claim, if $s(\gamma) \neq 1$, then note that $|a| \neq |2b|$ as a is odd.

- If $|a| < |2b|$, then $\min\{|b \pm a|\} < |b|$. This means $s(\gamma T^{\pm 1}) = a^2 + (b \pm a)^2 < s(\gamma)$.
- If $|a| > |2b|$, then $\min\{|a \pm 4b|\} < |a|$, so $s(\gamma U^{\pm 1}) = (a \pm 4b)^2 + b^2 < s(\gamma)$. □

Proof of theorem. It is enough to prove that

$$f\big|_2 T = f\big|_2 U = f.$$

This is now easy to prove, as it is just a computation. Since $\vartheta(z+2) = \vartheta(z)$, we know

$$f\big|_2 T = f(z+1) = f(z).$$

We also know that

$$f\big|_2 W_4 = 4(4z)^{-2} f\left(\frac{-1}{4z}\right) = \frac{1}{4z^2}\vartheta\left(-\frac{1}{2z}\right)^4 = -f(z),$$

as

$$\vartheta\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{1/2}\vartheta(z).$$

So we have

$$f\big|_2 U = f\big|_2 W_4\big|_2 T^{-1}\big|_2 W_4 = (-1)(-1)f = f.$$ □

Proposition. We have $g \in M_2(\Gamma_0(2))$, and $g\big|_2 W_2 = -g$.

Proof. We compute

$$\begin{aligned} g\big|_2 W_2 &= \frac{2}{(2z)^2} g\left(-\frac{1}{2z}\right) \\ &= \frac{1}{z^2}E_2\left(-\frac{1}{z}\right) - \frac{2}{(2z)^2}E_2\left(\frac{-1}{2z}\right) \\ &= E_2(z) + \frac{1}{2\pi i z} - 2\left(E_2(2z) + \frac{12}{2\pi i \cdot 2z}\right) \\ &= -g(z). \end{aligned}$$

We also have

$$g\big|_2 T = g(z+1) = g(z),$$

and so

$$g\big|_2 \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right) = g\big|_2 W_2 T^{-1} W_2^{-1} = g.$$

Moreover, g is holomorphic at ∞, and hence so is $g\big|_2 W_2 = -g$. So g is also holomorphic at $0 = W_2(\infty)$. As ∞ has width 1 and 0 has width 2, we see that these are all the cusps, and so g is holomorphic at the cusps. So $g \in M_2(\Gamma_0(2))$. □

Theorem.

$$M_2(\Gamma_0(4)) = \mathbb{C}g \oplus \mathbb{C}h.$$

Theorem (Lagrange's 4-square theorem)**.** For all $n \geq 1$, we have

$$r_4(n) = 8\left(\sigma_1(n) - 4\sigma_1\left(\frac{n}{4}\right)\right) = 8 \sum_{d \mid n \, 4 \nmid d} d.$$

In particular, $r_4(n) > 0$.

9 Hecke theory for $\Gamma_0(N)$

Theorem. Let $f \in S_k(\Gamma_0(N))^\varepsilon$, where $\varepsilon = \pm 1$. Then define

$$L(f, s) = \sum_{n \geq 1} a_n n^{-s}.$$

Then $L(f, s)$ is am entire function, and satisfies the functional equation

$$\Lambda(f, s) = (2\pi)^{-s}\Gamma(s)L(f, s) = \varepsilon(-N)^{k/2}\Lambda(f, k - s).$$

Proof. We have $f \underset{k}{|} W_N = \varepsilon f$, and then we can apply our earlier result. □

Theorem (Strong multiplicity one for $\mathrm{SL}_2(\mathbb{Z})$)**.** Let $f, g \in S_k(\Gamma(1))$ be normalized Hecke eigenforms, i.e.

$$\begin{aligned} f|T_p &= \lambda_p f & \lambda_p &= a_p(f) \\ g|T_p &= \mu_p g & \mu_p &= a_p(g). \end{aligned}$$

Suppose there exists a finite set of primes S such that such that for all $p \notin S$, then $\lambda_p = \mu_p$. Then $f = g$.

Idea of proof. We use the functional equations

$$\begin{aligned} \Lambda(f, k - s) &= (-1)^{k/2}\Lambda(f, s) \\ \Lambda(g, k - s) &= (-1)^{k/2}\Lambda(g, s) \end{aligned}$$

So we know

$$\frac{L(f, k - s)}{L(f, s)} = \frac{L(g, k - s)}{L(g, s)}.$$

Since these are eigenforms, we have an Euler product

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

and likewise for g. So we obtain

$$\prod_p \frac{1 - \lambda_p p^{s-k} + p^{2s-k-1}}{1 - \lambda_p p^{-s} + p^{k-1-2s}} = \prod_p \frac{1 - \mu_p p^{s-k} + p^{2s-k-1}}{1 - \mu_p p^{-s} + p^{k-1-2s}}.$$

Now we can replace this $\prod_p$ with $\prod_{p \in S}$. Then we have some very explicit rational functions, and then by looking at the appropriate zeroes and poles, we can actually get $\lambda_p = \mu_p$ for all p. □

Proposition. T_p, U_p send $S_k(\Gamma_0(N))$ to $S_k(\Gamma_0(N))$, and they all commute.

Proof. T_p, U_p do correspond to double coset actions

$$\Gamma_0(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_0(N) = \begin{cases} \Gamma_0(N)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \amalg \coprod_b \Gamma_0(N)\left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right) & p \nmid N \\ \coprod_b \Gamma_0(N)\left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right) & p \mid N \end{cases}.$$

Commutativity is checked by carefully checking the effect on the q-expansions. □

Theorem (Atkin–Lehner)**.** The Hecke algebra $\mathcal{H}(G, \Gamma_0(N))$ fixes $S_k(\Gamma_0(N))^{\text{new}}$ and $S_k(\Gamma_0(N))^{\text{old}}$, and on $S_k(\Gamma_0(N))^{\text{new}}$, it acts as a *commutative* subalgebra of the endomorphism ring, is closed under adjoint, and hence is diagonalizable. Moreover, strong multiplicity one holds, i.e. if S is a finite set of primes, and we have $\{\lambda_p : p \notin S\}$ given, then there exists at most one $N \geq 1$ and at most one $f \in S_k(\Gamma_0(N), 1)^{\text{new}}$ (up to scaling, obviously) for which

$$T_p f = \lambda_p f \text{ for all } p \nmid N, p \notin S.$$

10 Modular forms and rep theory

Proposition.

- We have $L_k^* f = 0$ iff f is holomorphic.
- If $f \in W_K(\Gamma(1))$, then $g \equiv L_k^* f \in W_{k-2}(\Gamma(1))$.

Proof. The first part is clear. For the second part, note that we have

$$f(\gamma(z)) = (cz + d)^k f(z).$$

We now differentiate both sides with respect to $\bar{z}$. Then (after a bit of analysis), we find that

$$(c\bar{z} + d)^{-2} \frac{\partial f}{\partial \bar{z}}(\gamma(z)) = (cz + d)^k \frac{\partial f}{\partial \bar{z}}.$$

On the other hand, we have

$$(\operatorname{Im} \gamma(z))^2 = \frac{y^2}{|cz + d|^4}.$$

So we find

$$g(\gamma(z)) = -2i \frac{y^2}{|2z + d|^4} (c\bar{z} + d)^2 (cz + d)^k \frac{\partial f}{\partial \bar{z}} = (cz + d)^{k-2} g(z).$$

The growth condition is easy to check. □

Theorem (Maass)**.** Let $S_{\text{Maass}}(\Gamma(1), \lambda)$ be the space of Maass cusp forms with eigenvalue λ. This space is finite-dimensional, and is non-zero if and only if $\lambda \in \{\lambda_n : n \geq 0\}$, where $\{\lambda_n\}$ is a sequence satisfying

$$0 < \lambda_0 < \lambda_1 < \lambda_2 < \cdots \to \infty.$$

Proposition. If $f \underset{k}{|} \gamma = f$, then $(R_k^* f) \underset{k+2}{|} \gamma = R_k^* f$.

Proposition. For $\Gamma \subseteq \Gamma(1)$, there is a bijection between functions $f : \mathcal{H} \to \mathbb{C}$ such that $f \underset{k}{|} \gamma = f$ for all $\gamma \in \Gamma$, and functions $\Phi : G \to \mathbb{C}$ such that $\Phi(\gamma g) = \Phi(g)$ for all $\gamma \in \Gamma$ and $\Phi(g r_\theta) = e^{ik\theta} \Phi(g)$.

Proof. Given an f, we define

$$\Phi(g) = (ci + d)^{-k} f(g(i)) = j(g, i)^{-k} f(g(i)).$$

We can then check that

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

On the other hand, using the fact that r_θ is in the stabilizer of i, we obtain

$$\begin{aligned} \Phi(g r_\theta) &= j(g r_\theta, i)^{-k} f(g r_\theta(i)) \\ &= j(g r_\theta, i)^{-k} f(g(i)) \\ &= j(g, r_\theta(i)) j(r_\theta, 1) f(g(i)) \\ &= \Phi(g) j(r_\theta, i)^{-k}. \end{aligned}$$

But $j(r_\theta, i) = -\sin\theta + \cos\theta$. So we are done. □

Proposition. The set of cuspoidal automorphic forms bijects with representations of $\mathfrak{sl}_2$ generated by holomorphic cusp forms f and their conjugates $\bar{f}$, and Maass cusp forms.

The holomorphic cusp forms f generate a representation of $\mathfrak{sl}_2$ with lowest weight; The conjugates of holomorphic cusp forms generate those with highest weight, while the Maass forms generate the rest.