MODULAR FORMS AND DIRICHLET SERIES

ANDREW OGG

Preface

These are the official notes for a course given at Berkeley during the fall and winter quarters of 1967–68 on Hecke's theory of modular forms and Dirichlet series. The reader who is conversant with Hecke's *Werke* will find nothing new here, except I have taken the liberty of including a recent paper of Weil, which stimulated my interest in this field.

The prerequisites for reading these notes are the theory of analytic functions of one complex variable and some number theory. Unattributed theorems are generally due to Hecke.

A. P. Ogg
Berkeley, California
March, 1968

TEX edition. This is a re-issue of Ogg's book [8] published in 1969, typeset with TEX. In particular, the numbering system (theorems, propositions) differs from [8]. Marked text in [8] is *emphasized* here and included in the index. Detected typos in [8] have been corrected; they are listed at the end.

 v1.0, 29th August 2018

Contents

Preface 1
TEX edition 1
Introduction 2
1. Dirichlet series with functional equation 4
2. Hecke operators for the full modular group 23
3. The Petersson inner product 29
4. Congruence subgroups of the modular group 34
5. A theorem of Weil 50
6. Quadratic forms 56
Corrected typos in Ogg's book 66
References 66
Index 68

2010 *Mathematics Subject Classification.* Primary 11F11; Secondary 11F25, 11F66.
Key words and phrases. modular forms, Dirichlet series.

Introduction

The simplest and most famous series is the *Riemann zeta-function* $\zeta(s)$, defined for $Re(s) > 1$ by

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} (1 - p^{-s})^{-1},$$

the product being over all primes p; the equality of the two expressions is just an analytic statement of the fundamental theorem of arithmetic. Riemann [10, VII.] proved in 1859 that $\zeta(s)$ has an analytic continuation to the whole s-plane except for a simple pole of residue 1 at $s = 1$ and satisfies the *functional equation*:

$$Z(s) = \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$$

is invariant under $s \mapsto 1 - s$. In fact, this functional equation almost characterizes $\zeta(s)$, for Hamburger [4] showed in 1921 that any Dirichlet series satisfying this functional equation and suitable regularity conditions is necessarily a constant multiple of $\zeta(s)$. However, the situation did not become clear until greatly generalized by Hecke in his paper "Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung", published in 1936 [5, 33.].

Let us sketch that proof of the functional equation for $\zeta(s)$ which leads naturally to Hecke's generalization. Starting from

$$\Gamma(s) = \int_0^{\infty} t^{s-1} e^{-t} dt \quad (\mathrm{Re}\,(s) > 0)$$

we find

$$\begin{aligned} \pi^{-s}\Gamma(s)\zeta(2s) &= \sum_{n=1}^{\infty} \int_0^{\infty} (\pi n^2)^{-s} t^{s-1} e^{-t} dt \quad (\mathrm{Re}\,(s) > 1) \\ &= \sum_{n=1}^{\infty} \int_0^{\infty} t^{s-1} e^{-\pi n^2 t} dt \\ &= \int_0^{\infty} t^{s-1} (\vartheta(it) - \frac{1}{2}) dt \end{aligned}$$

where

$$\begin{aligned} \vartheta(\tau) &= \frac{1}{2} \sum_{-\infty}^{\infty} e^{+\pi i n^2 \tau} \quad (\mathrm{Im}\,\tau > 0) \\ &= \frac{1}{2} + \sum_{n=1}^{\infty} e^{\pi i n^2 \tau} \end{aligned}$$

is the basic *theta-function*. Now $\vartheta(\tau)$ is holomorphic on the upper half plane, and satisfies

$$\begin{aligned} \vartheta(\tau + 2) &= \vartheta(\tau) \\ \vartheta(-1/\tau) &= (\frac{\tau}{i})^{1/2} \vartheta(\tau), \end{aligned}$$

where the square root is defined on $\mathrm{Re}\,(z) > 0$ to be real on the real axis. These two equations say that $\vartheta(\tau)$ is a modular form of dimension $-\frac{1}{2}$ for the group $G(2)$ generated by $\tau \mapsto \tau + 2$, $\tau \mapsto -1/\tau$, and ϑ is up to a constant multiple the only solution of these equations. (These facts have been known for ages, and will be

proved later in these notes.) The functional equation for $\zeta(s)$ is now a consequence of that for $\vartheta(\tau)$:

$$\begin{aligned}\pi^{-s}\Gamma(s)\zeta(2s) &= \int_1^\infty t^{s-1}(\vartheta(it)-\frac{1}{2})dt - \frac{1}{2}\frac{t^s}{s}|_0^1 + \int_0^1 t^{s-1}\vartheta(it)dt \\ &= \int_1^\infty t^{s-1}(\vartheta(it)-\frac{1}{2})dt - \frac{1}{2s} + \int_1^\infty t^{-s-1}\vartheta(\frac{i}{t})dt \\ &= \int_1^\infty (t^{s-1}+t^{1/2-s-1})(\vartheta(it)-\frac{1}{2})dt - \frac{1}{2s} - \frac{1}{1-2s},\end{aligned}$$

visibly invariant under $s \mapsto \frac{1}{2}-s$; furthermore, the integral is entire, since $\vartheta(it)-\frac{1}{2} = O(e^{-ct})$, for some $c>0$. On the other hand, by Mellin inversion we have

$$\vartheta(ix) - \frac{1}{2} = \frac{1}{2\pi i}\int_{\mathrm{Re}\,(s)=c} x^{-s}(\pi^{-s}\Gamma(s)\zeta(2s))ds$$

for sufficiently large $c>0$, and by similar reasoning (carried out in detail in a more general situation) the functional equation for $\vartheta(\tau)$ can be derived from that for $\zeta(s)$; this is Hecke's proof that $\zeta(s)$ is determined by its functional equation.

The above proof generalizes directly, as follows. Given a sequence of complex numbers $a_0, a_1, a_2, \ldots, a_n = O(n^c)$ for some $c>0$, and given $\lambda>0$, $k>0$, $C=\pm 1$, form

$$\varphi(s) = \sum_{n=1}^\infty a_n n^{-s} \qquad \Phi(s) = (\frac{2\pi}{\lambda})^{-s}\Gamma(s)\varphi(s) \qquad f(\tau) = \sum_{n=0}^\infty a_n e^{2\pi i n\tau/\lambda}$$

(the O-condition ensures that $\varphi(s)$ converges somewhere, and $f(s)$ is holomorphic in the upper half plane.)

Theorem. The following two conditions are equivalent:

(A) $\Phi(s) + \frac{a_0}{s} + \frac{Ca_0}{k-s}$ is entire and bounded in every vertical strip (henceforth abbreviated to *EBV*) and satisfies $\Phi(k-s) = C\Phi(s)$;
(B) $f(-1/\tau) = C(\frac{\tau}{i})^k f(\tau)$.

($(\frac{\tau}{i})^k = e^{k\log\frac{\tau}{i}}$, where log is real on the real axis.)

Note for $\varphi(s)=\zeta(2s)$, $f(\tau)=\vartheta(\tau)$, we have $C=1, \lambda=2, k=\frac{1}{2}$.

Generally, let $G(\lambda)$ be the group of substitutions of the upper half plane generated by $\tau\mapsto\tau+\lambda$, $\tau\mapsto -1/\tau$. A *modular form of dimension $-k$ and multiplier C* for $G(\lambda)$ is a holomorphic function $f(\tau)$ on the upper half plane satisfying

(1) $f(\tau+\lambda) = f(\tau)$
(2) $f(-1/\tau) = C(\frac{\tau}{i})^k f(\tau)$
(3) the expansion of $f(\tau)$ in a Laurent series in $e^{2\pi i\tau/\lambda}$ (from (1)) has no negative terms: $f(\tau) = \sum_{n=0}^\infty a_n e^{2\pi i n\tau/\lambda}$, i.e. f is "holomorphic at ∞".

We denote the space of such f by $\mathcal{M}(\lambda,k,C)$. We also denote by $\mathcal{M}_0(\lambda,k,C)$ the subspace of those f which satisfy the additional condition that the Fourier coefficients a_n satisfy $a_n = O(n^c)$ for some $c>0$. The theorem then says there is a one-one correspondence between the elements of $\mathcal{M}_0(\lambda,k,C)$ and Dirichlet series satisfying (A); note that $\varphi(s)$ is regular at $s=k$ if and only if $a_0=0$, i.e. $f(\tau)$ "vanishes at ∞". We say $\varphi(s)$ has *signature* (λ,k,C) if (A) holds.

Remark. If $\varphi(s) = \zeta(K,s)$ is the zeta-function of an algebraic number field K, its functional equation is that

$$|d|^{s/2}((2\pi)^{-s}\Gamma(s))^{r_2}(\pi^{-s/2}\Gamma(\frac{s}{2}))^{r_1}\varphi(s)$$

is invariant under $s \mapsto 1-s$, where d is the discriminant of K and r_1 resp. r_2 is the number of real resp. complex primes of K. Note this falls within the scope of the theorem only when there is only one Γ-function, i.e. K is rational or imaginary quadratic. If K is imaginary quadratic, then $\varphi(s)$ has signature $(\lambda,k,C) = (\sqrt{|d|},1,1)$; it turns out that $\varphi(s)$ is determined by its signature when $d = -3,-4$ but not for $d < -4$.

The other part of Hecke's theory concerns the question of whether $\varphi(s)$ has an *Euler product*, i.e. $\varphi(s) = \prod_p \varphi_p(s)$, where $\varphi_p(s)$ is a power series in p^{-s}. Suppose for concreteness that $\lambda = 1$, so $G(\lambda) = \Gamma$ is the *modular group*. It turns out that $\mathcal{M}(1,k,C) = \mathcal{M}_0(1,k,C)$, and this space is 0 unless k is an even integer ≥ 4, and $C = i^k$, and the only possible Euler product for $\varphi(s)$, of signature $(1,k,i^k)$, is

$$\varphi(s) = \sum_{n=1}^{\infty} a_n n^{-s} = \prod_p (1 - a_p p^{-s} + p^{k-1-2s})^{-1},$$

and $\varphi(s)$ has this Euler product if and only if the associated modular form f is an eigenfunction for a certain ring of operators on $\mathcal{M}(1,k,i^k)$, the *Hecke operators*. The question of the existence of Euler products is of course fundamental for number theory, since in practice the numbers a_n will be the number of solutions of some number-theoretic problem and the knowledge of an Euler product reduces knowledge of all the a_n to knowledge of the a_p for primes p.

1. Dirichlet series with functional equation

All that we need about Dirichlet series is that if $a_n = O(n^c)$, then $\varphi(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ converges absolutely and uniformly in $\mathrm{Re}\,(s) \geq c+1+\varepsilon$, since it is dominated term-by-term uniformly by $\sum_{n=1}^{\infty} n^{-1-\varepsilon} < \infty$, and hence $\varphi(s)$ defines a holomorphic function in (at least) the half plane $\mathrm{Re}\,(s) > c+1$. Conversely, if $\varphi(s)$ converges at $s_0 = \sigma_0 + it$, we see $a_n = O(n^{\sigma_0})$ since the general term $a_n n^{-s}$ tends to 0. Thus $\varphi(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ converges somewhere if and only if $a_n = O(n^c)$.

As to the gamma-function, we need:

(a) $\Gamma(s) = \int_0^{\infty} t^{s-1}e^{-t}dt$, for $\mathrm{Re}\,(s) > 0$
(b) $\Gamma(s+1) = s\Gamma(s)$, $\Gamma(1) = 1$, $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.
(c) $\Gamma(s)$ is never 0, and it is entire except for simple poles at $s = -n$ of residue $\frac{(-1)^n}{n!}$, $n = 0,1,2,\ldots$.
(d) *Stirling's formula* (cf., e.g., Ahlfors [1, chap 5, 2.5, (38), p.204])
  (i) $\Gamma(s) = \sqrt{2\pi}s^{s-\frac{1}{2}}e^{-s+\mu(s)}$, where $\mu(s) \to 0$ as $|s| \to \infty$, uniformly in a half plane $\sigma \geq \sigma_0 > 0$, where $s = \sigma + it$,
  (ii) $\Gamma(s) \sim \sqrt{2\pi}t^{\sigma-\frac{1}{2}}e^{-\frac{\pi}{2}|t|}$, as $t \to \infty$, uniformly in $\sigma_1 \leq \sigma \leq \sigma_2$. (This follows from (di) when $\sigma_1 > 0$, and then in general from (b).)
(e) *Mellin inversion formula.* $e^{-x} = \frac{1}{2\pi i}\int_{\sigma=c>0} x^{-s}\Gamma(s)ds$, for $x > 0$, the integral taken upwards on a vertical line. In fact, by the calculus of residues, the right side is

$$\sum_{n=0}^{\infty} \mathrm{Res}_{s=-n}\, x^{-s}\Gamma(s) = \sum_{n=0}^{\infty} \frac{(-x)^n}{n!} = e^{-x}$$

This being said, let us begin the basic theorem. Given $a_0, a_1, a_2, \dots$ with $a_n = O(n^c)$, we form $\varphi(s) = \sum_{n=1}^{\infty} a_n n^{-s}$, $f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n\tau/\lambda}$ for some fixed $\lambda > 0$. We have already noted that the growth condition on the a_n means that $\varphi(s)$ converges somewhere; for $f(\tau)$ it means that $f(x+iy)$ grows only as a power of y as $y \to 0$, a condition on the growth of $f(\tau)$ as τ approaches the real axis, the boundary of the upper half plane. More precisely:

Proposition 1.1. *Given $f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n\tau/\lambda}$, with the series converging in the upper half plan.*

(a) *If $a_n = O(n^c)$, then $f(x+iy) = O(y^{-c-1})$ as $y \to 0$, uniformly in all real x.*
(b) *If $f(x+iy) = O(y^{-c})$ as $y \to 0$, uniformly in x, then $a_n = O(n^c)$.*

Proof. By Stirling's formula $\Gamma(x) \sim \sqrt{2\pi} x^{x-\frac{1}{2}} e^{-x}$, we see that

$$(-1)^n \binom{-c-1}{n} = \frac{(c+1)\cdots(c+n)}{n!} = \frac{\Gamma(c+n+1)}{\Gamma(c+1)\Gamma(n+1)} \sim (\text{const.}) n^c,$$

so if $a_n = O(n^c)$, then $f(x+iy)$ is dominated term-by-term by

$$\sum_{n=0}^{\infty} (-1)^n \binom{-c-1}{n} e^{-2\pi y n/\lambda} = (1 - e^{-2\pi y/\lambda})^{-c-1} = O(y^{-c-1}).$$

Conversely, if $|f(x+iy)| \le B y^{-c}$, then

$$|a_n| = \left| \int_0^1 f(x + \frac{i}{n}) e^{-2\pi i n(x+\frac{i}{n})/\lambda} \right| \le B n^c e^{2\pi/\lambda}$$

□

For future convenience, we state our theorem for two functions instead of one. Thus we are given two sequences $a_0, a_1, a_2, \dots$ and $b_0, b_1, b_2, \dots$ of complex numbers, $a_n, b_n = O(n^c)$ for some $c > 0$, and $\lambda > 0$, $k > 0$, $C \neq 0$. (C need not be real.) We form

$$\varphi(s) = \sum_{n=1}^{\infty} a_n n^{-s} \qquad \Phi(s) = (\frac{2\pi}{\lambda})^{-s}\Gamma(s)\varphi(s) \qquad f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n\tau/\lambda}$$

$$\psi(s) = \sum_{n=1}^{\infty} b_n n^{-s} \qquad \Psi(s) = (\frac{2\pi}{\lambda})^{-s}\Gamma(s)\psi(s) \qquad g(\tau) = \sum_{n=0}^{\infty} b_n e^{2\pi i n\tau/\lambda}$$

(φ, ψ are analytic in some right half plane; f, g are analytic in the upper half plane, with the boundary growth condition of Proposition 1.1.)

Theorem 1.2. *The following two conditions are equivalent:*

(A) $\Phi(s) + \frac{a_0}{s} + \frac{Cb_0}{k-s}$ *is EBV and* $\Phi(s) = C\Psi(k-s)$;
(B) $f(\tau) = C(\frac{\tau}{i})^{-k} g(-1/\tau)$.

Proof.

$$\begin{aligned}\Phi(s) &= \sum_{n=1}^{\infty} \int_0^{\infty} a_n (\frac{2\pi n}{\lambda})^{-s} t^{s-1} e^{-t} dt \\ &= \sum_{n=1}^{\infty} \int_0^{\infty} a_n t^{s-1} e^{-2\pi n\tau/\lambda} dt \\ &= \int_0^{\infty} t^{s-1} (f(it) - a_0) dt,\end{aligned}$$

for Re (s) sufficiently large, the interchange of integral and summation being justified by absolute convergence. The integral is improper at both ends, but since $f(it) - a_0 = O(e^{-ct})$ as $t \to \infty$ for some $c > 0$, we see $\int_0^\infty t^{s-1}(f(it) - a_0)dt$ converges uniformly on vertical strips, and so is EBV.

Now assume (B). Then

$$\int_0^1 t^{s-1}(f(it) - a_0)dt = -a_0\frac{t^s}{s}|_0^1 + \int_1^\infty t^{1-s}f(\frac{i}{t})\frac{dt}{t^2} =$$
$$= \frac{-a_0}{s} + C\int_1^\infty t^{k-s-1}(g(it) - b_0)dt - \frac{Cb_0}{k-s}$$

Thus

$$\Phi(s) + \frac{a_0}{s} + \frac{Cb_0}{k-s} = \int_1^\infty \big(t^{s-1}(f(it) - a_0) + t^{k-s-1}C(g(it) - b_0)\big)dt$$

is EBV, with $\Phi(s) = C\Psi(k-s)$, which is (A).

Similarly, by Mellin inversion, or directly from $e^{-x} = \frac{1}{2\pi i}\int_{Re(s)=c>0} x^{-s}\Gamma(s)ds$, we have

$$f(ix) - a_0 = \frac{1}{2\pi i}\int_{\sigma=c} x^{-s}\Phi(s)ds,$$

for $x > 0$, where $\sigma = \text{Re}\,(s)$, and c is chosen large enough to be in the domain of absolute convergence of $\varphi(s)$. Assuming now (A), we can push the line of integration to the left, past 0, picking up residues of Cb_0x^{-k} at $s = k$ and $-a_0$ at $s = 0$. Then

$$f(ix) - Cb_0x^{-k} = \frac{1}{2\pi i}\int_{\sigma=c<0} x^{-s}\Phi(s)ds =$$
$$= \frac{C}{2\pi i}\int_{\sigma=c<0} x^{-s}\Psi(k-s)ds =$$
$$= \frac{C}{2\pi i}\int_{\sigma=c>k} x^{-(k-s)}\Psi(s)ds =$$
$$= Cx^{-k}(g(\frac{i}{x}) - b_0) \quad \text{or}$$
$$f(ix) = Cx^{-k}g(\frac{i}{x}),$$

which is (B) □

Theorem 1.2 was a great step forward, 75 years after the functional equation for the zeta-function, for it reduces a question about Dirichlet series to one about modular forms, which are easier to work with. Taking for some time hereafter $a_n = b_n$, $f = g$, $\varphi = \psi$, etc., and hence $C = \pm 1$, we now have the problem of finding the $\varphi(s)$ of signature (λ, k, C), i.e. the $f(\tau) \in \mathcal{M}(\lambda, k, C)$.

We consider the domain $B(\lambda)$: Re $(\tau) \le \lambda/2$, $|\tau| \ge 1$, which will turn out to be a fundamental domain for $G(\lambda)$ in certain cases, and has different topological character as $\lambda > 2$, $\lambda = 2$, or $\lambda < 2$.

Proposition 1.3. *Every τ in the upper half plane is a translate under $G(\lambda)$ of a point in $B(\lambda)$.*

Proof. Let $G^*(\lambda)$ be the group generated by the three reflections T_1, T_2, T_3:

(1) T_1 = reflection in unit circle, i.e. $T_1(\tau) = \tau/|\tau|^2$
(2) T_2 = reflection in y-axis, i.e. $T_2(\tau) = -\overline{\tau}$
(3) T_3 = reflection in $x = -\lambda/2$, i.e. $T_3(\tau) = -(\overline{\tau} + \lambda)$.

Then $T_j^2 = 1$, $T_1T_2(\tau) = -1/\tau$, $T_1T_3(\tau) = -1/\tau + \lambda$, $T_2T_3(\tau) = \tau + \lambda$, so $G^*(\lambda) \supset G(\lambda)$, and in fact $G(\lambda)$ consists of all words of even length in T_1, T_2, T_3. Let $B^*(\lambda) : |\tau| \geq 1, -\lambda/2 \leq \mathrm{Re}\,(\tau) \leq 0$ be the left half of $B(\lambda)$; the proposition is equivalent with showing that the $G^*(\lambda)$-translates of $B^*(\lambda)$ cover the upper half plane.

Given $\tau = x + iy$, we can assume $-\lambda/2 \leq x \leq 0$; if $|\tau| \geq 1$ we are done, so assume $|\tau| < 1$. Then $\tau' = T_1(\tau) = \tau/|\tau|^2$ is higher, $y' = y/|\tau|^2$, and so we have only to verify that we arrive in $B^*(\lambda)$ after finitely many steps. If $\lambda < 2$ or $\lambda > 2$, we can cover the arc at the bottom of $B^*(\lambda)$, i.e. the unit circle, and the upper half plane, by reflecting in the sides of $B^*(\lambda)$, and hence assume $|\tau| \leq c < 1$, and the result is clear. If $\lambda = 2$, then an element of $G(2)$ is a substitution $\tau' = \frac{a\tau+b}{c\tau+d}$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z})$, $y' = y/|c\tau + d|^2$; if τ' is higher than τ, then $|c\tau + d|^2 < 1$, and there are only finitely many possibilities for c, d, given τ, since $c, d \in \mathbf{Z}$. If τ' is $G(2)$-equivalent to τ and maximally high, and $|\mathrm{Re}\,(\tau')| \leq \frac{\lambda}{2}$, then $\tau' \in B(\lambda)$. □

We now dispose of the least interesting case $\lambda > 2$, where $\mathcal{M}_0(\lambda, k, C)$ has infinite dimension for every value of k and C. Roughly speaking, the great number of solutions is because we can solve our problem in the upper half plane with arbitrary singularities in the lower half plane, since $B(\lambda)$ extends into the lower half plane.

Given $\lambda > 2$, let $z = g(\tau)$ map the interior of $B^*(\lambda)$ one-one conformally on the upper half plane, so that g defines a homeomorphism of $B^*(\lambda)$ onto the closed upper half plane, normalized by $\infty, i, -i \mapsto 1, 0, \infty$. For the existence of $g(\tau)$, one can appeal to a strong form of the Riemann mapping theorem (cf. [11, 14.8 Theorem]), or a generalized Schwarz-Christoffel transformation. By the reflection principle, and Proposition 1.3, we extend g to a function defined on the upper half plane and invariant under $G(\lambda)$. The only corner of $B^*(\lambda)$ in the upper half plane is at $\tau = i$, where there is an angle of $\frac{\pi}{2}$, so the extended g is analytic on the upper half plane, single-valued by the monodromy theorem. g is bounded on the upper half plane since g is $G(\lambda)$-invariant and $g(-i) = \infty$. It is clear that $g(\tau)$ is one-one near points τ not equivalent to i or ∞. At ∞ we have the Fourier expansion

$$g(\tau) = 1 + \sum_{n=1}^{\infty} a_n e^{2\pi i n\tau/\lambda}$$

with $a_1 \neq 0$ since g is one-one near ∞ as a function of $e^{2\pi i\tau/\lambda}$; $g(\tau)$ has a double zero at $\tau = i$ and a double pole at $\tau = -i$. To show $\dim \mathcal{M}_0(\lambda, k, C) = \infty$ it suffices to show $\mathcal{M}_0(\lambda, k, C) \neq 0$, since if $f \neq 0$ is one such function, so is fg^n for $n = 0, 1, 2, \ldots$, and they are linearly independent since g^n has a pole of order $2n$ at $\tau = -i$.

Thus we only have to construct one non-zero function $f \in \mathcal{M}_0(\lambda, k, C)$. We have already noted g is locally one-one except at points equivalent to i or ∞, so $g'(\tau) \neq 0$ except at thoses points. Since $g(\tau)$ has a double zero at i, we can define a function $\sqrt{g(\tau)}$ in the upper half plane, since it is simply connected; since $g(\tau) = 1 + a_1 e^{2\pi i\tau/\lambda} + \ldots$, $a_1 \neq 0$, we have $\sqrt{g(\tau)} = 1 + \sum_{n=1}^{\infty} b_n e^{2\pi i n\tau/\lambda}$ near ∞, so $\sqrt{g(\tau + \lambda)} = \sqrt{g(\tau)}$. Since $g(-1/\tau) = g(\tau)$, we get $\sqrt{g(-1/\tau)} = \pm\sqrt{g(\tau)}$; the minus sign is correct, for $\sqrt{g(\tau)} = \frac{\tau - i}{\tau + i} \cdot g_1(\tau)$, where $g_1(i) \neq 0$, so $\pm 1 = \frac{\sqrt{g(-1/\tau)}}{\sqrt{g(\tau)}} = -\frac{g_1(1/\tau)}{g_1(\tau)} = -1$, substituting $\tau = i$.

Now let $h(\tau) = \frac{g'(\tau)}{\sqrt{g(\tau)(g(\tau)-1)}}$, analytic and never 0 in the upper half plane and at ∞ ($g'(\tau)$ has simple zeros at i and at ∞, canceling zeros of the denominator; the

zero at ∞ is measured in $z = e^{2\pi i\tau/\lambda}$.) Then $h(\tau+\lambda) = h(\tau)$, and $g(-1/\tau) = g(\tau)$ gives $g'(\tau) = g'(-1/\tau)\cdot\frac{1}{\tau^2}$, so $h(-1/\tau) = -\tau^2 h(\tau) = (\frac{\tau}{i})^2 h(\tau)$.

Thus $h \in \mathcal{M}(\lambda, 2, 1)$. Now let $k > 0$. Since h is never 0, we can define $h(\tau)^{k/2} = e^{\frac{k}{2}\log h(\tau)}$, analytic in the upper half plane and at ∞; we have $h(\tau+\lambda)^{k/2} = \varepsilon_1 h(\tau)^{k/2}$, $h(-1/\tau)^{k/2} = \varepsilon_2(\frac{\tau}{i})^k h(\tau)^{k/2}$ for some constants $\varepsilon_1, \varepsilon_2$; evaluating at $\tau = \infty$, we see $\varepsilon_1 = 1$, and at $\tau = i$, we see $\varepsilon_2 = 1$. Thus $h^{k/2} \in \mathcal{M}(\lambda, k, 1)$. Finally, to obtain the O-condition, consider $f(\tau) = h(\tau)^{k/2}\cdot(g(\tau)-1)^n$, where n is an integer $> k/2$; then $f \in \mathcal{M}(\lambda, k, 1)$, and to show that f satisfies the O-condition, it suffices to show that $\left|\frac{g'(x+iy)}{\sqrt{g(x+iy)}}\right| = O(y^{-1})$, which is true since $\left|\frac{yg'(x+iy)}{\sqrt{g(x+iy)}}\right|$ is invariant under $G(\lambda)$ and bounded in the intersection of $B(\lambda)$ and the upper half plane (vanishes at ∞), and so bounded in the upper half plane. Thus $f \in \mathcal{M}_0(\lambda, k, 1)$, and $f\sqrt{g} \in \mathcal{M}_0(\lambda, k, -1)$, which proves:

Theorem 1.4. *If $\lambda > 2$, then $\mathcal{M}_0(\lambda, k, C)$ has infinite dimension for every $k > 0$, $C = \pm 1$.*

We consider next the case $\lambda < 2$. This time we work in the upper half plane only, so let us change the notation so $B(\lambda)$, $B^*(\lambda)$ are the intersections of the previous domains with the upper half plane. Let τ_0 be the lower left corner of $B(\lambda)$, so $|\tau_0| = 1$, $\mathrm{Re}\,(\tau_0) = -\lambda/2$, and τ_0 is a fixed point of $\tau \mapsto -1/\tau + \lambda$, which is in $G(\lambda)$. Let $\pi\alpha$ be the angle of $B(\lambda)$ at τ_0, i.e. $\cos\pi\alpha = \frac{\lambda}{2}$, $0 < \alpha < \frac{1}{2}$. i is a fixed point of $\tau \mapsto -1/\tau$; the two halves of the bottom of $B(\lambda)$ are equivalent under $\tau \mapsto -1/\tau$, and the two vertical sides under $\tau \mapsto \tau + \lambda$.

Let $f \in \mathcal{M}(\lambda, k, C)$, $f \neq 0$. Let N be the number of zeros of f in $B(\lambda)$, counting multiplicities, except at τ_0, i, ∞, with appropriate identifications, e.g. a zero on a side of $B(\lambda)$ should be counted on only one of the two sides. Let n_0, n_i, n_∞ be the order of zero of f at τ_0, i, ∞, the zero at ∞ measured in $z = e^{2\pi i\tau/\lambda}$.

Lemma 1.5.

(a) $N + n_\infty + \frac{n_i}{2} + n_0\alpha = \frac{k}{2}(\frac{1}{2} - \alpha)$
(b) $\dim \mathcal{M}(\lambda, k, C) \leq 1 + [\frac{k}{2}(\frac{1}{2} - \alpha)]$.

Proof. Let C be a contour enclosing the zeros of f in the interior of $B(\lambda)$; the bottom of C follows the unit circle from τ_0 to $\tau_0 + \lambda$, the right side follows $x = \frac{\lambda}{2}$ to $\frac{\lambda}{2} + iT$, the top follows $y = T$ to $-\lambda/2 + iT$, and the left side follows $x = -\frac{\lambda}{2}$ back down to τ_0, except that we must detour around small circular arcs to avoid any zeros on the boundary of $B(\lambda)$. Then

$$N = \frac{1}{2\pi i}\int_C d\log f(\tau)$$

and the integrals over the arcs about $i, \tau_0, \tau_0+\lambda$ approaches $-\frac{n_i}{2}$, $-\frac{n_0\alpha}{2}$, $-\frac{n_0\alpha}{2}$, while the integrals over the top approaches $-n_\infty$, and the two integrals on the vertical sides cancel. Thus we want the integral on the bottom to be $\frac{k}{2}(\frac{1}{2} - \alpha)$. Now

$f(-1/\tau) = C(\frac{\tau}{i})^k f(\tau)$, so $d\log f(-1/\tau) = k\frac{d\tau}{\tau} + d\log f(\tau)$, so this last integral is

$$\begin{aligned}\frac{1}{2\pi i}\int_i^{\tau_0+\lambda} & d\log f(\tau) - d\log f(-1/\tau) \\ &= \frac{1}{2\pi i}\int_i^{\tau_0+\lambda} \frac{-k d\tau}{\tau} \\ &= \frac{-k}{2\pi}\arg\tau|_i^{\tau_0+\lambda} \\ &= \frac{k}{2\pi}(\frac{\pi}{2} - \pi\alpha),\end{aligned}$$

as desired. Finally, if $m > 1 + [\frac{k}{2}(\frac{1}{2} - \alpha)] > n_\infty$, and $f_1, \ldots, f_m \in \mathcal{M}(\lambda, k, C)$, then a suitable non-trivial linear combination of $f_1, \ldots, f_m$ has a zero of order $\geq m - 1 > n_\infty$ at ∞, and so vanishes, by (a); this proves (b). □

Remark. The zeta function of $\mathbf{Q}(\sqrt{-3})$ is

$$\varphi(s) = \frac{1}{6}\sum_{n,m\in\mathbf{Z}}{}' (n^2 + nm + m^2)^{-s}$$

and is known to have signature $(\sqrt{3}, 1, 1)$. Here $\alpha = \frac{1}{6}$, and $\dim \mathcal{M}(\sqrt{3}, 1, 1) \leq 1$ by the above. Hence $\varphi(s)$ is determined by its functional equation.

At this point we digress briefly for some general considerations. A substitution $L(\tau) = \frac{a\tau+b}{c\tau+d}$, where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{R})$ is *elliptic* if it has two non-real fixed points $\tau_1, \overline{\tau}_1$, where $\operatorname{Im}\tau_1 > 0$. Since $c\tau_1^2 + (d-a)\tau_1 - b = 0$, L is elliptic $\iff$ $(d-a)^2 < -4bc \iff (d+a)^2 < 4 \iff$ the eigenvalues of L, i.e. the roots of $x^2 - (a+d)x + 1 = 0$, are non-real. We now prove a very useful result:

Proposition 1.6. *Let L be elliptic, with fixed point τ_1 in the upper half plane. Suppose there is a non-zero holomorphic function $f(\tau)$ on $\operatorname{Im}\tau > 0$ such that*

(a) $f(\tau + \lambda) = f(\tau)$
(b) $f(-1/\tau) = \varepsilon(\frac{c\tau+d}{i})^k f(\tau)$

for some constants $\lambda > 0$, $k > 0$, and ε. Then L is periodic, i.e. its eigenvalues are roots of 1.

Proof. In the variable $t = \frac{\tau-\tau_1}{\tau-\overline{\tau}_1}$, L is a (complex) linear fractional transformation fixing 0 and ∞ , i.e. $L(t) = \rho \cdot t$, and we want ρ to be a root of 1.

Let $g(\tau) = (\tau - \overline{\tau}_1)^k$, for $\operatorname{Im}(\tau) > 0$. Then

$$\begin{aligned} g(L(\tau)) &= \left(\frac{a\tau+b}{c\tau+d} - \frac{a\overline{\tau}_1+b}{c\overline{\tau}_1+d}\right)^k \\ &= \left(\frac{c\tau+d}{i}\right)^{-k} g(\tau)\eta\end{aligned}$$

for some constant η; evaluating at $\tau_1 = L(\tau_1)$, we see $\eta = \left(\frac{c\tau_1+d}{i}\right)^k$. Now let $h(\tau) = f(\tau)g(\tau)$. Then $h(L(\tau)) = \varepsilon\eta h(\tau)$, and writing $h(\tau) = \sum_{n=0}^\infty c_n t^n$, we have $\sum_{n=0}^\infty c_n\rho^n t^n = \varepsilon\eta\sum c_n t^n$. Now $c_n \neq 0$ for two distinct values of n, since $f(\tau+\lambda) = f(\tau)$, and $\rho^n = \varepsilon\eta$ when $c_n \neq 0$; hence ρ is a root of 1. Furthermore, if n_1 is the order of zero of f at τ_1, we have the formula $\rho^{n_1} = \varepsilon\eta = \varepsilon\left(\frac{c\tau_1+d}{i}\right)^k$. □

As an incidental result, if $0 \neq f \in \mathcal{M}(\lambda, k, C)$, then applying this last formula to $L(\tau) = -1/\tau$, $\tau_1 = i$, we have clearly $\rho = -1$, so $(-1)^{n_i} = \varepsilon = C$.

Proposition 1.7. *For arbitrary λ, if $0 \neq f \in \mathcal{M}(\lambda, k, C)$, and n_i is the order of zero of f at i, then $C = (-1)^{n_i}$.*

Returning to our development of the case $\lambda < 2$:

Lemma 1.8. *If $\mathcal{M}(\lambda, k, C) \neq 0$, then α and k are rational.*

Proof. τ_0 is a fixed point of $L(\tau) = \frac{-1}{\tau+\lambda}$, whose eigenvalues are the roots of $x^2 - \lambda x + 1$, i.e. $\rho, \overline{\rho}$, where $\rho = \tau_0 + \lambda = e^{\pi i \alpha}$. Then α is rational, by Proposition 1.6, as is then k, by Lemma 1.5. □

Example. $\lambda = 1$ (modular group), i.e. $\alpha = \frac{1}{3}$. If $0 \neq f \in \mathcal{M}(1, k, C)$, then $\frac{n_i}{2} + \frac{n_0}{3} \equiv \frac{k}{2}(\frac{1}{6}) \pmod 1$, and then $\frac{n_i}{2} \equiv \frac{1}{4} \pmod 1$. Hence k is an even integer, and $C = (-1)^{n_i} = (-1)^{k/2}$. Also $\frac{k}{12} \geq \frac{1}{3}$, so $k \geq 4$, and $\dim \mathcal{M}(1, k, (-1)^{k/2}) \leq 1 + \left[\frac{k}{12}\right]$.

Lemma 1.9. *If $\mathcal{M}(\lambda, k, C) \neq 0$, then $\alpha = \frac{1}{q}$, where q is an integer ≥ 3 (and hence $\lambda \geq 2\cos\frac{\pi}{3} = 1$.)*

Proof. Assume $\alpha = p/q$, where p, q are relatively prime and $p \geq 2$; we will then find an element of $G(\lambda)$ which is elliptic but not periodic, contrary to Proposition 1.6. In fact, one computes that $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & \lambda \end{pmatrix}^n = L$ has trace $s = 2\frac{\sin(n+1)p\pi/q}{\sin p\pi/q}$; choosing n so $(n+1)p \equiv 1 \pmod q$, we have $|s| < 2$, so L is elliptic. But s has conjugates s' with $|s'| > 2$, so the eigenvalues of L are imaginary but not roots of 1, which is the desired contradiction. □

Remark. We shall see there are forms when $\alpha = \frac{1}{q}$; $G(\lambda)$ is discrete exactly in that case. Note that $\lambda = 2\cos\frac{\pi}{q} = \zeta + \zeta^{-1}$, $\zeta = e^{\pi i/q}$ is conjugate to $\lambda' = 2\cos\frac{\pi p}{q} = \zeta^p + \zeta^{-p}$ for $(p, q) = 1$, so $G(\lambda)$ and $G(\lambda')$ are isomorphic as abstract groups, but only $G(\lambda)$ is of interest for modular forms.

So far we have proved that if $0 \neq f \in \mathcal{M}(\lambda, k, C)$, $\lambda < 2$, then

(1) $\lambda = 2\cos\frac{\pi}{q}, \quad q \in \mathbf{Z}, \quad q \geq 3,$
(2) $N + n_\infty + \frac{n_i}{2} + \frac{n_0}{q} = \frac{k(q-2)}{4q}$
(3) $C = (-1)^{n_i}$

Lemma 1.10. *Given $\lambda = 2\cos\frac{\pi}{q}$. Then there exist $f_0.f_i, f_\infty \in \mathcal{M}(\lambda, k, C)$, for suitable k and C in each case, with simple zeros at τ_0, i, ∞, respectively, and no other zeros. Thus:*

(a) *for f_0, $C = +1$ and $k = \frac{4}{q-2}$, the smallest possible value for k;*
(b) *for f_i, $C = -1$, $k = \frac{2q}{q-2}$;*
(c) *for f_∞, $C = +1$, $k = \frac{4q}{q-2}$.*

Proof. As in the case $\lambda > 2$, by the mapping theorem there exists a homeomorphism g of $B^*(\lambda)$: $-\frac{\lambda}{2} \leq \mathrm{Re}\,(\tau) \leq 0, |\tau| \geq 1, \mathrm{Im}\,\tau > 0$ onto the closed upper half plane, mapping the interior of $B^*(\lambda)$ conformally onto the open upper half plane, normalized by $\tau_0, i, \infty \mapsto 0, 1, \infty$. We continue $g(\tau)$ to the upper half plane by repeated reflections in the sides of $B^*(\lambda)$, obtaining an analytic function $g(\tau)$ on the upper half plane by Proposition 1.3, the simple connectivity of the upper half

plane, and the fact that the angles at the corners of $B^*(\lambda)$ are $\frac{\pi}{q}$ at τ_0 and $\frac{\pi}{2}$ at i, an integral fraction of π, which makes the extended g analytic at the corners. Thus $g(\tau)$ is analytic for $\operatorname{Im}\tau > 0$, invariant under $G(\lambda)$, and one-one on the interior of $B(\lambda)$. The opposite sides of $B(\lambda)$ are equivalent under $\tau \mapsto \tau + \lambda$ and $\tau \mapsto -1/\tau$. Thus we have made $\widehat{G(\lambda)\backslash\mathcal{H}} = G(\lambda)\backslash(\mathcal{H} \cup \{\infty\})$, where $\mathcal{H} : \operatorname{Im}\tau > 0$, into a Riemann surface of genus zero, in fact so $g : \widehat{G(\lambda)\backslash\mathcal{H}} \xrightarrow{\sim} \widehat{\mathbf{C}} =$ Riemann sphere. $B(\lambda)$ is a *fundamental domain* for $G(\lambda)$. (If $\lambda = 1$, $g = J$ is called the *elliptic modular invariant*.)

Since g is one-one on $G(\lambda)\backslash\mathcal{H}$, we see g has a zero of order q at τ_0, takes the value 1 doubly at i, and has a simple pole at ∞, i.e. $g(\tau) = \sum_{n=-1}^{\infty} a_n z^n$, $z = e^{2\pi i\tau/\lambda}$, $a_{-1} \neq 0$. Note $g'(\tau) = -a_{-1}z^{-2}\frac{dz}{d\tau} + \cdots = \frac{-a_{-1}}{z^2} \cdot \frac{2\pi i z}{\lambda} + \ldots$ also has a simple pole at ∞. We also have $g'(\tau+\lambda) = g'(\lambda)$, $g'(-1/\tau) = \tau^2 g'(\tau)$. By comparing zeros and poles at τ_0, i, ∞, we check the desired f_0, f_i, f_∞ are:

$$f_0 = \left(\frac{(g')^2}{g(g-1)}\right)^{1/(q-2)}$$

$$f_\infty = \left(\frac{(g')^{2q}}{g^{2q-2}(g-1)^q}\right)^{1/(q-2)}$$

$$f_i = \left(\frac{(g')^q}{g^{q-1}(g-1)}\right)^{1/(q-2)}$$

□

It is now easy to compute the dimension of $\mathcal{M}(\lambda, k, C)$. Let $f \in \mathcal{M}(\lambda, k, +1)$, $f \neq 0$. Then, in the above notation, n_i is even and $m = \frac{k(q-2)}{4}$ is an integer, i.e. $k = mk_0$, $k_0 = \frac{4}{q-2}$ (the minimal value of k, corresponding to f_0.) Then for a unique constant α_0, $f - \alpha_0 f_0^m$ vanishes at ∞. Since $f_0^m \in \mathcal{M}(\lambda, k, +1)$ also, we have $f - \alpha_0 f_0^m = f_\infty \cdot f_1$, where $f_1 \in \mathcal{M}(\lambda, k - qk_0, +1)$ (if $m > q$; f_1 is constant if $m \leq q$). Continuing, we see that

$$f = \sum_{\nu=0}^{[m/q]} \alpha_\nu f_0^{m-q\nu} f_\infty^\nu$$

is a polynomial in f_0, f_∞, in a unique way. Thus $\dim \mathcal{M}(\lambda, mk_0, +1) = 1 + [m/q]$.

Similarly, if $0 \neq f \in \mathcal{M}(\lambda, k, -1)$, then n_i is odd and $f/f_i \in \mathcal{M}(\lambda, k - \frac{2q}{q-2}, +1)$. Thus $k - \frac{2q}{q-2} = (m-1)k_0$, where m is an integer ≥ 1, $k = mk_0 + \frac{2q-4}{q-2} = mk_0 + 2$; $\dim \mathcal{M}(\lambda, k, -1) = \dim \mathcal{M}(\lambda, (m-1)k_0, +1) = 1 + [(m-1)/q]$. Finally, $f_i^2 \in \mathcal{M}(\lambda, \frac{4q}{q-2}, +1)$, so $f_i^2 = \alpha f_0^q + \beta f_\infty$, with $\alpha, \beta \neq 0$ (look at the zeros). Thus f_∞, hence any $f \in \mathcal{M}(\lambda, k, \pm 1)$, is a polynomial in f_0, f_i. Summing up:

Theorem 1.11. *Given $0 < \lambda < 2$. Then $\mathcal{M}(\lambda, k, C) = 0$ except in the case $\lambda = 2\cos\frac{\pi}{q}$, where q is an integer ≥ 3, and $k = \frac{4m}{q-2} + 1 - C$; in this case*

$$\dim \mathcal{M}(\lambda, k, C) = 1 + \left[\frac{m + \frac{C-1}{2}}{q}\right]$$

Of course, from the point of view of Theorem 1.2, Theorem 1.11 gives the answer to the wrong question. Let us call $f \in \mathcal{M}(\lambda, k, C)$ a *cusp form* (of dimension $-k$ and multiplier C for $G(\lambda)$) if it vanishes at ∞, and let $\mathcal{S}(\lambda, k, C)$ be the space of all such cusp forms. Thus $\mathcal{S}(\lambda, k, C) \subset \mathcal{M}(\lambda, k, C)$, and $\dim \mathcal{M}(\lambda, k, C) - \dim \mathcal{S}(\lambda, k, C) \leq 1$.

Theorem 1.12. *Given* $\lambda = 2\cos\frac{\pi}{q}$, $k = \frac{4m}{q-2} + 1 - C$ *as in Theorem 1.11. Then:*

(a) $\mathcal{S}(\lambda, k, C) \subset \mathcal{M}_0(\lambda, k, C)$*; in fact* $f(x+iy) = O(y^{-k/2})$ *if* $f \in \mathcal{S}(\lambda, k, C)$
(b) $\dim \mathcal{S}(\lambda, k, C) = \left[\frac{m + \frac{C-1}{2}}{q}\right]$*, the dimension of the space of Dirichlet series of signature* (λ, k, C) *which are regular at* $s = k$*.*
(c) $\dim \mathcal{M}_0(\lambda, k, C) = \delta(\lambda) + \dim \mathcal{S}(\lambda, k, C)$*, where* $\delta(\lambda) = 0$ *or* 1 *is independent of* k *and* C*.*

Proof. (b) follows from the proof of Theorem 1.11, since we did construct modular forms not vanishing at ∞, so $\dim \mathcal{M}(\lambda, k, C) = 1 + \dim \mathcal{S}(\lambda, k, C)$. For (a), $F(x+iy) = y^{k/2}|f(x+iy)|$ is bounded on $B(\lambda)$ (vanishes at ∞) and $G(\lambda)$-invariant and so bounded. (c) is equivalent with the following statement: if there exists one function $f \in \mathcal{M}_0(\lambda, k, C)$ with $f(\infty) \neq 0$, then every $h \in \mathcal{M}(\lambda, k', C')$ also satisfies the O-condition. In fact, since k, k' are rational, we can choose positive integers n, m and a constant α so that $\alpha f^n + h^m \in \mathcal{S}(\lambda, k'', +1)$ and hence satisfies the O-condition; then h must also satisfy the O-condition. □

The question of whether $\delta(\lambda) = 0$ or 1 appears to be open in general. For $\lambda = 1$, the functions not vanishing at ∞ are provided explicitly by the *Eisenstein series*, as follows.

Lemma 1.13. *If* $k > 2$*, then* $\sum'_{n,m\in\mathbf{Z}} |n\tau + m|^{-k}$ *converges in* $\operatorname{Im}\tau > 0$*, uniformly on compact subsets. (The prime on the summation symbol means the term for* $(m, n) = (0, 0)$ *is omitted.)*

Proof. For τ in a compact set, there exists $B > 0$ with $|x\tau + y| \geq B(|x| + |y|)$ for all real x, y. Since there are only $4r$ pairs (n, m) with $|n| + |m| = r$, our series is dominated term-by-term by

$$\sum_{r=1}^{\infty} \frac{4r}{r^k} = 4\zeta(k-1),$$

which is finite for $k > 2$. □

Hence for $k = 4, 6, 8, \ldots$, the *Eisenstein series*

$$G_k(\tau) = \sum'_{n,m\in\mathbf{Z}} (n\tau + m)^{-k}$$

is holomorphic on $\operatorname{Im}\tau > 0$, and satisfies

$$G_k\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k G_k(\tau) \quad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z}).$$

(The g_2 and g_3 of Weierstrass theory are $g_2 = 60G_4$, $g_3 = 140G_6$.) The Fourier expansion is:

Proposition 1.14.

$$G_k(\tau) = 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) z^n,$$

where $z = e^{2\pi i\tau}$, $\sigma_\nu(n) = \sum_{\substack{d|n \\ d>0}} d^\nu$.

Proof. Clearly $G_k(\tau) = 2\zeta(k) + \sum_{n=1}^{\infty} \sum_{m\in\mathbf{Z}} (m+n\tau)^{-k}$. Now

$$\frac{\pi^2}{\sin^2 \pi\tau} = \sum_{m\in\mathbf{Z}} (m+\tau)^{-2},$$

for the difference is entire, of period 1, even, and $\to 0$ as $\operatorname{Im}\tau \to \infty$. Thus

$$\sum_{m\in\mathbf{Z}} (m+\tau)^{-2} = \frac{(2\pi i)^2 e^{2\pi i\tau}}{(1-e^{2\pi i\tau})^2} = \frac{(2\pi i)^2 z}{(1-z)^2} = (2\pi i)^2 \sum_{n=1}^{\infty} n z^n.$$

Differentiating with respect to τ ($\frac{dz}{d\tau} = 2\pi i z$):

$$\sum_{m\in\mathbf{Z}} (m+\tau)^{-k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} z^n.$$

Thus

$$\sum_{n=1}^{\infty} \sum_{m\in\mathbf{Z}} (m+n\tau)^{-k} = \frac{(2\pi i)^k}{(k-1)!} \sum_{n,\nu=1}^{\infty} \nu^{k-1} z^{n\nu}$$

□

Thus G_k has signature $(1, k, (-1)^{k/2})$ for $k = 4, 6, \ldots$, and satisfies the O-condition, so $\delta(1) = 1$ in the notation of Theorem 1.12. The corresponding Dirichlet series is

$$\varphi_k(s) = \zeta(s)\zeta(s+1-k) = \sum_{n=1}^{\infty} \sigma_{k-1}(n) n^{-s},$$

which satisfies the functional equation

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

where $\Phi_k(s) = (2\pi)^{-s}\Gamma(s)\varphi_k(s)$, which of course can also be derived from the functional equation for $\zeta(s)$, which we have not yet proved. Note

$$(-1)^{k/2} a_0 = \operatorname{Res}_{s=k} \Phi_k(s) = (2\pi)^{-k}\Gamma(k),$$

in agreement with the above, assuming known that $\operatorname{Res}_{s=1} \zeta(s) = 1$.

Actually, since $\dim \mathcal{M}(1, k, (-1)^{k/2}) = 1$ for $k = 4, 6$, we see that G_4, G_6 are the f_0, f_i of lemma 1.10 (up to a constant multiple) and in particular $\tau_0 = e^{2\pi i/3}$ is the only zero of G_4 in $B(1)$. It follows that the *modular group* $\Gamma = SL(2, \mathbf{Z})/\pm I$, the group of all linear fractional transformations from $SL(2, \mathbf{Z})$, is generated by $\tau \mapsto \tau + 1$, $\tau \mapsto -1/\tau$, since G_4 is a modular form for Γ but has only one zero in the fundamental domain for the subgroup.

The *normalized Eisenstein series* are the series

$$E_k(\tau) = \frac{G_k(\tau)}{2\zeta(k)} = 1 + (-1)^{k/2} A_k \sum_{n=1}^{\infty} \sigma_{k-1}(n) z^n$$

for $k = 4, 6, \ldots$, where $A_k = \frac{(2\pi)^k}{\Gamma(k)\zeta(k)}$ is a positive real number. Actually A_k is rational ($A_k = 2k/B_{2k}$, $B_{2k} = k^{th}$ Bernoulli number), as follows. Starting from

$\sin s = s\prod_{n=1}^{\infty}(1-\frac{s^2}{n^2\pi^2})$, we get

$$\begin{aligned} s\cot s &= s\frac{d}{ds}\log\sin s \\ &= 1 - 2s^2\sum_{n=1}^{\infty}\frac{1}{n^2\pi^2(1-s^2/n^2\pi^2)} \\ &= 1 - 2\sum_{n=1}^{\infty}\sum_{\nu=1}^{\infty}\left(\frac{s^2}{n^2\pi^2}\right)^{\nu} \\ &= 1 - 2\sum_{\nu=1}^{\infty}\frac{\zeta(2\nu)}{\pi^{2\nu}}s^{2\nu} \end{aligned}$$

which shows A_k is rational since $s\cot s$ is a power series in s with rational coefficients. One finds $A_4 = 240$, $A_6 = 504$.

Recalling that the first cusp form occurs when $k = 12$ (since the formula of Theorem 1.12 gives $\dim \mathcal{S}(1,k,(-1)^{k/2}) = [\frac{k}{12}]$ if $k \not\equiv 2 \pmod{12}$, $[\frac{k}{12}]-1$ if $k \equiv 2 \pmod{12}$) let us define $\Delta(\tau) = \frac{E_4(\tau)^3 - E_6(\tau)^2}{1728}$. Then $\Delta \in \mathcal{S}(1,12,1)$. Writing

$$\begin{aligned} \Delta(\tau) = \sum_{n=1}^{\infty} a_n z^n = \frac{1}{1728}\big((1+240\sum_{n=1}^{\infty}\sigma_3(n)z^n)^3 \\ -(1-504\sum_{n=1}^{\infty}\sigma_5(n)z^n)^2\big) \end{aligned}$$

one finds $a_1 = (3\cdot 240 + 2\cdot 504)/1728 = 1$, and all $a_n \in \mathbf{Q}$. Actually, the a_n are integers; to see this, we need, in an obvious notation,

$$(1+240U)^3 \equiv (1-504V)^2 \pmod{12^3}, \quad \text{i.e.}$$

$$3\cdot 240U \equiv -2\cdot 504V \pmod{12^3},$$

for which it suffices that $U \equiv V \pmod{12}$, i.e. $\sigma_3(n) \equiv \sigma_5(n) \pmod{12}$, which is true since $d^3 \equiv d^5 \pmod{12}$.

Thus $\Delta \in \mathcal{S}(1,12,1)$, $\Delta(\tau) = \sum_{n=1}^{\infty} a_n z^n$, where $a_n \in \mathbf{Z}$, $a_1 = 1$. By the formula for the number of zeros, we see $\Delta(\tau) \neq 0$ for $\operatorname{Im}\tau > 0$ ($\frac{k}{12} = n_\infty = 1$); in the Weierstrass theory of elliptic functions $\Delta(\tau) = (2\pi)^{-12}(g_2^3 - 27g_3^2)$ is the discriminant. Now we take the quotient of two forms of dimension -12 to get the *elliptic modular invariant*

$$j(\tau) = \frac{E_4(\tau)^3}{\Delta(\tau)} = \frac{1}{z} + \sum_{n=0}^{\infty} b_n z^n,$$

where $b_n \in \mathbf{Z}$, a crucial fact in arithmetic applications; $j(\tau) = j(\tau')$ if and only if τ' is equivalent to τ under the modular group.

Remark. Δ has the product expansion

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

cf. Siegel [14] for a short proof. Another proof follows Theorem 1.18 in these notes.

Thus we have shown $\mathcal{M}(\lambda,k,C) = \mathcal{M}_0(\lambda,k,C)$ in the case $\lambda = 1$ by explicit construction (the *Eisenstein series*) of forms not vanishing at ∞ which do satisfy the O-condition. We can use this result for $\lambda = 1$ to prove the same thing for $\lambda = \sqrt{2}, \sqrt{3}$, as follows. Let $f \in \mathcal{M}(1,k,C)$. If $\ell = 1,2,3,\ldots$, then $g(\tau) =$

$f(\sqrt{\ell}\tau) + \ell^{-k/2} f(\tau/\sqrt{\ell}) \in \mathcal{M}(\sqrt{\ell}, k, C)$. Taking $\ell = 2, 3$, so $\sqrt{\ell} < 2$, we conclude that $\mathcal{M}(\lambda, k, C) = \mathcal{M}_0(\lambda, k, C)$ for $\lambda = \sqrt{2}, \sqrt{3}$.

Finally we consider the case $\lambda = 2$; note $G(2)$ is a subgroup of $G(1) = \Gamma$, and $B(2)$ contains three copies of $B(1)$. Since every point of $\mathcal{H}$ is $G(2)$-equivalent to a point of $B(2)$, by Proposition 1.3, and $B(1)$ is a fundamental domain for $G(1)$, we see that $(\Gamma : G(2)) \leq 3$. Defining $\Gamma(2)$, the *principal congruence subgroup* of Γ of level 2, by

$$0 \to \Gamma(2) \longrightarrow \Gamma \xrightarrow{f} SL(2, \mathbf{Z}/2\mathbf{Z}) \to 0$$

where f is reduction modulo 2, one checks f is onto and so $(\Gamma : \Gamma(2)) = 6$. Since clearly $(G(2)\Gamma(2) : \Gamma(2)) = 2$, we conclude $G(2) \supset \Gamma(2)$ and $G(2)$ has index 3 in Γ, and hence that $B(2)$ is a fundamental domain for $G(2)$.

Now $B(2)$ has two *cusps* (points where it meets the boundary of the upper half plane), ∞ and -1; $+1$ is equivalent to -1 under $\tau \mapsto \tau + 2$ and so is not counted. Note $B(2)$ has an angle of 0 at each cusp. We make $\widehat{G(2)\backslash\mathcal{H}} = \mathcal{H} \cup \{\infty, -1\}$ modulo $G(2)$ into a Riemann surface (of genus 0) by assigning local parameters t as follows:

(1) $t = \tau$ at points not equivalent to $i, \infty, -1$
(2) $t = \left(\frac{\tau - i}{\tau + i}\right)^2$ at i
(3) $t = e^{\pi i \tau}$ at ∞
(4) $t = e^{-2\pi i/(\tau+1)}$ at -1

The reason for these choices is as follows. Except at the three corners $i, \infty, -1$, a neighborhood of τ contains no equivalent point, whence (1). At those three points, one computes the stability groups in $G(2)$, which has order 2 (generated by $\tau \mapsto -1/\tau$) at i, an *elliptic fixed point*, and infinite cyclic (generated by the *least translation* $\tau \mapsto \tau + 2$) at ∞, a *parabolic fixed point*, or *cusp*, whence (2), (3). Now -1 is a fixed point of $\tau \mapsto -1/(\tau + 2)$ (in $G(2)$), and $\tau' = -1/(\tau + 1)$ throws -1 to ∞, changes $\tau \mapsto -1/(\tau + 2)$ into

$$\tau' \mapsto \frac{-1}{\frac{-1}{\tau+2} + 1} = \frac{-\tau - 2}{\tau + 1} = \tau' - 1$$

thus $t = e^{2\pi i \tau'} = e^{-2\pi i/(\tau+1)}$ is the appropriate local variable at -1. (Generally speaking, to treat questions of analyticity at any rational cusp, the procedure is to send it to ∞ by a linear fractional transformation and proceed as before.)

We now investigate the meaning of the O-condition:

Lemma 1.15. *If $f \in \mathcal{M}_0(2, k, C)$, then f is* quasi-regular *at $\tau = -1$, in the variable $t = e^{-2\pi i/(\tau+1)}$, in the sense that*

$$f(\tau)(\frac{\tau + 1}{i})^k = t^n h(t)$$

where $h(t)$ is holomorphic and $\neq 0$ at $t = 0$, and $n \geq 0$; $t^n = e^{-2\pi i n/(\tau+1)}$. ($n$ is fractional in general, and is called the order of zero *of $f(\tau)$ at $\tau = -1$.)*

Proof. Let $\tau' = -1/(\tau + 1)$, as above, so $\tau \mapsto -1/(\tau + 2)$ is $\tau' \mapsto \tau' - 1$. Now $f(\tau)\left(\frac{\tau+2}{i}\right)^k = Cf(-1/(\tau + 2))$, so

$$f(\tau)\left(\frac{\tau + 1}{i}\right)^k = f(\tau)\left(\frac{\tau'}{i}\right)^{-k} = \varepsilon\left(\frac{\tau' - 1}{i}\right)^{-k} f(\frac{-1}{\tau + 2})$$

for some constant ε of absolute value 1. Write $\varepsilon = e^{2\pi i \rho}$, where ρ is real, in general irrational. Then

$$f(\tau)\left(\frac{\tau'}{i}\right)^{-k} e^{-2\pi i \rho \tau'}$$

is invariant under $\tau \mapsto -1/(\tau+2)$ (i.e. $\tau' \mapsto \tau'-1$) and so has a Laurent expansion $\sum_{-\infty}^{\infty} a_n e^{2\pi i n\tau'}$:

$$f(\tau)\big(\frac{\tau+1}{i}\big)^k = \sum_{-\infty}^{\infty} a_n e^{2\pi i(n+\rho)\tau'}$$

We now show that $a_n = 0$ if $n+\rho < 0$. We have

$$a_n = \int_{\tau_0'}^{\tau_0'+1} f(\tau)\big(\frac{\tau+1}{i}\big)^k e^{-2\pi i(n+\rho)\tau'} d\tau'$$

Take $\tau' = u+ib$, $1 \le u \le 2$, b large. The term $\big(\frac{\tau+1}{i}\big)^k = \big(\frac{\tau'}{i}\big)^{-k}$ can be ignored; if

$$f(x+iy) = O(y^{-c}),$$

then

$$f(\tau) = f\big(-\frac{\tau'+1}{\tau'}\big) = O(b^c),$$

so $a_n = O(e^{2\pi b(n+\rho)} b^c)$ for large b, so $a_n = 0$ for $n+\rho < 0$. □

Let us denote $\mathcal{M}_1(2,k,C)$ the subspace of $\mathcal{M}(2,k,C)$ consisting of those f which are quasi-regular at $\tau = -1$; thus $\mathcal{M}_0(2,k,C) \subset \mathcal{M}_1(2,k,C)$.

Remark (1). If k is an integer, $f \in \mathcal{M}_1(2,k,C)$, then the order of zero n_{-1} of f at -1 satisfies

$$e^{2\pi i n_{-1}} = Ci^k.$$

Remark (2). Let $f \in \mathcal{M}(1,k,(-1)^{k/2}) \subset \mathcal{M}_0(2,k,(-1)^{k/2})$. Then n_{-1} is an integer, by Remark (1). In fact, $f(\tau)\big(\frac{\tau+1}{i}\big)^k = Cf(-1/(\tau+1))$, so $n_{-1} = n_\infty$, the order of zero at ∞ as previously defined. This is as it should be, since the cusps -1 and ∞ are equivalent under $\Gamma = G(1)$. Note that if $f \in \mathcal{M}_1(2,k,C)$ and $k = p/q$ is rational, then $h = f^{12q}/\Delta^p$ is a quotient of elements of $\mathcal{M}(2,12p,+1)$ and is then a meromorphic function on $\widehat{G(2)\backslash\mathcal{H}}$. (By remark (1), the numerator and denominator are regular, not just *quasi-regular*, at the cusps.) Thus h has as many zeros as poles on the Riemann surface. Now Δ has one zero on $B(1)$, hence 3 on $B(2)$, so f has $\frac{3p}{12q} = \frac{k}{4}$ zeros on $B(2)$, measured in local parameters on the Riemann surface. This is actually true generally:

Lemma 1.16. *The number of zeros of $f \in \mathcal{M}_1(2,k,C)$ in $B(2)$ is*

$$N + n_\infty + \frac{n_i}{2} + n_{-1} = \frac{k}{4}$$

($n_i/2$ would be called n_i in local variables; the others are adjusted. This lemma can be considered as a limiting case, as $\alpha \to 0$, of the similar formula for $\lambda < 2$, see lemma 1.5)

Proof. This is proved exactly as the analogous result for $\lambda < 2$; we only have to check that $\frac{1}{2\pi i}\int_\gamma d\log f(\tau)$ tends to $-n_{-1}/2$ as a little arc γ about $\tau = -1$ in $B(2)$ shrinks to zero. Now $\int_\gamma d\log(\frac{\tau+1}{i})^k \to 0$, so we want

$$\frac{1}{2\pi i}\int_\gamma d\log f(\tau)(\frac{\tau+1}{i})^k \to \frac{-n_{-1}}{2},$$

which follows from the substitution $\tau' = \frac{-1}{\tau+1}$, which carries $\mathrm{Re}\,(\tau) = -1$ on $\mathrm{Re}\,(\tau') = 0$ and $|\tau| = 1$ on $\mathrm{Re}\,(\tau') = -\frac{1}{2}$. □

We also have

$$C = (-1)^{n_i}$$
$$\dim \mathcal{M}_1(2, k, +1) \leq 1 + [\frac{k}{4}]$$
$$\dim \mathcal{M}_1(2, k, -1) \leq 1 + [\frac{k-2}{4}]$$

as before. Hence $\zeta(2s)$, if known to have signature $(2, \frac{1}{2}, 1)$, is determined by its functional equation, as is the zeta-function of $\mathbf{Q}(i)$,

$$\varphi(s) = \frac{1}{4} \sum_{n,m \in \mathbf{Z}}{}' (n^2 + m^2)^{-s},$$

which has signature $(2, 1, 1)$.

Lemma 1.17. *The theta-function* $\vartheta(\tau) = \frac{1}{2} \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau}$ *belongs to* $\mathcal{M}_0(2, \frac{1}{2}, 1)$, *and its only zero in* $B(2)$ *is one of order* $\frac{1}{8}$ *at* $\tau = -1$.

Proof. $\vartheta(\tau)$ is clearly holomorphic in $\operatorname{Im} \tau > 0$, satisfies $\vartheta(\tau + 2) = \vartheta(\tau)$, is holomorphic at ∞, and satisfies the O-condition. We want now to show $\vartheta(-1/\tau) = (\tau/i)^{1/2} \vartheta(\tau)$. For this we apply the *Poisson summation formula*: if $\sum_{n=-\infty}^{\infty} f(x+n)$ converges absolutely, uniformly on compact subsets, to a continuously differentiable function $F(x)$, where x is a real variable, then

$$F(x) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n x}$$

is represented by its Fourier series;

$$a_n = \int_0^1 F(t) e^{-2\pi i n t} dt = \int_{-\infty}^{\infty} f(t) e^{-2\pi i n t} dt.$$

Applying this to $f(x) = e^{\pi i \tau x^2}$, where τ is a parameter with $\operatorname{Im} \tau > 0$:

$$\begin{aligned} \vartheta(\tau, x) &= \sum_{n=-\infty}^{\infty} e^{\pi i \tau (n+x)^2} \\ &= \sum_{n=-\infty}^{\infty} e^{2\pi i n x} \int_{-\infty}^{\infty} e^{\pi i (\tau u^2 - 2nu + n^2/\tau - n^2/\tau)} du \\ &= \sum_{n=-\infty}^{\infty} e^{2\pi i n x - \pi i n^2/\tau} \int_{-\infty}^{\infty} e^{\pi i \tau (u - n/\tau)^2} du. \end{aligned}$$

We claim the integral is $(\tau/i)^{-1/2}$; it suffices to take $\tau = iy$, $y > 0$:

$$\begin{aligned} \int_{-\infty}^{\infty} e^{-\pi y (u + in/y)^2} du &= \int_{-\infty}^{\infty} e^{-\pi y n^2} du, \\ &\quad \text{by Cauchy's theorem,} \\ &= (\pi y)^{-1/2} \int_{-\infty}^{\infty} e^{-u^2} du = y^{-1/2}. \end{aligned}$$

Thus $\vartheta(\tau, x)(\tau/i)^{1/2} = \sum_{-\infty}^{\infty} e^{-\pi i n^2/\tau + 2\pi i n x}$. Taking $x = 0$, we get $\vartheta(\tau)(\tau/i)^{1/2} = \vartheta(-1/\tau)$. To find n_{-1} = order of zero of $\vartheta(\tau)((\tau + 1)/i)^{1/2}$, measured in $t =$

$e^{-2\pi i/(\tau+1)}$:

$$\begin{aligned}\vartheta(\tau)(\frac{\tau+1}{i})^{1/2} &= \left(\frac{\tau+1}{i}\right)^{1/2}\sum e^{\pi i n^2(\tau+1)+\pi i n}\\ &= \vartheta(\frac{-1}{\tau+1},\frac{1}{2})\\ &= \sum e^{-\pi i(n^2+n+1/4)/(\tau+1)}\\ &= e^{-\pi i/4(\tau+1)}h(t)\\ &= t^{1/8}h(t),\end{aligned}$$

where $h(0)\neq 0$. This proves the lemma 1.17 □

We can now prove $\dim \mathcal{M}_0(2,k,1)\geq 1+[\frac{k}{4}]$, whence $\mathcal{M}_0(2,k,1)=\mathcal{M}_1(2,k,1)$, of dimension $1+[\frac{k}{4}]$. Since $\vartheta(\tau)\neq 0$ for $\operatorname{Im}\tau>0$, and $\vartheta(\tau)$ is a power series in $z=e^{\pi i\tau}$ with non-zero constant term, we can define $\log\vartheta(\tau)$ in $\operatorname{Im}\tau>0$, still a power series in z. We then define, for $k>0$, $\vartheta^{2k}(\tau)=e^{2k\log\vartheta(\tau)}$, satisfying $\vartheta^{2k}(\tau+2)=\vartheta^{2k}(\tau)$, holomorphic at ∞, and satisfying the O-condition; also

$$\vartheta^{2k}(-1/\tau)=\left(\frac{\tau}{i}\right)^k\vartheta^{2k}(\tau)\cdot\varepsilon$$

for some constant ε; substituting $\tau=i$ we see $\varepsilon=1$. Thus $\vartheta^{2k}\in\mathcal{M}_0(2,k,1)$, with its only zero at $\tau=-1$.

The Eisenstein series $E_4(\tau)\in\mathcal{M}(1,4,1)\subset\mathcal{M}_0(2,4,1)$, with its only zero at $\tau_0=e^{2\pi i/3}$. Now if $f\in\mathcal{M}_1(2,k,1)$, then $f-\alpha_0\vartheta^{2k}$ vanishes at τ_0 for a unique constant α_0, so $f-\alpha_0\vartheta^{2k}=E_4\cdot f_1$, where $f_1\in\mathcal{M}(2,k-4,1)$. ($f_1$ is constant if $k=4$, 0 if $k<4$.) Continuing, any such f is uniquely of the form

$$\sum_{i\leq k/4}\alpha_i\vartheta^{2k-4i}E_4^i$$

which proves $\mathcal{M}_1(2,k,1)=\mathcal{M}_0(2,k,1)$, of dimension $1+[\frac{k}{4}]$.

For $C=-1$, choose $\alpha\neq 0$ so that $g=\vartheta^8-\alpha E_4$ vanishes at i. Clearly g does not have a zero at $\tau=-1$, so the formula $1=\frac{k}{4}=N+n_\infty+\frac{n_i}{2}$ shows that g has a double zero at $\tau=i$ and no other zeros. Then $h=\sqrt{g}\in\mathcal{M}(2,2,-1)$. If $f\in\mathcal{M}_1(2,k,-1)$, $f\neq 0$, then $-1=(-1)^{n_i}$, so $f(i)=0$, $f=h\cdot f_1$, where $f_1\in\mathcal{M}_1(2,k-2,-1)$. Thus $\dim\mathcal{M}_1(2,k,-1)=\dim\mathcal{M}_0(2,k,-1)=1+[\frac{k-2}{4}]$. Note E_4 is a polynomial in ϑ and h, so any $f\in\mathcal{M}_1(2,k,C)$ is of form $f=\sum\alpha_i\vartheta^{2k-2i}h^i$. We have proved:

Theorem 1.18. *$\mathcal{M}_0(2,k,C)=\mathcal{M}_1(2,k,C)$, and*

$$\dim\mathcal{M}_0(2,k,C)=1+\left[\frac{k+C-1}{4}\right]$$

Remark.

$$(2\vartheta(\tau))^r=\sum_{n_1,\dots,n_r\in\mathbf{Z}}e^{\pi i\tau(n_1^2+\cdots+n_r^2)}=1+\sum_{\nu=1}^{\infty}a_r(\nu)e^{\pi i\nu\tau},\qquad\text{where } a_r(\nu)$$

is the number of ways of writing ν as the sum of r squares; $(2\vartheta(\tau))^r\in\mathcal{M}(2,\frac{r}{2},1)$. If one knows an explicit basis for $\mathcal{M}(2,\frac{r}{2},1)$, one can write $1+\sum_{n=1}^{\infty}a_r(n)e^{\pi i n\tau}$ in terms of this basis (which involves only knowing the first few coefficients) and thus get an explicit formula for $a_r(n)$ for all n. For example:

(1) $\sum_{n=1}^{\infty}a_2(n)n^{-s}=4\zeta(\mathbf{Q}(i),s)=4\sum_{n=1}^{\infty}n^{-s}\sum_{d|n}\left(\frac{-4}{d}\right)$. Thus $a_2(n)=4\sum_{d|n}\left(\frac{-4}{d}\right)$, as is well known.

(2) $\sum_{n=1}^{\infty} a_4(n)n^{-s} = C \cdot 2^{-s}\zeta(s)\zeta(s-1)(2^s - 2^{2-s})$
(3) $\sum_{n=1}^{\infty} a_8(n)n^{-s} = 2^{-s}\zeta(s)\zeta(s-3)(C_1 + C_2(2^s + 2^{4-s}))$
(4) $\sum_{n=1}^{\infty} a_{12}(n)n^{-s} = C_1 2^{-s}\zeta(s)\zeta(s-5)(2^s - 2^{6-s}) + C_2\varphi(s)$ where $\varphi(s)$ is associated to $\sqrt{\Delta(\tau)}$.

(The first three formulas are classical.) The general principle has vast applicability—if you know a basis of a space of forms, then you get arithmetic identities. For example, for the modular group Γ, we have $E_4^2 = E_8$, $E_{10} = E_4E_6$, etc.

Remark. Now that we have the functional equation for $\zeta(s)$, we can give a very natural proof, due to Weil, of the product expansion $\Delta(\tau) = z\prod_{n=1}^{\infty}(1-z^n)^{24}$, where $z = e^{2\pi i\tau}$. Taking this product as the definition of $\Delta(\tau)$, it suffices to show $\Delta(-1/\tau) = \tau^{12}\Delta(\tau)$, since clearly $\Delta(\tau+1) = \Delta(\tau)$ and so $\Delta(\tau)$ is the unique cusp form of dimension -12 for Γ. Extracting the 24^{th} root, we have *Dedekind's function*

$$\eta(\tau) = e^{\pi i\tau/24}\prod_{n=1}^{\infty}(1-z^n) = \Delta^{1/24}(\tau)$$

and it suffices to prove $\eta(-1/\tau) = \left(\frac{\tau}{i}\right)^{1/2}\eta(\tau)$. Now let $f(\tau) = \frac{\pi i\tau}{12} - \log\eta(\tau) = \sum_{n,m=1}^{\infty} m^{-1}z^{nm}$, to which we associate as usual the Dirichlet series

$$\varphi(s) = \sum_{m,n=1}^{\infty} m^{-1}(mn)^{-s} = \zeta(s)\zeta(s+1).$$

Thus

$$f(\tau) = \frac{1}{2\pi i}\int_{\sigma=\sigma_1}\left(\frac{\tau}{i}\right)^{-s}\Phi(s)ds$$

where $\sigma_1 > 1$, and $\Phi(s) = (2\pi)^{-s}\Gamma(s)\vartheta(s)$. The functional equation for $\zeta(s)$ (and identities for the Γ-function) give the functional equation $\Phi(s) = \Phi(-s)$. Furthermore, $\Phi(s)$ is entire except for simple poles at $s = \pm 1$ of residue $\pm\frac{\pi}{12}$ and a double pole at $s = 0$ with $\Phi(s) + \frac{1}{2s^2}$ regular at 0; excluding a neighborhood of the poles, $\Phi(s)$ is bounded on vertical strips. The method of Theorem 1.2 is therefore applicable–shifting the line of integration to the left of -1, noting that $\left(\frac{\tau}{i}\right)^{-s}\Phi(s)ds$ has residues $\frac{\pi i}{12\tau}, \frac{1}{2}\log\frac{\tau}{i}, \frac{-\pi\tau}{12i}$ at $s = 1, 0, -1$, and applying $\Phi(s) = \Phi(-s)$, we get

$$f(\tau) = \frac{\pi i}{12\tau} + \frac{1}{2}\log\frac{\tau}{i} - \frac{\pi\tau}{12i} + f(-1/\tau)$$

i.e. $\log\eta(-1/\tau) = \log\eta(\tau) + \frac{1}{2}\log\frac{\tau}{i}$.

Quite similarly, we can derive the product expansion for the theta-function:

$$\vartheta(\tau) = \sum_{n\in\mathbf{Z}} z^{n^2} = \prod_{n=1}^{\infty}(1-z^{2n})(1+z^{2n-1})^2,$$

where $z = e^{2\pi i\tau}$; as above, it suffices to take the product as a definition of $\vartheta(\tau)$ and prove

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

Here

$$\log\vartheta(\tau) = \sum_{n,m=1}^{\infty}\left(\frac{-z^{mn}}{m} + \frac{2(-1)^{m-1}z^{m(2n-1)}}{m}\right)$$

is associated to the Dirichlet series

$$\varphi(s) = \sum_{n,m=1}^{\infty} \frac{-(2mn)^{-s}}{m} + \frac{2(-1)^{m-1}m^{-s}(2n-1)^{-s}}{m})$$
$$= 2^{-s}\zeta(s)\zeta(s+1)(-5+2(2^s+2^{-s})).$$

Thus $\log \vartheta(\tau) = \frac{1}{2\pi i}\int_{\sigma=\sigma_1} \left(\frac{\tau}{i}\right)^{-2} \Gamma(s)\Phi(s)ds$, where $\sigma_1 > 1$ and $\Phi(s) = \pi^{-s}\Gamma(s)\varphi(s)$. Again $\Phi(s) = \Phi(-s)$; since $-5+2(2^s+2^{-s})$ vanishes at $s = \pm 1$, we have this time $\Phi(s) - \frac{1}{2s^2}$ is entire. By the same method as before, we get $\log \vartheta(\tau) + \frac{1}{2}\log\frac{\tau}{i} = \log \vartheta(-1/\tau)$.

This completes our general program of determining all solutions to the functional equation of Theorem 1.2, except for the ambiguity on the O-condition of Theorem 1.2. Before going on to the theory of the Euler product, we close this chapter with a theorem on the zeros of a Dirichlet series with functional equation; this theorem, due to Hardy and Hecke, is a good illustration of the technique of passing back and forth between Dirchlet series and associated Fourier series, à la Theorem 1.2. First we need:

Definition 1.1. A function $f(s)$, regular in some domain, has *order* c if $f(s) = O(e^{|s|^{c+\varepsilon}})$ as $|s| \to \infty$ in that domain, for all $\varepsilon > 0$.

Theorem 1.19 (Phragmen-Lindelöf)**.** *Let $f(s)$ be regular and of finite order in the strip $\sigma_1 \le \sigma \le \sigma_2$, $1 \le t$, where $s = \sigma + it$, and suppose*

$$f(\sigma_j + it) = O(t^{k_j}) \text{ for } j = 1, 2.$$

Then $f(\sigma + it) = O(t^{k(\sigma)})$, uniformly in $\sigma_1 \le \sigma \le \sigma_2$, where $k(\sigma)$ is the linear function with $k(\sigma_j) = k_j$, $j = 1, 2$.

Proof. Say $|f(\sigma + it)| \le Ae^{t^c}$. Let us consider first the case $k_1 = k_2 = 0$, so $|f(s)| \le B$ on $\sigma = \sigma_1$, $\sigma = \sigma_2$, and $t = 1$. Let m be an interger $> c$, $m \equiv 2 \pmod 4$. Then $\mathrm{Re}\,(s^m) = -t^m + p(\sigma, t)$, where $p(\sigma, t)$ is a polynomial in σ and t^2 of degree $< m$ in t, so $|p(\sigma, t)| \le at^{m-2}$. Note $\mathrm{Re}\,(s^m) \le -t^m + at^{m-2} \le D$ (some constant).

For any $\varepsilon > 0$, let $g(s) = e^{\varepsilon s^m} f(s)$. Then $|g(s)| \le Be^{\varepsilon D}$ on $\sigma = \sigma_1$, $\sigma = \sigma_2$, and $t = 1$, and $|g(s)| \le Ae^{t^c + \varepsilon(-t^m + at^{m-2})} \le B$ for $t \ge T(\varepsilon)$, Hence $|g(s)| \le Be^{\varepsilon D}$ for all s, by the maximum principle, so $|f(s)| \le Be^{\varepsilon(D + |s|^m)}$. Letting $\varepsilon \to 0$ (for fixed s), we get $|f(s)| \le B$.

For the general case, let $h(s) = e^{k(s)\log\frac{s}{i}}$. Now

$$\mathrm{Re}\,(k(s)\log\frac{s}{i}) = k(\sigma)\log|s| - at\arg(t - i\sigma) = k(\sigma)\log t + O(1)$$

so $h(s) = t^{k(\sigma)}e^{O(1)}$. Then $\frac{f(s)}{h(s)}$ satisfies the conditions of the special case, so

$$f(s) = O(h(s)) = O(t^{k(\sigma)})$$

□

Corollary 1.20. *Let $f(s)$ be regular and of finite order in $\sigma_1 \le \sigma \le \sigma_2$, $1 \le t$, and suppose*

$$f(\sigma + it) = O(t^{c(\sigma)})$$

for some constant $c(\sigma)$, for each $\sigma \in [\sigma_1, \sigma_2]$. Let $\mu(\sigma)$ be the growth function *of f, $\sigma_1 \le \sigma \le \sigma_2$, i.e. $\mu(\sigma)$ is the infimum of the numbers $c(\sigma)$ so that $f(\sigma + it) = O(t^{c(\sigma)})$. Then $\mu(\sigma)$ is a convex function.*

Proposition 1.21. *Given $\varphi(s) = \sum_{n=1}^{\infty} a_n n^{-s}$, a Dirichlet series converging somewhere, and $\lambda > 0$, $k > 0$, $C = \pm 1$. Then $\varphi(s)$ has signature (λ, k, C), i.e. satisfies the condition (A) of Theorem 1.2, if and only if $\varphi(s)$ satisfies the following condition:*

(A') *$(k-s)\varphi(s)$ is entire of finite order, and satifies the functional equation $\Phi(s) = C\Phi(k-s)$, where $\Phi(s) = (\frac{2\pi}{\lambda})^{-s}\Gamma(s)\varphi(s)$.*

Proof. Let $\varphi(s)$ have signature (λ, k, C). Now $\Gamma(s)$ has order 1 in $\sigma \geq \sigma_0 > 0$, by Stirling's formula, as does then $\frac{1}{\Gamma(s)} = \frac{\sin \pi s}{\pi}\Gamma(1-s)$ in $\sigma \leq -\sigma_0 < 0$. By absolute convergence, $\varphi(s)$ is bounded in $\sigma \geq \sigma_1 > k$, so $\Phi(s) = (\frac{2\pi}{\lambda})^{-s}\Gamma(s)\varphi(s)$ has order 1 there and also in $\sigma \leq k - \sigma_1$ by the functional equation, as does $\varphi(s) = (\frac{2\pi}{\lambda})^{s}\frac{\Phi(s)}{\Gamma(s)}$. Only the strip $k - \sigma_1 \leq \sigma \leq \sigma_1$ remains; $\varphi(s)$ is of order 1 there since $\Phi(s) + \frac{a_0}{s} + \frac{Ca_0}{k-s}$ is bounded. Thus if $\varphi(s)$ satisfies (A), then it has order 1. Conversely, if $\varphi(s)$ satisfies (A'), then $\varphi(\sigma + it) = O(1)$ for $\sigma \geq \sigma_1$, so also $\Phi(\sigma + it) = O(1)$ for $\sigma \geq \sigma_1$ and $\sigma \leq k - \sigma_1$ (by the functional equation). Hence $\Phi(\sigma + it) = O(1)$ in any strip $a \leq \sigma \leq b$, $1 \leq t$, by the Phragmen-Lindelöf theorem, which proves (A). □

Remark. You can state Proposition 1.21 for two functions, as in Theorem 1.2. (A') is actually the condition in Hecke's papers.

Theorem 1.22. *Let $\varphi(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ be a non-zero* real *Dirichlet series (i.e. $a_n \in \mathbf{R}$) of signature (λ, k, C) and $f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n\tau/\lambda}$ the associated modular form. Fix σ_0, $0 < \sigma_0 < k$, and let*

$$R(t) = \operatorname{Re}\Phi(\sigma_0 + it),$$
$$I(t) = \operatorname{Im}\Phi(\sigma_0 + it),$$

where $\Phi(s) = (\frac{2\pi}{\lambda})^{-2}\Gamma(s)\varphi(s)$. Suppose $f(e^{iy}) = O(y^{-\beta})$ as $y \to 0$ through positive values, for some constant β, $0 \leq \beta < \sigma_0 + \frac{1}{2}$. Then either $R(t)$ or $I(t)$ changes sign infinitely many times. (In particular, if $\sigma_0 = \frac{k}{2}$, $\Phi(\frac{k}{2} + it)$ is real, if $C = 1$, or purely imaginary, if $C = -1$, and so $\varphi(s)$ has infinitely many zeros on the middle line $\sigma = \frac{k}{2}$, provided $\beta < \frac{k+1}{2}$.)

Proof. Since $\Phi(s)$ is real on the real axis,

$$\begin{aligned} R(t) &= \frac{1}{2}\big(\Phi(\sigma_0 + it) + \overline{\Phi(\sigma_0 + it)}\big) \\ &= \frac{1}{2}\big(\Phi(\sigma_0 + it) + \Phi(\sigma_0 - it)\big) \\ &= \frac{1}{2}\big(\Phi(\sigma_0 + it) + C\Phi(k - \sigma_0 + it)\big); \end{aligned}$$

similarly,

$$I(t) = \frac{1}{2i}\big(\Phi(\sigma_0 + it) - C\Phi(k - \sigma_0 + it)\big).$$

Note that replacing σ_0 by $k - \sigma_0$ does not affect the statement to be proved, so we may assume $k/2 \leq \sigma_0 < k$.

For any σ_1, $0 < \sigma_1 < k$, we have as usual:

$$f(\tau) - a_0 - Ca_0\left(\frac{\tau}{i}\right)^{-k} = \frac{1}{2\pi i}\int_{\sigma=\sigma_1}\left(\frac{\tau}{i}\right)^{-s}\Phi(s)ds.$$

Put $\tau = e^{iy}$, $y > 0$, so $\frac{\tau}{i} = e^{i(y-\pi/2)}$. The right side above is then

$$\frac{1}{2\pi}\int_{-\infty}^{\infty} e^{-i(\sigma_1+it)(y-\pi/2)}\Phi(\sigma_1+it)dt = \frac{e^{-i\sigma_1(y-\pi/2)}}{2\pi}\int_{-\infty}^{\infty} e^{t(y-\pi/2)}\Phi(\sigma_1+it)dt$$

Hence

$$\int_{-\infty}^{\infty} e^{t(y-\pi/2)}\Phi(\sigma_1+it)dt = O(y^{-\beta})$$

Since

$$\int_{0}^{\infty} e^{t(y-\pi/2)}\Phi(\sigma_1+it)dt = O(1),$$

say for $0 < y \leq \frac{\pi}{4}$, we get (change $t \to -t$, and conjugate):

$$\int_{0}^{\infty} e^{-t(y-\pi/2)}\Phi(\sigma_1+it)dt = O(y^{-\beta}).$$

Hence $G(t) = R(t)$ or $I(t)$ satisfies

$$\int_{0}^{\infty} e^{-t(y-\pi/2)}G(t)dt = O(y^{-\beta}).$$

Now assume $G(t)$ has constant sign for $t >> 0$. Then the integral converges absolutely:

$$\int_{0}^{\infty} e^{-t(y-\pi/2)}|G(t)|dt = O(y^{-\beta}).$$

If the theorem is false, this is true for both $R(t)$ and $I(t)$ and hence for

$$|\Phi(\sigma_0+it)| \leq |R(t)| + |I(t)| :$$

$$\int_{0}^{\infty} e^{-t(y-\pi/2)}|\Phi(\sigma_0+it)|dt = O(y^{-\beta})$$

Now $\Gamma(\sigma_0+it) \sim \sqrt{2\pi}e^{-\pi t/2}t^{\sigma_0-1/2}$ $(t \to +\infty)$, so we get

$$\int_{0}^{\infty} e^{-ty}t^{\alpha}|\varphi(\sigma_0+it)|dt = O(y^{-\beta})$$

where $\alpha = \sigma_0 - \frac{1}{2}$, so $\alpha + 1 > \beta$. Setting $y = \frac{1}{T}$ we have *a fortiori*

$$\int_{0}^{T} t^{\alpha}|\varphi(\sigma_0+it)|dt = O(T^{\beta})$$

$$\text{Then } \int_{\sigma_0+i}^{\sigma_0+iT} |s^{\alpha}\varphi(s)||ds| = O(T^{\beta}), \text{ so}$$

$$\int_{\sigma_0+i}^{\sigma_0+iT} |m^s s^{\alpha}\varphi(s)||ds| = O(T^{\beta})$$

for any natural number m, and so *a fortiori*

$$\int_{\sigma_0+i}^{\sigma_0+iT} m^s s^{\alpha}\varphi(s)ds = O(T^{\beta})$$

where $\beta < \alpha + 1$, which leads to a contradiction, via Phragmen-Lindilöf, as follows.

Choose m so $a_m \neq 0$ and let

$$Z(s) = \int_{\sigma_0+i}^{s} z^{\alpha}m^z\varphi(z)dz$$

for $\sigma > 0$, $t \geq 1$. Since $\varphi(z)$ is of finite order (of order 1, actually), we see $Z(s)$ has finite order, $Z(\sigma_0+it) = O(t^{\beta})$. We will now show the growth function $\mu(\sigma)$

for $Z(s)$ is $\alpha+1$ for σ sufficiently large (in the domain of absolute convergence of $\varphi(s)$), contrary to the convexity of $\mu(\sigma)$. In fact, for large σ:

$$\begin{aligned} Z(\sigma+it) &= a_m \int_{\sigma+i}^{\sigma+it} z^\alpha dz + \sum_{n\neq m} a_n \int_{\sigma+i}^{\sigma+it} z^\alpha (\frac{m}{n})^z dz \\ &= a_m \frac{(\sigma+it)^{\alpha+1}}{\alpha+1} + O(t^\alpha) + O(1) \\ &= \frac{a_m}{\alpha+1} t^{\alpha+1} + O(t^\alpha) \end{aligned}$$

since

$$\begin{aligned} \int_{\sigma+i}^{\sigma+it} z^\alpha (\frac{m}{n})^z dz &= \left[\frac{z^\alpha (\frac{m}{n})^z}{\log \frac{m}{n}} \right]_{\sigma+i}^{\sigma+it} - \int_{\sigma+i}^{\sigma+it} \frac{\alpha z^{\alpha-1} (\frac{m}{n})^z}{\log \frac{m}{n}} dz \\ &= O(t^\alpha n^{-\sigma}). \end{aligned}$$

□

Remark. Looking at other lines in the critical strip besides the middle line was suggested by Berlowitz [2].

Examples. (1) If $\lambda < 2$, and $a_0 = 0$, i.e. $f \in \mathcal{S}(\lambda, k, C)$, then one can take $\beta = \frac{k}{2}$ by Theorem 1.12. Hence the theorem applies for any σ_0.

(2) $\varphi(s) = \zeta(s)\zeta(s+1-k)$, for $k = 4, 6, \ldots$ corresponds to the *Eisenstein series* $G_k(\tau)$. Now $G_k(\tau)(\tau-1)^k = G_k(\frac{-1}{\tau-1}) \neq 0, \infty$ as $\tau \to 1$. Thus we can only take $\beta = k$; the theorem applies for $k - \frac{1}{2} < \sigma_0 < k$.

2. Hecke operators for the full modular group

Let k be a fixed positive *integer* (unlike the first chapter, where k was only required to be real.) If $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a real matrix with positive determinant, and $f(\tau)$ is a holomorphic function on the upper half plane, let $f|L$ be the holomorphic function on the upper half plane defined by

$$f|L(\tau) = (ad-bc)^{k/2}(c\tau+d)^{-k} f(\frac{a\tau+b}{c\tau+d});$$

note $f|\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = f$ for $a > 0$. Passing to the corresponding homgeneous function

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

(on the space of two variables (ω_1, ω_2) with $\text{Im}\,(\omega_1/\omega_2) > 0$) we get

$$\begin{aligned} (F \circ L)\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} &= (c\omega_1 + d\omega_2)^{-k} f\left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}\right) \\ &= (ad-bc)^{-k/2} \omega_2^{-k} (f|L)(\omega_1/\omega_2). \end{aligned}$$

Thus $f \leftrightarrow F$ induces

$$f|L \leftrightarrow (ad-bc)^{k/2} f \circ L = |L| f \circ L$$

which proves the rule

$$(f|L)|M = f|(LM)$$

f will be a *modular form* of dimension $-k$ for a subgroup G of $GL^+(2, \mathbf{R})$ if, besides certain regularity conditions, $f|L = f$ for all $L \in G$; note that it suffices to check this for a set of generators of G. For the *homogeneous modular group* $SL(2, \mathbf{Z})$,

$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$ will do (the *modular group* is $\Gamma = SL(2,\mathbf{Z})/\pm I$, generated by $\tau \mapsto \tau+1$, $\tau \mapsto -1/\tau$); the regularity condition is just that $f(\tau)$ is *holomorphic at* ∞. We let $\mathcal{M}(\Gamma,k)$ be the space of all such, where we now take k to be an even integer; $\mathcal{M}(\Gamma,k) = \mathcal{M}(1,k,(-1)^{k/2}) = \mathcal{M}_0(1,k,(-1)^{k/2})$ in the earlier notation. Similarly, $\mathcal{S}(\Gamma,k)$ is the space of $f \in \mathcal{M}(\Gamma,k)$ vanishing at ∞, the *cusp forms* for Γ of dimension $-k$. We know

$$\mathcal{M}(\Gamma,k) = \mathbf{C}E_k \oplus \mathcal{S}(\Gamma,k).$$

We now give a "geometric" definition of the Hecke operators. Let X be the set of lattices L in $\mathbf{C}$; each L has a basis ω_1,ω_2 with $\mathrm{Im}\,(\omega_1/\omega_2) > 0$, unique up to the action of $SL(2,\mathbf{Z})$. Let D be the *divisor group* of X, i.e. the free abelian group on X, i.e. the set of formal finite sums $\sum_{L\in X} n_L \cdot L = A$, with $n_L \in \mathbf{Z}$; A is *positive* if all $n_L \geq 0$, written $A \geq 0$; the *degree* of A is $\deg A = \sum_L n_L$. An *abstract correspondence* on X of degree n is a "one-to-n mapping" of X into itself, i.e. a homomorphism $D \to D$ which carries each positive divisor of degree 1 to a positive divisor of degree n. For $n = 1,2,3,\ldots$ we define three types of correspondences:

(1) $T(n)$ associates to a lattice L all sublattices L' of index n.
(2) $T(1,n)$ associates to a lattice L all *primitive* sublattices of index n, i.e. such that L/L' is cyclic of order n.
(3) $T(n,n)$ associates nL to L.

Lemma 2.1. *Any $T(a,a)$ commutes with any $T(n)$ and any $T(n,n)$.*

Proof. Reading from left to right, say, $T(a,a)T(n)$ associates to a lattice L all L' of index n in aL; note $(L:L') = a^2 n$. Since $L' \subset aL$, $L' = aL''$ for a unique L'' of index n in L. □

Theorem 2.2. *$T(n)T(m) = \sum_{d|n,m} dT(d,d)T(\frac{nm}{d^2})$; in particular, $T(n)$ is multiplicative, i.e. $T(n)T(m) = T(nm)$ if $(n,m) = 1$. Hence the $T(n)$ generate a commutative ring of correspondences on X.*

Remark. The correspondences were known to Hurwitz, but he did not know their commutativity.

Proof. The first and key step is the special case $n = p$ is prime, $m = p^s$, so we want:

$$T(p)T(p^s) = T(p^{s+1}) + pT(p,p)T(p^{s-1}).$$

The left side takes a lattice L to the $p+1$ sublattices $L'_1,\ldots,L'_{p+1}$ of L of index p, and then takes each L'_i to the L'' of index p^s in L'_i. Thus L'' has index p^{s+1} in L, and each L'' certainly occurs; what duplication takes place? If L'' comes from $L'_i \neq L'_j$, then

$$L'' \subset L'_i \cap L'_j = pL$$

and then L'' is contained in all $(p+1)$ of the L'_i; thus we get the right side.

By induction, left to the reader, we get

$$T(p^r)T(p^s) = \sum_{v\leq r,s} p^v T(p^v,p^v)T(p^{r+s-2v}).$$

Finally, if $(n,m) = 1$, then $T(n)T(m) = T(nm)$, for if L'' has index nm in L, then $L \supset L' \supset L''$ for a unique L' of index n in L; this proves the theorem. □

Remark (C.T.C. Wall). A facetious proof that

$$T(n)T(m) = T(m)T(n)$$

for arbitrary m, n is to observe that given L'' of index nm, on the one side we wish to know the number of subgroups of order n of L/L'' and on the other the number of factor groups of order n, and these two numbers are the same, by Pontrjagin duality.

Now let $F(\omega_1, \omega_2)$, for $\mathrm{Im}\,(\omega_1/\omega_2) > 0$, be a homogeneous function of dimension $-k$ which is invariant under $SL(2, \mathbf{Z})$. Then $F(\omega_1, \omega_2) = F(L)$ may be regarded as a function of the lattice $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$. Define an operator $T(n)$ on such functions by

$$F \cdot T(n)(L) = n^{k-1} \sum_{L'} F(L')$$

where L' runs over the sublattices of index n in L. (The factor n^{k-1} turns out to be convenient.) Similarly,

$$F \cdot T(d, d)(L) = (d^2)^{k-1} F(dL) = d^{k-2} F(L)$$

so the identity of Theorem 2.2 becomes

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

operating on F.

Another way to do all this is as follows. Let $M(n)$ be the set of all 2×2 integer matrices of determinant n, and $M^*(n)$ the primitive ones.

Lemma 2.3.

$$M^*(n) = \Gamma' \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma' = \bigcup_{\substack{ad=n \\ d>0 \\ b \bmod d \\ (a,b,d)=1}} \Gamma' \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

where $\Gamma' = SL(2, \mathbf{Z})$, *and the union is disjoint; the index (number of cosets) is*

$$(M^*(n) : \Gamma') = \psi(n) = n \prod_{p|n} (1 + \frac{1}{p}).$$

Similarly,

$$M(n) = \bigcup_{\substack{ad=n \\ d>0 \\ a|d}} \Gamma' \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \Gamma' = \bigcup_{\substack{ad=n \\ b \bmod d \\ d>0}} \Gamma' \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

Proof. The decompositions follow from the fact that left multiplications from Γ' are row operations, right multiplications are column operations. For the index formula, note first that the index is multiplicative, for if $(n, m) = 1$, $M^*(n) = \bigcup \Gamma' \alpha_i$, $M^*(m) = \bigcup \Gamma' \beta_j$. then

$$M^*(mn) = \Gamma' \begin{pmatrix} 1 & 0 \\ 0 & mn \end{pmatrix} \Gamma' = M^*(n) M^*(m) = \bigcup \Gamma' \alpha_i \beta_j;$$

the union is disjoint, for if

$$(\alpha_i \beta_j)(\alpha_{i'} \beta_{j'})^{-1} \in \Gamma',$$

then $\beta_j\beta_{j'}^{-1}$ is a matrix with coefficients in $\frac{1}{n}\mathbf{Z}$ and $\frac{1}{m}\mathbf{Z}$, hence in $\mathbf{Z}$, so $j = j'$, $i = i'$. For $n = p^r$, we get p^r representatives $\begin{pmatrix} 1 & b \\ 0 & p^r \end{pmatrix}$, $p^{r-1} - p^{r-2}$ representatives $\begin{pmatrix} p & b \\ 0 & p^{r-1} \end{pmatrix}$, $\ldots$, $p-1$ representatives $\begin{pmatrix} p^{r-1} & b \\ 0 & p \end{pmatrix}$, and $\begin{pmatrix} p^r & 0 \\ 0 & 1 \end{pmatrix}$, so

$$\psi(p^r) = p^r + p^{r-1} = p^r(1 + \frac{1}{p}).$$

□

Now given a lattice L, and a matrix α of determinant n, αL is a sublattice of index n, primitive if and only if α is a primitive matrix; furthermore, αL depends only on the coset $\Gamma'\alpha$, and we get a one-one correspondence between cosets $\Gamma'\alpha$ and sublattices αL of L. Hence if $f \in \mathcal{M}(\Gamma, k)$, and $F(\omega_1, \omega_2) = \omega_2^{-k} f(\frac{\omega_1}{\omega_2})$ is the corresponding homogeneous function, we define the n^{th} *Hecke operator* by

$$f|T(n) = n^{\frac{k}{2}-1} \sum_{\alpha} f|\alpha$$

where $M(n) = \bigcup_\alpha \Gamma'\alpha$, which is the inhomogeneous function corresponding to $F \cdot T(n)$. Then $f|T(n)|A = f|T(n)$ for all $A \in \Gamma'$, so $f|T(n)$ is still formally a modular form for Γ, of dimension $-k$; we will verify shortly that $f|T(n)$ is holomorphic at ∞. We still have the same identities:

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

on $\mathcal{M}(\Gamma, k)$.

Proposition 2.4. *Let $f \in \mathcal{M}(\Gamma, k)$, say*

$$f(\tau) = \sum_{\nu=0}^{\infty} a_\nu e^{2\pi i \nu \tau}.$$

Then

$$f|T(n)(\tau) = \sum_{\nu=0}^{\infty} a_\nu(n) e^{2\pi i \nu \tau},$$

where

$$a_\nu(n) = \sum_{d|\nu,n} d^{k-1} a_{\frac{n\nu}{d^2}}, \quad a_0(n) = \sigma_{k-1}(n) \cdot a_0.$$

Hence $f|T(n) \in \mathcal{M}(\Gamma, k)$, and is a cusp form if f is.

Proof.

$$\begin{aligned} f|T(n)(\tau) &= \sum_{ad=n} \sum_{\nu=0}^{\infty} a_\nu e^{2\pi i a \nu \tau/d} \sum_{b \bmod d} \frac{n^{k-1}}{d^k} e^{2\pi i b\nu/d} \\ &= \sum_{ad=n} \sum_{\nu=0}^{\infty} a_{\nu d} e^{2\pi i a\nu\tau} a^{k-1} \\ &= \sum_{\mu=0}^{\infty} e^{2\pi i \mu \tau} \sum_{a|\mu,n} a^{k-1} a_{\frac{\mu n}{a^2}} \end{aligned}$$

□

(We used the fact that the character sum $\sum_{b \bmod d} e^{2\pi i b\nu/d}$ is d if $d|\nu$ and 0 otherwise.)

We now form the formal Dirichlet series $D(s) = \sum_{n=1}^{\infty} T(n)n^{-s}$, whose coefficients $T(n)$ are operators on $\mathcal{M}(\Gamma, k)$, a finite dimensional vector space. The identities among the Hecke operators are most neatly expressed as:

Theorem 2.5.

$$D(s) = \sum_{n=1}^{\infty} T(n)n^{-s} = \prod_p (I - T(p)p^{-s} + p^{k-1-2s}I)^{-1}$$

where I is the identity matrix.

Proof. In view of the multiplicativity, we have only to check that

$$I = \sum_{\nu=0}^{\infty} T(p^\nu)p^{-\nu s}(I - T(p)p^{-s} + p^{k-1-2s}I),$$

which follows from the previous identities (and vice versa). □

Corollary 2.6. *Let $f \in \mathcal{M}(\Gamma, k)$, $f(\tau) = \sum_{\nu=0}^{\infty} a_\nu e^{2\pi i\nu\tau}$, and suppose f is an eigenfunction for the Hecke algebra, say $f|T(n) = c_n \cdot f$. Then $c_n \cdot a_1 = a_n$, so normalizing to have $a_1 = 1$, the eigenvalue c_n of $T(n)$ is the same as Fourier coefficient a_n, and the associated Dirichlet series has the* Euler product

$$\varphi(s) = \sum_{n=1}^{\infty} a_n n^{-s} = \prod_p (1 - a_p p^{-s} + p^{k-1-2s})^{-1}$$

Proof. By Proposition 2.4, $c_n a_1 = a_1(n) = a_n$; the rest is clear. □

We now prove the converse of the corollary in a strong form–the only possible Euler product for $\varphi(s)$ is when $f(\tau)$ is an eigenfunction for the $T(n)$. First we prove a useful preliminary result:

Proposition 2.7. *Let $f \in \mathcal{M}(\Gamma, k)$, $f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n\tau}$.*

(1) *If $f|\alpha \in \mathcal{M}(\Gamma, k)$ for some $\alpha \in M^*(n)$, $n > 1$, then $f = 0$.*
(2) *Let p be a fixed prime.*
   (a) *If $a_m = 0$ for all m with $p \nmid m$, then $f = 0$.*
   (b) *If $a_{pn} = 0$ for all n, then $f = 0$.*

Proof. (1) We may as well take $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$, since $\alpha \in \Gamma' \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma'$. Then $f|\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = f|\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$, so $f = f|\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} = f|\begin{pmatrix} n & 1 \\ 0 & n \end{pmatrix}$. Now $\begin{pmatrix} n & 1 \\ 0 & n \end{pmatrix} = L\begin{pmatrix} 1 & 0 \\ 0 & n^2 \end{pmatrix}M$, where $L, M \in \Gamma'$, so $f|\begin{pmatrix} 1 & 0 \\ 0 & n^2 \end{pmatrix} = f$, i.e. $f(\tau) = f(\frac{\tau}{n^2}) \cdot n^{-k}$. But then $f = 0$ (look at the Fourier series).

(2) If $a_m = 0$ for $p \nmid m$, then $f(\tau + \frac{1}{p}) = f(\tau)$, i.e. $f = f|\begin{pmatrix} p & 1 \\ 0 & p \end{pmatrix}$, so $f = 0$. If all $a_{pn} = 0$, then $f|T(p) = p^{\frac{k}{2}-1} f|\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{M}(\Gamma, k)$, so $f = 0$.

□

Now let $\varphi(s) = \sum_{n=1}^{\infty} a_n n^{-s} \neq 0$ correspond to $f \in \mathcal{M}(\Gamma, k)$. We say $\varphi(s)$ has an *Euler product relative to the prime* p if

$$\varphi(s) = (\sum_{p \nmid m} a_m m^{-s})(\sum_{\nu=0}^{\infty} c(p^\nu) p^{-\nu s})$$

i.e. $a_{mp^\nu} = a_m c(p^\nu)$ for $p \nmid m$, $\nu \geq 0$. Note $c(1) = 1$, by (2a) of Proposition 2.7.

Theorem 2.8. *$\varphi(s)$ has an Euler product relative to p if and only if f is an eigenfunction for $T(p)$, say $f|T(p) = c \cdot f$. If so, then the p-factor is necessarily*

$$\sum_{\nu=0}^{\infty} c(p^\nu) p^{-\nu s} = (1 - cp^{-s} + p^{k-1-2s})^{-1}$$

Proof. Assume first $\varphi(s)$ has an Euler product relative to p, i.e. $a_{mp^\nu} = a_m c(p^\nu)$ for $p \nmid m$, $\nu \geq 0$. Now

$$\begin{aligned} f|T(p)(\tau) &= p^{k-1} f(p\tau) + \frac{1}{p} \sum_{\ell \bmod p} f(\frac{\tau + \ell}{p}) \\ &= p^{k-1} f(p\tau) + \sum a_{pn} z^n \end{aligned}$$

so

$$f|T(p)(\tau) - c(p) f(\tau) = p^{k-1} f(p\tau) + \sum (a_{pn} - c(p) a_n) z^n = \text{a power series in } z^p$$

so is 0, by Proposition 2.7.

Conversely, suppose $f|T(p) = c \cdot f$. Then, for any n

$$c \cdot a_n = a_n(p) = \begin{cases} a_{np} & \text{if } p \nmid n \\ a_{np} + p^{k-1} a_{n/p} & \text{if } p | n \end{cases}$$

by Proposition 2.4. Hence

$$\begin{aligned} &\varphi(s)(1 - cp^{-s} + p^{k-1-2s}) = \\ &\sum_n a_n n^{-s} + p^{k-1} \sum_n a_n (np^2)^{-s} - \sum_n a_{pn} (pn)^{-s} - p^{k-1} \sum_n a_n (np^2)^{-s} \\ &= \sum_{p \nmid m} a_m m^{-s} \end{aligned}$$

□

Thus $\varphi(s)$ has an Euler product if and only if the associated $f(\tau)$ is an eigenfunction for the Hecke operators. For example, we know the Eisenstein series G_k corresponds to (a constant times) $\varphi(s) = \zeta(s)\zeta(s + 1 - k)$, which has an Euler product, so G_k is an eigenfunction. Thus the decomposition

$$\mathcal{M}(\Gamma, k) = \mathbf{C} \cdot G_k \oplus \mathcal{S}(\Gamma, k)$$

is preserved by all Hecke operators, and to show $\mathcal{M}(\Gamma, k)$ has a basis of eigenvectors it suffices to show $\mathcal{S}(\Gamma, k)$ does, which is the goal of the next chapter. There we will show $\mathcal{S}(\Gamma, k)$ has an inner product in which the $T(n)$ are Hermitian operators, and so can be simultaneously diagonalized by standard linear algebra.

$\mathcal{S}(\Gamma, 12)$ is one-dimensional, generated by

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

$z = e^{2\pi i\tau}$; hence the corresponding Dirichlet series $\varphi(s) = \sum_{n=1} a_n n^{-s}$ has the Euler product

$$\varphi(s) = \prod_p (1 - a_p p^{-s} + p^{11-2s})^{-1},$$

first proved by Mordell [7] in 1917. *Ramanujan's conjecture* says that the polynomial $1 - a_p t + p^{11} t^2$ has conjugate roots, i.e. $|a_p| \leq 2p^{11/2}$. *Petersson's conjecture* is that any eigenvalue a_p of $T(p)$ on $\mathcal{S}(\Gamma, k)$ satisfies $|a_p| \leq 2p^{\frac{k-1}{2}}$, for any prime p.

As a final remark, the Eisenstein series G_k is characterized as the eigenfunction not vanishing at ∞. In fact, if $f|T(n) = \lambda_n \cdot f$, for all n, where f is not a cusp form, we write $f = a \cdot G_k + g$, where g is a cusp form; then $(\lambda_n - \sigma_{k-1}(n))f = g|T(n) - \sigma_{k-1}(n) \cdot g$ is a cusp form, so $\lambda_n = \sigma_{k-1}(n)$, $f =$ constant times G_k.

3. The Petersson inner product

Although we are mainly interested in the full modular group Γ, it is convenient at this point to develop some machinery relative to a subgroup G of Γ of finite index μ. In particular, we want to make $\widehat{G\backslash\mathcal{H}}$ into a Riemann surface, so that the natural map $\widehat{G\backslash\mathcal{H}} \to \widehat{\Gamma\backslash\mathcal{H}}$ is holomorphic; there is very little to do, since the fundamental domain $\mathcal{D}(G)$ will be a union of μ copies of the fundamental domain $\mathcal{D}(\Gamma)$.

Any element of Γ carries ∞ onto ∞ or a rational number; in this way we get σ, say, inequivalent (under G) points $P_1 = \infty, P_2, \ldots, P_\sigma$, the *cusps* of G. Let $U(\tau) = \tau + 1$, so the stability group $\Gamma(P_1)$ of P_1 in Γ is infinite cyclic, generated by U. If e_1 is the least positive integer with $U^{e_1} \in G$, then the stability group of P_1 in G is infinite cyclic, generated by U^{e_1}. We take $z_1 = e^{2\pi i\tau/e_1}$ as local parameter at P_1 (it is one-one on $G\backslash\mathcal{H}$ near P_1). At one of the other cusps $P_j = L_j P_1$, where $L_j \in \Gamma$, the stability group $\Gamma(P_j)$ is infinite cyclic on $U_j = L_j U L_j^{-1}$, $G(P_j)$ is cyclic on $U_j^{e_j}$ $(e_j > 0)$, and $z_j = e^{2\pi i L_j^{-1}\tau/e_j}$ is the appropriate local parameter. Then

$$\mathcal{D}(G) = \bigcup_{j=1}^{\sigma} \bigcup_{i=0}^{e_j - 1} U_j^i L_j \mathcal{D}(\Gamma)$$

is a fundamental domain for G, and we have made $\widehat{G\backslash\mathcal{H}} = G\backslash(\mathcal{H} \cup \{P_1, \ldots, P_\sigma\})$ into a Riemann surface, with $\widehat{G\backslash\mathcal{H}} \longrightarrow \widehat{\Gamma\backslash\mathcal{H}}$ holomorphic (and e_j the ramification index of P_j over ∞, i.e. the number of sheets in the covering which stick together there), except we still have to treat the elliptic fixed points. But this is trivial, for $\mathcal{H} \longrightarrow \Gamma\backslash\mathcal{H}$ ramifies only over i and $\tau_0 = e^{2\pi i/3}$, with stability groups of order 2 and 3, so if P is an elliptic fixed point, we take the same local parameter for G as for Γ. Note if $P \mapsto i$ or τ_0, then P is an elliptic fixed point if and only if P is unramified over i or τ_0. Hence if μ_i resp. μ_0 is the number of elliptic fixed points of order 2 resp. 3, then $\frac{\mu - \mu_i}{2}$ resp. $\frac{\mu - \mu_0}{3}$ are the number of ramified points over i resp. τ_0. Now the Riemann-Hurwitz formula for the genus $p(G)$ of $\widehat{G\backslash\mathcal{H}}$ is (since $\widehat{\Gamma\backslash\mathcal{H}}$ has genus 0):

$$2p(G) - 2 = \mu(-2) + \sum_P (e_P - 1)$$

where $P \in \widehat{G\backslash\mathcal{H}}$, and e_P is the ramification index of P over $\widehat{\Gamma\backslash\mathcal{H}}$. By the above,

$$\sum_{P \mapsto i} (e_P - 1) = \frac{\mu - \mu_i}{2}, \quad \sum_{P \mapsto \tau_0} (e_P - 1) = 2(\frac{\mu - \mu_0}{3}), \quad \sum_{P \mapsto \infty} (e_P - 1) = \mu - \sigma$$

Thus

$$p(G) = 1 - \mu + \frac{\mu - \mu_i}{4} + \frac{\mu - \mu_0}{3} + \frac{\mu - \sigma}{2}$$
$$= 1 + \frac{\mu}{12} - \frac{\mu_i}{4} - \frac{\mu_0}{3} - \frac{\sigma}{2},$$

proving:

Proposition 3.1. *If G is a subgroup of Γ of finite index μ, the genus of $\widehat{G\backslash\mathcal{H}}$ is*

$$p(G) = 1 + \frac{\mu}{12} - \frac{\mu_i}{4} - \frac{\mu_0}{3} - \frac{\sigma}{2},$$

where μ_i resp. μ_0 is the number of elliptic fixed points of order 2 resp. 3, and σ is the number of cusps.

To define modular forms, it is convenient to use homogeneous notation. Let G' be s subgroup of $\Gamma' = SL(2, \mathbf{Z})$, of finite index, and G the group of linear fractional transformations defined by G'; thus $G = G'/\pm I$ if $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in G'$, and otherwise $G = G'$. We have already defined

$$f|\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = (ad - bc)^{k/2}(c\tau + d)^{-k} f(\frac{a\tau + b}{c\tau + d});$$

A *modular form* for G' is a holomorphic function $f(\tau)$ on $\mathcal{H}$ such that

(1) $f|L = f$ for all $L \in G'$,
(2) f is holomorphic at the cusps.

The meaning of (2) is as follows. At the cusp ∞, we can write $f(\tau) = \sum_{n=-\infty}^{\infty} a_n z_1^n$ as a Laurent series in $z_1 = e^{2\pi i\tau/e_1}$, and the condition is that $a_n = 0$ for $n < 0$; a_0 is called the *value* of f at ∞. At a cusp $P_j = L_j(\infty)$, where $L_j \in \Gamma'$, we throw P_j to ∞ by L_j^{-1} and proceed as before. More precisely, $f|L_j$ satisfies condition (1) for the conjugate group $L_j^{-1}G'L_j$, and condition (2) at P_j is just that $f|L_j$ is holomorphic at ∞; the value of $f|L_j$ at ∞ will be called the *value* of f at P_j. We denote by $\mathcal{M}(G', k)$ the space of all such f. Actually, if $-I \in G'$ then k must be even (if $\mathcal{M}(G', k) \neq 0$) and there is no danger in confusing G and G', so let us write $\mathcal{M}(G, k) = \mathcal{M}(G', k)$. $f \in \mathcal{M}(G, k)$ is a *cusp form* if f vanishes at all cusps; $\mathcal{S}(G, k)$ denotes the space of cusp forms.

If $f \in \mathcal{M}(G, k)$, then f is not a function on $\widehat{G\backslash\mathcal{H}}$, but we can still speak of the *order of zero* of f at $P \in \widehat{G\backslash\mathcal{H}}$, measured in local parameters on the Riemann surface.

Proposition 3.2. *Let $f \in \mathcal{M}(G, k)$, $f \neq 0$. Then the total number of zeros of f, counting multiplicities, is $\frac{\mu k}{12}$. Hence* $\dim \mathcal{M}(G, k) \leq 1 + [\frac{\mu k}{12}]$.

Proof. $f^{12}, \Delta^k \in \mathcal{M}(G, 12k)$, so $h = \frac{f^{12}}{\Delta^k}$ is a meromorphic function on $\widehat{G\backslash\mathcal{H}}$, with $k\mu$ poles and hence an equal number of zeros. □

Remark. This is not a good bound. For $k \geq 2$, an exact formula for $\dim \mathcal{M}(G, k)$ follows from the Riemann-Roch theorem; cf. Gunning [3, Chap. II, § 8, Th. 1].

Remark. Take $k = 2$. Since for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{R})$, $d(\frac{a\tau+b}{c\tau+d}) = \frac{d\tau}{(c\tau+d)^2}$, we see f satisfies condition (1) if and only if $f(\tau)d\tau$ is G-invariant, i.e. can be regarded as a differential on $\widehat{G\backslash\mathcal{H}}$. If $f \in \mathcal{M}(G, 2)$, then $f(\tau)d\tau$ is certainly holomorphic

on $\widehat{G\backslash\mathcal{H}}$ except at the cusps. At ∞, $f(\tau) = \sum_{n=0}^{\infty} a_n z^n$, $z = e^{2\pi i\tau/e}$; then $\frac{dz}{z} = \frac{2\pi i d\tau}{e}$, so $f(\tau)d\tau = (\frac{e}{2\pi i})a_0\frac{dz}{z} + \dots$, is holomorphic at ∞ if and only if f vanishes at ∞. A similar consideration holds at the other cusps, so we see that there is an isomorphism of $\mathcal{S}(G,2)$ onto the space of holomorphic differentials (and hence $\dim \mathcal{S}(G,2) = p(G)$.)

The holomorphic differentials on a compact Riemann surface X have a natural inner product

$$(\omega, \omega') = \int_X \omega \wedge \overline{\omega'}$$

The *Petersson inner product* is the natural generalization of this inner product to $\mathcal{S}(G,k)$ for arbitrary k.

Given holomorphic functions f and g on the upper half plane, consider the double differential

$$\delta(f,g) = \frac{i}{2} f(\tau)\overline{g(\tau)}(\operatorname{Im}\tau)^{k-2} d\tau \wedge \overline{d\tau} = f(x+iy)\overline{g(x+iy)}y^{k-2}dx \wedge dy$$

Proposition 3.3. *For any real matrix* $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *of positive determinant, we have*

$$\delta(f|L, g|L) = \delta(f,g) \circ L$$

Proof. The right side means replace τ by $L(\tau) = \frac{a\tau+b}{c\tau+d}$ throughout and so depends only on the linear fractional transformation $L(\tau)$, as is also the case with the left side; hence we can assume $\det L = 1$. Then

$$\begin{aligned} f(L(\tau)) &= (c\tau+d)^k f|L(\tau) \\ dL(\tau) &= (c\tau+d)^{-2} d\tau \\ \operatorname{Im} L(\tau) &= |c\tau+d|^{-2}\operatorname{Im}\tau \end{aligned}$$

and the proposition follows. □

In view of Proposition 3.3, if $f, g \in \mathcal{M}(G,k)$, then

$$(f,g) = (f,g)_G = \int_{\mathcal{D}(G)} \delta(f,g)$$

is well defined, i.e. independent of the choice of fundamental domain $\mathcal{D}(G)$, provided the integral converges.

Lemma 3.4. (f,g) *exists if* f *or* g *is a cusp form.*

Proof. Clearly the integral converges if we exclude a neighborhood of the cusps. At the cusp ∞, $f(\tau)\overline{g(\tau)} = O(e^{-cy})$, for some $c > 0$, so the integral is dominated by $\int_{y_1}^{\infty} e^{-cy}y^{k-2}dy < \infty$. The other cusps go the same way, using Proposition 3.3. □

The inner product satisfies the rules:

(1) (f,g) is linear in f, conjugate linear in g
(2) $(g,f) = \overline{(f,g)}$
(3) $(f,f) \geq 0$, and $(f,f) = 0$ only if $f = 0$
(4) If H is a subgroup of G of finite index ν, then $(f,g)_H = \nu(f,g)_G$ ($\mathcal{D}_H$ contains ν copies of $\mathcal{D}_G$).

Thus $\mathcal{S}(G,k)$ is a finite-dimensional Hilbert space.

We wish to show the Hecke operators $T(n)$ are Hermitian on $\mathcal{S}(G,k)$, i.e. $(f|T(n),g) = (f,g|T(n))$. Since the $T(n)$ are polynomials in the $T(p)$ with real coefficients, it suffices to treat the case $n=p$ is prime.

Lemma 3.5. *There exists a set $\{\alpha\}$ of common representatives for the left and right cosets of $M(p)$ modulo $\Gamma' = SL(2,\mathbf{Z})$, i.e.*

$$M(p) = \bigcup \Gamma'\alpha = \bigcup \alpha\Gamma'.$$

Proof. Since $M(p) = \Gamma'\alpha\Gamma'$ is a single double coset, every right coset meets every left coset, which proves the lemma. □

Lemma 3.6. *Let* $\Gamma'(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma' : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{n} \right\}$, *and $\Gamma(n)$ the corresponding group of linear fractional transformations. Let $\gamma \in M(n)$. Then $\Gamma(mn) \subset \gamma^{-1}\Gamma(m)\gamma$.*

Proof. Say $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\gamma^{-1} = \frac{1}{n}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$, $\alpha \in \Gamma(mn)$. Then $\gamma\alpha n\gamma^{-1} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \pmod{mn}$. □

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}' = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = (ad-bc)\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$. Now $M(p) = \bigcup \Gamma'\alpha = \bigcup \alpha\Gamma'$, so $M(p) = M(p)' = \bigcup \Gamma'\alpha'$. Then $T(p) = p^{\frac{k}{2}-1}\sum \alpha = p^{\frac{k}{2}-1}\sum \alpha'$, so to show $(f|T(p),g)_\Gamma = (f,g|T(p))_\Gamma$, for $f,g \in \mathcal{S}(\Gamma,k)$, or equivalently $(f|T(p),g)_{\Gamma(p)} = (f,g|T(p))_{\Gamma(p)}$ (by rule (4) above), it suffices to prove $(f|\alpha,g)_{\Gamma(p)} = (f,g|\alpha')_{\Gamma(p)}$, since by Lemma 3.6, $f|\alpha, g|\alpha' \in \mathcal{S}(\Gamma(p),k)$.

Let $\mathcal{D}(p)$ be a fundamental domain for $\Gamma(p)$, so $\alpha^{-1}\mathcal{D}(p)$ is one for $\alpha^{-1}\Gamma(p)\alpha$; then $f|\alpha$ and g are forms for both $\Gamma(p)$ and $\alpha^{-1}\Gamma(p)\alpha$, which have the same index. Hence:

$$\begin{aligned}
(f|\alpha,g)_{\Gamma(p)} &= (f|\alpha,g)_{\alpha^{-1}\Gamma(p)\alpha} \\
&= \int_{\alpha^{-1}\mathcal{D}(p)} \delta(f|\alpha,g) \\
&= \int_{\mathcal{D}(p)} \delta(f|\alpha,g)\circ\alpha^{-1} \\
&= \int_{\mathcal{D}(p)} \delta(f,g|\alpha^{-1}), \qquad \text{by Proposition 3.3,} \\
&= \int_{\mathcal{D}(p)} \delta(f,g|\alpha') = (f,g|\alpha')_{\Gamma(p)}
\end{aligned}$$

This proves:

Theorem 3.7 (Petersson [9])**.** *The Hecke operators $T(n)$ are Hermitian on $\mathcal{S}(\Gamma,k)$, i.e.*

$$(f|T(n),g) = (f,g|T(n))$$

Corollary 3.8. *The eigenvalues of $T(n)$ are totally real algebraic numbers.*

Proof. The eigenvalues are real by the theorem. Now any element of $\mathcal{S}(\Gamma, k)$ is a polynomial in E_4 and E_6, so $\mathcal{S}(\Gamma, k)$ has a basis $g_1, \dots, g_r$ of elements g_i with rational Fourier coefficients. Hence $T(n)$ is represented by a rational matrix, so its characteristic polynomial

$$\prod_{j=1}^{r}(x - \lambda_n^{(j)}) = \det(xI - T(n))$$

has rational coefficients; hence $\lambda_n = \lambda_n^{(1)}$ is algebraic and all its conjugates are real. □

If $f(\tau) = \sum_{n=1}^{\infty} a_n z^n$, $z = e^{2\pi i\tau}$, is an eigenfunctions for all $T(n)$, then we know $a_1 \neq 0$, and if we normalize to have $a_1 = 1$, then the Fourier coefficients are the eigenvalues, i.e. $f|T(n) = a_n \cdot f$ for all n (Corollary to Theorem 2.5).

Proposition 3.9. *Let f, g be normalized eigenfunctions. Then either $f = g$ or $(f, g) = 0$.*

Proof. Say $f(\tau) = \sum_{n=-\infty}^{\infty} a_n z^n$, $g(\tau) = \sum_{n=-\infty}^{\infty} b_n z^n$, $a_1 = b_1 = 1$. If $(f, g) \neq 0$, then for all n,

$$a_n(f, g) = (f|T(n), g) = (f, g|T(n)) = \bar{b}_n(f, g)$$

so $a_n = \bar{b}_n = b_n$. Hence $f = g$. □

It follows that if $f_1, \dots, f_r$ are a maximal set of normalized eigenfunctions, then they are linearly independent and $r \leq \dim \mathcal{S}(\Gamma, k)$. That actually there exists a basis of eigenfunctions follows from Theorem 3.7 and linear algebra:

Lemma 3.10. *Let R be a commutative ring of Hermitian operators on a finite dimensional Hilbert space V. Then V has an orthogonal basis $f_1, \dots, f_n$ of eigenvectors of R.*

Proof. Let $S_1, \dots, S_m$ span R (finite-dimensional, being a matrix ring). Assume $V \neq 0$. We show first V contains one eigenvector f_1 of $S_1, \dots, S_m$, by induction on m. Let λ_1 be an eigenvalue of S_1, and $V_1 = \{f \in V : S_1 f = \lambda_1 \cdot f\}$ the corresponding eigenspace. Then $S_j V_1 \subset V_1$ since $S_j S_1 = S_1 S_j$, and so V_1 contains an eigenvector f_1 of $S_2, \dots, S_m$ by the induction hypothesis. Then $V = (\mathbf{C}f_1) \oplus (\mathbf{C}f_1)^{\perp}$, where $(\mathbf{C}f_1)^{\perp} = \{g \in V : (f_1, g) = 0\}$ is invariant under $S_1, \dots, S_m$ since the S_j are Hermitian, and then has an orthogonal basis $f_2, \dots, f_n$, by induction on n. □

Hence $\mathcal{S}(\Gamma, k)$ has an orthogonal basis $f_1, \dots, f_r$ of normalized eigenfunctions of the Hecke operators. The set $\{f_1, \dots, f_r\}$ is the set of all normalized eigenfunctions, by Proposition 3.9. The ring R of Hecke operators is a ring of diagonal $r \times r$ matrices, and so has rank $\leq r$; actually the rank is r, since the $r \times \infty$ matrix of Fourier coefficients (eigenvalues) of $f_1, \dots, f_r$ has rank r. We have proved:

Theorem 3.11. *$\mathcal{S}(\Gamma, k)$ has a basis $f_1, \dots, f_r$ of normalized eigenfunctions of the Hecke operators R, and $\{f_1, \dots, f_r\}$ is the set of all normalized eigenfunctions of R. R has maximal rank $r = \dim \mathcal{S}(\Gamma, k)$.*

In terms of Dirichlet series, there exist exactly $r = \dim \mathcal{S}(\Gamma, k)$ normalized Dirichlet series $\varphi_1(s), \dots, \varphi_r(s)$ with Euler product, which have signature $(1, k, (-1)^{k/2})$ and are regular at $s = k$. They have real coefficients and so have infinitely many zeros on the line $\sigma = k/2$, by Theorem 1.22.

If $T(n_1), \dots, T(n_r)$ are a basis of R, their eigenvalues lie in a totally real number field F; then F contains all eigenvalues of all $T(n)$. For example, if $\dim \mathcal{S}(\Gamma, k) = 2$, i.e. $24 \le k \le 48$, $k \ne 26, 36$, then R is spanned by $I = T(1)$ and some $T(n)$, diagonalized over a real field $F(k) = \mathbf{Q}(\sqrt{d})$, $d > 0$. When $k = 24$, Hecke found $d = 144169$, a prime.

4. Congruence subgroups of the modular group

If N is an integer ≥ 1, the *homogeneous principal congruence subgroup* of level N of $\Gamma' = SL(2, \mathbf{Z})$ is

$$\Gamma'(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma' : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\}.$$

Proposition 4.1. *We have an exact sequence*

$$0 \to \Gamma'(N) \longrightarrow \Gamma' \longrightarrow SL(2, \mathbf{Z}/N\mathbf{Z}) \to 0$$

Hence $(\Gamma' : \Gamma'(N)) = N^3 \prod_{p|N} (1 - \frac{1}{p^2})$.

Proof. We have only to show $SL(2, \mathbf{Z}) \to SL(2, \mathbf{Z}/N\mathbf{Z})$ is onto, since the kernel is $\Gamma'(N)$ by definition, i.e. given $a, b, c, d \in \mathbf{Z}$ with $ad - bc \equiv 1 \pmod N$, we have to adjust $a, \dots, d$ by a multiple of N to get determinant 1. Now $ad - bc = 1 + kN$, so $(c, d, N) = 1$, so $(c, d + \ell N) = 1$ for some ℓ and we can assume $(c, d) = 1$. Thus we want $\begin{vmatrix} a + eN & b + fN \\ c & d \end{vmatrix} = 1$, i.e. $1 = ad - bc + (ed - fc)N$, i.e. $ed - fc = \frac{1 - ad + bc}{N} = -k$; e and f can be so chosen since $(c, d) = 1$.

The index formula is the same as showing that $GL(2, \mathbf{Z}/N\mathbf{Z}) = \mathrm{Aut}((\mathbf{Z}/n\mathbf{Z})^2)$ has order $\varphi(N) N^3 \prod_{p|N} (1 - \frac{1}{p^2})$. The question is multiplicative, so assume $N = p^r$ is a prime power. The order is then the number of ways choosing a basis of $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$; if a, b is a fixed basis, there are $N^2(1 - \frac{1}{p^2})$ choices for $\sigma(a)$ (σ is an automorphism), and, given $\sigma(a)$, $N \cdot \varphi(N)$ choices for $\sigma(b)$, for this is the order of the union of the cosets of $\{\sigma(a)\}$ which are primitive in $\mathbf{Z}/N\mathbf{Z}$. □

The *principal congruence subgroup* of Γ of level N is the group of linear fractional transformations determined by $\Gamma'(N)$. $\Gamma(N) = \Gamma'(N)$ if $N > 2$. $\Gamma(N)$ is a normal subgroup of Γ of index

$$(\Gamma : \Gamma(N)) = \begin{cases} 1 & \text{if } N = 1 \\ 6 & \text{if } N = 2 \\ \frac{1}{2} N^3 \prod_{p|N} (1 - \frac{1}{p^2}) & \text{otherwise.} \end{cases}$$

A *congruence subgroup* of level N is an intermediate group G, $\Gamma(N) \subset G \subset \Gamma$.

A *modular form of level N and dimension $-k$* is an element of $\mathcal{M}(\Gamma(N), k)$.

Modular forms of higher level arise from modular forms of level 1 as follows. If $f \in \mathcal{M}(\Gamma, k)$, and $L \in M(N)$, then $f|L$ is a form for the group

$$G_L = \Gamma \cap L^{-1} \Gamma L,$$

and G_L contains $\Gamma(N)$ (Lemma 3.6). In particular, $L = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$ gives

$$\Gamma_0(N) = G \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : N \mid c \right\}$$

Any other *primitive* L of determinant N is in the double coset $\Gamma L_0 \Gamma$, $L_0 = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$, say $L = AL_0B$, where $A, B \in \Gamma$, giving

$$G_L = B^{-1} G_{L_0} B = B^{-1} \Gamma_0(N) B,$$

a conjugate subgroup. In particular $L = \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}$ gives

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : N \mid b \right\}.$$

All these conjugate subgroups have isomorphic Riemann surfaces; we will give particular attention to $\Gamma_0(N)$. Note that the function field of $X_0(N) = \widehat{\Gamma_0(N)\backslash \mathcal{H}}$ is $\mathbf{C}(j(\tau), j(N\tau))$, where $j(\tau)$ is the *elliptic modular invariant*.

Remark. Write $M^*(N) = \Gamma L_0 \Gamma = \bigcup_L \Gamma L$ (disjoint), where $L_0 = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$. Γ permutes the cosets ΓL transitively, and the stability group of ΓL_1 is G_{L_1}, so the index is

$$\mu(N) = (\Gamma : \Gamma_0(N)) = (\Gamma : G_{L_1}) = \psi(N) = N \prod_{p|N} (1 + \frac{1}{p})$$

a formula from section 2, Lemma 2.3 (it is the degree of $T(1, N)$.)

Proposition 4.2. *The genus of* $X_0(N) = \widehat{\Gamma_0(N)\backslash \mathcal{H}}$ *is*

$$p_0(N) = 1 + \frac{\mu(N)}{12} - \frac{\mu_i(N)}{4} - \frac{\mu_0(N)}{3} - \frac{\sigma(N)}{2}$$

where

$$\mu(N) = N \prod_{p|N} (1 + \frac{1}{p}),$$

$$\mu_i(N) = \begin{cases} 0 & \text{if } 4|N \\ \prod_{p|N} (1 + (\frac{-4}{p})) & \text{otherwise} \end{cases}$$

$$\mu_0(N) = \begin{cases} 0 & \text{if } 2|N \text{ or } 9|N \\ \prod_{p|N} (1 + (\frac{-3}{p})) & \text{otherwise} \end{cases}$$

$$\sigma(N) = \sum_{d|N} \varphi((d, \frac{N}{d}))$$

Proof. This is the formula of Proposition 3.1; we have to check that the number of elliptic fixed points of order 2 rep. 3 is μ_i resp. μ_0 as claimed, and that the number of cusps is σ.

Now $\Gamma L_0 \Gamma = \bigcup_L \Gamma L$, where we can take the L's to be $L = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $d > 0$, $ad = N$, $b \bmod d$, $(a, b, d) = 1$, i.e. $(b, t) = 1$ where $t = (a, d)$. Thus there are $d \cdot \frac{\varphi(t)}{t}$ b's for each d, and hence

$$\mu(N) = \sum_{d|N} \frac{d}{t} \varphi(t).$$

Let $G = G_{L_0} = \Gamma_0(N)$; let $P = MP_0$, where $P_0 = i, \tau_0 = e^{2\pi i/3}$, or ∞, and $M \in \Gamma$. The stability group $G(P)$ is determined as follows. Let $A \in G$. Then $A \in G(P) \iff AP = P \iff M^{-1}AMP_0 = P_0$. Now write $L_0 M = BL$, $B \in \Gamma$.

Then $A \in G(P) \iff A \in M\Gamma(P_0)M^{-1} \iff A = MEM^{-1}$, where $E \in \Gamma(P_0)$, and $E \in M^{-1}GM$, i.e. $E \in M^{-1}L_0^{-1}\Gamma L_0 M = L^{-1}\Gamma L$.

For $P = \infty$, the ramification index e is the least positive integer such that Γ contains $L\begin{pmatrix}1 & e\\ 0 & 1\end{pmatrix}L^{-1} = \begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\begin{pmatrix}1 & e\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}^{-1} = \begin{pmatrix}1 & \frac{ea}{d}\\ 0 & 1\end{pmatrix}$, i.e. $ea \equiv 0 \pmod{d}$, i.e. $e \equiv 0 \pmod{\frac{d}{t}}$. Thus $e = \frac{d}{t}$. We noted above there are $\frac{d}{t}\varphi(t) = e\varphi(t)$ values of b for each d, so $\varphi(t)$ cusps corresponding to d, whence $\sigma = \sum_{d|N}\varphi(t) = \sum_{d|N}\varphi((d, \frac{N}{d}))$.

For $P = i$, since $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ generates $\Gamma(P_0)$, we see P is an elliptic fixed point if and only if γ contains $\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}^{-1} = \begin{pmatrix}\frac{b}{a} & -\frac{b^2+a^2}{N}\\ \frac{d}{a} & \frac{b}{a}\end{pmatrix}$, i.e. $a = 1$, $b^2 + 1 \equiv 0 \pmod{N}$. Thus μ_i is the number of solutions $\pmod{N}$ of $x^2 + 1 \equiv 0 \pmod{N}$, which is given by the formula stated, where $\left(\frac{-4}{p}\right)$ is the *Legendre symbol*.

For $P_0 = \tau_0$, the question is whether Γ contains $\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}^{-1} = \begin{pmatrix}\frac{b}{a} & -\frac{b^2-ab+a^2}{N}\\ \frac{d}{a} & 1-\frac{b}{a}\end{pmatrix}$, i.e. $a = 1$, $b^2 - b + 1 \equiv \pmod{N}$; this gives the formula for μ_0. □

Remark. If G is a subgroup of the modular group, of finite index, then the definition of a modular form for G can be stated as

(1) $f|L = f$ for $L \in G$
(2) for all $A \in \Gamma$, $f|A$ is holomorphic at ∞ (resp. vanishes at ∞ for cusp forms), i.e. $f|A(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n\tau/N}$ (resp. also $a_0 = 0$),

for some positive integer N. If we replace G by a smaller group, then f is a form for that group, for condition (2) is independent of what group we regard f as being a form for. In particular, if G is a congruence subgroup, f can be regarded as a form of various levels, and the question of whether f is a cusp form is independent of the level.

We now define the *Hecke operators* in a reasonably general setting. Let G be a subgroup of $\Gamma' = SL(2, \mathbf{Z})$ of finite index and $\Delta \subset GL^+(2, \mathbf{R})$ a set of real matrices of positive determinant, closed under multiplication, and such that for each $\alpha \in \Delta$, the double coset $(\alpha) = G\alpha G$ contains only finitely many right and left cosets with respect to G. (Chapter 2 treated the case $G = \Gamma'$, $\Delta =$ integer matrices of positive determinant.) Let $R = R(G, \Delta)$ be the free $\mathbf{Z}$-module (or $\mathbf{C}$-module) on the double cosets $(\alpha) = G\alpha G$, for $\alpha \in \Delta$. R is a ring under

$$(\alpha)\cdot(\beta) = \sum_{(\gamma)} C^{\gamma}_{\alpha,\beta}\cdot(\gamma)$$

where if $(\alpha) = \bigcup G\alpha_i$, $(\beta) = \bigcup G\beta_j$ (disjoint), then $C^{\gamma}_{\alpha,\beta}$ is the number of pairs (i, j) with $G\alpha_i\beta_j = G\gamma$; $C^{\gamma}_{\alpha,\beta}$ depends only on the double cosets $(\alpha), (\beta), (\gamma)$. We leave the verification of the associative law to the reader.

Now take $G = \Gamma' = SL(2, \mathbf{Z})$, $\Delta =$ integer matrices of positive determinant. A double coset $(\alpha) = \Gamma'\alpha\Gamma' = \bigcup_i \Gamma'\alpha_i$ operates on the group $\mathcal{D}$ of divisors (i.e. the free abelian group on the set X of lattices) by $L \mapsto \sum \alpha_i(L)$. Thus the mapping

$$T : R(\Gamma', \Delta) \longrightarrow R(X) = \mathrm{End}(\mathcal{D})$$

of R into the ring of correspondences which is linear (by definition) and multiplicative:

$$T((\alpha)\cdot(\beta))L = \sum_{(\gamma)}\sum_{k}\sum_{\Gamma'\alpha_i\beta_j=\Gamma'\gamma_k}\alpha_i\beta_j L$$
$$= \sum_{i,j}\alpha_i\beta_j L = T(\alpha)(T(\beta)\cdot L)$$

(where $(\alpha)=\bigcup\Gamma'\alpha_i$, $(\beta)=\bigcup\Gamma'\beta_j$, $(\gamma)=\bigcup\Gamma'\gamma_k$.) For fixed L, the left cosets $\Gamma'\alpha$ correspond one-one to sublattices αL of L, so $T: R\longrightarrow R(X)$ is injective. Furthermore, any double coset (α) may be written $(\alpha)=\Gamma'\begin{pmatrix}a&0\\0&d\end{pmatrix}\Gamma'$, where $d>0$, $a\mid d$, and we write $T(a,d)=T\left(\begin{pmatrix}a&0\\0&d\end{pmatrix}\right)$, and $T(n)=\sum_{\substack{ad=n\\a|d}}T(a,d)$. Then $R(\Gamma',\Delta)$ is the ring of Hecke operators defined in Chapter 2, and we have the basic identity

$$T(n)T(m)=\sum_{d|n,m}dT(d,d)T(\frac{nm}{d^2})$$

In general, we get a representation of $R(G,\Delta)$ on $V=\mathcal{M}(G,k)$ or $\mathcal{S}(G,k)$ by

$$f|T(\alpha)=|\alpha|^{\frac{k}{2}-1}\sum f|\alpha_i$$

$((\alpha)=\bigcup G\alpha_i)$.

Now let $G=\Gamma'(N)$. Let $\Delta'(N)$ be the set of integer matrices of positive determinant n such that $(n,N)=1$, and $\Delta(N)$ the set of $\alpha\in\Delta'(N)$ with $\alpha\equiv\begin{pmatrix}1&0\\0&n\end{pmatrix}$ (mod N). We have a natural map

$$\varphi(N): R(\Gamma'(N),\Delta(N))\longrightarrow R(\Gamma',\Delta'(N))$$

by $\Gamma'(N)\alpha\Gamma'(N)\mapsto\Gamma'\alpha\Gamma'$.

Lemma 4.3. *$\varphi(N)$ is an isomorphism.*

Proof. We know the set of primitive matrices of determinant m is

$$M_m^*=\Gamma'\begin{pmatrix}1&0\\0&m\end{pmatrix}\Gamma'=\bigcup_{\substack{ad=m,d>0\\b \bmod d\\(a,b,d)=1}}\Gamma'\begin{pmatrix}a&b\\0&d\end{pmatrix}$$

We claim that the set $M_m^*(N)$ of primitive matrices of determinant m and $\equiv\begin{pmatrix}1&0\\0&m\end{pmatrix}$ (mod N) (for $(m,N)=1$) is similarly

$$M_m^*(N)=\Gamma'(N)\begin{pmatrix}1&0\\0&m\end{pmatrix}\Gamma'(N)=\bigcup_{\substack{ad=m,d>0\\b \bmod d\\(a,b,d)=1}}\Gamma'(N)R_a\begin{pmatrix}a&bN\\0&d\end{pmatrix}$$

where $R_a\in\Gamma'$ satisfies $R_a\equiv\begin{pmatrix}a^{-1}&0\\0&a\end{pmatrix}$ (mod N). (R_a is not well defined, but the coset $\Gamma(N)\cdot R_a$ is.) It is clear (from the decomposition of M_m^*) we have distinct cosets adding up to $M_m^*(N)$, and so only have to check there is only a single double coset mod $\Gamma'(N)$. Thus we have to solve

$$\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}\begin{pmatrix}a&bN\\0&d\end{pmatrix}\in\begin{pmatrix}1&0\\0&m\end{pmatrix}\Gamma'(N)$$

with

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \Gamma', \quad \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \equiv \begin{pmatrix}a^{-1} & 0\\ 0 & a\end{pmatrix} \pmod N.$$

Now

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}a & bN\\ 0 & d\end{pmatrix} = \begin{pmatrix}* & *\\ a\gamma & d\delta + bN\gamma\end{pmatrix},$$

so take $\gamma = dN$, $\delta + bN^2 = ax \equiv a \pmod N$ with $(\gamma, \delta) = 1$, i.e. $x \equiv 1 \pmod N$ and $(dN, ax - bN^2) = 1$; we can choose x, hence γ, δ, since $(a, b, d) = 1$. Then $r\delta - s\gamma N = 1$, and $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \begin{pmatrix}r & sN\\ \gamma & \delta\end{pmatrix} \equiv \begin{pmatrix}* & 0\\ 0 & a\end{pmatrix}$ will do. The lemma now follows. □

Let $T^N(a, d)$, $T^N(n)$ be the elements of $R(\Gamma'(N), \Delta(N))$ mapped on $T(a, d)$, $T(n)$ by $\varphi(N)$. The basic identity in $R'(N) = R(\Gamma'(N), \Delta(N))$ is then

$$T^N(n)T^N(m) = \sum_{d|n,m} dT^N(d, d)T^N(\frac{nm}{d^2})$$

for $(nm, N) = 1$.

However, when we operate on $\mathcal{M}(\Gamma(N), k)$, $T^N(d, d)$ operates as $(d^2)^{\frac{k}{2}-1}R_d\begin{pmatrix}d & 0\\ 0 & d\end{pmatrix} = d^{k-2}R_d$, since $R_d\begin{pmatrix}d & 0\\ 0 & d\end{pmatrix} \equiv \begin{pmatrix}1 & 0\\ 0 & d^2\end{pmatrix} \pmod N$. Thus, on $\mathcal{M}(\Gamma(N), k)$, the basic identity is

$$T^N(n)T^N(m) = \sum_{d|n,m} d^{k-1}R_dT^N(\frac{nm}{d^2})$$

for $(nm, N) = 1$.

This suggests we should make the following decomposition of $V = \mathcal{M}(\Gamma(N), k)$ or $\mathcal{S}(\Gamma(N), k)$. $d \mapsto R_d$ is a representation of the abelian group $(\mathbf{Z}/N\mathbf{Z})^\times$ on V, and so the irreducible subspaces are one-dimensional. If $f|R_d = \varepsilon(d) \cdot f$ for all $d \in (\mathbf{Z}/N\mathbf{Z})^\times$, then $\varepsilon(d)$ is a character of $(\mathbf{Z}/N\mathbf{Z})^\times$. Thus

$$V = \bigoplus_\varepsilon V(\varepsilon),$$

summed over all characters of $(\mathbf{Z}/N\mathbf{Z})^\times$, where R_d operates as $\varepsilon(d)$ on $V(\varepsilon)$.

Lemma 4.4. *R_n and $T^N(m)$ commute, $(nm, N) = 1$. Hence $V(\varepsilon)$ is invariant under $T^N(m)$.*

Proof. $T^N(m) = m^{\frac{k}{2}-1}\sum_L L$, where the set of all matrices of determinant m, $\equiv \begin{pmatrix}1 & 0\\ 0 & m\end{pmatrix} \pmod N$ is

$$M_m(N) = \bigcup \Gamma'(N) \cdot L$$

But $M_m(N) = R_n^{-1}M_m(N)R_n = \bigcup \Gamma'(N)R_n^{-1}LR_n$, so $T^N(m) = R_n^{-1}T^N(m)R_n$. □

Thus $T^N(n)$ operates on $V(\varepsilon)$, with basic identity

$$T^N(n)T^N(m) = \sum_{d|n,m} d^{k-1}\varepsilon(d)T^N(\frac{nm}{d^2})$$

for $(nm, N) = 1$, or equivalently: the Dirichlet series $D^N(s) = \sum_{(n,N)=1} T^N(n)n^{-s}$ (whose coefficients are operators on $V(\varepsilon)$) has the Euler product

$$D^N(s) = \prod_{p \nmid N} (1 - T^N(p)p^{-s} + \varepsilon(p)p^{k-1-2s})^{-1}.$$

Thus the Hecke operators $T^N(n)$ for $(n, N) = 1$ behave much as in level 1, except for the introduction of the characters $\varepsilon(n)$. We will prove later they are *ε-Hermitian*, i.e.

$$(f|T^N(n), g) = \varepsilon(n)(f, g|T^N(n))$$

for $f, h \in \mathcal{S}(\Gamma(N), k)(\varepsilon)$.

In order to define $T^N(n)$ for $n \mid N$ we must split V up further. Let $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. If $f \in V$, then $f|U^N = f$ and

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

Let $t \mid N$. Let us say f has *divisor* t if $a_n \neq 0 \implies (n, N) = t$. The set of all $f \in V$ of divisor t is then a subspace $V(t)$.

Now $\nu \in \mathbf{Z}/N\mathbf{Z}$ operates on V by $f \mapsto f|U^\nu$; since the group is abelian we can again decompose V according to characters, say $V = \bigoplus_\chi V_\chi$, where $f \in V_\chi \implies f|U^\nu = \chi(\nu) \cdot f$, for each character χ of $\mathbf{Z}/N\mathbf{Z}$. If the exact period of χ is $\frac{N}{t}$, i.e. $f|U = \zeta \cdot f$, $\zeta =$ primitive $\frac{N}{t}$-th root of 1, then $a_n \neq 0 \implies \zeta = e^{2\pi in/N}$, and then $(n, N = t)$; thus $V_\chi \subset V(t)$. This proves that

$$V = \bigoplus_{t|N} V(t)$$

Note $f \in V(t) \iff f = \sum f_i$, where $f_i|U = \zeta_i \cdot f_i$, $\zeta_i =$ primitive $\frac{N}{t}$-th root of 1.

Lemma 4.5. *$V(t)$ is invariant under R_n and $T^N(n)$, for $(n, N) = 1$.*

Proof. $R_n U^n \equiv U R_n \pmod N$; if $f|U = \zeta \cdot f$ then $f|R_n U^n = \zeta f|R_n$, which shows R_n carries $V(t)$ into itself, since n^2 generates $\mathbf{Z}/N\mathbf{Z}$. Similarly, if $L \in M_n(N)$, so $L \equiv \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \pmod N$, then $U^{-1}LU^n \in M_n(N)$; hence $T^N(n) = U^{-1}T^N(n)U^n$, and $T^N(n)$ carries $V(t)$ into itself. □

Thus $V = \bigoplus_{\varepsilon,t} V(\varepsilon, t)$, where any element f of $V(\varepsilon, t)$ has divisor t and $f|R_n = \varepsilon(n) \cdot f$, $(n, N) = 1$. Note that if $V = \mathcal{M}(\Gamma(N), k)$, then $V(1, k) = \mathcal{M}(\Gamma_0(N), k)$.

We now define Hecke operators $T^t(p) = T^{N,t}(p)$ for $p \mid N$ on $V(t)$; as the notation suggests, they will be different for the various t.

Lemma 4.6. *On $V(t)$, $\begin{pmatrix} 1 & b\frac{N}{t} \\ 0 & m \end{pmatrix}$ depends only on $b \bmod m$.*

Proof. If $f \in V(t)$, then $f|U^{N/t} = f$, so

$$f|\begin{pmatrix} 1 & b\frac{N}{t} \\ 0 & m \end{pmatrix} = f|\begin{pmatrix} 1 & \frac{N}{t} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b\frac{N}{t} \\ 0 & m \end{pmatrix} = f|\begin{pmatrix} 1 & (b+m)\frac{N}{t} \\ 0 & m \end{pmatrix}.$$

□

Now if m is such that every prime factor of m divides N, we define

$$T^t(m) = m^{\frac{k}{2}-1} \sum_{b \bmod m} \begin{pmatrix} 1 & b\frac{N}{t} \\ 0 & m \end{pmatrix}$$

on $V(t)$. We will check shortly that $f|T^t(m) \in V$; to show the divisor is still t, we look at the Fourier expansion:

$$f(\tau) = \sum_{(n,\frac{N}{t})=1} a_n e^{2\pi i n\tau \cdot \frac{t}{N}}$$

(change of notation). Then

$$\begin{aligned} f|T^t(m)(\tau) &= \frac{1}{m} \sum_{b \bmod m} f\left(\frac{\tau + b\frac{N}{t}}{m}\right) \\ &= \sum_{(n,\frac{N}{t})=1} a_n e^{2\pi i n\tau t/Nm} \cdot \frac{1}{m} \sum_{b \bmod m} e^{2\pi i n b/m} \\ &= \sum_{(n,\frac{N}{t})=1} a_{nm} e^{2\pi i n\tau t/Nm}. \end{aligned}$$

Thus $T^t(m)$ has the effect of replacing a_n by a_{nm}, whence

(1) $f|T^t(m)$ still has divisor t,
(2) the $T^t(m)$ commute with each other,
(3) $T^t(m) = 0$ if $(m, \frac{N}{t}) \neq 1$

To check that $f|T^t(m)$ is still a form for $\Gamma(N)$, we can assume $m = p$ is prime, and $p \nmid \frac{N}{t}$, by the remarks above. Let $A \in \Gamma'$, $A \equiv \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \pmod N$. One computes that $A' = \begin{pmatrix} 1 & b\frac{N}{t} \\ 0 & p \end{pmatrix} A \begin{pmatrix} 1 & b\frac{N}{t} \\ 0 & m \end{pmatrix}^{-1} \in \Gamma'$, $A' \equiv \begin{pmatrix} \alpha & \beta' \\ 0 & \delta \end{pmatrix} \pmod N$, $\beta' \equiv 0 \pmod{\frac{N}{t}}$. This proves $f|T^t(p) \in V(t)$ if $f \in V(t)$, and that $T^t(p)$ commutes with R_n for $(n, N) = 1$; hence $T^t(p)$ operates on $V(t, \varepsilon)$, and hence also $T^t(m)$.

Finally, the $T^t(m)$ (where $p \mid m \implies p \mid N$) and the $T(n) = T^N(n)$ (for $(n, N) = 1$) commute on $V(t)$. To see this, we can take $n = p$ to be prime. Now $T(p)$ is the sum of the operator $p^{\frac{k}{2}-1} R_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ and the one which replaces the Fourier coefficient a_n by a_{np}; this second operator certainly commutes with $T^t(m)$, by the remarks above, and we just proved that R_p does, so it remains to prove that the $T^t(m)$ and $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ commute. But

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & m \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & bp \\ 0 & m \end{pmatrix}$$

which proves it.

Finally, we define $T^t(nm) = T(n)T^t(m)$ on $V(t)$, where $(n, N) = 1$ and $p \mid m \implies p \mid N$. If we agree that $\varepsilon(n) = 0$ for $(n, N) \neq 1$ by the usual convention, then we have defined Hecke operators $T^t(n)$ on $V(t, \varepsilon)$ for all $n \geq 1$, satisfying

$$T^t(n)T^t(m) = \sum_{d|n,m} \varepsilon(d) d^{k-1} T^t(\frac{nm}{d^2})$$

(for all $n, m \geq 1$). Equivalently, we have an identity of formal Dirichlet series

$$\sum_{n=1}^{\infty} T^t(n) n^{-s} = \prod_p (1 - T^t(p)p^{-s} + \varepsilon(p)p^{k-1-2s})^{-1};$$

note $\varepsilon(p) = 0$ if $p \mid N$ and $T^t(p) = 0$ if $p \mid \frac{N}{t}$.

Proposition 4.7. *If $f \in V(t, \varepsilon)$ has Fourier expansion $f(\tau) = \sum_n a_n z^n$, $z = e^{2\pi i \tau \cdot t/N}$, then*

$$f|T^t(n)(\tau) = \sum_\nu a_\nu(n) z^\nu,$$

where $a_\nu(n) = \sum_{d|\nu,n} \varepsilon(d) d^{k-1} a_{\frac{\nu n}{d^2}}$.

Proof. We can assume $(n, N) = 1$, by the remarks above; in that case the proof is the same as that of Proposition 2.4 in Chapter 2. □

Theorem 4.8. *Let $T(n) = T^t(n)$ be the Hecke operator on $\mathcal{M}(\Gamma(N), k, t, \varepsilon)$, for $n \geq 1$.*

(1)
$$\sum_{n=1}^{\infty} T(n) n^{-s} = \prod_p (1 - T(p)p^{-s} + \varepsilon(p)p^{k-1-2s})^{-1}$$

(2) *If f is an eigenfunction for all the $T(n)$, normalized to have $a_1 = 1$, then the associated Dirichlet series has the Euler product*
$$\sum_{n=1}^{\infty} a_n n^{-s} = \prod_p (1 - a_p p^{-s} + \varepsilon(p)p^{k-1-2s})^{-1}.$$

Next we generalize Theorem 2.8 on the uniqueness of the p-factor in the Euler product (for $p \nmid N$). We need first the corresponding generalization of Proposition 2.7:

Theorem 4.9. *Let $f, f|\alpha \in \mathcal{M}(\Gamma(N), k)$, where α is a primitive integer matrix of determinant n, with $n > 1$, $(n, N) = 1$. Then $f = 0$.*

Proof. Since $\alpha \in \Gamma' \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Gamma'$, assume $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$. Since $f| \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} = f| \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$,

$$f = f| \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} = f| \begin{pmatrix} n & N \\ 0 & n \end{pmatrix}.$$

The powers of $\begin{pmatrix} n & N \\ 0 & n \end{pmatrix}$ are not all primitive, so replace it by $V = A \begin{pmatrix} n & N \\ 0 & n \end{pmatrix}$, where $A \in \Gamma(N)$, $A \equiv \begin{pmatrix} 1 & * \\ 1 & * \end{pmatrix} \pmod n$. Then $V \equiv \begin{pmatrix} 0 & N \\ 0 & N \end{pmatrix} \pmod n$, $V^\ell \equiv \begin{pmatrix} 0 & N^\ell \\ 0 & N^\ell \end{pmatrix} \pmod n$, and all powers V^ℓ are primitive. Since V^ℓ is primitive of determinant $n^{2\ell}$, write $V^\ell = B \begin{pmatrix} 1 & 0 \\ 0 & n^{2\ell} \end{pmatrix} C$, where $B, C \in \Gamma'$. Now $V \equiv \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \pmod N$, so if we choose ℓ so that $n^\ell \equiv 1 \pmod N$, we have $BC \in \Gamma(N)$, so $f|B = f|C^{-1}$. Finally,

$$f = f|V^\ell = f|B \begin{pmatrix} 1 & 0 \\ 0 & n^{2\ell} \end{pmatrix} C,$$

so $g = f|B \in \mathcal{M}(\Gamma(N), k)$ satisfies

$$g(\tau) = g(\tau/n^{2\ell}) \cdot n^{-k\ell},$$

so $g = 0$, $f = 0$.

□

Corollary 4.10. *Let p be a prime, $p \nmid N$; let $f \in \mathcal{M}(\Gamma(N), k)$, $f(\tau) = \sum a_n e^{2\pi i n\tau/N}$.*

(1) *If $a_m = 0$ for all m with $p \nmid m$, then $f = 0$.*
(2) *If $a_{pn} = 0$ for all n, then $f = 0$.*

Proof. (1): Then $f(\tau) = f(\tau + \frac{N}{p})$; taking $\alpha = \begin{pmatrix} p & N \\ 0 & p \end{pmatrix}$, we get $f = 0$.
(2): Then

$$f|T(p) = p^{\frac{k}{2}-1} f|R_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

has level N; taking $\alpha = R_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$, we get $f = 0$. □

We recall that $\varphi(s) = \sum a_n n^{-s}$ has an *Euler product relative to p* if

$$\varphi(s) = (\sum_{p \nmid m} a_m m^{-s})(\sum_{\nu=0}^{\infty} c(p^\nu) p^{-\nu s})$$

i.e. $a_{mp^\nu} = a_m c(p^\nu)$ for $p \nmid \nu$. If $\varphi(s) \neq 0$, and $p \nmid N$, then $c(1) = 1$, by (1) of the corollary.

Theorem 4.11. *Let $\varphi(s) \neq 0$ be the Dirichlet series associated to $f(\tau) = \sum a_n e^{2\pi i n\tau/N} \in \mathcal{M}(\Gamma(N), k)$. Let $p \nmid N$. Then $\varphi(s)$ has an Euler product relative to p if and only if f is an eigenfunction for R_p and $T(p) = T^N(p)$, say $f|R_p = \varepsilon \cdot f$, $f|T(p) = c \cdot f$. If so, the p-factor is necessarily of the form*

$$\sum_{\nu=0}^{\infty} c(p^\nu) p^{-\nu s} = (1 - cp^{-s} + \varepsilon p^{k-1-2s})^{-1}$$

Proof. For "only if", assume $a_{p^\nu m} = a_m c(p^\nu)$ for $p \nmid m$, $\nu \geq 0$. Then

$$\begin{aligned} f|T(p) - c(p) \cdot f &= p^{\frac{k}{2}-1} f|R_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} + \sum_n (a_{pn} - c(p)a_n) e^{2\pi i n\tau/N} \\ &= \text{power series in } e^{2\pi i p\tau/N} \\ &= 0, \text{ by (1) in the corollary.} \end{aligned}$$

Similarly,

$$\begin{aligned} p^{\frac{k}{2}-1} f|R_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} &= f|T(p) - \sum a_{pn} z^n \\ &= \sum_n (c(p)a_n - a_{pn}) z^n \\ &= \sum_n (c(p)a_{pn} - a_{p^2 n}) z^{pn}, \end{aligned}$$

where $z = e^{2\pi i\tau/N}$. Then

$$\begin{aligned} p^{k-1} f|R_p &= \sum_n (c(p)a_{pn} - a_{p^2n}) z^n \\ &= (c(p)^2 - c(p^2))f + \text{ power series in } z^p \\ &= (c(p)^2 - c(p^2))f \end{aligned}$$

Conversely, suppose $f|T(p) = c \cdot f$, $f|R_p = \varepsilon \cdot f$. Then $c \cdot f(\tau) = p^{k-1}\varepsilon f(p\tau) + \sum a_{pn} z^n$, so

$$c \cdot a_n = \begin{cases} a_{pn} & \text{if } p \nmid n \\ a_{pn} + p^{k-1}\varepsilon a_{n/p} & \text{if } p \mid n \end{cases}$$

Thus

$$\begin{aligned} &\varphi(s)(1 - cp^{-s} + \varepsilon p^{k-1-2s}) \\ &\quad = \sum a_n n^{-s} + \varepsilon \sum a_n p^{k-1} (np^2)^{-s} - \sum a_{pn} (pn)^{-s} - \varepsilon p^{k-1} \sum a_n (np^2)^{-2} \\ &\quad = \sum_{p \nmid m} a_m m^{-s} \end{aligned}$$

□

Theorem 4.12 (Petersson)**.** *Let f, g be cusp forms for $\Gamma(N)$, of character ε. Then*

$$(f|T(n), g) = \varepsilon(n)(f, g|T(n)),$$

for $(n, N) = 1$, where $T(n) = T^N(n)$.

Proof. It suffices to prove this for n a prime power, and then for $n = p$, for if we have the result for $n = p, p^2, \ldots, p^\nu$, then from

$$T(p^\nu)T(p) = T(p^{\nu+1}) + \varepsilon(p)p^{k-1}T(p^{\nu-1}),$$

we get

$$\begin{aligned} (f|T(p^{\nu+1}), g) &= (f|T(p^\nu)T(p), g) - \varepsilon(p)p^{k-1}(f|T(p^{\nu-1}), g) \\ &= \varepsilon(p^{\nu+1})((f, g|T(p^\nu)T(p)) - \overline{\varepsilon(p)}p^{k-1}(f, g|T(p^{\nu-1}))) \\ &= \varepsilon(p^{\nu+1})(f, g|T(p^{\nu+1})) \end{aligned}$$

using the fact that (f, g) is conjugate-linear in g. Thus we assume $n = p$ is prime, $p \nmid N$.

Now the set of integer matrices of determinant p and $\equiv \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \pmod N$ is a single double coset

$$M_p^*(N) = \Gamma'(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma'(N),$$

which shows (as in the case $N = 1$, Theorem 3.7) that every left coset meets every right coset, and so there exists a set $\{\alpha\}$ of left and right representatives:

$$M_p^*(N) = \bigcup \Gamma'(N)\alpha = \bigcup \alpha\Gamma'(N).$$

Letting $\begin{pmatrix} a & b \\ c & d \end{pmatrix}' = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, we see that

$$\bigcup \Gamma'(N)\alpha = M_p^*(N) = R_p(M_p^*(N))' = \bigcup \Gamma'(N)R_p\alpha'.$$

Hence

$$T(p) = p^{\frac{k}{2}-1} \sum \alpha = p^{\frac{k}{2}-1} \sum R_p\alpha',$$

so we are to prove $(\sum f|\alpha, g)_{\Gamma(N)} = (f, \sum g|\alpha')_{\Gamma(N)}$. For this it suffices to prove that

$$(f|\alpha, g)_{\Gamma(pN)} = /f, g|\alpha')_{\Gamma(pN)}.$$

($f|\alpha$ and $g|\alpha'$ are forms for Γ_{pN}.) This is proved as before; in the notation of Chapter 3, we have

$$\begin{aligned}(f|\alpha, g)_{\Gamma(pN)} &= (f|\alpha, g)_{\alpha^{-1}\Gamma(pN)\alpha} \\ &= \int_{\alpha^{-1}\mathcal{D}(pN)} \delta(f|\alpha, g) \\ &= \int_{\mathcal{D}(pN)} \delta(f|\alpha, g) \circ \alpha^{-1} \\ &= \int_{\mathcal{D}(pN)} \delta(f, g|\alpha^{-1}) \\ &= \int_{\mathcal{D}(pN)} \delta(f, g|\alpha') \\ &= (f, g|\alpha')_{\Gamma(pN)},\end{aligned}$$

where $\mathcal{D}(pN)$ is a fundamental domain for $\Gamma(pN)$, and so $\alpha^{-1}\mathcal{D}(pN)$ is one for $\alpha^{-1}\Gamma(pN)\alpha$. □

Note the eigenvalues λ_n of $T(n)$ $((n, N) = 1)$ are not necessarily real this time; the rule is that

$$\lambda_n = \varepsilon(n)\overline{\lambda}_n$$

i.e. $\lambda_n \varepsilon(n)^{-\frac{1}{2}}$ is real. In particular, λ_n is real if $\varepsilon(n) = 1$, purely imaginary if $\varepsilon(n) = -1$.

It follows as before that the space $\mathcal{S}(N, k, t, \varepsilon)$ of cusp forms of dimension $-k$ divisor t, and character ε for $\gamma(N)$ has an orthogonal basis $f_1, \ldots, f_r$ of eigenfunctions for all $T(n)$ with $(n, N) = 1$. If f is any eigenfunction, and $(f, f_j) \neq 0$, say, then

$$\begin{aligned}\lambda_n(f, f_j) &= (f|T(n), f_j) \\ &= \varepsilon(n)(f, f_j|T(n)) \\ &= \varepsilon(n)\overline{\lambda_n^{(j)}}(f, f_j) = \lambda_n^{(j)}(f, f_j)\end{aligned}$$

and so f and a suitable constant times f_j have the same Fourier coefficients a_n for $(n, N) = 1$. This is all you can say in general; however, if $p \mid t \implies p \mid \frac{N}{t}$, then $T(n) = 0$ for $(n, N) \neq 1$, and f is a constant times f_j.

We have the following general estimate on the Fourier coefficients of cusp forms:

Proposition 4.13. *Let G be a subgroup of Γ of finite index, and $f \in \mathcal{S}(G, k)$. Then $f(\tau) = O(y^{-k/2})$ as $y \to 0$, uniformly in x, and hence the Fourier coefficients of f satisfy $a_n = O(n^{k/2})$.*

Proof. Write $\Gamma = \bigcup_L GL$ (disjoint). Then

$$h(\tau) = (\operatorname{Im} \tau)^k \sum_L |f(L(\tau))|^2$$

is invariant under Γ, and bounded on the fundamental domain $\mathcal{D}$ of Γ since it vanishes at ∞. Thus $h(\tau) = O(y^{-k})$, so $f(\tau) = O(y^{-k/2})$. Then $a_n = O(n^{k/2})$ by Proposition 1.1. □

Now if $f \in \mathcal{S}(\Gamma(N), k, \varepsilon)$ is an eigenfunction for $T(p)$, where $p \nmid N$, then the p-factor of the associated Dirichlet series is

$$(1 - a_p p^{-s} + \varepsilon(p) p^{k-1-2s})^{-1}.$$

Let η satisfy $\eta\overline{\eta} = 1$, $\overline{\eta}^2 = \varepsilon(p)$, so $a_p\eta$ is real, *Petersson's conjecture* states that

$$1 - a_p\eta t + p^{k-1}t^2,$$

which has real coefficients, has conjugate roots, i.e. $|a_p| \leq 2p^{\frac{k-1}{2}}$, which would of course be much stronger than the general estimate of Proposition 4.13.

Thus we see that the theory of the Hecke operators $T(n)$ in level N, for cusp forms, parallels that in level 1, at least for $(n, N) = 1$. To treat the non-cusp forms, we again need the explicit construction of *Eisenstein series*.

Let $k \geq 3$ and $c, d \in \mathbf{Z}$, and consider the *Eisenstein series*

$$G_k(\tau; c, d; N) = \sum_{\substack{m \equiv c \pmod N \\ n \equiv d \pmod N}}{}' (m\tau + n)^{-k};$$

since $k \geq 3$, this is an absolutely converging double series, for $\operatorname{Im}(\tau) > 0$. (There are also Eisenstein series for $k = 1, 2$; a modification to ensure convergence is necessary—cf. Hecke's paper [5, No. 24].) If $L \in \Gamma' = SL(2, \mathbf{Z})$, then $G_k|L$ has the term for (m, n) replaced by that for $(m, n)L$:

$$G_k(\tau; (c, d); N)|L = G_k(\tau; (c, d)L; N).$$

Since clearly $G_k(\tau; c, d; N)$ depends only on c and d modulo N, we see it is a form for $\Gamma(N)$, provided it is holomorphic at the cusps. To show this, we determine the Fourier expansion:

Proposition 4.14. *$G_k(\tau; c, d; N) = \sum_{\lambda=0}^{\infty} a_\lambda z^\lambda$, $z = e^{2\pi i\tau/N}$, where*

$$a_0 = \begin{cases} 0 & \text{if } c \not\equiv 0 \pmod N \\ \sum_{n \equiv d\ (N)} n^{-k} & \text{if } c \equiv 0 \pmod N \end{cases}$$

and for $\lambda \geq 1$,

$$a_\lambda = \frac{(-2\pi i)^k}{N^k \Gamma(k)} \sum_{\substack{m\nu = \lambda \\ m \equiv c\ (N)}} (\operatorname{sgn}\nu)\nu^{k-1} e^{2\pi i\nu d/N}$$

Proof. As in the proof of Proposition 1.14, we start from

$$\sum_m (m + \tau)^{-k} = \frac{(-2\pi i)^k}{\Gamma(k)} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi i n\tau}.$$

Clearly

$$\begin{aligned} G_k(\tau) - a_0 &= \sum_{\substack{m \equiv c \\ m \neq 0}} \sum_n (m\tau + nN + d)^{-k} \\ &= \frac{N^{-k}(-2\pi i)^k}{\Gamma(k)} \Big(\sum_{\substack{m \equiv c \\ m > 0}} \sum_{\nu=1}^{\infty} \nu^{k-1} e^{2\pi i\nu \frac{m\tau + d}{N}} + \sum_{\substack{m \equiv c \\ m < 0}} \sum_{\nu=-1}^{-\infty} (-\nu)^{k-1} e^{2\pi i\nu \frac{m\tau + d}{N}} \Big), \end{aligned}$$

and this proves the proposition. □

Thus $G_k(\tau; c, d; N) \in \mathcal{M}(\Gamma(N), k)$.

$G_k(\tau; c, d; N)$ is called *primitive* if $(c, d, N) = 1$; if $(c, d, N) = t > 1$, then

$$G_k(\tau; c, d; N) = t^{-k} G_k(\tau; \frac{c}{t}, \frac{d}{t}; \frac{N}{t})$$

is a primitive Eisenstein series of level $\frac{N}{t}$. Let $\mathcal{E}(N) = \mathcal{E}(N, k)$ be the space generated by all primitive Eisenstein series of level N.

Now N fundamental domains for Γ meet at ∞; since $\Gamma(N)$ is a normal subgroup of Γ, the same is true at any other cusp. The number of cusps is then

$$\sigma(N) = \frac{(\Gamma : \Gamma(N))}{N} = \begin{cases} 1 & \text{if } N = 1 \\ 3 & \text{if } N = 2 \\ \frac{1}{2} N^2 \prod_{p|N} (1 - \frac{1}{p^2}) & \text{if } N > 2 \end{cases}$$

We have an obvious map

$$\mathcal{E}(N) \longrightarrow \mathbf{C}^{\sigma(N)}$$

by evaluating at the cusps, and we want to show this is an isomorphisms. Now the number of primitive pairs (c, d) mod N is $N^2 \prod_{p|N} (1 - \frac{1}{p^2})$, and clearly

$$G_k(\tau; c, d; N) = (-1)^k G_k(\tau; -c, -d; N),$$

so $\dim \mathcal{E}(N) \leq \sigma(N)$ and so it suffices to prove the map is onto.

For this, it is convenient to consider the *restricted Eisenstein series*

$$G_k^*(\tau; c, d; N) = \sum_{\substack{m \equiv c \ (N) \\ n \equiv d \ (N) \\ (m,n)=1}} (m\tau + n)^{-k};$$

again a form for $\Gamma(N)$, with

$$G_k^*(\tau; c, d; N)|L = G_k^*(\tau; (c, d)|L; N)$$

for $L \in \Gamma'$. To connect the two kinds of Eisenstein series, we use the *Möbius function* $\mu(n)$, the multiplicative function of positive integers n with $\mu(1) = 1$, $\mu(p) = -1$ for p prime, and $\mu(n) = 0$ if n has a square factor. The Möbius function satisfies

$$\sum_{\substack{d|n \\ (d>0)}} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

Thus

$$\begin{aligned} G_k^*(\tau; c, d; N) &= \sum_{\substack{m \equiv c \\ n \equiv d}}{}' (m\tau + n)^{-k} \sum_{a|(n,m)} \mu(a) \\ &= \sum_{a=1}^{\infty} \mu(a) a^{-k} \sum_{\substack{ma \equiv c \\ na \equiv d}}{}' (m\tau + n)^{-k}. \end{aligned}$$

Now assume $(c, d, N) = 1$ (otherwise $G_k^*(\tau; c, d; N) = 0$). Then in the sum above we can assume $(a, N) = 1$. For such an a, choose a' with $aa' \equiv 1 \pmod{N}$. Then

$$\begin{aligned} G_k^*(\tau; c, d; N) &= \mu(a) a^{-k} G_k(\tau; a'c, a'd; N) \\ &= \sum_{\substack{(t,N)=1 \\ t \bmod N}} c_t \cdot G_k(\tau; ct, dt; N), \end{aligned}$$

where $c_t = \sum_{\substack{at \equiv 1 \ (N) \\ a>0}} \mu(a) a^{-k}$. Thus $G_k^*(\tau; c, d; N) \in \mathcal{E}(N)$.

The value of $G_k^*(\tau; c, d; N)$ at ∞, i.e. its 0^{th} Fourier coefficient, is visibly

$$a_0 = \sum_{\substack{m=0\equiv c \\ n\equiv d \\ (m,n)=1}} n^{-k} = \begin{cases} 1 & \text{if } (c,d) \equiv (0,1) \pmod N \\ 0 & \text{otherwise.} \end{cases}$$

Since $G_k^*(\tau; 0, 1; N)|\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = G_k^*(\tau; \gamma, \delta; N)$, we see $G_k^*(\tau; 0, 1; N)$ takes the value 1 at the cusp ∞ and 0 at the other cusps; similarly, $G_k^*(\tau; c, d; N)$ takes the value 1 at the cusp $-d/c$ and 0 at all other cusps. This proves:

Proposition 4.15. *The map $\mathcal{E}(N) \to \mathbf{C}^{\sigma(N)}$ is an isomorphism, and $\mathcal{E}(N, k)$ is generated by the restricted Eisenstein series.*

Proposition 4.16. *If $N' \mid N$, then $\mathcal{E}(N', k) \subset \mathcal{E}(N, k)$. Hence $\mathcal{E}(N)$ is the space of all Eisenstein series of level N, primitive or not.*

Proof.

$$G_k^*(\tau; c', d'; N') = \sum_{\substack{c\equiv c' \ (N) \\ d\equiv d' \ (N) \\ c,d \bmod N}} G_k^*(\tau; c, d; N)$$

which proves the first statement, in view of Proposition 4.15; we have already observed that an imprimitive series of level N is a primitive series of lower level $\frac{N}{t}$, which proves the second statement. □

Proposition 4.17. *If L is a primitive integer matrix of determinant $m \geq 1$, and $f \in \mathcal{E}(N)$, then $f|L \in \mathcal{E}(mN)$. Also, $\mathcal{E}(mN, k) \cap \mathcal{M}(\Gamma(N), k) = \mathcal{E}(N, k)$.*

Proof. We have proved this for $m = 1$, i.e. $L \in \Gamma'$, so we may as well take $L = \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix}$; then $G_k(\tau; c, d; N)|L = \sum_{\nu=1}^{m} G_k(\tau; c + \nu N, dm; Nm)$.

For the second statement, note that we have as a result of Proposition 4.15 a direct sum decomposition $\mathcal{M}(\Gamma(N), k) = \mathcal{E}(N, k) \oplus \mathcal{S}(N, k)$. If $f \in \mathcal{E}(mN, k) \cap \mathcal{M}(\Gamma(N), k)$, write $f = E + g$, where $E \in \mathcal{E}(N, k)$, $g \in \mathcal{S}(N, k)$. Then $g \in \mathcal{E}(mN, k)$, by Proposition 4.16, and g is a cusp form, so $g = 0$ by Proposition 4.15. □

In view of these propositions, let us call any element of $\mathcal{E}(N, k)$ an *Eisenstein series*.

Since $\mathcal{E}(N, k)$ is invariant under all modular transformations, in particular by R_n for $(n, N) = 1$ and $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, we can decompose $\mathcal{E}(N, k)$ according to divisors t of N and characters ε of $(\mathbf{Z}/N\mathbf{Z})^\times$, getting

$$\mathcal{M}(\Gamma(N), k, \varepsilon, t) = \mathcal{E}(N, k, \varepsilon, t) \oplus \mathcal{S}(N, k, \varepsilon, t).$$

Furthermore, this decomposition is respected by all Hecke operators $T(n) = T^t(n)$, $n \geq 1$, by Proposition 4.17.

A way to construct modular forms (of higher level) from given ones, using characters, is given by the following theorem; this technique is also emphasized in the following chapter. Given an integer $m \geq 1$, a *character* modulo m is a character χ on $(\mathbf{Z}/m\mathbf{Z})^\times$; we extend χ to a function of all positive integers n by the usual convention that $\chi(n) = 0$ if $(n, m) > 1$. Note that we do not in general require χ to be *primitive* (not defined modulo a proper divisor of m); in particular, even the identity character $\chi = 1$ modulo m satisfies the convention $\chi(n) = 0$ for $(n, m) > 1$.

Theorem 4.18. *Let* $f(\tau) = \sum_{(n,\frac{N}{t})=1} a_n z^{nt} \in \mathcal{M}(\Gamma(N), k, \varepsilon, t)$, $z = e^{2\pi i\tau/N}$, *and let* χ *be a character modulo* $m \cdot \frac{N}{t}$, *where* $(n, N) = 1$. *Let*

$$f_\chi(\tau) = \sum_n \chi(n) a_n z^{nt}$$

Then $f_\chi \in \mathcal{M}(\Gamma(m^2N), k, \varepsilon\chi^2, tm^2)$, *and* f_χ *is a cusp form (resp. Eisenstein series) if* f *is.*

Proof. Let $M = m \cdot \frac{N}{t}$, and consider the operator

$$L_\chi = \frac{1}{n} \sum_{x,y \bmod M} \chi(x) e^{-2\pi i xy/M} \begin{pmatrix} m & y \\ 0 & m \end{pmatrix};$$

then $f|L_\chi \in \mathcal{M}(\Gamma(m^2N), k)$. Applying L_χ to $a_n z^{nt} = a_n e^{2\pi i n\tau t/N}$ contributes a factor of

$$\frac{1}{M} \sum_{x,y \bmod M} \chi(x) e^{2\pi i(n-x)y/M},$$

which is $\chi(n)$, since the sum over y is 0 for $x \neq n$. Thus $f_\chi = f|L_\chi$ is a form of level m^2N and divisor m^2t, and a cusp form (resp. Eisenstein series) if f is; it remains to check that the character is $\varepsilon\chi^2$. Let $R_n \in \Gamma'$, $R_n \equiv \begin{pmatrix} n^{-1} & 0 \\ 0 & n \end{pmatrix} \pmod{m^2N}$. Then $\begin{pmatrix} m & y \\ 0 & m \end{pmatrix} R_n \equiv R_n \begin{pmatrix} m & yn^2 \\ 0 & m \end{pmatrix} \pmod N$, so

$$\begin{aligned} f_\chi|R_n &= \frac{\varepsilon(n)}{M} \sum_{x,y \bmod M} \chi(xn^2) e^{-2\pi i x n^2 y/M} f| \begin{pmatrix} m & yn^2 \\ 0 & m \end{pmatrix} \\ &= (\varepsilon\chi^2)(n) f_\chi \end{aligned}$$

□

For example, we know the Eisenstein series of level 1 is associated to the Dirichlet series

$$\zeta(s)\zeta(s+1-k) = \sum_{n=1}^\infty \sigma_{k-1}(n) n^{-s};$$

if χ is a character modulo m, then

$$L(\chi, s)L(\chi, s+1-k) = \sum_{n_1} \chi(n_1) n_1^{-s} \sum_{n_1} \chi(n_2) n_2^{-s-1+k} = \sum_{n=1}^\infty \chi(n)\sigma_{k-1}(n) n^{-s}$$

is associated to an Eisenstein series of level m^2, divisor m^2 and character χ^2, and is an eigenfunction for the $T(n)$, $(n, m) = 1$. More generally:

Theorem 4.19. *The space of Dirichlet series associated to* $\mathcal{E}(N, k)$ *is generated by the series of form*

$$(t_1t_2)^{-s} L(\chi_1, s)L(\chi_2, s)$$

where $t_1, t_2 \mid N$, χ_j *is a character module* $\frac{N}{t_j}$, $(\chi_1\chi_2)(-1) = (-1)^k$, $L(\chi, s) = \sum_{n=1}^\infty \chi(n) n^{-s}$. *The corresponding Eisenstein series* E^{χ_1,χ_2} *has character* $\varepsilon = \chi_1\chi_2$, *divisor* $t = (t_1t_2, N)$, *and is an eigenfunction of the* $T(n)$, $(n, N) = 1$.

Proof. By Proposition 4.14, the Dirichlet series $\zeta_{c,d}(s)$ associated to $G_k(\tau; c, d; N)$ is (a constant times)

$$\zeta_{c,d}(s) = \sum_{n=1}^\infty n^{-s} \sum_{\substack{m\nu=n \\ m\equiv c\ (N)}} \operatorname{sgn}(\nu) \nu^{k-1} e^{2\pi i\nu d/N}.$$

Let $\zeta^{c,d}(s) = \frac{1}{N}\sum_{a \bmod N} e^{-2\pi iad/N}\zeta_{c,a}(s)$; the $\zeta^{c,d}(s)$ generate the same space. The coefficient of n^{-s} in $\zeta^{c,d}(s)$ is

$$\begin{aligned}
&\frac{1}{N}\sum_{a \bmod N} e^{-2\pi iad/N} \sum_{\substack{m\nu=n \\ m\equiv c\ (N)}} \operatorname{sgn}(\nu)\nu^{k-1}e^{2\pi ia\nu/N} \\
&\quad = \sum_{\substack{m\nu=n \\ m\equiv c \\ \nu\equiv d}} \operatorname{sgn}(\nu)\nu^{k-1} \\
&\quad = \sum_{\substack{m\nu=n \\ m\equiv c \\ \nu\equiv d,\nu>0}} \operatorname{sgn}(\nu)\nu^{k-1} + (-1)^k \sum_{\substack{m\nu=n \\ m\equiv -c \\ \nu\equiv -d,\nu>0}} \operatorname{sgn}(\nu)\nu^{k-1}
\end{aligned}$$

and so $\zeta^{c,d}(s) = \psi^{c,d}(s) + (-1)^k\psi^{-c,-d}(s)$, where

$$\psi^{c,d}(s) = \sum_{m\equiv c\ (N)} m^{-s} \sum_{n\equiv d\ (N)} n^{k-1-s}.$$

Now fix $t_1, t_2 \mid N$. Then the space generated by the $\zeta^{c,d}(s)$ with $(c,n) = t_1$ and $(d,N) = t_2$ is the same as that generated by the

$$L^{\chi_1,\chi_2}(s) = \sum_{b_i \bmod \frac{N}{t_i}} \chi_1(b_1)\chi_2(b_2)\zeta^{b_1t_1,b_2t_2}(s),$$

where χ_i is a character modulo $\frac{N}{t_i}$. Now

$$\begin{aligned}
&\sum_{b_i \bmod \frac{N}{t_i}} \chi_1(b_1)\chi_2(b_2)\psi^{b_1t_1,b_2t_2}(s) \\
&\quad = \sum_{b_i \bmod \frac{N}{t_i}} \chi_1(b_1)\chi_2(b_2)t_1^{-s}t_2^{k-1-s} \sum_{m\equiv b_1\ (\frac{N}{t_1})} m^{-s} \sum_{n\equiv b_2\ (\frac{N}{t_2})} n^{k-1-s} \\
&\quad = t_2^{k-1}L(\chi_1,s)L(\chi_2,s)(t_1t_2)^{-s}
\end{aligned}$$

hence

$$L^{\chi_1,\chi_2}(s) = t_2^{k-1}(1+(-1)^k(\chi_1\chi_2)(-1))(t_1t_2)^{-s}L(\chi_1,s)L(\chi_2,s).$$

This proves the theorem. □

Corollary 4.20. *$\mathcal{M}(\Gamma(N),k,\varepsilon,t)$ has a basis of eigenfunctions for all $T(n)$ with $(n,N)=1$.*

Proof. In view of the decomposition

$$\mathcal{M}(\Gamma(N),k,\varepsilon,t) = \mathcal{E}(N,k,\varepsilon,t) \oplus \mathcal{S}(N,k,\varepsilon,t),$$

and the fact we have already diagonalized the $T(n)$ on the cusp forms, we only have to diagonalize the $T(n)$ on the Eisenstein series; this is done by Theorem 4.19, in view of Theorem 4.11. □

That one cannot in general diagonalize the $T(p)$ for $p \mid N$ is shown by the following example. Let q be an odd prime, $N = q^3$, $t_1 = t_2 = q^2$, and χ_1, χ_2 characters modulo q with $(\chi_1\chi_2)(-1) = (-1)^k$. (They exist.) The theorem gives

an Eisenstein series

$$\begin{aligned} f(\tau) &= E^{\chi_1,\chi_2}(\tau) \\ &= a_0 + \sum_{q\nmid n} a_n e^{2\pi i n q^4\tau/q^3} \\ &= a_0 + \sum_{q\nmid n} a_n e^{2\pi i n q\tau}, \end{aligned}$$

with divisor $t = N = q^3$. Since $T(q)$ replaces the n^{th} Fourier coefficient by the $(nq)^{th}$, we have

$$h(\tau) = f|T(q)(\tau) = a_0 + \sum_{q\nmid n} a_n e^{2\pi i n\tau},$$

$h(\tau)|T(q) = 0$. Thus $T(q)$ has matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ on the space spanned by f, h, and so $T(q)$ is not diagonalizable.

Remark. We have shown that any form f of level N has an associated Dirichlet series, i.e. $a_n = O(n^{const.})$; by Theorem 4.19 if f is an Eisenstein series and by Proposition 4.13 if f is a cusp form.

5. A theorem of Weil

From now on we deal only with forms f of level N and maximal divisor $t = N$, i.e. $f(\tau+1) = f(\tau)$. If ε is a character modulo N, let $\mathcal{M}(N,k,\varepsilon) = \mathcal{M}(\Gamma(N),k,\varepsilon,N)$, and similarly (at least for $k \geq 3$) $\mathcal{S}(N,k,\varepsilon)$, $\mathcal{E}(N,k,\varepsilon)$. Thus if $f \in \mathcal{M}(N,k,\varepsilon)$, and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0'(N)$, i.e. $N|c$, then $f|\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varepsilon(d)\cdot f$; $f = 0$ unless $\varepsilon(-1) = (-1)^k$, since $f|\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = (-1)^k f$. Note $\mathcal{M}(\Gamma_0(N),k) = \mathcal{M}(N,k,1)$.

Let $H_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Note that $H_N \begin{pmatrix} a & b \\ c & d \end{pmatrix} H_N^{-1} = \begin{pmatrix} d & -c/N \\ -bN & a \end{pmatrix} \in \Gamma_0'(N)$ if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0'(N)$, and so:

(1) $\Gamma_*(N) = \Gamma_0(N) \cup \Gamma_0(N)\cdot H_N$ is a group (of substitutions of the upper half plane), containing $\Gamma_0(N)$ as a (normal) subgroup of index 2 (for $N > 1$).
(2) $f \mapsto f|H_N$ defines an isomorphism $\mathcal{M}(N,k,\varepsilon) \xrightarrow{\sim} \mathcal{M}(N,k,\bar{\varepsilon})$.
(3) In particular, if $\varepsilon = \bar{\varepsilon}$ is real (i.e. its values are ± 1), then $f \mapsto f|H_N$ is an automorphism of $\mathcal{M}(N,k,\varepsilon)$, and $f|H_N^2 = f|\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = (-1)^k f$.

We can diagonalize this representation of the group of order 2:

$$\mathcal{M}(N,k,\varepsilon) = \mathcal{M}^+(N,k,\varepsilon) \oplus \mathcal{M}^-(N,k,\varepsilon)$$

where $f \in \mathcal{M}^{\pm}(N,k,\varepsilon) \implies f|H_N = \pm i^k f$. ($f = f^+ + f^-$, where $f^+ = f + i^{-k} f|H_N$, $f^- = f - i^{-k} f|H_N$). If $f \in \mathcal{M}^{\pm}(N,k,\varepsilon)$, we will say f has a *functional equation*, or that f is a form for the extended group $\Gamma_*(N)$, of character ε and multiplier $C = \pm 1$. The $T(n)$, for $(n,N) = 1$, operate on $\mathcal{M}^{\pm}(N,k,\varepsilon)$, as follows from:

Lemma 5.1. *$H_N T(n) = \overline{\varepsilon(n)} T(n) H_N$, on $\mathcal{M}(N,k,\varepsilon)$*

Proof. $T(n) = n^{k/2-1}\sum L$, where $\bigcup \Gamma' L$ is all matrices of determinant n, and $L \equiv \begin{pmatrix} 1 & * \\ 0 & n \end{pmatrix} \pmod N$. Now $\bigcup \Gamma' H_N L H_N^{-1}$ is still disjoint, as one checks, and $H_N L H_N^{-1} \equiv \begin{pmatrix} n & * \\ 0 & 1 \end{pmatrix} \pmod N$, so $R_N H_N T(n) H_N^{-1} = T(n)$. □

The theorem of Weil [15] we are about to prove is in the spirit of Hecke's basic Theorem 1.2. When $N = 1$, $\Gamma = \Gamma_*(1)$ is generated by two elements $H_N = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, so modular forms for Γ are defined by two functional equations (plus regularity); periodicity (functional equation for U) gives an associated Dirichlet series $\varphi(s)$, and the functional equation for H_1 gives a functional equation for $\varphi(s)$, and vice versa. Weil's result is to characterize forms for $\Gamma_*(N)$, which has in general more than two generators, by functional equations for many associated Dirichlet series.

Besides Theorem 1.2, we need the notion of *Gauss sums*. Let χ be a character of *conductor* m, i.e. χ is a *primitive* character modulo m, i.e. χ is a character modulo m and not modulo any proper divisor of m. For $n \in \mathbf{Z}/m\mathbf{Z}$, we have the *Gauss sum*

$$g_\chi(n) = \sum_{x \bmod m} \chi(x) e^{2\pi i x n/m}$$

Let $g_\chi = g_\chi(1)$.

Proposition 5.2.

(1) $g_\chi(n) = \bar\chi(n) g_\chi$
(2) $|g_\chi| = \sqrt{m}$.

Proof. If $(n, m) = 1$, then

$$\chi(n) g_\chi(n) = \sum_{x \bmod m} \chi(nx) e^{2\pi i n x/m} = g_\chi,$$

as desired. Now suppose $(n, m) = t > 1$; we want to show $g_\chi(n) = 0$. Write $n_0 t = n$, $m_0 t = m$. Then

$$\begin{aligned} g_\chi(n) &= \sum_{x \bmod m_0 t} \chi(x) e^{2\pi i n_0 x/m_0} \\ &= \sum_{\substack{x_0 \bmod m_0 \\ (x_0, m)=1}} e^{2\pi i n_0 x_0/m_0} \sum_{\substack{y \equiv 1 \pmod{m_0} \\ y \bmod m}} \chi(x_0 y), \end{aligned}$$

and this is 0, since $\sum \chi(y) = 0$, because χ is a non-trivial character on the group of $y \equiv 1 \pmod{m_0}$, since χ is not a character modulo m_0. For (2),

$$\begin{aligned} |g_\chi|^2 = g_\chi \overline{g_\chi} &= \sum_{(x,m)=1} \chi(x) \sum_y \overline{\chi(xy)} e^{2\pi i x(1-y)/m} \\ &= \sum_{(x,m)=1} \overline{\chi}(y) e^{2\pi i x(1-y)/m} \end{aligned}$$

If $(x, m) > 1$, then $\sum_y \overline{\chi(xy)} e^{2\pi i x(1-y)/m} = e^{2\pi i x/m} \overline{g_\chi(x)} = 0$. Thus

$$|g_\chi|^2 = \sum_{x,y} \overline{\chi}(y) e^{2\pi i x(1-y)/m} = m,$$

since the sum over x is 0 for $y \neq 1$, m for $y = 1$. □

Now if $f(\tau)=\sum_{n=0}^{\infty}a_ne^{2\pi in\tau}$ is a Fourier series, and χ a character of conductor m, we define, as in Theorem 4.18,

$$f_\chi(\tau)=\sum_{n=0}^{\infty}a_n\chi(n)e^{2\pi in\tau}.$$

By the proof of Theorem 4.18, this is also

$$\begin{aligned}f_\chi(\tau)&=\frac{1}{m}\sum_{x,y \bmod m}\chi(x)e^{-2\pi ixy/m}f(\tau+\frac{y}{m})\\&=\frac{1}{m}\sum_{y \bmod m}g_\chi(-y)f(\tau+\frac{y}{m})\\&=\frac{g_\chi}{m}\sum_{y \bmod m}\chi(-y)(\tau+\frac{y}{m})\end{aligned}$$

Now let $a_0,a_1,a_2,\dots$ and $b_0,b_1,b_2,\dots$ be two sequences of complex numbers, $a_n,b_n=O(n^\sigma)$ for some $\sigma>0$, and form

$$f(\tau)=\sum_{n=0}^{\infty}a_ne^{2\pi in\tau}\qquad\varphi(s)=\sum_{n=1}^{\infty}a_nn^{-s}\qquad\Phi(s)=(2\pi)^{-s}\Gamma(s)\varphi(s)$$

$$g(\tau)=\sum_{n=0}^{\infty}b_ne^{2\pi in\tau}\qquad\psi(s)=\sum_{n=1}^{\infty}b_nn^{-s}\qquad\Psi(s)=(2\pi)^{-s}\Gamma(s)\psi(s)$$

Let $C\neq0$, $A>0$, $k>0$; recall that EBV means *entire and bounded in every vertical strip*.

Lemma 5.3. *Equivalent are:*

(A1) $\Phi(s)+A^{-s/2}\left(\frac{a_0}{s}+\frac{Cb_0}{k-s}\right)$ *is EBV, and* $\Phi(s)=CA^{\frac{k}{2}-s}\Psi(k-s)$

(B1) $f(\tau)=CA^{k/2}\left(\frac{A\tau}{i}\right)^{-k}g\left(\frac{-1}{A\tau}\right)$.

Proof. This is a reformulation of Theorem 1.2, with $A=\lambda^2$, $f_1(\tau)=f(\frac{\tau}{\lambda})$, $\Phi_1(s)=\lambda^s\Phi(s)$, etc. □

Now assume k is a positive integer, and so we have the notation $f|\begin{pmatrix}a&b\\c&d\end{pmatrix}$ for k. Letting $H_A=\begin{pmatrix}0&-1\\A&0\end{pmatrix}$, (B1) reads $f=Ci^kg|H_A$. The group ring $\mathbf{C}[GL^+(2,\mathbf{R})]=R$ operates on f by $f|\sum c_iL_i=\sum c_if|L_i$, and

$$\Omega_f=\{\omega\in R: f|\omega=0\}$$

is a right ideal in R.

We now change the notation. Given $a_0,a_1,a_2,\dots$, $a_n=O(n^\sigma)$, and a character χ of conductor m, define

$$f_\chi(\tau)=\sum_{n=0}^{\infty}\chi(n)a_ne^{2\pi in\tau},\quad L_\chi(s)=\sum_{n=1}^{\infty}\chi(n)a_nn^{-s},\quad\Lambda_\chi(s)=(\frac{2\pi}{m})^{-s}\Gamma(s)L_\chi(s).$$

For $m=1$, we write simply $f=f_1$, $L=L_1$, $\Lambda=\Lambda_1$. Letting $\alpha(x)=\begin{pmatrix}1&x\\0&1\end{pmatrix}$ for $x\in\mathbf{R}$, we have

$$f_\chi=\frac{g_\chi}{m}\sum_{y \bmod m}\overline{\chi}(-y)f|\alpha(\frac{y}{m}).$$

Let N be a fixed positive integer, and $C=\pm1$.

Lemma 5.4. *Equivalent are:*

(A2) $\Lambda(s) + N^{-s/2}\big(\frac{a_0}{s} + \frac{Ca_0}{k-s}\big)$ *is EBV, and* $\Lambda(s) = CN^{\frac{k}{2}-s}\Lambda(k-s)$
(B2) $1 \equiv Ci^k H_N \pmod{\Omega_f}$.

Proof. This is immediate from lemma 5.3, with $f = g$ etc., $A = N$. □

Lemma 5.5. *Equivalent are (for* $m > 1$, $C_\chi \neq 0$*):*

(A3) $\Lambda_\chi(s)$ *is EBV, and* $\Lambda_\chi(s) = C_\chi N^{\frac{k}{2}-s}\Lambda_{\overline{\chi}}(k-s)$
(B3) $g_\chi \sum_{y \bmod m} \overline{\chi}(y)\alpha(\frac{y}{m}) \equiv C_\chi i^k g_{\overline{\chi}} \sum \chi(y)\alpha(\frac{y}{m}) H_{m^2N} \pmod{\Omega_f}$.

Proof. Again immediate from lemma 5.3, with $A = m^2N$. □

Remark. If the a_n are real, then $\overline{\Lambda_\chi} = \Lambda_{\overline{\chi}}$, and $|c_\chi| = 1$ (if (A3) holds.)

Now suppose $(m, N) = 1$. Then for each a with $(a, m) = 1$, there exists a b with $abN \equiv -1 \pmod{m}$, and so

$$\gamma(a,b) = \begin{pmatrix} m & -b \\ -Na & n \end{pmatrix}$$

belongs to $\Gamma_0'(N)$, for some n. One computes

$$\alpha(\frac{a}{m})H_{Nm^2} = H_N \gamma(a,b)\alpha(\frac{b}{m}) \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix};$$

since b runs over $(b, m) = 1$, $b \bmod m$ as a does, and writing $\gamma(b) = \begin{pmatrix} m & -b \\ -Na & n \end{pmatrix} = \gamma(a, b)$, we see that (B3) is equivalent with

(B3') $$\sum_{b \bmod m} \overline{\chi}(b)\big(1 - \frac{C_\chi i^k g_{\overline{\chi}}}{g_\chi \chi(-N)} H_N \gamma(b)\big)\alpha(\frac{b}{m}) \equiv 0 \pmod{\Omega_f}.$$

($-abN \equiv 1 \ (m)$, so $\chi(x) = \overline{\chi}(-bN)$.)

Now let $f \in \mathcal{M}(N, k, \varepsilon)$, with functional equation $f = Ci^k f|H_N$ ($C = \pm 1$); here ε is a real character modulo N. Then $f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n\tau}$ with $a_n = O(n^\sigma)$ by the preceding chapter. Thus (B2) holds by hypothesis, so (A2) is true; also $\gamma(b) \equiv \varepsilon(n) = \varepsilon(m) \pmod{\Omega_f}$. Thus, taking $C_\chi = \frac{Cg_\chi \chi(-N)\varepsilon(m)}{g_{\overline{\chi}}}$, we see (B3') holds, and hence (A3). This proves:

Theorem 5.6. *Let* $f \in \mathcal{M}(N, k, \varepsilon)$ *with functional equation* $f = Ci^k f|H_N$, $C = \pm 1$ *(so* ε *is real). Then* Λ *satisfies* (A2)*, and* Λ_χ *satisfies* (A3)*, for every character* χ *whose conductor* m *is relatively prime to* N*, the values of* C_χ *being taken as*

$$C_\chi = C\varepsilon(m)\chi(-N)g_\chi/g_{\overline{\chi}}$$

We now turn to the converse, in a strong form: i.e. assuming the functional equation for L_χ for "sufficiently many" χ's. Let $\mathcal{M} = \{4, 3, 5, 7, 11, \dots\}$; any non-identity character χ modulo $m \in \mathcal{M}$ is primitive.

Lemma 5.7. *Let* $m \in \mathcal{M}$*, with* $(m, N) = 1$*; let* $C_m' \neq 0$*. Then equivalent are:*

(A4) *for every primitive* χ *modulo* m*,* (A3) *holds with* $C_\chi = \frac{C_m' \chi(-N) g_\chi}{i^k g_{\overline{\chi}}}$
(B4) $\lambda(b) \equiv \lambda(b') \pmod{\Omega_f}$*, whenever* $(b, m) = (b', m) = 1$*, where* $\lambda(b) = (1 - C_m' H_N \gamma(b))\alpha(\frac{b}{m})$*;*
(C4) $\sum_{b \bmod m} \overline{\chi}(b)\lambda(b) \equiv 0 \pmod{\Omega_f}$*, for every primitive* χ *modulo* m.

Proof. That (A4) is equivalent with (C4) follows from Lemma 5.5. Clearly (B4) implies (C4); conversely, given (C4), we have

$$0 \equiv \sum_{\chi,b} \big(\chi(b') - \chi(b'')\big)\overline{\chi}(b)\lambda(b) = \zeta(m)\big(\lambda(b') - \lambda(b'')\big)$$

where the sum is over all primitive χ, hence over all χ. □

The last key lemma is:

Lemma 5.8. *Let* $\gamma = \begin{pmatrix} m & -b \\ -aN & n \end{pmatrix} \in \Gamma_0'(N)$, *with* $m, n \in \mathcal{M}$. *Assume* (A4) *holds for* m *and* n, *with* $C_m' C_n' = (-1)^k$, *and assume* (A2) *holds. Then* $f|\gamma = \frac{Ci^k}{C_m'} f$.

Proof. Let $\gamma' = \begin{pmatrix} m & b \\ aN & n \end{pmatrix}$, so $\gamma' = \gamma(-b)$, $\gamma = \gamma(b)$ in the notation above. Now (A2), hence (B2), holds, so $1 \equiv Ci^k H_N \pmod{\Omega_f}$, and (A4), hence (B4), holds; taking $b, b' = b, -b$, we have $(1 - \xi\gamma)\alpha(\frac{b}{m}) \equiv (1 - \xi\gamma')\alpha(\frac{-b}{m})$ where $\xi = C_m' C i^{-k}$. Thus

$$1 - \xi\gamma' \equiv (1 - \xi\gamma)\alpha(\frac{2b}{m}) \pmod{\Omega_f}. \tag{1}$$

Now $\gamma^{-1} = \begin{pmatrix} n & b \\ Na & m \end{pmatrix}$, $\gamma'^{-1} = \begin{pmatrix} n & -b \\ -Na & m \end{pmatrix}$, so we get similarly ($m$ replaced by n):

$$(1 - \xi^{-1}\gamma^{-1}) \equiv (1 - \xi^{-1}\gamma'^{-1})\alpha(\frac{2b}{m}) \pmod{\Omega_f} \tag{2}$$

since $C_n' C i^{-k} = \xi^{-1}$. Thus

$$\begin{aligned} 1 - \xi\gamma' &= -(1 - \xi^{-1}\gamma'^{-1})\xi\gamma' \\ &\equiv -\xi(1 - \xi^{-1}\gamma^{-1})\alpha(\frac{-2b}{n})\gamma' && \text{by (2)} \\ &\equiv (1 - \xi\gamma)\gamma^{-1}\alpha(\frac{-2b}{n})\gamma' \\ &\equiv (1 - \xi\gamma)\alpha(\frac{2b}{m}), && \text{by (1).} \end{aligned}$$

Thus $(1 - \xi\gamma)(1 - \mu) \equiv 0 \pmod{\Omega_f}$, where

$$\mu = \gamma^{-1}\alpha(\frac{-2b}{n})\gamma'\alpha(\frac{2b}{m}) = \begin{pmatrix} 1 & \frac{-2b}{m} \\ \frac{2Na}{n} & \frac{4}{mn} - 3 \end{pmatrix}.$$

The eigenvalues of μ are the root of $x^2 - (\frac{4}{mn} - 2)x + 1$, and are imaginary but not roots of 1; thus μ is elliptic of infinite order. Hence, by Proposition 1.6, $f|(1 - \xi\gamma) = 0$. □

Theorem 5.9. *Let* $\mathcal{M}'$ *be a subset of* $\mathcal{M}$ *meeting every primitive arithmetic progression* $a + nb$, $(a, b) = 1$, *with* $(m, N) = 1$ *for* $m \in \mathcal{M}'$. *Let* ε *be a character modulo* N, *and* $C = \pm 1$. *Suppose* (A2) *is satisfied, and* (A3) *is satisfied for every character* χ *of conductor* $m \in \mathcal{M}'$, *with* $C_\chi = C\varepsilon(m)\chi(-N)g_\chi/g_{\overline{\chi}}$. *Then* $f \in \mathcal{M}(N, k, \varepsilon)$, *and* f *satisfies the functional equation* $f = Ci^k f|H_N$. *If* $L(s)$ *converges absolutely at* $s = k - \delta$ *for some* $\delta > 0$, *then* f *is a cusp form.*

Proof. (A2) holds, hence (B2), so $f = Ci^k f|H_N$. Let $\gamma = \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_0'(N)$. We are to show $f|\gamma = \varepsilon(d) \cdot f$. If $b = 0$, then $\gamma = \begin{pmatrix} a & 0 \\ Nc & d \end{pmatrix} = H_N \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} H_N^{-1}$ and $f = f|\gamma$, as desired. Assume now $b \neq 0$. Then $(a, Nb) = (d, Nb) = 1$, so

$$m = a + Nbs$$
$$n = d + Nbt$$

for some $m, n \in \mathcal{M}'$ and $s, t \in \mathbf{Z}$. Now (A4) holds, with $C_m' = Ci^k\varepsilon(m)$, $C_n' = Ci^k\varepsilon(n)$, so $C_m'C_n' = (-1)^k$. Let $\gamma' = \begin{pmatrix} 1 & 0 \\ Nt & 1 \end{pmatrix} \gamma \begin{pmatrix} 1 & 0 \\ Ns & 1 \end{pmatrix} = \begin{pmatrix} m & b \\ * & n \end{pmatrix} \in \Gamma_0'(N)$; then $f|\gamma' = \varepsilon(m)^{-1} f = \varepsilon(n) f = \varepsilon(d) f$, by Lemma 5.8. Hence

$$f|\gamma = f| \begin{pmatrix} 1 & 0 \\ -Nt & 1 \end{pmatrix} \gamma' \begin{pmatrix} 1 & 0 \\ -Ns & 1 \end{pmatrix} = f.$$

Thus f is formally a modular form for $\Gamma_0(N)$, with character ε, and with the desired functional equation; it remains to verify the regularity conditions at the cusps.

Lemma 5.10. *Let $f(\tau)$ be holomorphic in the upper half plane, satisfying*

(a) $f|L = f$ *for* $L \in \Gamma(N)$
(b) f *is holomorphic at* ∞, *i.e. at* 0 *in the variable* $z = e^{2\pi i\tau/N}$
(c) $f(x + iy) = O(y^{-\sigma})$ *as* $y \to 0$, *uniformly in* x.

Then $f(\tau)$ is a modular form of level N, and a cusp form if $\sigma < k$, and $f(\infty) = 0$.

Proof. Let $\tau_0 = L(\infty)$ be a rational cusp, where $L \in \Gamma$. By (a), $f|L$ has a Laurent expansion in $z = e^{2\pi i\tau/N}$:

$$f|L(\tau) = \sum_{n=-\infty}^{\infty} a_n z^n$$

and we want to show $a_n = 0$ for $n < 0$ (and also $a_0 = 0$ if $\sigma < k$.) Now

$$a_n = \int_{\tau_0}^{\tau_0+1} f|L(\tau) z^{-n} d\tau$$

Let $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$; note $c \neq 0$; let $\tau = u + ib$, where b is a large constant, $u_0 \leq u \leq u_0 + 1$. Then $x + iy = L(\tau)$, where $y = \frac{\operatorname{Im}\tau}{|c\tau+d|^2} = O(\frac{1}{b})$. Hence $f(L(\tau)) = O(b^\sigma)$, $f|L(\tau) = O(b^{\sigma-k})$, $a_n = O(b^{\sigma-k}e^{2\pi nb/N})$ as $b \to \infty$; thus $a_n = 0$ for $n < 0$, and $a_0 = 0$ if $\sigma < k$. □

Remark. It is reasonable that the condition (c), uniform in all x, should imply regularity at the cusps; we know the converse only for congruence subgroups, via the Eisenstein series.

Returning to the proof of Theorem 5.9, we are given $a_n = O(n^c)$, and so by Proposition 1.1, $f(x + iy) = O(y^{-c-1})$, and f is then a modular form, by the lemma. Finally, suppose $L(s)$ converges absolutely at $s = \sigma$, $\sigma < k$. Then $L(s)$ converges absolutely in the half plane $\operatorname{Re}(s) > \sigma$ and so $a_0 = 0$, by (A2). By the lemma, it suffices to show that $f(x + iy) = O(y^{-\sigma})$ as $y \to 0$. Now

$$s_n = \sum_{\nu=1}^{n} |a_\nu| \leq n^\sigma \sum_{\nu=1}^{\infty} |a_\nu| \nu^{-\sigma} = O(n^\sigma).$$

Hence

$$\begin{aligned}|f(x+iy)| &\le \sum |a_n| e^{-2\pi n y} \\ &\le (1-e^{2\pi y}) \sum s_n e^{-2\pi n y} \\ &= O(y) O(y^{-\sigma-1}) = O(y^{-\sigma}),\end{aligned}$$

(Cf. proof of Proposition 1.1.) □

Weil's theorem leads to a very interesting conjecture on the zeta-function of an elliptic curve E defined over $\mathbf{Q}$. This zeta-function can be written $\frac{\zeta(s)\zeta(s-1)}{L(s)}$, where $L(s) = \prod_p L_p(s)$, the local factor $L_p(s)$being defined as follows. If E has non-degenerate reduction at p (which will be the case for all but a finite number of the p), then $L_p(s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$, where $1 + p - a_p$ is the number of points on the reduced curve with coordinates in the field $\mathbf{F}_p$ of p elements. If the reduction of E at p is singular, we set $L_p(s) = 1$ if the singular point is a cusp, and $L_p(s) = (1 - a_p p^{-s})^{-1}$ if the singular point is a node, where $a_p = +1$ if the tangents at the double point are rational over $\mathbf{F}_p$, and $a_p = -1$ otherwise. One can define an integer $N = \prod_p p^{n_p}$, the *conductor* of E, with $n_p = 0$ if E is non-degenerate at p, $n_p = 1$ if the reduction has a node, and $n_p \ge 2$ if the reduction has a cusp (and $n_p = 2$ for $p \ne 2, 3$). The *Hasse-Weil conjecture* is that the hypotheses of Theorem 5.9 hold for $L(s)$, with N the conductor of E, $k = 2$, and $\varepsilon = 1$. It would then follow that $L(s)$ is associated to a form f of dimension -2 for $\Gamma_0(N)$, with a functional equation. Actually, one knows $|a_p| \le 2p^{1/2}$; this is the *Riemann hypothesis* for elliptic curves, proved by Hasse in 1934. Hence $L(s)$ converges for $\mathrm{Re}\,(s) > 3/2$, so f will be a cusp form. Note the agreement of the *Riemann hypothesis* and the *Petersson conjecture*. A good introduction to algebra-geometric aspects of this subject is Shimura [13] (and many other papers of Shimura.)

6. Quadratic forms

The most fruitful method of constructing modular forms of higher level is to form theta-series of positive integral quadratic forms. The basic references are Hecke's "Analytische Arithmetik der positiven quadratischen Formen" [5, No. 41], and Schoeneberg [12]; we will give only a very small part of the theory here.

Let

$$Q(x) = \frac{1}{2} x^t A x = \frac{1}{2} \sum_{i,j=1}^{r} a_{ij} x_i x_j, \quad x^t = (x_1, \dots, x_r), x_j \in \mathbf{R}, A = r \times r \text{ matrix}$$

be a positive definite integral quadratic form, i.e. $Q(x) > 0$ for $x \ne 0$, and $a_{ij} = a_{ji}$ is an integer, a_{ii} is an even integer, i.e. $A = (a_{ij})$ is an *integral symmetric matrix*. The *theta-function* associated to Q is

$$\vartheta(\tau; Q) = \sum_n e^{2\pi i Q(n)\tau} = 1 + \sum_{\nu=1}^{\infty} a_Q(\nu) e^{2\pi i \nu \tau}$$

where $n^t = (n_1, \dots, n_r) \in \mathbf{Z}^r$, and $a_Q(\nu)$ is the number of integral solutions of $Q(x) = \nu$. We will show eventually that $\vartheta(\tau; Q)$ is a modular form of dimension $-k$ of a certain level N, in the case where $r = 2k$ is even. Note $Q(x) \ge C \sum_{i=1}^r x_i^2$, for some $C > 0$, since Q is positive definite, and so $\vartheta(\tau; Q)$ is dominated term-by-term by-term

$$\sum_{n \in \mathbf{Z}^r} e^{-2\pi y C \sum n_i^2} = \Big(\sum_{m \in \mathbf{Z}} e^{-2\pi y C m^2} \Big)^r,$$

where $y = \operatorname{Im}\tau$, and so $\vartheta(\tau; Q)$ is a holomorphic function on the upper half plane.

A is the *matrix* of Q, its determinant D is the *determinant* of Q, and (if $r = 2k$ is even) $\Delta = (-1)^k D$ is the *discriminant* of Q.

Lemma 6.1. *Let $A = (a_{ij})$ be an integral symmetric matrix (a_{ii} even). If r is odd, then $D = \det A$ is even; if r is even, then $\Delta = (-1)^{r/2} D$ is $\equiv 0, 1 \pmod 4$.*

Proof. $D = \sum_\sigma \operatorname{sgn}(\sigma) a_{1\sigma_1} a_{2\sigma_2} \cdots a_{r\sigma_r}$, the sum ranging over all permutations σ of r letters. Since A is symmetric, the terms for σ and σ^{-1} are the same, and so cancel modulo 2 if $\sigma \neq \sigma^{-1}$, i.e. $\sigma^2 \neq 1$. If r is odd, any σ with $\sigma^2 = 1$ fixes some letter i, and since a_{ii} is even, we get $D \equiv 0 \pmod 2$. We leave the second statement, which we do not need, to the reader. □

Let A be integral symmetric, with $r = 2k$ even. Then $DA^{-1} = (A_{ij})$ is the cofactor mytrix, which is still integral symmetric, by the lemma. Thus DA^{-1} is again the matrix of an integral positive definite quadratic form $\frac{1}{2} x^t D A^{-1} x$. The least positive integer N with $NA^{-1} = A^*$ integral is the *level* (Stufe) of Q, and the corresponding quadratic form

$$Q^*(x) = \frac{1}{2} x^t N A^{-1} x$$

is the *adjoint form* to Q; note $N \mid D$, and $Q^*(x)$ is *primitive*; i.e. $\frac{1}{\nu} Q^*(x)$ is not integral for $\nu > 1$, i.e. the greatest common divisor of the coefficients $\frac{1}{2} a^*_{ii}$ and a^*_{ij} is 1. The adjoint Q^{**} of Q^* has matrix $A^{**} = N^* A^{*-1} = \frac{N^*}{N} A = \frac{1}{\beta} A$, where $\beta = gcd(\frac{1}{2} a_{ii}, a_{ij})$. In particular, if Q is primitive, then $N = N^*$, i.e. Q and its adjoint Q^* have the same level, and $Q^{**} = Q$. In general, $N^* \mid N$, and $D^* = N^{2k} D^{-1}$, so $D \mid N^{2k}$. Thus:

Proposition 6.2. *The determinant D and level N of Q satisfy $N \mid D \mid N^{2k}$; hence N and D have the same prime factors, and for a given level N and number of variables $2k$, there are only finitely many corresponding discriminants Δ.*

The basic result, due to Schoeneberg [12], which we prove eventually, is that $\vartheta(\tau; Q) \in \mathcal{M}(N, k, \varepsilon)$, where $\varepsilon(n) = \left(\frac{\Delta}{n}\right)$ (Jacobi symbol) for $n > 0$, $\varepsilon(-n) = (-1)^k \varepsilon(n)$; the two uses of the word level then agrees.

We also need a modified theta-function, using spherical functions. Let A be a symmetric positive definite real matrix of degree r, defining a quadratic form $x^t A x$. By linear change of variables $y = Bx$, we diagonalize the quadratic form:

$$\sum_{i=1}^{r} y_i^2 = x^t A x = y^t (B^{-1})^t A B^{-1} y$$

i.e. $I = (B^{-1})^t A B^{-1}$, or $A = B^t B$. (B is a real matrix.)

Now a function $f(x)$ is a *spherical function* with respect to the quadratic form $x^t A x$ if $\sum \frac{\partial^2 f}{\partial y_i^2} = 0$, i.e. $0 = \sum_{i,j,k} \frac{\partial^2 f}{\partial x_j \partial x_k} \frac{\partial x_j}{\partial y_i} \frac{\partial x_k}{\partial y_i}$. Letting $A^{-1} = (a^*_{ij})$, $B^{-1} = (b_{ij})$, we see $\sum_i \frac{\partial x_j}{\partial y_i} \frac{\partial x_k}{\partial y_i} = \sum_i b^*_{ji} b^*_{ki} = a^*_{jk}$, since $A^{-1} = B^{-1}(B^{-1})^t$, so $f(x)$ is a spherical function relative to Q if and only if $\sum a^*_{ij} \frac{\partial^2 f}{\partial x_j \partial x_k} = 0$.

There is an inner product on functions $f(x)$, $x \in \mathbf{R}^r$, by

$$\begin{aligned}(f, g)_A &= \int_{x^t A x \leq 1} f(x) \overline{g(x)} dx_1 \ldots dx_r \\ &= \frac{1}{|B|} \int_{y^t y \leq 1} f(x) \overline{g(x)} dy_1 \ldots dy_r\end{aligned}$$

Theorem 6.3. *Let $f(x)$ be a homogeneous polynomial of degree ν in $x_1, \dots, x_r$, with complex coefficients. Then the following statements are equivalent:*

(1) *$f(x)$ is a spherical function with respect to $x^t Ax$*
(2) *$f(x)$ is orthogonal (in the above inner product) to all homogeneous polynomials of degree $< \nu$.*
(3) *f is a linear sum of functions of the form $(\zeta^t Ax)^\nu$, where $\zeta \in \mathbf{C}^r$, $\zeta^t A\zeta = 0$.*

Proof. Translating (3) into variables y, if we let $\eta = B\zeta$, then $\zeta^t A\zeta = \eta^t\eta$, and $\zeta^t Ax = \eta^t y$; thus we can assume without loss of generality that $A = I$ is the identity.

If (3) holds, then so does (1), since

$$\sum \frac{\partial^2 f}{\partial x_i^2} = \sum \frac{\partial^2}{\partial x_i^2}(\sum \zeta_j x_j)^\nu = \nu(\nu-1)(\sum \zeta_i^2)(\quad)^{\nu-2} = 0 \quad \text{if } \sum \zeta_i^2 = 0.$$

In general, f is homogeneous of degree ν, and so $\sum \frac{\partial f}{\partial x_i} \cdot x_i = \nu f$; hence the divergence theorem gives:

1) $$\nu \int_{\partial K} f\omega = \int_{\partial K} (\sum_i \frac{\partial f}{\partial x_i} \cdot x_i)\omega = \int_K \Delta f dx$$

where $K : \sum x_i^2 \le 1$, $\partial K : \sum x_i^2 = 1$, $\Delta f = \sum \frac{\partial^2 f}{\partial x_i^2}$ and $\omega = \sum x_i\omega_i$, $\omega_i = (-1)^{i-1} dx_1 \dots \widehat{dx_i} \dots dx_r$, $dx = dx_i\omega_i = dx_1 \dots dx_r$. Δ satisfies

2) $$\Delta(fg) = f\Delta g + g\Delta f + 2\sum \frac{\partial f}{\partial x_i}\frac{\partial g}{\partial x_i}.$$

By Stokes' theorem,

$$\int_{\partial K} f\omega = \int_{\partial K} \sum f x_i \omega_i = \int_K \sum \frac{\partial}{\partial x_i}(f x_i) dx = (\nu + r)\int_K f dx.$$

Thus:

3) $$\int_K \Delta f = \nu(\nu + r)\int_K f.$$

We now prove (1) $\implies$ (2) by induction on ν. Note that $\Delta f = 0 \implies \Delta(\frac{\partial f}{\partial x_i}) = 0$. Assuming $\Delta f = 0$, and $\deg(g) < \deg(f)$:

$$\begin{aligned} \int_K fg &= (\quad)\int_K \Delta(fg), && \text{by 3)} \\ &= (\quad)\int_K f\Delta g, && \text{by 2) and induction} \\ &= (\quad)\int_K f\Delta^2 g = \dots = 0. \end{aligned}$$

Finally, to show (2) $\implies$ (3), let f be orthogonal to all g of lower degree, and orthogonal to all $(\zeta^t x)^\nu$, where $\zeta^t\zeta = 0$; we are to show $f = 0$. Let $g(x) = (\zeta^t x)^\nu$; then g and all of its partial derivatives satisfy (3), hence (1) and (2). Then

$$\begin{aligned} 0 = \int_K fg &= (\quad)\int_K \Delta(fg) = (\quad)\int_K \sum \frac{\partial f}{\partial x_i}\frac{\partial g}{\partial x_i} \\ &= \dots = (\quad)\int_K \sum \frac{\partial^\nu f}{\partial x_{i_1}\dots\partial x_{i_\nu}}\frac{\partial^\nu g}{\partial x_{i_1}\dots\partial x_{i_\nu}}. \end{aligned}$$

Now iteration of $\nu f = \sum \frac{\partial f}{\partial x_i} \cdot x_i$ gives $\nu! f = \sum \frac{\partial^\nu f}{\partial x_{i_1} \dots \partial x_{i_\nu}}$, $\nu! \zeta_{i_1} \dots \zeta_{i_\nu} = \frac{\partial^\nu g}{\partial x_{i_1} \dots \partial x_{i_\nu}}$, so the above gives simply that $f(\zeta) = 0$ when $\zeta^t \zeta = 0$, and hence $f(x)$ is divisible by $\delta(x) = x^t x = \sum x_i^2$, say $f(x) = \delta(x) g(x)$. Then, from the equation 1) and 3):

$$\begin{aligned} \int_K g\overline{g} &= (\quad) \int_{\partial K} g\overline{g}\omega \\ &= (\quad) \int_{\partial K} \delta g\overline{g}\omega \qquad\qquad \text{since } \delta = 1 \text{ on } \partial K \\ &= (\quad) \int_K f\overline{g} = 0. \end{aligned}$$

Thus $g = 0$, so $f = 0$. □

Corollary 6.4. *The space H_ν of spherical functions which are homogeneous polynomials of degree ν has dimension*

$$\binom{r-1+\nu}{r-1} - \binom{r-3+\nu}{r-1}$$

Proof. Let P_ν be the homogeneous polynomials of degree ν. Then $H_\nu = \{f \in P_\nu : f \perp P\mu \text{ for } \mu < \nu\}$. Now $P_\mu \perp P_\nu$ if $\mu + \nu$ is odd, so given $f \in P_\nu$, $f \in H_\nu \iff f \perp P_{\nu-2}, P_{\nu-4}, \dots$. On the other hand, $(f, g) = (\quad)(f, \delta g)$, so $f \in H_\nu \iff f \perp P_{\nu-2}$; thus $\dim H_\nu = \dim P_\nu - \dim P_{\nu-2} = \binom{r-1+\nu}{r-1} - \binom{r-1+\nu-2}{r-1}$. □

Given an integral positive definite quadratic form $Q(x) = \frac{1}{2} x^t A x$, and $P(x)$ a spherical function of order ν with respect to Q, we have a *theta-series*

$$\vartheta(\tau; Q, P) = \sum_{n \in \mathbf{Z}^r} P(n) e^{2\pi i Q(n)\tau}$$

which we will prove is a modular form with character ε for $\Gamma_0(N)$, of dimension $-(k+\nu)$ (if $r = 2k$ is even), and a cusp form if $\nu > 0$. The introduction of the $P(x)$ is somewhat like passing from zeta-functions to L-series by introducing characters.

Proposition 6.5. *Given a positive definite symmetric real matrix A of degree r, $Q(x) = \frac{1}{2} x^t A x$, define*

$$\vartheta(\tau, x) = \sum_{n \in \mathbf{Z}^r} e^{2\pi i Q(n+x)\tau}$$

for a parameter $x \in \mathbf{R}^r$. Then

$$\vartheta(\tau, x) \left(\frac{\tau}{i}\right)^{r/2} = \frac{1}{\sqrt{D}} \sum_n e^{2\pi i n^t x - (\pi i/\tau) n^t A^{-1} n}.$$

Proof. (Cf. the same result for $r = 1$ in Chapter 1.)

$$\begin{aligned} \vartheta(\tau, x) &= \text{periodic function of } x \\ &= \text{its Fourier series} \\ &= \sum_{m \in \mathbf{Z}^r} a_m e^{2\pi i m^t x} \end{aligned}$$

where

$$\begin{aligned} a_m &= \int_0^1 \cdots \int_0^1 \vartheta(\tau, x) e^{-2\pi i m^t x} dx_1 \dots dx_r \\ &= \int_{-\infty}^1 \cdots \int_{-\infty}^1 e^{\pi i \tau x^t A x - 2\pi i m^t x} dx_1 \dots dx_r. \end{aligned}$$

Completing the square,

$$\tau(x-\tau^{-1}A^{-1}m)^tA(x-\tau^{-1}A^{-1}m)=\tau x^tAx-2m^tx+\tau^{-1}m^tA^{-1}m.$$

Hence $a_m=e^{-\pi i\tau^{-1}m^tA^{-1}m}b_m$, where

$$\begin{aligned}b_m&=\int_{\mathbf{R}^r}e^{\pi i\tau(x-\tau^{-1}A^{-1}m)^tA(x-\tau^{-1}A^{-1}m)}dx\\&=\int_{\mathbf{R}^r}e^{\pi i\tau x^tAx}dx, &&\text{by Cauchy's theorem}\\&=\frac{1}{\sqrt{D}}\int_{\mathbf{R}^r}e^{\pi i\tau y^ty}dy,\end{aligned}$$

where $y=Bx$, $dy=|B|dx$, $A=B^tB$

$$\begin{aligned}&=\frac{1}{\sqrt{D}}\left(\int_{-\infty}^{\infty}e^{2\pi i\tau u^2}du\right)^r\\&=\frac{1}{\sqrt{D}}\left(\frac{\tau}{i}\right)^{-r/2}\end{aligned}$$

□

Corollary 6.6. *If $Q(x)$ is integral in $r=2k$ variables, then*

$$\vartheta(\tau,Q)\left(\frac{\tau}{i}\right)^k=D^{-1/2}\vartheta\left(\frac{-1}{N\tau},Q^*\right).$$

Proof. Set $x=0$, and note Q^* has matrix NA^{-1}. □

We now generalize the above corollary to $\vartheta(\tau;Q,P)=\sum P(n)e^{2\pi iQ(n)\tau}$, where $P(x)$ is a spherical function relative to $Q(x)$. From now on, $Q(x)$ will always be an integral positive definite quadratic form in an even number $2k$ of variables.

We take first a typical spherical function $P(x)=(\zeta^tAx)^\nu$, where $Q(\zeta)=0$. The transformed theta-function will involve $P^*(x)=P(A^{-1}x)=(\eta^tA^{-1}x)^\nu$, where $\eta=A\zeta$ satisfies $\eta^tA^{-1}\eta=\zeta^tA\zeta=0$, i.e. $Q^*(\eta)=0$; thus $P^*(x)$ is a spherical function relative to $Q^*(x)$.

We start with $\vartheta(\tau,x)=\sum_n e^{2\pi iQ(n+x)\tau}$ and apply $L=\sum\zeta_i\frac{\partial}{\partial x_i}$, ν times. Note $LQ(x)=\zeta^tAx$, $L^2Q(x)=\zeta^tA\zeta=0$. Thus:

$$L^\nu\vartheta=\sum_n(2\pi i\tau)^\nu(\zeta^tA(xn+x))^\nu e^{2\pi iQ(n+x)\tau} \tag{1}$$

But by the transformation formula (Proposition 6.5), we have also

$$\vartheta=\left(\frac{\tau}{i}\right)^{-k}D^{-1/2}\sum_n e^{(-\pi i/\tau)n^tA^{-1}n+2\pi in^tx}$$

and hence

$$L^\nu\vartheta=\left(\frac{\tau}{i}\right)^{-k}D^{-1/2}(2\pi i)^\nu\sum_n(\zeta^tn)^\nu e^{(-\pi i/\tau)n^tA^{-1}n+2\pi in^tx} \tag{2}$$

and since $P^*(x)=P(A^{-1}x)=(\zeta^tx)^\nu$, we have proved for the spherical function and hence (by Theorem 6.3) for any spherical function $P(x)$, by comparing (1) and (2):

Theorem 6.7 (Schoeneberg)**.** *If $P(x)$ is a spherical function for $Q(x)$, and $P^*(x)=P(A^{-1}x)$ the adjoint function (a spherical function for $Q^*(x)$), then:*

$$\sum_n P(n+x)e^{2\pi iQ(n+x)\tau}=\frac{i^k}{\sqrt{D}\tau^{k+\nu}}\sum_n P^*(x)e^{(-\pi i/\tau)n^tA^{-1}n+2\pi in^tx}$$

This suggests our 'k' will be $k+\nu$, so we set

$$f|\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = (ad-bc)^{\frac{k+\nu}{2}}(c\tau+d)^{-(k+\nu)} f\Big(\frac{a\tau+b}{c\tau+d}\Big);$$

setting $x=0$ above, and $H_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ as usual, we have

$$\begin{aligned}\vartheta(\tau;Q,P) &= \frac{i^k}{\sqrt{D}\tau^{k+\nu}}\vartheta\Big(\frac{-1}{N\tau};Q^*,P^*\Big)\\ &= \frac{i^k N^{\frac{k+\nu}{2}}}{\sqrt{D}}\vartheta(\tau;Q^*,P^*)|H_N\end{aligned}$$

Thus:

Corollary 6.8.

$$\vartheta(\tau;Q,P) = \frac{i^k N^{\frac{k+\nu}{2}}}{\sqrt{D}}\vartheta(\tau;Q^*,P^*)|H_N$$

Taking $x=\frac{h}{N}$, where $h^t=(h_1,\dots,h_{2k})$ is integral, the formula of Theorem 6.7 reads:

$$\begin{aligned}\vartheta(\tau;Q,P,h) &:= N^{-\nu}\sum_{n\equiv h\ (N)} P(n)e^{2\pi i Q(n)\tau/N^2} \\ &= \frac{i^k}{\sqrt{D}\tau^{k+\nu}}\sum_n P^*(n)e^{(-\pi i/\tau)n^tA^{-1}n+2\pi i n^t h/N}.\end{aligned} \tag{3}$$

On the right, substitute $m=NA^{-1}n$. Then m is integral, and $Am\equiv 0\pmod N$; on the other hand, if m is integral, and $Am\equiv 0\pmod N$, then $n=N^{-1}Am$ is integral. Also, $P^*(n)=P(A^{-1}n)=N^{-\nu}P(m)$. The right side of (3) is thus:

$$\frac{i^k}{\sqrt{D}\tau^{k+\nu}N^\nu}\sum_{\substack{m\\ Am\equiv 0\ (N)}} P(m)e^{(-2\pi i/\tau)Q(m)/N^2+2\pi i m^tAh/N^2} \tag{4}$$

Now suppose $Ah\equiv 0\pmod N$. Then $e^{2\pi i m^tAh/N^2}$ depends only on m modulo N, so (4) becomes:

$$\frac{i^k}{\sqrt{D}\tau^{k+\nu}}\sum_{\substack{g \bmod N\\ Ag\equiv 0\ (N)}} e^{2\pi i g^tAh/N^2}\vartheta\Big(\frac{-1}{\tau};Q,P,g\Big). \tag{5}$$

This proves:

Corollary 6.9. *For an integral vector h with $Ah\equiv 0\pmod N$, define*

$$\vartheta(\tau;Q,P,h) = N^{-\nu}\sum_{n\equiv h\ (N)} P(n)e^{2\pi i Q(n)\tau/N^2}.$$

(Note $\vartheta(\tau;Q,P,0)=\vartheta(\tau;Q,P)$.) Then

$$\vartheta(\tau;Q,P,h) = \frac{i^k}{\sqrt{D}}\sum_{\substack{g \bmod N\\ Ag\equiv 0\ (N)}} e^{2\pi i g^tAh/N^2}\vartheta(\tau;Q,P,g)|H_1$$

We also have obviously that

$$\vartheta(\tau+1;Q,P,h) = e^{2\pi i Q(h)/N^2}\vartheta(\tau;Q,P,h)$$

Hence the vector space generated by the $\vartheta(\tau; Q, P, h)$ is operated on by the full modular group Γ. These series are clearly regular at ∞, and vanishing at ∞ if $\nu > 0$. Hence we only need to check their invariance under $\Gamma(N)$ to know they are modular forms of level N (cusp forms if $\nu > 0$).

Remark. Suppose $N = 1$, i.e. $D = 1$. Then $\vartheta(\tau + 1; Q) = \vartheta(\tau; Q)$ and $\vartheta(\tau; Q) = (\frac{\tau}{i})^{-k}\vartheta(\frac{-1}{\tau}; Q)$. By Chapter 1, we know $i^k = 1$, i.e. $4 \mid k$; the number of variables is thus divisible by 8. We have $\vartheta(\tau, Q)$ is a modular form of dimension $-k$ and level 1. An example with $r = 8$ is

$$Q(x) = \frac{1}{2}\sum_{i=1}^{8} x_i^2 + \frac{1}{2}(\sum_{i=1}^{8} x_i)^2 - x_1x_2 - x_2x_8,$$

with $\vartheta(\tau, Q) = 1 + \sum_{\nu=1}^{\infty} a_Q(\nu)e^{2\pi i\nu\tau}$. Since $\dim \mathcal{M}(\Gamma, 4) = 1$, we have necessarily

$$\vartheta(\tau, Q) = E_4(\tau) = 1 + 240\sum_{\nu=1}^{\infty} \sigma_3(\nu)e^{2\pi i\nu\tau},$$

so Q has representation numbers $a_Q(\nu) = 240\sigma_3(\nu)$. Similarly, if Q has 16 variables, then $a_Q(\nu) = 480\sigma_7(\nu)$. For $k = 12$, Siegel has proved there exists two forms Q_1, Q_2 in 24 variables with discriminant 1 and different theta-series; then

$$\vartheta(\tau; Q_1) - \vartheta(\tau; Q_2) = \sum_{\nu=1}^{\infty}(a_{Q_1}(\nu) - a_{Q_2}(\nu))e^{2\pi i\nu\tau}$$

is a non-zero cusp form of dimension -12, i.e. $c\Delta(\tau)$, $c \neq 0$. Ramanujan's conjecture can be thought of an assertion about the differences $a_{Q_1}(\nu) - a_{Q_2}(\nu)$. In general, if $Q(x)$ is a form of discriminant 1 in $2k$ variables ($4 \mid k$), then

$$\vartheta(\tau, Q) = E_k(\tau) + g(\tau)$$

where $g(\tau)$ is a cusp form. In terms of Fourier coefficients, we have

$$a_Q(\nu) = A_k\sigma_{k-1}(\nu) + b_\nu$$

where $b_\nu = O(\nu^{k/2})$, by Proposition 4.13, so the theory of modular forms gives asymptotic results about the representation numbers $a_Q(\nu)$.

Returning to our general development, besides the rules above, we also have, for any natural number c:

$$\vartheta(\tau; Q, P, h) = \sum_{\substack{g \equiv h \ (N) \\ g \bmod cN}} \vartheta(c\tau; cQ, P, g) \tag{6}$$

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma'$, with $c > 0$. Then $c\frac{a\tau+b}{c\tau+d} = a - \frac{1}{c\tau+d}$, so:

$$\begin{aligned}\vartheta(\tau; Q, P, h)|\begin{pmatrix} a & b \\ c & d \end{pmatrix} &= (c\tau+d)^{-(k+\nu)} \sum_{\substack{g \equiv h\ (N) \\ g \bmod cN}} \vartheta(a - \frac{1}{c\tau+d}; cQ, P, g) \\ &= \sum_{\substack{g \equiv h\ (N) \\ g \bmod cN}} \frac{e^{2\pi i a Q(g)/cN^2}}{(c\tau+d)^{k+\nu}} \vartheta(\frac{-1}{c\tau+d}; cQ, P, g) \\ &= \frac{i^k(-1)^{k+\nu}}{c^k\sqrt{D}} \sum_{\substack{g \equiv h\ (N) \\ g \bmod cN}} e^{2\pi i a Q(g)/cN^2} \times \\ &\sum_{\substack{\ell \bmod cN \\ A\ell \equiv 0\ (N)}} e^{2\pi i \ell^t A g/cN^2} \vartheta(c\tau+d; cQ, P, \ell)\end{aligned}$$

(The last by Corollary 6.9; the determinant of cQ is $c^{2k}D$.) Thus:

$$\vartheta(\tau; Q, P, h)|\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{i^{-k-2\nu}}{c^k\sqrt{D}} \sum_{\substack{\ell \bmod cN \\ A\ell \equiv 0\ (N)}} \zeta(h, \ell)\vartheta(c\tau; cQ, P, \ell) \tag{7}$$

where

$$\zeta(h, \ell) = \sum_{\substack{g \equiv h\ (N) \\ g \bmod cN}} e^{2\pi i(aQ(g) + \ell^t A g + dQ(\ell))/cN^2} \tag{8}$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma'$, $c > 0$. One computes:

$$\zeta(h, \ell) = e^{-2\pi i(h^t A\ell + dQ(\ell))b/N^2}\zeta(h + d\ell, 0). \tag{9}$$

This shows that $\zeta(h, \ell)$ depends only on ℓ modulo N; hence, using (6), we rewrite (7) as

$$\vartheta(\tau; Q, P, h)|\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{i^{-k-2\nu}}{c^k\sqrt{D}} \sum_{\substack{\ell \bmod N \\ A\ell \equiv 0\ (N)}} \zeta(h, \ell)\vartheta(\tau; Q, P, \ell) \tag{10}$$

In particular, if $d \equiv 0 \pmod N$, then (10) becomes

$$\vartheta(\tau; Q, P, h)|\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{\zeta(h, 0)}{i^{k+2\nu}c^k\sqrt{D}} \sum_{\substack{\ell \bmod N \\ A\ell \equiv 0\ (N)}} e^{-2\pi i h^t A\ell \cdot b/N^2} \vartheta(\tau; Q, P, \ell) \tag{11}$$

and applying $H_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, we get

$$\vartheta(\tau; Q, P, h)|\begin{pmatrix} b & -a \\ d & -c \end{pmatrix} = \frac{\zeta(h, 0)}{(-1)^k c^k D} \sum_{\ell, g} e^{2\pi i \ell^t A(g - bh)/N^2} \vartheta(\tau; Q, P, g) \tag{12}$$

Now $\sum_{\substack{\ell \bmod N \\ A\ell \equiv 0\ (N)}} e^{2\pi i \ell^t A(g-bh)/N^2}$ is a character sum on a finite group with D elements, so this sum is D if $g \equiv bh \pmod N$ and 0 otherwise. Thus (12) becomes:

$$\vartheta(\tau; Q, P, h)|\begin{pmatrix} b & -a \\ d & -c \end{pmatrix} = \frac{\zeta(h, 0)}{(-c)^k}\vartheta(\tau; Q, P, bh) \tag{13}$$

for $c > 0$ and $N \mid D$. This then holds also for $c < 0$, since if we replace $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ by $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$, this gives a factor of $(-1)^{k+\nu}$ on both sides of (13), since $\vartheta(-h) = (-1)^\nu \vartheta(h)$. Changing the notation,

$$\vartheta(\tau; Q, P, h)|\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{\varphi(h)}{d^k}\vartheta(\tau; Q, P, ah), \tag{14}$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0'(N)$, where (cf. (8))

$$\varphi(h) = \sum_{\substack{g \equiv h \ (N) \\ g \bmod dN}} e^{2\pi i b Q(g)/dN^2} \tag{15}$$

In this sum, we can write $g = adh + Ng_1$, $g_1 \bmod d$, and (15) becomes

$$\varphi(h) = e^{2\pi i a b Q(h)/N^2} \sum_{g_1 \bmod d} e^{2\pi i b Q(g_1)/d} \tag{16}$$

Thus, (14) becomes

$$\vartheta(\tau; Q, P, h)|\begin{pmatrix} a & b \\ c & d \end{pmatrix} = e^{2\pi i a b Q(h)/N^2}\vartheta(\tau; Q, P, ah)\Phi(b, d) \tag{17}$$

where $\Phi(b, d) = d^{-k}\sum_{g \bmod d} e^{2\pi i b Q(g)/d}$, for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0'(N)$.
In order to investigate the $\Phi(b, d)$ further, let us take $P = 1$, $h = 0$, so we know $\vartheta(\tau; Q, P, h) = \vartheta(\tau; Q) \neq 0$. Applying $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ to both sides of (17), we find $\Phi(b, d) = \Phi(b + na, d + nc)$ is in the field of $(d + nc)^{th}$ roots of 1 for all $n \geq 1$ and hence $\Phi(b, d)$ is rational. Applying the automorphism $e^{2\pi i b/d} \mapsto e^{2\pi i/d}$, we find $\Phi(b, d) = \Phi(1, d) = \varepsilon(d)$. Finally, since $\begin{pmatrix} a & bc' \\ N & d \end{pmatrix} \in \Gamma_0'(N)$ if $\begin{pmatrix} a & b \\ Nc' & d \end{pmatrix} \in \Gamma_0'(N)$, we see $\varepsilon(d)$ depends only on d modulo N. We have proved:

Theorem 6.10 (Schoeneberg)**.** *We have*

$$\vartheta(\tau; Q, P, h)|\begin{pmatrix} a & b \\ c & d \end{pmatrix} = e^{2\pi i a b Q(h)/N^2}\varepsilon(d)\vartheta(\tau; Q, P, ah)$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0'(N)$*, where* ε *is a real character modulo* N*, satisfying* $\varepsilon(-1) = (-1)^k$*. In particular, taking* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma'(N)$*,*

$$\vartheta(\tau; Q, P, h)|\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \vartheta(\tau; Q, P, h),$$

and hence $\vartheta(\tau; Q, P, h)$ *is a modular form of dimension* $-(k + \nu)$*, of level* N*, and a cusp form if* $\nu > 0$*.*

It remains to determine $\varepsilon(d)$ for $d > 0$ (we know $\varepsilon(-1) = (-1)^k$). We have

$$\varepsilon(d) = d^{-k} \sum_{g \bmod d} e^{2\pi i Q(g)/d},$$

and $\varepsilon(d)$ depends only on d modulo N. Let p be an odd prime with $p \equiv d \pmod N$ and so that $Q(x)$ can be diagonalized modulo p with integers, say $Q(x) \equiv \sum_j a_j x_j^2$

(mod p), where $a_j \in \mathbf{Z}$. Then

$$\begin{aligned}\varepsilon(d) = \varepsilon(p) &= p^{-k} \sum_{j=1}^{2k} \sum_{g_j=1}^{p} e^{2\pi i \sum a_j g_j^2/p} \\ &= p^{-k} \prod_{j=1}^{2k} \sum_{g_j \bmod p} e^{2\pi i a_j g_j^2/p} \\ &= p^{-k} \prod_{j=1}^{2k} \sum_{z_j \bmod p} \left(1 + \left(\frac{z_j}{p}\right)\right) e^{2\pi i a_j z_j/p}\end{aligned}$$

where $\left(\frac{z_j}{p}\right) = \chi(z_j)$ is the *Legendre symbol*, i.e. $\left(\frac{z_j}{p}\right) = 0, 1, -1$ as $p \mid z_j$, $x^2 \equiv z_j$ (mod p) is solvable, or otherwise. Note that $D \equiv \prod_{j=1}^{2k}(2a_j)$ (mod p); hence $p \nmid a_j$ (otherwise $p \mid D$, $p \mid N$, $p \mid d$, contrary to $(d, N) = 1$). Thus $\sum_{z_j \bmod p} e^{2\pi i a_j z_j/p} = 0$, and the above becomes:

$$\begin{aligned}\varepsilon(d) = \varepsilon(p) &= p^{-k} \prod_{j=1}^{2k} \sum_{z_j \bmod p} \chi(z_j) e^{2\pi i a_j z_j/p} \\ &= p^{-k} \prod_{j=1}^{2k} g_\chi(a_j) && \text{(Gauss sums)} \\ &= p^{-k} \prod_{j=1}^{2k} (\chi(a_j) g_\chi), && \text{by Proposition 5.2} \\ &= p^{-k} g_\chi^{2k} \chi(D),\end{aligned}$$

since $D \equiv \prod_{j=1}^{2k}(2a_j)$ (mod p). Now $p = |g_\chi|^2 = g_\chi \overline{g}_\chi = \chi(-1) g_\chi^2$, so we have finally that

$$\varepsilon(d) = \varepsilon(p) = \chi((-1)^k D) = \chi(\Delta).$$

Thus we have proved that $\varepsilon(d) = \left(\frac{\Delta}{p}\right)$ for any prime p which is sufficiently large and satisfies $p \equiv d$ (mod N). Hence Δ is a *discriminant*, we necessarily have $\Delta \equiv 0, 1$ (mod 4), and $\varepsilon(d) = \left(\frac{\Delta}{d}\right)$ (Jacobi symbol). (Here we are appealing to basic facts about quadratic number fields; if $\Delta \equiv 2, 3$ (mod 4), then the conductor N' of $\left(\frac{\Delta}{x}\right)$ is 4 or 8 times some of the odd primes dividing D, whence N' does not divide N, since $N \mid D$. Cf., e.g., Hecke's book [6, Chapter VII.]) Thus:

Theorem 6.11. *$\Delta \equiv 0, 1$ (mod 4), and $\varepsilon(d) = \left(\frac{\Delta}{d}\right)$ for $d > 0$.*

Remark. As sketched earlier for the case $N = 1$, one gets asymptotic results on the representation numbers $a_Q(\nu)$ by writing $\vartheta(\tau, Q)$ as an Eisenstein series plus a cusp form.

Finally, the theory of the $T(n)$ gives a way of deriving knowledge of the representation numbers $a_Q(n)$ from those for primes. Starting from

$$f_1(\tau) = \vartheta(\tau, Q) = \sum_{n=0}^{\infty} a_Q(n) e^{2\pi i n \tau},$$

one gets a basis $f_1, \ldots, f_r$ for the least space $V(Q)$ containing $\vartheta(\tau, Q)$ and closed under all $T(n)$, $(n, N) = 1$, by taking $f_j = f_1 | T(n_j)$ for suitable integers $1 = n_1 < n_2 < \cdots < n_r$. Note each f_j has integral Fourier coefficients; hence we can diagonalize the $T(n)$ over a certain number field K. Thus certain K-linear sums $g_1, \ldots, g_r$ of $f_1, \ldots, f_r$ will be eigenfunctions for the $T(n)$, $(n, N) = 1$, and hence their Fourier coefficients a_n, $(n, N) = 1$, are known once the a_p, $p \nmid N$, are known

(for $g_1, \ldots, g_r$). Furthermore, one can determine $f_2, \ldots, f_r$, $g_1, \ldots, g_r$ from Q by a finite process. For details and examples, we refer again to Hecke's "Analytische Arithmetik der positiven quadratischen Formen" [5, No. 41].

Corrected typos in Ogg's book

Typos in Ogg's book [8] are listed with reference to the chapter, page, line (from the top > 0, from the bottom < 0). They have been corrected in this TEX edition. Typos occurring on several lines repeatedly have only been listed once (like $\tau' = -1/\tau + 1$ instead of $\tau' = -1/(\tau + 1)$)

Chap.	Page	Line	replace this	by this
Intro	xv	-5	$c = i^k$	$C = i^k$
I	27	$+3$	$(m + \tau)^{-k}$	$(m + n\tau)^{-k}$
I	29	-7	$k \not\equiv= 2 \pmod{12}$	$k \not\equiv 2 \pmod{12}$
I	32	-3	$t = e^{-2\pi i/\tau+1}$	$t = e^{-2\pi i/(\tau+1)}$
I	37	-2	$(n^2 + m^2)^{-5}$	$(n^2 + m^2)^{-s}$
II	16	$+5$	Peterson's	Petersson's
III	2	-6	$P_1, \ldots, P_0$	$P_1, \ldots, P_\sigma$
III	13	$-4, -3$	f	f_1
IV	3	-9	$\mathcal{M}(N)$	$M(N)$
IV	13	$+5$	ineducible	irreducible
IV	16	$+1$	if $f\|U = \zeta \cdot U$	$f\|U = \zeta \cdot f$
IV	17	-2	$(m, \frac{N}{t}) \neq 0$	$(m, \frac{N}{t}) \neq 1$
V	9	$+5$	$abN \equiv -1 \pmod{M}$	$abN \equiv -1 \pmod{m}$
V	13	-8	$C_\chi = C\varepsilon(m)\chi(-N)g_\chi\|g_{\overline{\chi}}$	$C_\chi = C\varepsilon(m)\chi(-N)g_\chi/g_{\overline{\chi}}$
V	14	$+7$	$C'_n = Ci^k\varepsilon(m)$	$C'_n = Ci^k\varepsilon(n)$
V	15	$+6$	x_0	τ_0
VI	2	-8	c	C
VI	3	$+4$	σ of n letters	σ of r letters
VI	8	-7	$\frac{\partial f_i}{\partial x_i}\frac{\partial g_i}{\partial x_i}$	$\frac{\partial f}{\partial x_i}\frac{\partial g}{\partial x_i}$
VI	17	-3	Ramamyan	Ramanujan
VI	19	-5	$A\ell\|0\ (N)$	$A\ell \equiv 0\ (N)$

References

[1] Lars V. Ahlfors, *Complex Analysis*, 3rd ed., McGraw-Hill, New York, 1979.

[2] B. Berlowitz, *Extensions of a theorem of Hardy*, Acta Arith. **14** (1968), 203–207.

[3] Robert C. Gunning, *Lectures on Modular Forms*, Annals of Mathematics Studies, vol. 48, Princeton University Press, Princeton, 1962.

[4] H. Hamburger, *Über die Riemannsche Funktionalgleichung der ζ-Funktion*, Math. Zeitschr. **10, 11, 13** (1921, 1921, 1922), 240–254, 224–245, 283–311.

[5] Erich Hecke, *Mathematische Werke*, Vandenhoeck & Ruprecht, Göttingen, 1959. 3. Auflage 1983.

[6] ———, *Vorlesungen über die Theorie der Algebraischen Zahlen*, 2nd ed., AMS Chelsea Publishing, New York, 1923. re-issue 1970.

[7] Louis Joel Mordell, *On Mr. Ramanujan's Empirical Expansions of Modular Functions*, Proc. Cambridge Phil. Soc. **19** (1917), 117–124.

[8] Andrew P. Ogg, *Modular Forms and Dirichlet Series*, Mathematics lecture note series, Benjamin, 1969.

[9] Hans Petersson, *Konstruktion der sämtlichen Lösungen einer Riemannschen Funktionalgleichung durch Dirichlet-Reihen mit Eulerscher Produktentwicklung*, Math. Ann. **116, 117** (1939, 1940/41), 401–412, 39–64, 277–300.

[10] Bernhard Riemann, *Gesammelte Mathematische Werke*, 2. Aufl., Teubner, Leipzig, 1892.

[11] Walter Rudin, *Real and complex analysis*, 3rd ed., McGraw-Hill, 1987.

[12] Bruno Schoeneberg, *Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen*, Math. Ann. **116** (1939), 511–523.
[13] Goro Shimura, *The zeta-function of an algebraic variety and automorphic functions*, Arithmetical Algebraic Geometry, Proc. Conf. at Purdue Univ., Harper and Row, New York, 1965, pp. 6–31.
[14] Carl Ludwig Siegel, *A simple proof of* $\eta(-1/\tau) = \eta(\tau)\sqrt{\tau/i}$, Mathematika **1** (1954), 4–4.
[15] André Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 149–156.

Index

A

adjoint form
of quadratic form Q 57

C

character . . 27, 38, 39, 43, 44, 47, 50, 52–55, 59, 63, 64
primitive 51
conductor 51–54, 56, 65
congruence subgroup 34
conjecture
Hasse-Weil 56
Petersson 29, 45, 56
Ramanujan 29, 62
correspondence 24, 37
cusp 15, 16, 29–31, 35, 36, 45–47, 55, 56
cusp form 11, 14, 19, 24, 26, 29–31, 36, 43–45, 47–50, 54–56, 59, 62, 64, 65

D

Dedekind's η-function 19
degree of divisor 24
determinant D
of quadratic form Q 57
discriminant Δ 65
of quadratic form Q 57
divisor 39
divisor group 24

E

EBV . . . *see* entire, bounded in vertical strip
Eisenstein series . . 12, 14, 18, 28, 45, 47–50, 55, 65
G_k 12, 23
normalized 13
primitive 46
restricted 46, 47
elliptic fixed point 15
elliptic modular invariant 11, 14, 35
elliptic substitution 9
entire, bounded in vertical strip 3, 52
ε-Hermitian 39
Euler product 4, 20, 27–29, 33, 39, 41
relative to p 28, 42

F

functional equation 2–4, 6, 9, 13, 17, 19–21, 50, 51, 53–56
fundamental domain . . 6, 11, 13, 15, 29, 31, 32, 44, 46

G

Gauss sum 51, 65
genus 29
growth function 20

H

Hasse-Weil conjecture 56
Hecke operator . 4, 24, 26–28, 32, 33, 36, 37, 39, 41, 45, 47
holomorphic at ∞ 3, 24
homogeneous modular group 23
homogeneous principal congruence subgroup 34

I

integral symmetric matrix 56

J

Jacobi symbol 57, 65

L

Legendre symbol 36, 65
level of quadratic form 57

M

Möbius function 46
matrix A
of quadratic form Q 57
Mellin inversion formula 4
modular form 23, 30
of dimension $-k$ 3
of level N and dimension $-k$ 34
modular group 4, 13, 24

O

O-condition 3
order of function 20
order of zero 15, 30

P

parabolic fixed point 15
Petersson conjecture 29, 45, 56
Petersson inner product 31
Poisson summation formula 17
positive divisor 24
primitive character 47, 51
primitive quadratic form 57
primitive sublattice 24
principal congruence subgroup
of level N 34
of level 2 15

Q

quasi-regular 15

R

Ramanujan conjecture 29, 62
Riemann hypothesis 56
Riemann zeta-function 2
Riemann-Hurwitz formula 29

S

signature (λ, k, C) 3
spherical function 57–60
Stirling's formula 4
Stufe 57

T

theta-function 2, 17, 19, 56, 57, 60
theta-series 56, 59, 62

V

value
of f at ∞ 30
vanishes at ∞ 3