ADVANCED ALGEBRA 1: MODULAR FORMS

DR. EDGAR ASSING

Abstract. In this lecture we will cover the basic theory of modular forms and applications to quadratic forms. The exercises and their solutions as well as some additional remarks were kindly added by Alberto Acosta Reche. I would like to thank all the students that followed the course and helped me to fix many typos. However, be aware there are probably more typos! For personal use only.

Contents

We assume familiarity with complex analysis as covered for example in:

- *Complex Analysis: An Introduction to The Theory of Analytic Functions of One Complex Variable* by L. Ahlfors.

In the beginning we will have a brief look at the theory of elliptic functions à la Eisenstein. More on this can be found in

- *Elliptic Functions according to Eisenstein and Kronecker* by André Weil.

Some good books on modular forms are for example:

- *Topics in classical automorphic forms* by H. Iwaniec;
- *Introduction to the arithmetic theory of automorphic forms* by G. Shimura;
- *Modular forms* by T. Miyake.
- *Introduction to Elliptic Curves and Modular Forms* by N. Koblitz.

1. Ouvertüre

Historically there has been much interest in computing elliptic integrals:

$$\int_a^z \frac{dt}{\sqrt{P(t)}},$$

where $P(t)$ is a (complex) polynomial of degree 3 or 4. (Technically this is an elliptic integral of the first kind.) Such integrals arise geometrically when computing the arc length of ellipses and also come up in physics.

Example 1.0.1. In 1718 Fagano studied

$$E(x) = \int_0^x \frac{dx}{\sqrt{1-t^4}},$$

which satisfies the peculiar law

$$E(x) + E(x) = E\left(\frac{2x\sqrt{1-x^4}}{1+x^4}\right).$$

It is a remarkable fact, that the inverse function of an elliptic integral is an elliptic function. This is a doubly periodic meromorphic function. It turns out that many interesting properties of elliptic integrals can be obtained from a general theory of elliptic functions. This motivates a systematic study of the latter and ultimately leads to modular forms.

As the name suggests a doubly periodic function $f\colon \mathbb{C} \to \overline{\mathbb{C}}$ has two $\mathbb{R}$-linear independent periods $u, v \in \mathbb{C}$:

$$f(z+u) = f(z+v) = f(z).$$

This naturally leads to the lattice $\Gamma \subseteq \mathbb{C}$ with generators u, v. Thus

$$\Gamma = \{\gamma = \mu u + \nu v \colon \mu, \nu \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Observe that the quotient $\frac{v}{u}$ can not be real so that we can write

$$\frac{v}{u} = \delta \cdot \tau,$$

where $\delta = \delta(u,v) \in \{\pm 1\}$ and $\tau \in \mathbb{H} = \{z \in \mathbb{C}\colon \operatorname{Im}(z) > 0\}$. Further lets set $q = e(\tau) = e^{2\pi i \tau}$. We use the branch $\sqrt{q} = e(\tau/2)$ of the square root. Finally observe that $|q| = e^{-2\pi \operatorname{Im}(\tau)} < 1$ and $u\overline{v} - \overline{u}v = -2\pi i \delta A$ for $A > 0$.

Exercise 1, Sheet 0: Let $\Gamma = u\mathbb{Z} + v\mathbb{Z}$ be a lattice in $\mathbb{C}$ (i.e. u, v are $\mathbb{R}$-linearly independent). Suppose that $\Gamma' = u'\mathbb{Z} + v'\mathbb{Z}$ is a sub-lattice of Γ. Show that there is a 2×2 matrix $A \in M_{2\times 2}(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})$ such that

$$(u' \;\; v') = (u \;\; v) \cdot A \tag{1}$$

Further show that $\delta' = \mathrm{sgn}(\det(A))\delta$ and $[\Gamma : \Gamma'] = |\det(A)|$. (Recall that $\frac{v}{u} = \delta \cdot \tau$ and $\frac{v'}{u'} = \delta'\tau'$ with $\delta, \delta' \in \{\pm 1\}$ and $\tau, \tau' \in \mathbb{H}$).

Solution. As $u', v' \in \Gamma := u\mathbb{Z} + v\mathbb{Z}$ we can find unique $a, b, c, d \in \mathbb{Z}$ such that $u' = du + cv$ and $v' = bu + av$. In matrix form this is written as

$$\begin{pmatrix} u' & v' \end{pmatrix} = \begin{pmatrix} u & v \end{pmatrix} \begin{pmatrix} d & b \\ c & a \end{pmatrix}$$

Because Γ' is also a lattice, the vectors u', v' are $\mathbb{R}$-linearly independent. Therefore, the matrix $A = \left(\begin{smallmatrix} d & b \\ c & a \end{smallmatrix}\right)$ has rank 2 over $\mathbb{R}$ and must be in $\mathrm{GL}_2(\mathbb{R})$. By the formula for the inverse we see that $A \in \mathrm{GL}_2(\mathbb{Q})$, as desired. For the assertion about imaginary parts, we calculate

$$\begin{aligned}\tau' &= \delta' \frac{v'}{u'} = \delta' \frac{av + bu}{cv + du} = \delta' \frac{a\delta\tau + b}{c\delta\tau + d} = \delta' \frac{(a\delta\tau + b)\,(c\delta\overline{\tau} + d)}{|c\delta\tau + d|^2} \\ &= \delta' \frac{ac|\tau|^2 + bd + \delta(ad + bc)\mathrm{Re}(\tau) + i\delta(ad - bc)\mathrm{Im}(\tau)}{|c\delta\tau + d|^2}\end{aligned}$$

As both $\mathrm{Im}(\tau), \mathrm{Im}(\tau') > 0$, we deduce $\delta' = \delta \cdot \mathrm{sgn}(\det(A))$, as desired. For the last assertion, we can bring A to its Smith normal form by $D = BAC$ with $B, C \in \mathrm{GL}_2(\mathbb{Z})$ and

$$D = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} \quad \text{where} \quad d_i \in \mathbb{Z}_{>0}, \text{ and } d_1 | d_2$$

Replacing A by BAC simply replaces the basis $(u,\, v)$ of Γ by $(u,\, v)B$ and the basis $(u',\, v')$ of Γ' by $(u',\, v')C^{-1}$, but the lattices remain the same. Therefore, this operation does not change the index $[\Gamma : \Gamma']$, and we can assume $A = D$ without loss of generality. From this presentation it is clear that $\Gamma' \backslash \Gamma \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$, so that $[\Gamma : \Gamma'] = d_1 d_2 = \det(D) = |\det(A)|$, as desired. ☐

We define the series

$$\mathbf{E}_n(x) = \mathbf{E}_n(x; \Gamma) = \sum_{\gamma \in \Gamma} (x + \gamma)^{-n}.$$

For $n \geq 3$ the series is absolutely convergent. On the other hand for $n = 1, 2$ the summation is to be understood as follows:

$$\mathbf{E}_n(x) = \sum_{\gamma \in \Gamma}^{(E)} (x + \gamma)^{-n} = \lim_{N \to \infty} \sum_{\nu = -N}^{N} \left(\lim_{M \to \infty} \sum_{\mu = -M}^{M} (x + \mu u + \nu v)^{-n} \right).$$

In this case the resulting function depends on the choice of generators u, v and we write $\mathbf{E}_n(x) = \mathbf{E}_n(x; u, v)$ if it is necessary to highlight this dependence.

Remark 1.0.2. This is a generalization of the one dimensional series

$$\epsilon_n(x) = \sum_{\mu\in\mathbb{Z}}^{(E)} (x+\mu)^{-n} = \lim_{M\to\infty} \sum_{\mu=-M}^{M} (x+\mu)^{-n}, \tag{2}$$

where the limiting process is of course only necessary for $n = 1$. The attentive reader will immediately realize that

$$\epsilon_1(x) = \pi\cot(\pi x).$$

Indeed this can be proved in the following way:

(1) Observe that both sides define meromorphic functions of period 1 with poles at the integers.
(2) Observe that the residues are all 1.
(3) Deduce that the difference $g(z)$ defines a entire function of period 1.
(4) Observe that both sides remain bounded when $|\mathrm{Im}(z)| \to \infty$.
(5) Deduce, by Liouville's theorem, that $g(z)$ is constant. Since g is odd, it must be identically 0.

One can also check directly that both sides tend to πi when $\mathrm{Im}(z) \to -\infty$. Write $z = x + iy$. For the right hand side

$$\pi i \frac{e(z)+1}{e(z)-1} = \pi i + \frac{2\pi i}{e^{2\pi i x} e^{-2\pi y} - 1} \to \pi i$$

when $y \to -\infty$. For the series, write

$$\frac{1}{z+\mu} = \frac{x+\mu}{(x+\mu)^2 + y^2} - i\frac{y}{(x+\mu)^2+y^2}$$

The series $\sum_\mu \frac{y}{(x+\mu)^2+y^2}$ converges absolutely for every $y \neq 0$. Therefore, we can write

$$\epsilon_1(z) = \lim_{N\to\infty} \sum_{\mu=-N}^{N} \frac{x+\mu}{(x+\mu)^2+y^2} - i\sum_\mu \frac{y}{(x+\mu)^2+y^2}$$

When $y \to -\infty$ the first term tends to 0, while the second tends to πi by the definition of Riemann integration, since the derivative of $\arctan(t)$ is $\frac{1}{1+t^2}$.

Exercise 2, Sheet 0: Use this definition (2) to show that

$$\epsilon_n(z) = \frac{1}{z^n} + (-1)^n \sum_{m\geq\lceil\frac{n}{2}\rceil}^{\infty} \binom{2m-1}{n-1} \gamma_{2m} z^{2m-n}$$

for small z, where

$$\gamma_{2m} = 2\sum_{\mu=1}^{\infty} \mu^{-2m}.$$

Proof. Recall the binomial power series

$$(1+z)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} z^k \quad \text{where} \quad \binom{\alpha}{k} = \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}$$

valid for $\alpha \in \mathbb{R}$ and $|z| < 1$, absolutely convergent for these z. The case relevant to us is $\alpha = -n$, where we have

$$(1+z)^{-n} = \sum_{k=0}^{\infty} (-1)^k \binom{n+k-1}{n-1} z^k$$

Inserting this expansion in the definition of ϵ_n we see that

$$\epsilon_n(z) = \frac{1}{z^n} + \lim_{N\to\infty} \sum_{|\mu|=1}^{N} \mu^{-n} \sum_{k=0}^{\infty} (-1)^k \binom{n+k-1}{n-1} \frac{z^k}{\mu^k}$$

(we sum μ from $-N$ to N omitting 0). If $n+k \geq 2$, then the double series above converges absolutely because of $\sum_{\mu=1}^{\infty} \mu^{-k-n} \leq \sum_{\mu=1}^{\infty} \mu^{-2} < \infty$ and the absolute convergence of (3). Therefore, if $n \geq 2$ we can swap the summation, observe that the summation over μ vanishes if the exponent is odd, and write $k+n = 2m$ for $m \geq \lceil n/2 \rceil$ to arrive at

$$\epsilon_n(z) = \frac{1}{z^n} + (-1)^n \sum_{m \geq \lceil \frac{n}{2} \rceil}^{\infty} \binom{2m-1}{n-1} \gamma_{2m} z^{2m-n}$$

as desired. For $n = 1$ we do the same after noting that the only problematic summation over μ, for $k = 0$, vanishes since the exponent is odd. ∎

Remark 1.0.3. Note that one can define the (even) Bernoulli numbers B_{2m} via the power series:

$$\frac{1}{2} \cdot \frac{e^t+1}{e^t-1} = \frac{1}{t} - \sum_{m=1}^{\infty} (-1)^m B_{2m} \frac{t^{2m-1}}{(2m)!}$$

Thus once the identity

$$\epsilon_1(z) = \pi \cdot \cot(\pi z) = \pi i \frac{e(z)+1}{e(z)-1}$$

is established one can compare coefficients in the two expansions and obtain

$$\gamma_{2m} = (2\pi)^{2m} \cdot \frac{B_{2m}}{(2m)!}$$

Lemma 1.0.4. *We have* $\mathbf{E}_n(-x) = (-1)^n \cdot \mathbf{E}_n(x)$ *for* $n \geq 1$. *Furthermore we have*

$$\frac{d}{dx}\mathbf{E}_n(x) = -n\mathbf{E}_{n+1}(x) \text{ for } n \geq 1.$$

Proof. While the first statement is clear, for the second statement we have to justify term-wise differentiation. ∎

Lemma 1.0.5. *We have*

$$\mathbf{E}_n(x;u,v) = u^{-n}\epsilon_n\left(\frac{x}{u}\right) + u^{-n}\sum_{\nu=1}^{\infty}\left(\epsilon_n\left(\frac{x+\nu v}{u}\right) + \epsilon_n\left(\frac{x-\nu v}{u}\right)\right) \tag{3}$$

and the right hand side is absolutely convergent.

Proof. The formula is easily verified by expressing the inner sum in terms of ϵ_n. The crux of the matter is to show absolute convergence. We write

$$\zeta = \frac{x}{u} \text{ and } z = e(\zeta).$$

Also recall $\frac{v}{u} = \pm\tau$ and $q = e(\tau)$. We will use the formula[1]

$$\epsilon_1(x) = \pi\cot(\pi x) = \pi i \cdot \frac{e(x)+1}{e(x)-1}.$$

It is now easily verified that

$$\epsilon_1(\frac{x+\nu v}{u}) + \epsilon_1(\frac{x-\nu v}{u}) = -2\pi i\left(\frac{1}{1-q^\nu z} - \frac{1}{1-q^\nu z^{-1}}\right).$$

Absolute convergence follows now from the estimate

$$2\pi\left|\frac{1}{1-q^\nu z} - \frac{1}{1-q^\nu z^{-1}}\right| \leq C\cdot|q|^\nu, \tag{4}$$

with $C = C(z) \in \mathbb{R}_+$ and ν sufficiently large.

For $n \geq 2$ we write the series as

$$\mathbf{E}_n(x) = u^{-n}\sum_{\nu\in\mathbb{Z}}^{(E)}\epsilon_n(\zeta+\nu\tau).$$

Observe that

$$\epsilon_n(\zeta) = \frac{(-1)^{n-1}}{(n-1)!}\cdot\frac{d^{n-1}}{d\zeta^{n-1}}\epsilon_1(\zeta) = \frac{(-2\pi i)^n}{(n-1)!}\left(z\frac{d}{dz}\right)^{n-1}\left(\frac{1}{1-z}\right).$$

We obtain

$$\epsilon_n(\zeta+\nu\tau) = \frac{(-2\pi i)^n}{(n-1)!}\left(z\frac{d}{dz}\right)^{n-1}\left(\frac{1}{1-q^\nu z}\right) = \frac{(-2\pi i)^n}{(n-1)!}\sum_{d=1}^{\infty}d^{n-1}q^{\nu d}z^d \tag{5}$$

for large $\nu > 0$. This can be bounded by $C|q|^\nu$ for some constant $C = C(z)$ as before. The case $\nu < 0$ is treated similarly and one easily obtains absolute convergence. ∎

[1] We take it for granted, but it can be derived from the series definition given in (3) directly.

Lemma 1.0.6. *Let $\Gamma \subseteq \mathbb{C}$ be a lattice generated by $u, v \in \mathbb{C}$. Then we have*

$$\mathbf{E}_1(x+\gamma_0; u, v) = \mathbf{E}_1(x; u, v) - 2\pi i \delta \cdot \frac{\nu_0}{u},$$

for $\gamma_0 = \mu_0 u + \nu_0 v \in \Gamma$. Furthermore, for $n \geq 2$ we have $\mathbf{E}_n(x+\gamma_0; u, v) = \mathbf{E}_n(x; u, v)$.

Proof. We write $\gamma_0 = \nu_0 v + \mu_0 u$. Note that $\epsilon_1(x)$ has period 1, so that by (3) we can assume $\mu_0 = 0$. For $\nu_0 > 0$ we compute

$$\mathbf{E}_1(x+\nu_0 v) - \mathbf{E}_1(x) = u^{-1} \cdot \lim_{N\to\infty} \left(\sum_{\nu=N+1}^{N+\nu_0} \epsilon_1\left(\frac{x+\nu v}{u}\right) - \sum_{\nu=-N}^{-N-1+\nu_0} \epsilon_1\left(\frac{x+\nu v}{u}\right) \right).$$

Observing that $\epsilon_1(\frac{x+\nu v}{u})$ approaches $\pm\pi i$ as $\nu\delta \to \mp\infty$ we get

$$\mathbf{E}_1(x+\nu_0 v) - \mathbf{E}_1(x) = -\frac{2\pi i \delta \nu_0}{u}$$

as desired. It is easy to verify the case $\nu_0 < 0$. ∎

Lemma 1.0.7. *Let Γ' be a sub-lattice of Γ with generators u' and v' and let R be a set of representatives for Γ/Γ'. (The case $\Gamma' = \Gamma$ with $R = \{0\}$ is included!) Then we have*

$$\sum_{\gamma\in R} \mathbf{E}_1(x+\gamma; u', v') = \mathbf{E}_1(x; u, v) + \frac{2\pi i \delta c x}{uu'} - \frac{\pi i \delta' \overline{\nu}}{u'},$$

where $\delta' = \delta(u', v')$ and

$$2\sum_{\gamma\in R} \gamma = \overline{\mu} u' + \overline{\nu} v'.$$

Proof. We write

$$\begin{pmatrix} u' & v' \end{pmatrix} = \begin{pmatrix} u & v \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ for } a, b, c, d \in \mathbb{Z} \text{ with } N = ad - bc \neq 0.$$

Note that $\sharp R = [\Gamma \colon \Gamma'] = |N|$. Furthermore, $\delta' = \delta \cdot \operatorname{sgn}(N)$. Without loss of generality we can assume that $0 \in R$.

We set $\mathbf{E}'_n(x) = \sum_{\gamma\in R} \mathbf{E}_n(x+\gamma; u', v')$. Note that for $n \geq 3$ we have $\mathbf{E}'_n(x) = \mathbf{E}_n(x)$, because the defining series is absolute convergent and $\mathbf{E}'_n$ amounts to a re-ordering of the sum. Thus, by differentiating we get

$$\mathbf{E}'_1(x) - \mathbf{E}_1(x; u, v) = Ax + B.$$

We will compute A and B using the formulae

$$Au = \mathbf{E}'_1(x+u) - \mathbf{E}'_1(x) \text{ and } 2B = \mathbf{E}'_1(-x) + \mathbf{E}'_1(x).$$

We write

$$r + u = r_1 + w_1(r) \text{ and } -r = r_2 + w_2(r)$$

with $r_1, r_2 \in R$ and $w_1(r), w_2(r) \in \Gamma'$. Note that $r \to r_1$ as well as $r \to r_2$ are permutations of R. We can write

$$w_i(r) = \mu_i(r)u' + \nu_i(r)v' \text{ for } i = 1, 2.$$

Opening the definition of E_1' we find that

$$\begin{aligned} Au &= \sum_{r\in R} \mathbf{E}_1(x+u+r; u', v') - \sum_{r\in R} \mathbf{E}_1(x+r; u', v') \\ &= \sum_{r\in R} [\mathbf{E}_1(x+w_1(r); u', v') - \mathbf{E}_1(x; u', v')] \\ &= -\frac{2\pi i\delta'}{u'} \sum_{r\in R} \nu_1(r). \end{aligned}$$

Similarly one finds

$$2B = \frac{2\pi i\delta'}{u'} \sum_{r\in R} \nu_2(r).$$

On the other hand we have

$$0 = \sum_{r\in R}(r_1 + w_1(r) - r - u) = \sum_{r\in R}(w_1(r) - u) = \left(\sum_{r\in R} \mu_1(r)\right) u' + \left(\sum_{r\in R} \nu_1(r)\right) v' - |N|u.$$

Writing $u = \frac{1}{N}(u'd - cv')$ and comparing coefficients yields

$$\sum_{r\in R} \nu_1(r) = -\frac{c\delta}{\delta'}.$$

This completes the computation of A. To get B we observe

$$0 = \sum_{r\in R}(r + r_2 + w_2(r)) = 2\sum_{r\in R} r + \left(\sum_{r\in R} \mu_2(r)\right) u' + \left(\sum_{r\in R} \nu_2(r)\right) v'.$$

$\square$

Corollary 1.0.8. *Let $M \in \mathrm{SL}_2(\mathbb{Z})$ and write $\begin{pmatrix} u' & v' \end{pmatrix} = \begin{pmatrix} u & v \end{pmatrix} \cdot M$. Then we have*

$$\mathbf{E}_2(x; u', v') = \mathbf{E}_2(x; u, v) - \frac{2\pi i\delta c}{uu'} \text{ where } M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Proof.

$$\mathbf{E}_2(x; u', v') = -\frac{d}{dx}\mathbf{E}_1(x; u', v') = -\frac{d}{dx}[\mathbf{E}_1(x; u', v') + \frac{2\pi i\delta cx}{uu'}] = \mathbf{E}_2(x; u, v) - \frac{2\pi i\delta c}{uu'}.$$

$\square$

Lemma 1.0.9. *Let x be close to 0. Then we have*

$$\mathbf{E}_n(x) = \frac{1}{x^n} + (-1)^n \sum_{m=\lceil \frac{n}{2} \rceil}^{\infty} \binom{2m-1}{n-1} e_{2m} x^{2m-n} \tag{6}$$

with

$$e_{2m} = \frac{(2\pi i)^{2m}}{u^{2m}\cdot(2m-1)!}\left(\frac{(-1)^m B_{2m}}{2m} + 2\sum_{k=1}^{\infty}\sigma_{2m-1}(k)q^k\right),$$

where $\sigma_s(k) = \sum_{d|k} d^s$.

Proof. We start by writing

$$\begin{aligned}\mathbf{E}_1(x) &= \frac{1}{2}[\mathbf{E}_1(x) - \mathbf{E}_1(-x)] = \frac{1}{x} + \frac{1}{2}\sum_{\gamma\in\Gamma\setminus\{0\}}^{(E)}\left(\frac{1}{x+\gamma} - \frac{1}{-x+\gamma}\right)\\ &= \frac{1}{x} - \sum_{\gamma\in\Gamma\setminus\{0\}}^{(E)}\sum_{m=1}^{\infty}\frac{x^{2m-1}}{\gamma^{2m}}.\end{aligned}$$

In the second line we have used the geometric series which is justified if $|x| < |\gamma|$ for all $\gamma \in \Gamma \setminus \{0\}$. Noting that everything but the part coming from $m = 1$ is absolutely convergent allows us to write

$$\mathbf{E}_1(x) = \frac{1}{x} - \sum_{m=1}^{\infty} e_m x^{m-1}$$

with $e_m = 0$ for odd m and

$$e_2 = \sum_{\gamma\in\Gamma\setminus\{0\}}^{(E)}\gamma^{-2} \text{ and } e_{2m} = \sum_{\gamma\in\Gamma\setminus\{0\}}\gamma^{-2m},$$

for $m \geq 2$. The expression (6) (with the convention that $\binom{2m-1}{n-1} = 0$ for $m < n$) is obtained by repeated differentiation.

It remains to give an alternative description of the coefficients e_{2m}. To do so we recall (5). For $|q| < |z| < |q|^{-1}$ we can write

$$\mathbf{E}_n(x) = u^{-n}\epsilon_n(\zeta) + \frac{(2\pi)^n}{(iu)^n(n-1)!}\sum_{\nu=1}^{\infty}\sum_{d=1}^{\infty} d^{n-1}q^{\nu d}[z^d + (-1)^n z^{-d}].$$

We observe that $e_{2m} = \lim_{x\to 0}\mathbf{E}_{2m}(x) - x^{-2m}$. Before we continue we recall that[2]

$$\epsilon_n(x) = \frac{1}{x^n} + (-1)^n\sum_{m=\lceil\frac{n}{2}\rceil}^{\infty}\binom{2m-1}{n-1}\gamma_{2m}x^{2m-n}$$

with

$$\gamma_{2m} = 2\sum_{\mu=1}^{\infty}\mu^{-2m} = (2\pi)^{2m}\frac{B_{2m}}{(2m)!}.$$

In particular we have $\lim_{\zeta\to 0}(\epsilon_{2m}(\zeta) - \zeta^{-2m}) = \gamma_{2m}$. Since with $x \to 0$ we have $\zeta \to 0$ and $z \to 1$ we directly get the desired formula. ∎

[2]This can be obtained by differentiating the well known expansion of the cotangent. Otherwise arguments similar to those conducted here apply to (2).

Remark 1.0.10. Note that the coefficients e_{2m} obviously depend on the generators u, v of Γ (or at least on the lattice). Thus we better write $e_{2m} = e_{2m}(u,v)$. Furthermore it follows directly from Lemma 1.0.7 that

$$e_2(u',v') = e_2(u,v) - \frac{2\pi i\delta c}{uu'} \text{ and } e_{2m}(u',v') = e_{2m}(u,v) \text{ for } m \geq 2, \tag{7}$$

where

$$\begin{pmatrix} u' & v' \end{pmatrix} = \begin{pmatrix} u & v \end{pmatrix} \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{\in \mathrm{SL}_2(\mathbb{Z})}.$$

Remark 1.0.11. Note that

$$\mathbf{E}_2(x) - e_2 = x^{-2} + \sum_{\gamma \in \Gamma \setminus \{0\}} [(x+\gamma)^{-2} - \gamma^{-2}].$$

However, the latter function is precisely the Weierstrass $\wp$-function. (In particular, the series is actually absolutely convergent.)

Our next goal is to prove some relations (for example functional equations) between the functions $\mathbf{E}_n$.

Lemma 1.0.12. *We have*

$$\begin{aligned}\mathbf{E}_2(x)\mathbf{E}_2(x') &- \mathbf{E}_2(x)\mathbf{E}_2(x+x') - \mathbf{E}_2(x')\mathbf{E}_2(x+x') \\ &= 2\mathbf{E}_3(x+x')[\mathbf{E}_1(x) + \mathbf{E}_1(x')] + \frac{2\pi i\delta}{u}\frac{\partial}{\partial v}\mathbf{E}_2(x+x';u,v).\end{aligned}$$

Proof. We first recall that

$$\mathbf{E}_n(x) = u^{-n}\sum_{\nu}^{(E)} \epsilon_n\left(\frac{x}{u} + \frac{\nu v}{u}\right).$$

To shorten notation we put $\zeta = \frac{x}{u}$ and $\tau = \frac{v}{u}$ assuming $\delta = 1$.

Now for ζ_1, ζ_2 we have the functional equation[3]

$$\epsilon_2(\zeta_1)\epsilon_2(\zeta_2) - \epsilon_2(\zeta_1)\epsilon_2(\zeta_1+\zeta_2) - \epsilon_2(\zeta_2)\epsilon_2(\zeta_1+\zeta_2) = 2\epsilon_3(\zeta_1+\zeta_2)[\epsilon_1(\zeta_1)+\epsilon_1(\zeta_2)]. \tag{8}$$

Putting $\zeta_1 = \zeta + \nu\tau$ and $\zeta_2 = \zeta' + (\rho - \nu)\tau$. Then we sum both sides of (8) first over ν (using the summation order $\sum^{(E)}$) and then over ρ. Note that on the left hand side we only encounter $n = 2$ where we have absolute convergence. This allows us to rearrange the sums to obtain

$$u^4[\mathbf{E}_2(x)\mathbf{E}_2(x') - \mathbf{E}_2(x)\mathbf{E}_2(x+x') - \mathbf{E}_2(x')\mathbf{E}_2(x+x')],$$

where we have written $x = \zeta u$ and $x' = \zeta' u$.

[3] This identity can be checked by recalling that $\epsilon_1(x) = \pi\cot(\pi x)$ and $\epsilon_2(x) = (\pi/\sin(\pi x))^2$. (Otherwise one can deduce it directly from the series definition of ϵ_n.)

Let us consider the right hand side of (8). After summing over ν we have

$$2u\epsilon_3(\zeta+\zeta'+\rho\tau)[\mathbf{E}_1(x)+\mathbf{E}_1(x'+\delta\rho v)] = 2u\epsilon_3(\zeta+\zeta'+\rho\tau)[\mathbf{E}_1(x)+\mathbf{E}_1(x')-\frac{2\pi i\rho}{u}].$$

The first two terms are easily summed over ρ, giving

$$2u^4\mathbf{E}_3(x+x')[\mathbf{E}_1(x)+\mathbf{E}_1(x')].$$

The result follows after observing

$$-2\rho\epsilon_3(\zeta+\zeta'+\rho\tau) = \frac{d}{d\tau}\epsilon_2(\zeta+\zeta'+\rho\tau)$$

and then executing the ρ-sum. ∎

Corollary 1.0.13. *The following identities hold:*

a)
$$\frac{2\pi i\delta}{u}\cdot\frac{\partial}{\partial v}\mathbf{E}_2(x;u,v) = 3\mathbf{E}_4(x;u,v) - 2\mathbf{E}_1(x;u,v)\mathbf{E}_3(x;u,v) - \mathbf{E}_2(x;u,v)^2$$

b)
$$(\mathbf{E}_2(x)-\mathbf{E}_2(x'))\,(\mathbf{E}_1(x+x')-\mathbf{E}_1(x)-\mathbf{E}_1(x')) + \mathbf{E}_3(x)-\mathbf{E}_3(x') = 0$$

This was **Exercise 3, Sheet 1:**

Proof. Recall Lemma 1.0.12 where it was proved that

$$\begin{aligned}\frac{2\pi i\delta}{u}\frac{\partial}{\partial v}\mathbf{E}_2(x+x';u,v) &= \mathbf{E}_2(x)\mathbf{E}_2(x') - \mathbf{E}_2(x)\mathbf{E}_2(x+x') - \mathbf{E}_2(x')\mathbf{E}_2(x+x')\\ &\quad - 2\mathbf{E}_3(x+x')\,(\mathbf{E}_1(x)+\mathbf{E}_1(x'))\end{aligned}$$

We evaluate this expression when $x\notin\Gamma$ and $x'\to 0$. We show that, although there are poles at $x'=0$ on the right hand side, they cancel out. To see this, recall that $\frac{d}{dx}\mathbf{E}_n(x) = -n\mathbf{E}_{n+1}(x)$. We obtain Taylor developments

$$\begin{aligned}\mathbf{E}_2(x+x') &= \mathbf{E}_2(x) - 2x'\mathbf{E}_3(x) + 3(x')^2\mathbf{E}_4(x) + O((x')^3)\\ \mathbf{E}_3(x+x') &= \mathbf{E}_3(x) - 3x'\mathbf{E}_4(x) + O((x')^2)\end{aligned}$$

and noting that $\mathbf{E}_1(x') = \frac{1}{x'}+O(1)$ and $\mathbf{E}_2(x') = \frac{1}{(x')^2}+O(1)$ we see that the limit of right hand side when $x'\to 0$ is

$$\begin{aligned}&\frac{2\pi i\delta}{u}\frac{\partial}{\partial v}\mathbf{E}_2(x)\\ &= \lim_{x'\to 0}\left[\mathbf{E}_2(x')\,(\mathbf{E}_2(x)-\mathbf{E}_2(x+x')) - 2\mathbf{E}_3(x+x')\mathbf{E}_1(x')\right] - \mathbf{E}_2(x)^2 - 2\mathbf{E}_3(x)\mathbf{E}_1(x)\\ &= \lim_{x'\to 0}\left[\frac{2}{x'}\mathbf{E}_3(x) - 3\mathbf{E}_4(x) - \frac{2}{x'}\mathbf{E}_3(x) + 6\mathbf{E}_4(x) + O(x')\right] - \mathbf{E}_2(x)^2 - 2\mathbf{E}_3(x)\mathbf{E}_1(x)\\ &= 3\mathbf{E}_4(x) - 2\mathbf{E}_1(x)\mathbf{E}_3(x) - \mathbf{E}_2(x)^2\end{aligned}$$

which proves part a). For part b), denote the left hand side by $B(x,x')$. We have

$$\begin{aligned}\frac{\partial}{\partial x}B(x,x') &= -2\mathbf{E}_3(x)\mathbf{E}_1(x+x') + 2\mathbf{E}_3(x)\mathbf{E}_1(x) + 2\mathbf{E}_3(x)\mathbf{E}_1(x') - \mathbf{E}_2(x)\mathbf{E}_2(x+x') \\ &\quad + \mathbf{E}_2(x')\mathbf{E}_2(x+x') + \mathbf{E}_2(x)^2 - \mathbf{E}_2(x')\mathbf{E}_2(x) - 3\mathbf{E}_4(x) \\ &= -2\mathbf{E}_3(x)\mathbf{E}_1(x+x') + 2\mathbf{E}_3(x)\mathbf{E}_1(x') - \mathbf{E}_2(x)\mathbf{E}_2(x+x') \\ &\quad + \mathbf{E}_2(x')\mathbf{E}_2(x+x') - \mathbf{E}_2(x')\mathbf{E}_2(x) - \frac{2\pi i\delta}{u}\frac{\partial}{\partial v}\mathbf{E}_2(x;u,v)\end{aligned}$$

where we used part a) to simplify. Now, if we first substitute $x' \mapsto -x'$ and then $x \mapsto x+x'$ and recall that $\mathbf{E}_1(-x') = -\mathbf{E}_1(x')$ and $\mathbf{E}_2(-x') = \mathbf{E}_2(x')$, we obtain the identity of Lemma 1.0.12. Thus, we have arrived at $\frac{\partial}{\partial x}B(x,x') \equiv 0$. By symmetry, we also have $\frac{\partial}{\partial x'}B(x,x') \equiv 0$. Since $B(x,x) \equiv 0$ by inspection, we deduce that $B \equiv 0$, as desired. ∎

Theorem 1.0.14. *We have*

$$\mathbf{E}_3^2 = (\mathbf{E}_2 - e_2)^3 - 15e_4(\mathbf{E}_2 - e_2) + 10(c - e_2e_4)$$

for

$$c = -\frac{\pi i\delta}{2u}\cdot\frac{\partial e_4}{\partial v}.$$

Furthermore,

$$\frac{2\pi i\delta}{u}\cdot\frac{\partial \mathbf{E}_1}{\partial v} = \mathbf{E}_3 - \mathbf{E}_1\mathbf{E}_2. \tag{9}$$

Proof. We start from the identity given in Lemma 1.0.12. For fixed x we view both sides of the identity as a function in $x'' = x + x'$. Expanding around $x'' = 0$ and comparing the constant term yields

$$\mathbf{E}_4(x) = \mathbf{E}_2(x)^2 - 2e_2\cdot\mathbf{E}_2(x) - \frac{2\pi i\delta}{u}\cdot\frac{\partial e_2}{\partial v}(u,v).$$

Expanding this again at $x = 0$ and considering the constant terms gives

$$\frac{2\pi i\delta}{u}\cdot\frac{\partial e_2}{\partial v}(u,v) = 5e_4 - e_2^2.$$

Combining these two identities gives

$$\mathbf{E}_4(x) = (\mathbf{E}_2(x) - e_2)^2 - 5e_4.$$

By differentiation one can reduce the first claimed identity to this. The second identity follows by integrating the first formula from Corollary 1.0.13. ∎

Remark 1.0.15. Of course the result given in the theorem above strongly resembles the famous equation

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

with $g_2 = 60e_4$ and $g_3 = 140e_6$. Note that in the proof we also encountered $\wp'' = 6\wp^2 - \frac{1}{2}g_2$.

We write

$$\prod_{n\in\mathbb{Z}}^{(E)} p_n = \prod_{n=-M}^{M} p_n \cdot \prod_{n=M+1}^{\infty} (p_n p_{-n}).$$

Note that we understand infinite products by taking the logarithm. We will always (if not otherwise stated) use the principal branch. We define the special infinite products

$$f(t,x) = \prod_{w}^{(E)} (1 - \frac{t}{x+w}) = \prod_{\nu}^{(E)} \prod_{\mu}^{(E)} \left(1 - \frac{t}{x+\mu u+\nu v}\right)$$

$$\text{and } \varphi(x) = x \prod_{w\neq 0}^{(E)} (1 - \frac{x}{w}).$$

To see that the definition of φ makes sense we write

$$\log(\varphi(x)) = \log(x) + \sum_{|w|\leq|x|} \log(1 - \frac{x}{w}) + \sum_{|w|>|x|}^{(E)} \sum_{n=1}^{\infty} \frac{1}{n}(x/w)^n.$$

The pieces for $n \geq 3$ are all absolutely convergent and the terms coming from $n = 1, 2$ are still well-defined when summing them in the specified order.

Remark 1.0.16. A different approach would be to consider the σ-function, which is defined by the absolutely convergent Weierstrass (canonical) product

$$\sigma(x) = x \prod_{w\neq 0} (1 - \frac{x}{w}) e^{\frac{x}{w} + \frac{x^2}{2w^2}}.$$

Then $\varphi(x) = \sigma \cdot e^{-e_2 x^2/2}$.

We make the following observations:

$$\begin{aligned} \mathbf{E}_1(x) &= \frac{d}{dx} \log(\varphi(x)), \\ f(t,x) &= \frac{\varphi(x-t)}{\varphi(x)} \text{ and} \\ \varphi(t) &= -[xf(t,x)]_{x=0}. \end{aligned} \tag{10}$$

Lemma 1.0.17. *We have*

$$\varphi(x) = \frac{u}{2\pi i} \cdot \frac{X_q(z)}{P(q)^2},$$

where $P(q) = \prod_{\nu=1}^{\infty}(1 - q^\nu)$,

$$X_q(z) = (z^{\frac{1}{2}} - z^{-\frac{1}{2}}) \prod_{\nu=1}^{\infty} (1 - q^\nu z)(1 - q^\nu z^{-1}),$$

$q = e(\tau)$ *and* $z = e(\frac{x}{u})$.

Proof. From the definition we get

$$f(t,x) = \prod_{\nu}{}^{(E)} \underbrace{\prod_{\mu}{}^{(E)} \left(1 - \frac{t}{x+\mu u+\nu v}\right)}_{=\frac{\sin(\pi(\frac{x-t+\nu v}{u}))}{\sin(\pi(\frac{x+\nu v}{u}))}=P_\nu}.$$

We put $\zeta^* = \frac{(x-t)}{u}$ and $z^* = e(\zeta^*)$. One easily verifies that

$$P_0 = \frac{(z^*)^{\frac{1}{2}} - (z^*)^{-\frac{1}{2}}}{z^{\frac{1}{2}} - z^{-\frac{1}{2}}} \text{ and } P_\nu P_{-\nu} = \frac{(1-q^\nu z^*)(1-q^\nu (z^*)^{-1})}{(1-q^\nu z)(1-q^\nu z^{-1})}.$$

Thus we have actually seen that

$$f(t,x) = \frac{X_q(z^*)}{X_q(z)}.$$

The result follows by using (10). The factor $\frac{u}{2\pi i}$ comes from the contribution of $\lim_{x\to 0} \frac{x}{x^{\frac{1}{2}}-x^{-\frac{1}{2}}} = \frac{u}{2\pi i}$. ∎

Lemma 1.0.18. *Let* $\gamma = \begin{pmatrix} d & b \\ c & a \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *and assume that* $\delta = 1$. *Then we have*

$$X_{q'}(z') = X_q(z) \cdot (c\tau+d)^{-1} \frac{P(q')^2}{P(q)} e\left(\frac{c\zeta\zeta'}{2}\right),$$

for

$$\tau' = \frac{a\tau+b}{c\tau+d},\ q' = e(\tau'),\ \zeta' = \frac{\zeta}{c\tau+d} \text{ and } z' = e(\zeta').$$

Proof. Looking closely at $\log f(t,x)$ and using the Taylor expansion of the logarithm (at 1) reveals that the sums remaining in

$$\log(f(t,x)) + t\sum_{\gamma\in\Gamma}{}^{(E)} (x+\gamma)^{-1} + \frac{t^2}{2}\sum_{\gamma\in\Gamma}{}^{(E)} (x+\gamma)^{-2}$$

are absolutely convergent. In particular the remainder depends only on Γ and not on the basis u, v. In view of the transformation behavior of E_1 and E_2 we obtain directly that

$$f(t,x;u',v') = f(t,x;u,v) \cdot e\left(\frac{c}{2uu'}(t^2-2xt)\right).$$

The proof is easily completed with the help of (10) and Lemma 1.0.17. ∎

Lemma 1.0.19. *We have*

$$\varphi(x+\mu u+\nu v) = (-1)^{\mu+\nu}\varphi(x) e\left(-\delta\nu\frac{x}{u} - \delta\nu^2\frac{v}{2u}\right).$$

Proof. One first checks that

$$X_q(q^\nu z) = q^{-\nu^2/2}(-z)^{-\nu} X_q(z). \tag{11}$$

The result follows from Lemma 1.0.17. ∎

Lemma 1.0.20. *We have*

$$X_q(z) = \frac{1}{P(q)} T(q,z), \text{ for } T(q,z) = z^{\frac{1}{2}} \sum_{n=-\infty}^{\infty} (-1)^n q^{(n^2+n)/2} z^n.$$

Proof. One starts by formally writing

$$X_q(z) = z^{\frac{1}{2}} \sum_{n\in\mathbb{Z}} F_n(q) z^{n+\frac{1}{2}}.$$

This will be absolutely convergent for $z \neq 0$ since $|q| < 1$. From (11) we deduce that

$$F_{n+\nu}(q) = (-1)^\nu F_n(q) \cdot q^{(\nu^2+\nu+2n\nu)/2}.$$

Rearranging the sum yields

$$X_q(z) = F_0(q) T(q,z).$$

It remains to identify $F_0(q)$. This is done as follows. We first check by differentiation that

$$\mathbf{E}_2(x) - \mathbf{E}_1(x)^2 = -\frac{1}{\varphi(x)} \cdot \frac{\partial^2 \varphi(x)}{\partial x^2} \text{ and } \mathbf{E}_3(x) - \mathbf{E}_1(x)\mathbf{E}_2(x) = \frac{1}{2}\frac{\partial}{\partial x}\left(\frac{1}{\varphi(x)} \cdot \frac{\partial^2 \varphi(x)}{\partial x^2}\right).$$

In view of (9) we get

$$\frac{\partial}{\partial x}\left(\frac{1}{\varphi(x)} \cdot \frac{\partial^2 \varphi(x)}{\partial x^2} - \frac{4\pi i\delta}{u\varphi(x)} \frac{\partial \varphi(x;u,v)}{\partial v}\right) = 0.$$

We conclude that the quantity in the brackets is constant (as function of x). By computing its value at 0 one finds

$$\frac{1}{\varphi(x)} \cdot \frac{\partial^2 \varphi(x)}{\partial x^2} - \frac{4\pi i\delta}{u\varphi(x)} \frac{\partial \varphi(x;u,v)}{\partial v} = -3e_2.$$

It is then straight forward to obtain the equation

$$\frac{\partial^2 T}{\partial x^2} - \frac{4\pi i\delta}{u} \cdot \frac{\partial T}{\partial v} + \frac{\pi^2}{u^2} T = 0$$

for $T(q,z)$. This gives

$$\frac{4\pi i\delta}{u} \cdot \frac{\partial}{\partial v} \log(FP^{-2}) = 3e_2 - \frac{\pi^2}{u^2}.$$

On the other hand, from the definition of P one obtains

$$\frac{\partial}{\partial v} \log(P(q)) = -\frac{2\pi i\delta}{u} \sum_{\nu=1}^{\infty} \frac{\nu q^\nu}{1-q^\nu}.$$

This lets us obtain

$$e_2 = -\frac{4\pi i\delta}{u} \cdot \frac{\partial}{\partial v} \log(q^{\frac{1}{24}} P(q)).$$

We conclude that FP^{-2} and P^{-3} differ only by a constant factor. Since F and P are both 1 at $q = 1$ this factor is one and we must have $F = P^{-1}$ as claimed. $\square$

Exercise 1, Sheet 2: Recall the function

$$T(q, z) = z^{\frac{1}{2}} \sum_{n\in\mathbb{Z}} (-1)^n q^{(n^2+n)/2} z^n$$

from the lecture notes.

a) Show that $T(q^4, q^2) = T\left(q, iq^{\frac{1}{2}}\right) \cdot e\left(\frac{1}{8} - \frac{3\tau}{4}\right)$, where $q = e(\tau)$ and $\tau \in \mathbb{H}$ as usual.
b) Use the identity $X_q(z) = F_0(q) \cdot T(q, z)$ to show that $F_0(q^4)P(q^4) = F_0(q)P(q)$.
c) Show that $\lim_{q\to 0} F_0(q) = 1$ and deduce that $F_0(q) = P(q)^{-1}$.

Solution. On the one hand

$$T(q^4, q^2) = q \sum_{n\in\mathbb{Z}} (-1)^n q^{2n^2+2n} q^{2n} = \sum_{n\in\mathbb{Z}} (-1)^n q^{2n^2+4n+1}$$

while, on the other hand

$$T\left(q, iq^{\frac{1}{2}}\right) = e^{\frac{\pi}{4}i} q^{\frac{1}{4}} \sum_{n\in\mathbb{Z}} (-1)^n q^{(n^2+n)/2} i^n q^{n/2} = e^{\frac{\pi}{4}i} \sum_{n\in\mathbb{Z}} (-1)^n i^n q^{n^2/2+n+1/4} \tag{12}$$

We observe that $n^2/2 + n = m^2/2 + m$ exactly when $n = m$ or $n + m = -2$. Thus, in equation (12) we can pair the terms with $n + m = -2$. Looking modulo 4 we see that only the odd terms survive. Thus, we can rewrite the above as

$$T\left(q, iq^{\frac{1}{2}}\right) = -e^{\frac{\pi}{4}i} \sum_{k\in\mathbb{Z}} i^{2k+1} q^{(2k+1)^2/2+2k+1+1/4} = -ie^{\frac{\pi}{4}i} \sum_{k\in\mathbb{Z}} (-1)^k q^{2k^2+4k+7/4}$$

If we compare this with (12) and recall $e(z) = e^{2\pi iz}$ we obtain part a).

For the claim of part b), note that using part a) and the identity $X_q(z) = F_0(q) \cdot T(q, z)$, the claim is equivalent to

$$X_{q^4}(q^2)P(q^4) = e\left(\frac{1}{8} - \frac{3\tau}{4}\right) X_q(iq^{1/2})P(q)$$

Recall that

$$X_q(z) := (z^{\frac{1}{2}} - z^{-\frac{1}{2}}) \prod_{\nu=1}^{\infty} (1 - q^\nu z)(1 - q^\nu z^{-1}) \qquad \text{and} \qquad P(q) := \prod_{\nu=1}^{\infty} (1 - q^\nu)$$

Thus we find

$$X_{q^4}(q^2)P(q^4) = (q - q^{-1}) \prod_{\nu=1}^{\infty}(1 - q^{4\nu+2})(1 - q^{4\nu-2})(1 - q^{4\nu}) \tag{13}$$

In the infinite triple product, the term $(1 - q^2)$ and the terms $(1 - q^{4\nu})$ for $\nu \geq 1$ appear once, while the terms for $\nu \geq 1$ appear twice. On the other hand

$$X_q(iq^{\frac{1}{2}})P(q) = (e^{\frac{\pi i}{4}} q^{\frac{1}{4}} - e^{-\frac{\pi i}{4}} q^{-\frac{1}{4}}) \left(\prod_{\nu=1}^{\infty}(1 - iq^{\nu+1/2})(1 + iq^{\nu-1/2}) \right) (1 - q^{\nu})$$

We pair the terms $(1 - iq^{\nu+1/2})$ and $(1 + iq^{\nu+1/2})$ whose product equals $(1 + q^{2\nu+1})$, thus we obtain

$$X_q(iq^{\frac{1}{2}})P(q) = (e^{\frac{\pi i}{4}} q^{\frac{1}{4}} - e^{-\frac{\pi i}{4}} q^{-\frac{1}{4}})(1 + iq^{\frac{1}{2}}) \prod_{\nu=1}^{\infty}(1 + q^{2\nu+1})(1 - q^{\nu})$$

now we pair the terms of the first product with the terms $(1 + q^{2\nu+1})$ with the terms $(1 - q^{2\nu+1})$, to obtain $(1 - q^{4\nu+2})$. We can rewrite the above as

$$X_q(iq^{\frac{1}{2}})P(q) = (e^{\frac{\pi i}{4}} q^{\frac{1}{4}} - e^{-\frac{\pi i}{4}} q^{-\frac{1}{4}})(1 + iq^{\frac{1}{2}})(1 - q) \prod_{\nu=1}^{\infty}(1 - q^{4\nu+2})(1 - q^{2\nu}) \tag{14}$$

We observe that in the infinite double product, the term $(1 - q^2)$ and the terms $(1 - q^{4\nu})$ for $\nu \geq 1$ appear exactly once, while the terms $(1 - q^{4\nu+2})$ for $\nu \geq 1$ appear twice. Comparing (13) with (14) we see that

$$X_{q^4}(q^2)P(q^4) = \frac{(q - q^{-1})}{(e^{\frac{\pi i}{4}} q^{\frac{1}{4}} - e^{-\frac{\pi i}{4}} q^{-\frac{1}{4}})(1 + iq^{\frac{1}{2}})(1 - q)} X_q(iq^{\frac{1}{2}})P(q)$$

Simplifying the factor we get

$$\frac{(q - q^{-1})}{(e^{\frac{\pi i}{4}} q^{\frac{1}{4}} - e^{-\frac{\pi i}{4}} q^{-\frac{1}{4}})(1 + iq^{\frac{1}{2}})(1 - q)} = e^{\frac{\pi i}{4}} q^{-3/4} \frac{q^2 - 1}{(iq^{1/2} - 1)(1 + iq^{1/2})(1 - q)} = e^{\frac{\pi i}{4}} q^{-3/4}$$

and we have proved part b).

For part c), first observe that $T(0, z) = (z^{\frac{1}{2}} - z^{-\frac{1}{2}}) = X_0(z)$ directly from the definitions. By the identity $X_q(z) = F_0(q) \cdot T(q, z)$ we obtain $F_0(0) = 1$. Also, $P(0) = 1$ from the definition. Thus, $F_0(0)P(0) = 1$. Seeing F_0 and P as functions of q, both are holomorphic on the disk $|q| < 1$. Thus $G(q) := F_0(q)P(q)$ is an holomorphic function on $|q| < 1$ with $G(q^4) = G(q)$ and $G(0) = 1$. Looking at the power series development, $G(q) = \sum_{n=0}^{\infty} a_n q^n$, and using $G(q^4) = G(q)$ we see that $a_n \neq 0$ only for n multiple of 4. Repeating the argument, $a_n \neq 0$ only for n multiple of 16, and proceeding inductively the only nonzero term is $a_0 = 1$. We deduce that $F_0(q) = P(q)^{-1}$, as desired. ∎

Remark 1.0.21. Usually one write $\eta(\tau) = q^{\frac{1}{24}}P(q)$. We have in particular seen above that
$$e_2 = -\frac{4\pi i}{u^2}\frac{d}{d\tau}\log(\eta(\tau)).$$
Recall transformation formula $e_2(u', v') = e_2(u, v) - 2\pi i\frac{c}{uu'}$, where $u' = cv + du$, $v' = av + bu$, $ad - bc = 1$ and $\frac{v}{u} \in \mathbb{H}$.[4] We set $\tau' = \frac{a\tau+b}{c\tau+d} = \frac{v'}{u'}$ and observe that $\frac{d\tau'}{d\tau} = \left(\frac{u}{u'}\right)^2$. We compute
$$\begin{aligned}\frac{d}{d\tau}\log\frac{\eta(\tau')}{\eta(\tau)} &= \frac{d}{d\tau}\log(\eta(\tau')) - \frac{d}{d\tau}\log(\eta(\tau)) \\ &= -\frac{u^2}{4\pi i}(e_2(u', v') - e_2(u, v)) \\ &= \frac{1}{2}\cdot\frac{u}{cv + du}\cdot c = \frac{1}{2}\cdot\frac{c}{c\tau + d} \\ &= \frac{d}{d\tau}\log(c\tau + d)^{\frac{1}{2}}.\end{aligned}$$
Integrating and exponentiating yields
$$\eta(\frac{a\tau + b}{c\tau + d}) = \epsilon_g \cdot (c\tau + d)^{\frac{1}{2}} \cdot \eta(\tau), \text{ for } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \tag{15}$$
for some constant ϵ_g depending on $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. The constant ϵ_g is very interesting and we will come back to it later.

Finally we come back to Theorem 1.0.14. Note that for $w \in \Gamma \setminus 2\Gamma$ we have
$$\mathbf{E}_3(\frac{w}{2}) = \mathbf{E}_3(-\frac{w}{2}) = -\mathbf{E}_3(\frac{w}{2}).$$
In particular we must have $\mathbf{E}_3(\frac{u}{2}) = \mathbf{E}_3(\frac{v}{2}) = \mathbf{E}_3(\frac{u+v}{2}) = 0$. Thus we write
$$\begin{aligned}&(\mathbf{E}_2(x) - e_2)^3 - 15e_4(E_2(x) - e_2) - 35e_6 \\ &\qquad = \mathbf{E}_3(x)^2 = (\mathbf{E_2}(x) - \mathbf{E}_2(\frac{u}{2}))(\mathbf{E_2}(x) - \mathbf{E}_2(\frac{v}{2}))(\mathbf{E_2}(x) - \mathbf{E}_2(\frac{u+v}{2})).\end{aligned}$$
Taking the discriminant on both sides gives the formula
$$4(15e_4)^3 - 27(35e_6)^2 = [(\mathbf{E_2}(\frac{u+v}{2}) - \mathbf{E}_2(\frac{u}{2}))(\mathbf{E_2}(\frac{u}{2}) - \mathbf{E}_2(\frac{u+v}{2}))(\mathbf{E_2}(\frac{u}{2}) - \mathbf{E}_2(\frac{v}{2}))]^2. \tag{16}$$

[4]Note the difference to (7), where a and d are swapped.

It can be computed that

$$\mathbf{E_2}(\frac{u+v}{2}) - \mathbf{E}_2(\frac{u}{2}) = \frac{16\pi^2}{u^2} q^{\frac{1}{2}} T_1(q)^4,$$
$$\mathbf{E_2}(\frac{u}{2}) - \mathbf{E}_2(\frac{u+v}{2}) = \frac{\pi^2}{u^2} T_2(q)^4 \text{ and}$$
$$\mathbf{E_2}(\frac{u}{2}) - \mathbf{E}_2(\frac{v}{2}) = \frac{\pi^2}{u^2} T_3(q)^4.$$

The functions $T_i(q)$ are given by the series

$$T_1(q) = \frac{1}{2}\sum_{n\in\mathbb{Z}} q^{(n^2+n)/2} = P(q^2)^2 P(q)^{-1},$$
$$T_2(q) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2/2} = P(q^{\frac{1}{2}})^2 P(q)^{-1} \text{ and}$$
$$T_3(q) = \sum_{n\in\mathbb{Z}} q^{n^2/2} = P(q)^5 P(q^2)^{-2} P(q^{\frac{1}{2}})^{-2},$$

but most importantly they satisfy

$$T_1(q)T_2(q)T_3(q) = \frac{1}{2}\sum_{n\in\mathbb{Z}} (-1)^n (2n+1) q^{(n^2+n)/2} = P(q)^3.$$

Thus after artificially adding a factor of 2^4 to both sides of (16) we obtain

$$\widetilde{\Delta} = g_2^3 - 27g_3^2 = 2^4 3^3 5^2 (20e_4^3 - 49e_6^2) = \left(\frac{2\pi}{u}\right) 12qP(q)^{24} = \left(\frac{2\pi}{u}\right)^{12} \eta^{24}. \tag{17}$$

2. Satz I: The Basic Theory of Modular Forms

We will now introduce the basic theory of automorphic forms in quite some generality.

2.1. **The Hyperbolic Plane and Fuchsian groups.** The hyperbolic plane is up to isometry the unique simply connected hyperbolic surface.[5] A (for us) very convenient model is the upper half plane:

$$\mathbb{H} = \{z = x + iy \in \mathbb{C} \colon y > 0\} \text{ equipped with } ds^2 = \frac{dx^2 + dy^2}{y^2}.$$

Given a matrix $\gamma \in \mathrm{SL}_2(\mathbb{R})$ we associate the Möbius transfomration

$$\gamma z = \frac{az+b}{cz+d}, \text{ where } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

This defines a transitive action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$. Note that the centre of $\mathrm{SL}_2(\mathbb{R})$ is $\{\pm 1\}$ and it acts trivially. Therefore we will often work with $\mathrm{PSL}_2(\mathbb{R}) =$

[5]A hyperbolic surface is a smooth surface equipped with a complete Riemannian metric of constant Gaussian curvature -1.

$\{\pm 1\}\backslash \mathrm{SL}_2(\mathbb{R})$.[6]

Exercise 1, Sheet 1: Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{C})$. Recall the Möbius transformation $f_A : \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ given by

$$f_A(z) = \frac{az+b}{cz+d} \quad \text{and} \quad f_A(\infty) = \frac{a}{c}$$

a) Show that every Möbius transformation has at least one fixpoint in $\overline{\mathbb{C}}$.
b) Suppose that f_A has exactly one fixed point in $\overline{\mathbb{C}}$. Show that there is $B \in \mathrm{SL}_2(\mathbb{C})$ and $b \in \mathbb{C}$ such that

$$B^{-1}AB = \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \tag{18}$$

c) Let $A \in \mathrm{SL}_2(\mathbb{C})$. Show that f_A maps the upper half-plane $\mathbb{H}$ onto itself if and only if $A \in \mathrm{SL}_2(\mathbb{R})$.

Solution. We look for $z = \frac{az+b}{cz+d}$, or equivalently, $cz^2 + (d-a)z - b = 0$. If $c = 0$, ∞ is a fixed point, and if in addition $d \neq a$, then $b/(d-a)$ is the second fixed point. On the other hand, if $c \neq 0$, the equation is equivalent to

$$\left(z + \frac{d-a}{2c}\right)^2 - \frac{b}{c} - \frac{(d-a)^2}{4c^2} = \left(z + \frac{d-a}{2c}\right)^2 - \frac{(a+d)^2 - 4}{4c^2}$$

where we used $\det(A) = ad - bc = 1$. Therefore, the equation has at most 2 fixed points, at least 1, and exactly 1 if and only if the trace satisfies $|\mathrm{Tr}(A)| = |a+d| = 2$.

For part b), note that $f_A \circ f_B = f_{AB}$. Also, recall the fact that for any two 3-tuples of distinct points (z_1, z_2, z_3) and (w_1, w_2, w_3) there is exactly one Möbius transformation that satisfies $f(z_1) = w_1$, $f(z_2) = w_2$ and $f(z_3) = w_3$. For the existence, consider

$$f_{z_1,z_2,z_3}(z) = \frac{z_1 - z_3}{z_1 - z_2} \frac{z - z_2}{z - z_3}$$

which sends (z_1, z_2, z_3) to $(1, 0, \infty)$. Then the transformation $f^{-1}_{w_1,w_2,w_3} \circ f_{z_1,z_2.z_3}$ sends (z_1, z_2, z_3) to (w_1, w_2, w_3). If two Möbius transformations f_A, f_B send (z_1, z_2, z_3) to (w_1, w_2, w_3), then $f_B^{-1} \circ f_A$ fixes three points, and therefore $f_A = f_B$.

Coming back to the proof of part b), if f_A has exactly one fixed point, after conjugating we can assume that the fixed point is ∞. Thus $c = 0$ and from the reasoning in part a) above, as f_A has only one fixed point, we must have $a = d$. As $1 = \det(A) = ad - bc = a^2$ we have $a = \pm 1$, as desired.

[6] For us an element in $\mathrm{PSL}_2(\mathbb{R})$ will just be represented by a 2×2 matrix. This is of course up to multiplication by ± 1, which we will usually suppress in the notation.

For part c), if $A \in \mathrm{GL}_2(\mathbb{R})$, then for $z \in \mathbb{H}$ we have

$$f_A(z) = \frac{az+b}{cz+d} = \frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = \frac{ac|z|^2 + (ad+bc)\mathrm{Re}(z) + i(ad-bc)\mathrm{Im}(z)}{|cz+d|^2}$$

and thus $f_A(z) \in \mathbb{H}$ if and only if $\det(A) > 0$. For the other direction, recall the one-point compactification $\overline{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ of $\mathbb{C}$, which has the topology that agrees with usual one on $\mathbb{C}$ and such that the open neighbourhoods of $\{\infty\}$ are the sets $(\mathbb{C} \setminus \{K\}) \cup \{\infty\}$ for compacts $K \subset \mathbb{C}$[7]. Also, recall that Möbius transformations act by homeomorphisms on $\mathbb{C}$. The boundary of $\mathbb{H}$ in $\overline{\mathbb{C}}$ is $\overline{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$, and since f_A is a homeomorphism of $\overline{\mathbb{C}}$ that sends $\mathbb{H}$ onto itself, it must send its boundary onto itself, that is, $f_A(\overline{\mathbb{R}}) = \overline{\mathbb{R}}$ bijectively. Letting (z_1, z_2, z_3) be the preimages of $(1, 0, \infty)$, we have $f_A = f_{z_1,z_2,z_3}$ by the uniqueness above. Since z_1, z_2, z_3 are real (or maybe one of them is ∞), then, by the formula for f_{z_1,z_2,z_3} above, $f_{z_1,z_2,z_3} = f_B$ for a matrix $B \in \mathrm{GL}_2(\mathbb{R})$. Since f_B sends $\mathbb{H}$ onto itself, we have $\det(B) > 0$, and since scalar matrices act like the identity, we can assume $B = \mathrm{SL}_2(\mathbb{R})$. Therefore $A = \lambda B$ for some $B \in \mathrm{SL}_2(\mathbb{R})$, and taking determinants $\lambda = \pm 1$, so $A \in \mathrm{SL}_2(\mathbb{R})$, as desired. ∎

Remark 2.1.1. We have seen the upper half plane before. Indeed starting with a lattice $\Gamma = \mathbb{Z}u + \mathbb{Z}v \subseteq \mathbb{C}$ we associated $\tau = \delta \frac{v}{u} \in \mathbb{H}$ for $\delta \in \{\pm 1\}$. After swapping u and v if necessary we can assume that $\delta = 1$. Note that, if

$$\begin{pmatrix} v' \\ u' \end{pmatrix} = \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{= g \in \mathrm{SL}_2(\mathbb{R})} \begin{pmatrix} v \\ u \end{pmatrix},$$

then we have

$$\tau' = \frac{a\tau + b}{c\tau + d} = g\tau.$$

On the other hand, given $\tau \in \mathbb{H}$ we can associate the lattice

$$\widetilde{\Gamma} = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau.$$

The lattice $\widetilde{\Gamma}$ is similar to Γ in the sense that it can be obtained from it by rotation and dilation.

Lemma 2.1.2. *The group of orientation preserving isometries of* $\mathbb{H}$ *is the group* $\mathrm{PSL}_2(\mathbb{R})$ *acting via Möbius transformations.*

Proof. Orientation preserving isometries of $\mathbb{H}$ are precisely conformal automorphisms of the upper half plane. It is a classical result that such maps are (real) Möbius transformations.

[7] With this topology $\overline{\mathbb{C}}$ is homeomorphic to S^2 as one sees from stereographic projection.

Let us check that the Möbius transforamtion given by $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an isometry. We compute

$$\operatorname{Im}(Tz) = \frac{\operatorname{Im}(z)}{|cz+d|^2} \text{ and } \frac{d}{dz}Tz = T'(z)\frac{1}{(cz+d)^2}.$$

We get

$$T^*(ds^2) = \frac{|T'(z)dz|^2}{\operatorname{Im}(Tz)^2} = \frac{|dz|^2}{\operatorname{Im}(z)^2} = ds^2.$$

□

Remark 2.1.3. Another model for the hyperbolic plane is the Poncaré disc

$$\mathbb{B} = \{z \in \mathbb{C} \colon |z| < 1\} \text{ with } ds^2 = 4\frac{dx^2+dy^2}{(1-|z|^2)^2}.$$

The map $z \mapsto \frac{z-i}{z+i}$ provides an isometry between the two.

The boundary of the upper half plane is $\partial\mathbb{H} = \mathbb{R} \cup \{\infty\}$.

Lemma 2.1.4. *The geodesics of $\mathbb{H}$ are precisely the arcs of circles intersecting $\partial\mathbb{H}$ orthogonally.*

Proof. We start by computing the geodesic arc connecting two points ia and ib with $0 < a < b$. Let $\eta(t) = x(t) + iy(t)$ be curve connecting these two points. Its length is given by

$$\begin{aligned} l(\eta) &= \int_{t_1}^{t_2} \frac{\sqrt{x'(t)^2 + y'(t)^2}}{y(t)} dt \\ &\geq \int_{t_1}^{t_2} \frac{y'(t)|}{y(t)} dt \\ &\geq \int_{t_1}^{t_2} (\log(y(t)))' dt = \log(b/a). \end{aligned}$$

The minimum is attained if and only if $y'(t) > 0$ and $x'(t) = 0$. We conclude that the path along the y-axis is the path of shortest distance and thus a geodesic.

The general case is reduced to this one via Möbius transformations. □

The previous lemma shows that for two distinct points $z_1, z_2 \in \mathbb{H} \cup \partial\mathbb{H}$ there is a unique geodesic segment, denoted by $[z_1, z_2]$ connecting these two points. The hyperbolic distance is given by

$$d(z_1, z_2) = l([z, w]).$$

One can check that

$$\cosh(d(z_1, z_2)) = 1 + \frac{|z_1 - z_2|^2}{2y_1 y_2},$$

for $z_1, z_2 \in \mathbb{H}$.

We equip $\mathbb{H}$ with the $\mathrm{PSL}_2(\mathbb{R})$ invariant measure

$$d\mu(z) = y^{-2}dxdy.$$

Elements in $\mathrm{PSL}_2(\mathbb{R})$ are classified according to their fixed points.

Definition 2.1.1. A non-trivial element $\gamma \in \mathrm{PSL}_2(\mathbb{R})$ is

- **elliptic** if $|\mathrm{tr}(\gamma)| < 2$; (In this case γ has one fixed point within $\mathbb{H}$.)
- **parabolic** if $|\mathrm{tr}(\gamma)| = 2$; (In this case γ has a single degenerate fixed point in $\partial\mathbb{H}$.)
- **hyperbolic** if $|\mathrm{tr}(\gamma)| > 2$; (In this case γ has two fixed points in $\partial\mathbb{H}$.)

Definition 2.1.2. A subgroup $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{R})$ is said to act properly discontinuous (on $\mathbb{H}$) if for each compact set $C \subseteq \mathbb{H}$ and $z \in \mathbb{H}$ the intersection $\Gamma z \cap C$ is finite.

Definition 2.1.3. A Fuchsian group is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$.

Lemma 2.1.5. *A subgroup $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{R})$ acts properly discontinuous if and only if it is Fuchsian.*

Proof. If Γ is Fuchsian, then Γz is discrete. This implies that $C \cap \Gamma z$ is discrete and compact and therefore finite.

Assume that Γ acts properly discontinuous. We first show that there are points in $\mathbb{H}$ that are not fixed by any non-trivial element in $\mathbb{H}$. To do so take $\gamma w = w$ and any $z \in \mathbb{H}$. Then one has

$$d(Tz, z) \leq d(Tz, Tw) + d(tw, z) = 2d(z, w).$$

Thus only finitely many points in any neighborhood of z can be fixed by non-trivial elements of Γ.

In particular we can fix some w not fixed by any element of $\Gamma \setminus \{1\}$. If Γ is not discrete, there is a sequence $\gamma_k \to 1$ contained in Γ. However, the sequence $\{\gamma_n w\}$ consists of distinct points and $\gamma_n w \to w$ as $n \to \infty$. This is a contradiction. ∎

Remark 2.1.6. It is an important theorem of Heinz Hopf that given a hyperbolic surface X, there is a Fuchsian group $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{R})$ without elliptic elements so that $X \cong \Gamma\backslash\mathbb{H}$. Note that in general, if Γ contains elliptic points then technically speaking $\Gamma\backslash\mathbb{H}$ is an orbifold (and not a smooth surface).

Definition 2.1.4. A fundamental domain $\mathcal{F} \subseteq \mathbb{H}$ for a Fuchsian group Γ is a closed region such that

$$\Gamma\mathcal{F} = \mathbb{H}$$

and for each non-trivial $\gamma \in \Gamma$ the interiors of $\mathcal{F}$ and $\gamma\mathcal{F}$ are disjoint.

Fundamental domains will play a crucial role for us. For $w \in \mathbb{H}$ we associate the Dirichlet domain

$$\mathcal{D}_w = \{z \in \mathbb{H} \colon d(z, w) \leq d(z, \gamma w) \text{ for all } \gamma \in \Gamma\}.$$

It turns out that if w not the fixed point of an elliptic element in Γ, then $\mathcal{D}_w$ is a fundamental domain. Furthermore, $\mathcal{D}_w$ is convex and bounded by a union of geodesics. One can even see that the sides of a Dirichlet domain can be used to find nice generating sets for Γ.

Definition 2.1.5. A Fuchsian group is geometrically finite if there is a fundamental domain that is fa finite sided convex polygon.

Theorem 2.1.7. *For a Fuchsian group* Γ *the following are equivalent:*

- $\Gamma\backslash\mathbb{H}$ *is topologically finite (i.e. finite Euler characteristic);*
- Γ *is finitely generated;*
- Γ *is geometrically finite.*

Proof. Omitted. ∎

Lemma 2.1.8. *Let* Γ *be a Fuchsian group and let* $z \in \mathbb{H} \cup \partial\mathbb{H}$. *Then the stabilizer*

$$\Gamma_z = \{\gamma \in \Gamma \colon \gamma z = z\}$$

is cyclic.

Proof. We will use the fact that two elements $\gamma, \gamma' \in \mathbb{PSL}_2(\mathbb{R})$ commute if and only if the have the same fixed point set. The result is now obvious since discrete subgroups of SO_2, $\mathbb{R}$ and $\mathbb{R}^\times$ are cyclic. ∎

Definition 2.1.6. A Fuchsian group is said to be of the first kind, if every point in $\partial\mathbb{H}$ is a limit point of Γ. (A point in $\partial\mathbb{H}$ is a limit point Γ if it is a limit point of some orbit Γz for $z \in \mathbb{H}$.)

Remark 2.1.9. A theorem due to Poincaré and Fricke-Klein classifies the possibilities for a limit set $\Lambda(\Gamma)$ of a Fuchsian grou Γ. There are three possibilities:

- $\Lambda(\Gamma)$ has 0, 1 or 2 points. (In this case Γ is called elementary.)
- $\Lambda(\Gamma) = \partial\mathbb{H}$. (In this case Γ is said to be of the first kind.)
- $\Lambda(\Gamma)$ is a perfect nowhere-dense subset of $\partial\mathbb{H}$. (In this case Γ is said to be of the second kind.)

Lemma 2.1.10. *Every geometricall finite Fuchsian group of the first kind has a fundamental domain of finite volume. (Furthermore, a Fuchsian group with a fundamental domain of finite volume is of the first kind.)*

Proof. See for example *Discontinuous groups* by C. L. Siegel (1943). ∎

Throughout we will restrict ourselves to geometricall finite Fuchsian groups of the first kind. These come in two flavors. If the fundamental domain is compact, then wecall Γ a co-compact group.

Lemma 2.1.11. *A geometrically finite Fuchsian group of the first kind is co-compact if and only of it has no parabolic elements.*

Proof. We will argue by contradiction and assume that Γ contains a parabolic element. Without loss of generality we can assume that this element fixes ∞.

We first show that there is $c_\Gamma > 0$ so that every $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfies $c = 0$ or $|c| \geq c_\Gamma$. To see this we suppose that Γ_∞ is generated by $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$. Now take $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $0 < |c| \leq 1$. Among the matrices

$$\sigma_{n,m} = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m \sigma \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^n$$

there is one, say σ' with

$$\frac{1}{(1+|h|)^2} \leq \mathrm{Im}(\sigma' i) \leq 1 \text{ and } 0 \leq \mathrm{Re}(\sigma' i) \leq |h|.$$

But this is a finite set which contains only finitely many elements of the orbit Γi.

Now define

$$U = \{z \in \mathbb{H} \colon \mathrm{Im}(z) > \frac{1}{c_\Gamma}\}.$$

Given $\gamma \in \Gamma \setminus \Gamma_\infty$ (i.e. bottom left entry is non-zero) we observe that for $z \in U$ we have $\gamma z \notin U$. We can take a sequence $z_n \in U$ with $z_n \to \infty$. Since two distinct points in this sequence can not be Γ equivalent we obtain infinitely many distinct points in $\Gamma \backslash \mathbb{H}$. If the latter is compact, then there must be an accumulation point τ. We can take a compact neighborhood C of τ and a neighbourhood V of ∞ with $\Gamma V \cap C = \emptyset$. But by construction of the sequence z_n there must be elements of z_n in V. This is a contradiction. ∎

The basic example of a Fuchsian group of the first kind is $\mathrm{PSL}_2(\mathbb{Z})$.

Lemma 2.1.12. *The group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the matrices*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Furthermore, a fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$ *is given by*

$$\mathcal{F} = \{Z = x + iy \colon |x| \leq \frac{1}{2}, |z| \geq 1\}.$$

Proof. We first note that $S^2 = -1$ and we compute

$$S \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}.$$

On the other hand we have

$$T^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + cn & b + dn \\ c & d \end{pmatrix}.$$

The procedure is now easy. Given any element $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we apply T^n with a suitable choice of n so that $T^n\gamma = \begin{pmatrix} a' & b' \\ c & d \end{pmatrix}$ with $0 \leq a < |c$. Then we apply S. Repeating the process allows us to create an upper triangular matrix, which then is ± 1 times a power of T.

We turn towards the fundamental domain. For $z \in \mathbb{H}$ we consider the lattice

$$\Lambda = \mathbb{Z} + \mathbb{Z}z.$$

The shortest vector $(a, b) \in \Lambda$ gives rise to the element $z' \in \Gamma z$ with the largest imaginary part:

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

Without loss of generality we can assume that $-\frac{1}{2} \leq \operatorname{Re}(z') \leq \frac{1}{2}$. We claim that $|z'| \geq 1$. Indeed of $|z'| < 1$, then Sz' has larger imaginary part, which is a contradiction.

It remains to be seen that elements in $z_1, z_2 \in \mathcal{F}^\circ$ are inequivalent. Suppose that $z_2 = \gamma z_1$ and $\operatorname{Im}(z_1) \geq \operatorname{Im}(z_2)$. This implies that

$$|cz_1 + d|^2 = \frac{\operatorname{Im}(z_1)}{\operatorname{Im}(z_2)} \leq 1.$$

This implies that $|c \operatorname{Im}(z_1)| \leq 1$ and because $z_1 \in \mathcal{F}^\circ$ we have $c \leq 1$. The case $c = 0$ is easily handled. Let us assume $c = 1$, then we can write

$$\gamma = \begin{pmatrix} a & ad - 1 \\ 1 & d \end{pmatrix} = T^a S T^d.$$

We see that $w_1 = z_1 - a$ and $w_2 = z_2 + d$ satisfy $w_1 = Sw_2$ and $|w_1|, |w_2| \geq 1$. This implies that z_1, z_2 must be on the boundary. ∎

Remark 2.1.13. The fundamental domain can be used to compute the co-volume of $\mathrm{PSL}_2(\mathbb{Z})$ (i.e. the volume of the fundamental domain with respect to the hyperbolic measure $d\mu(z)$). Further, it can be seen from the fundamental domain that $\mathrm{PSL}_2(\mathbb{Z})$ is not co-compact. (One can also just note that T is a parabolic element and apply Lemma 2.1.11.)

Exercise 2, Sheet 2: Determine all parabolic and elliptic conjugacy classes of $\mathrm{SL}_2(\mathbb{Z})$ and find the corresponding fixed points in the standard fundamental domain.

Solution. Recall that $A \in \mathrm{SL}_2(\mathbb{R})$ is elliptic if and only if $|\operatorname{Tr}(A)| < 2$ and parabolic when $|\operatorname{Tr}(A)| = 2$ but $A \neq \pm\mathrm{Id}$. Equivalently, A is elliptic when it has a simple fixed point in $\mathbb{H}$ (not in the ideal boundary), and A is parabolic when it has a double fixed point in $\mathbb{R} \cup \{\infty\}$. For $A \in \mathrm{SL}_2(\mathbb{Z})$, we have $\operatorname{Tr}(A) \in \mathbb{Z}$. Therefore, the only posibilities for the trace of an elliptic $A \in \mathrm{SL}_2(\mathbb{Z})$ are $\operatorname{Tr}(A) = -1, 0, 1$.

After multiplying by $-\mathrm{Id}$ if necessary we can assume that $\mathrm{Tr}(A) = 0$ or 1. Recall also that $D := \{x + iy \mid -\frac{1}{2} \le x \le \frac{1}{2} \text{ and } x^2 + y^2 \ge 1\}$ is a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$.

Let z_A be the fixed point of the elliptic element $A \in \mathrm{SL}_2(\mathbb{Z})$ with $\mathrm{Tr}(A) \in \{0, 1\}$. By definition of the fundamental domain, there is $B \in \mathrm{SL}_2(\mathbb{Z})$ such that $Bz_A \in D$. Thus, $C = BAB^{-1}$ is an elliptic element with fixed point Bz_A in the fundamental domain. As can be checked easily, the formula for the fixed point is

$$z_C := \frac{a - d + \sqrt{(a+d)^2 - 4}}{2c} \quad \text{where} \quad C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where have to choose the square root so that $z_C \in \mathbb{H}$. If $\mathrm{Tr}(C) = 0$ then $d = -a$ and the fixed point is $z_C = (a + i)/|c|$. As $z_C \in D$, we have $2|a| \le |c|$ and $a^2 + 1 \ge c^2$. The only possibility is $|c| = 1$ and $a = 0$. Therefore, in this case $C = \pm\omega_0 = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ with fixed point i.

Suppose now that $\mathrm{Tr}(C) = 1$. Then $d = 1 - a$ and $z_C = (2a - 1 + \sqrt{3}i)/(2|c|)$. As $z_C \in D$ we have $|2a - 1| \le |c|$ and $|2a - 1|^2 + 3 \ge 4|c|^2$. Thus $|c| = 1$ and $a = 0$ or $a = 1$. This leads to the four possibilities

$$\omega_1 := \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \omega_2 := \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \quad \omega_3 := \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad \omega_4 := \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

Note that $\omega_0^{-1}\omega_3\omega_0 = \omega_1$ and $\omega_0^{-1}\omega_4\omega_0 = \omega_2$. However, ω_1 and ω_2 are not conjugate over $\mathrm{SL}_2(\mathbb{R})$. Indeed, the equality

$$\begin{pmatrix} a+b & -a \\ c+d & -c \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ -a+c & -b+d \end{pmatrix}$$

leads to $a+d = 0$ and $d = b-c$. Together with $ad-bc = 1$ we obtain $-b^2+bc-c^2 = 1$, which is impossible if $b, c \in \mathbb{R}$. Observe also that ω_0 and $-\omega_0$ are not conjugate over $\mathrm{SL}_2(\mathbb{R})$. Indeed, the equations

$$\begin{pmatrix} -c & -d \\ a & b \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$$

lead to $a = -d$ and $b = c$ so that $1 = -a^2 - b^2 < 0$, a contradiction. Therefore, a list of pairwise not conjugate elliptic elements in $\mathrm{SL}_2(\mathbb{Z})$ is given by $\{\omega_0, \omega_1, \omega_2, -\omega_0, -\omega_1, -\omega_2\}$. Working on $\mathrm{PSL}_2(\mathbb{Z})$, equivalently, working with the group of Möbius transformations induced by matrices in $\mathrm{SL}_2(\mathbb{Z})$, the list is given by $\{f_{\omega_0}, f_{\omega_1}, f_{\omega_2}\}$, with fixed points i, $\frac{1+\sqrt{3}i}{2}$ and $\frac{-1+\sqrt{3}i}{2}$ respectively.

Consider now a parabolic element in $\mathrm{SL}_2(\mathbb{Z})$, say

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad \mathrm{Tr}(A) = 2$$

By hypothesis, A has a double fixed point with formula $z_A := \frac{1-d}{c}$, in particular $z_A \in \mathbb{Q} \cup \{\infty\}$. Recall that the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{Q} \cup \{\infty\}$ is transitive.[8] Thus after a conjugation we can assume without loss of generality that the double fixed point of A is at infinity. Since $\mathrm{Tr}(A) = 2$, we arrive at the conclusion that A must be equal to

$$A_n := \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

for some $n \in \mathbb{Z} \setminus \{0\}$. Suppose that A_n, A_m are conjugate in $\mathrm{SL}_2(\mathbb{Z})$ for $n \neq m$. In that case we could find $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with integers entries and determinant 1 such that

$$\begin{pmatrix} a & an+b \\ c & cn+d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+mc & b+md \\ c & d \end{pmatrix}$$

As $m, n \neq 0$, we deduce $c = 0$, and thus $ad = 1$. As $a, d \in \mathbb{Z}$ we must have $a = d$, which implies $n = m$. Therefore, a list of the parabolic conjugacy classes in $\mathrm{SL}(2, \mathbb{Z})$ is $\{A_n\} \cup \{-A_n\}$ with fixed point ∞ (A_n is not conjugate to $-A_m$ since the traces are different). On $\mathrm{PSL}(2, \mathbb{Z})$ the list is $\{f_{A_n}\}$. ∎

Another important example are the so called (Hecke) congruence subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon N \mid c \right\}$$

of level $N \in \mathbb{N}$. Note that

$$[\mathrm{SL}_2(\mathbb{Z}) \colon \Gamma_0(N)] = N \cdot \prod_{p \mid N} \left(1 + \frac{1}{p}\right).$$

This will be proved in Proposition 4.1.7 below.

Exercise 3, Sheet 2: Show that $\Gamma_0(4)$ is generated by

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

Solution. First, observe that this matrices are in $\Gamma_0(4)$. Next, consider an arbitrary element of $\Gamma_0(4)$, of the form

$$A = \begin{pmatrix} a & b \\ 4c & d \end{pmatrix} \quad a, b, c, d \in \mathbb{Z}.$$

Let's look at the pair $(a, 4c)$. If $c = 0$ we skip the following discussion. Otherwise, we perform a series of transformation by multiplying on the left by powers of

[8] Given $r \in \mathbb{Q}$, write it as $r = a/c$ for coprime integers, $(a, c) = 1$. Then find $b, d \in \mathbb{Z}$ such that $da - bc = 1$ (this is possible by Bezout's theorem). Then for $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we have $A \in \mathrm{SL}_2(\mathbb{Z})$ and $A\infty = \frac{a}{c} = r$, proving transitivity.

the generators above. Operation 1 consists of multiplying by $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ on the left, which has the effect $(a, 4c) \mapsto (a + 4cx, 4c) =: (a_1, 4c_1)$. By euclidean division, we can choose a unique $x \in \mathbb{Z}$ such that $|a_1| \leq |2c| = 2|c_1|$. Since $(a_1, c_1) = 1$, we actually have $|a_1| < 2|c_1|$. Operation 2 consists of multiplying by $\begin{pmatrix} 1 & 0 \\ 4y & 1 \end{pmatrix}$ on the left, which has the effect $(a_1, 4c_1) \mapsto (a_1, 4ya_1 + 4c) =: (a_2, 4c_2)$. We can choose a unique y such that $|c_2| \leq |a_1|/2 = |a_2|/2$, and since $(a_2, 4c_2) = 1$, we actually have $2|c_2| < |a_2|$. While $c_n \neq 0$ we apply the operations alternating between the two. If $|a| > 2|c|$ we start applying operation 1, and if $|a| < 2|c|$ we start applying operation 2. Since after any operation $|a_{n+1}| + |c_{n+1}| < |a_n| + |c_n|$ the process has to stop, and it must be $c_n = 0$. Thus after multiplying on the left by certain powers of generators we arrive at

$$B = \begin{pmatrix} r & s \\ 0 & t \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Because $r, s, t \in \mathbb{Z}$ and $rs = \det(B) = 1$ we must have either $r = 1 = t$ or $r = -1 = t$. After multiplying by $-\mathrm{Id}$ if necessary we can assume we are in the first case, but then

$$B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^s$$

and we are finished. ⧉

Remark 2.1.14. Note that, $\Gamma_0(4) = \alpha^{-1}\Gamma(2)\alpha$, where $\alpha = \mathrm{diag}(2, 1)$. Therefore, the exercise is equivalent to proving that $\Gamma(2)$ is generated by

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

One can prove that, in fact, the elements $T_1 := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $T_2 := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ have no nontrivial relations, and that $\{-I_2\}$ does not belong the group they generate, so that $\Gamma(2) \simeq F_2 \times (\mathbb{Z}/2\mathbb{Z})$, where F_2 is the free group in the two generators T_1 and T_2. There is a beautiful classical proof of this fact, which we now present.

As usual, let f_A be the Möbius transformation associated to a matrix $A \in \mathrm{GL}_2(\mathbb{C})$. Consider the Möbius transformation

$$f_A(z) := -i\frac{z-1}{z+1}$$

It satisfies $f_A(0) = i$, $f_A(1) = 0$, $f_A(-1) = \infty$ and $f_A(i) = 1$, so f_A sends the unit disc bijectively onto $\mathbb{H}$. Note that f_A is the Möbius transformation associated to

$$A := \begin{pmatrix} -i & i \\ 1 & 1 \end{pmatrix}$$

Define $R_i = A^{-1}T_iA$. We calculate

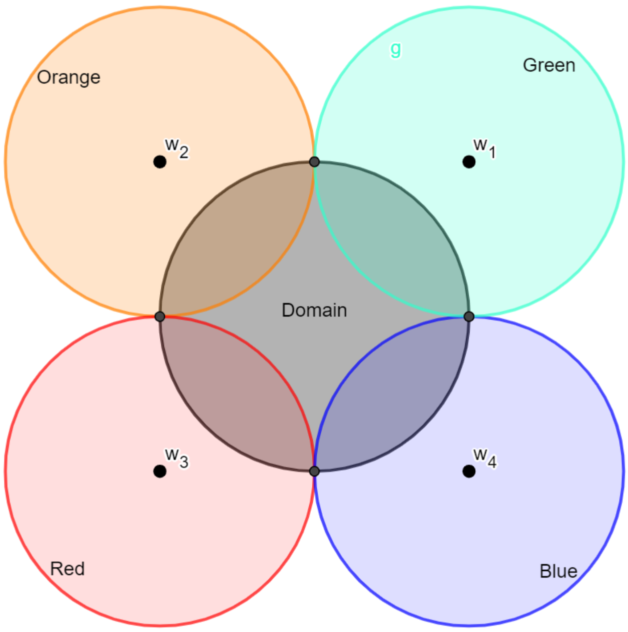
$$R_1 = \frac{1}{2}\begin{pmatrix} i & 1 \\ -i & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -i & i \\ 1 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} i & 1 \\ -i & 1 \end{pmatrix}\begin{pmatrix} -i+2 & i+2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1+i & i \\ -i & 1-i \end{pmatrix}$$

$$R_2 = \frac{1}{2}\begin{pmatrix} i & 1 \\ -i & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} -i & i \\ 1 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} i & 1 \\ -i & 1 \end{pmatrix}\begin{pmatrix} -i & i \\ -2i+1 & 2i+1 \end{pmatrix} = \begin{pmatrix} 1-i & i \\ -i & 1+i \end{pmatrix}$$

Letting $S_i := R_i^{-1}$, we compute

$$S_1 = \begin{pmatrix} 1-i & -i \\ i & 1+i \end{pmatrix} \quad \text{and} \quad S_2 = \begin{pmatrix} 1+i & -i \\ i & 1-i \end{pmatrix}$$

To deduce that T_1 and T_2 have no nontrivial relations it is enough to show that f_{R_1} and f_{R_2} have no nontrivial relations, and this is equivalent to show that any nonempty word in the letters $f_{R_1}, f_{S_1}, f_{R_2}, f_{S_2}$ such that there no occurrences of R_1, S_1 or of R_2, S_2 one after the other. Now comes the beautiful geometric fact. Consider the following figures, where the black circle is $\{|z| = 1\}$, the points are $w_1 = 1+i$, $w_2 = -1+i$, $w_3 = -1-i$, $w_4 = -i+1$ and all circles are of radius 1.



Recall that Möbius transformations preserve angles and send generalized circles to generalized circles. Since $f_{R_1}(-1) = -1$ and $f_{R_1}(-i) = i$, the transformation f_{R_1} sends the red circle to a circle that passes through -1 and i and is orthogonal to the black circle. The only such circle is the orange one. Since $f_{R_1}(0) = (i-1)/2$, which is in the interior of the orange circle, we see that f_{R_1} sends the exterior of the red circle to the interior of the orange circle. Arguing similarly, one gets the following relations

$$f_{R_1}(\text{Exterior of red}) = \text{Interior of orange} \qquad f_{S_1}(\text{Exterior of orange}) = \text{Interior of red}$$
$$f_{R_2}(\text{Exterior of blue}) = \text{Interior of green} \qquad f_{S_2}(\text{Exterior of green}) = \text{Interior of blue}$$

Now we look at the action of a nonempty reduced word $f_{x_1} \circ \cdots \circ f_{x_n}$ on the set labeled as *Domain* in the diagram. This open set is the part of the circle $\{|z| < 1\}$ that is exterior to the other circles. We claim that

$$f_{x_1} \circ \cdots \circ f_{x_n}(\text{Domain}) \subset \begin{cases} \text{Interior of orange} & \text{if } x_1 = R_1 \\ \text{Interior of red} & \text{if } x_1 = S_1 \\ \text{Interior of green} & \text{if } x_1 = R_2 \\ \text{Interior of blue} & \text{if } x_1 = S_2 \end{cases}$$

This is proved inductively, the case $n = 1$ being clear. For the induction step, observe that

$$f_{x_1} \circ \cdots \circ f_{x_n}(\text{Domain}) \subset f_{x_1}(f_{x_2} \circ \cdots \circ f_{x_n}(\text{Domain})) \subset \begin{cases} f_{x_1}(\text{Interior of orange}) & \text{if } x_2 = R_1 \\ f_{x_1}(\text{Interior of red}) & \text{if } x_2 = S_1 \\ f_{x_1}(\text{Interior of green}) & \text{if } x_2 = R_2 \\ f_{x_1}(\text{Interior of blue}) & \text{if } x_2 = S_2 \end{cases}$$

Now the claim follows using that, since the word is reduced, x_2 is not the inverse of x_1. For example, if $x_1 = R_1$, then x_2 is not S_1. Therefore, $f_{x_2} \circ \cdots \circ f_{x_n}(\text{Domain})$ is exterior to the red circle, and since f_{x_1} sends the exterior of the red circle to the interior of the orange circle, we deduce the claim in this case. The other cases are similar. The conclusion is that, since $f_{x_1} \circ \cdots \circ f_{x_n}(\text{Domain}) \neq \text{Domain}$, the elements f_{R_1} and f_{R_2} have no nontrivial relations. Therefore, after conjugating we deduce that f_{T_1} and f_{T_2} have no nontrivial relations. This not only shows that T_1, T_2 have no nontrivial relations, but also that $-I_2$ is not in the group generated by T_1, T_2, and we have proved

$$\Gamma(2) \simeq F_2 \times \{\pm I_2\} \quad \text{where} \quad F_2 \text{ is free in the two generators } T_1, T_2.$$

Remark 2.1.15. The circles in the diagram above are the *isometric circles* of the respective transformations: the red circle is the isometric circle of R_1, the orange circle is the isometric circle of S_1, the blue circle is the isometric circle of R_2 and the green circle is the isometric circle of S_2. The area labelled as Domain is actually a fundamental domain for the group generated by R_1, R_2, and is an example of a *Ford domain*. More details can be found in the beautiful classical paper titled *The fundamental region for a Fuchsian group* by L. R. Ford.

Exercise 1, Sheet 3: Compute the co-volume of the Hecke congruence subgroup $\Gamma_0(4) \subset \mathrm{SL}_2(\mathbb{Z})$. In case the facts

(1) $\mathrm{SL}_2(\mathbb{Z})$ has co-volume $\frac{\pi}{3}$
(2) $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right)$;

are used, these should be proved (in the relevant cases).

Solution. Note that $-I$ is in $\Gamma_0(4)$, so $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = [\mathrm{PSL}_2(\mathbb{Z}) : \{\pm I_2\}\backslash\Gamma_0(N)]$. Therefore, $\mathrm{Vol}(\Gamma_0(4)\backslash\mathbb{H}) = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4)]\mathrm{Vol}(\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H})$. We calculate the index for general N. Consider the principal congruence subgroup, $\Gamma(N) \subset \Gamma_0(N)$, consisting of matrices

$$\begin{pmatrix} 1+Na & Nb \\ Nc & 1+Nd \end{pmatrix} \text{ for } a,b,c,d \in \mathbb{Z} \text{ with determinant equal to } 1$$

Look at the exact sequence

$$1 \longrightarrow \Gamma(N) \longrightarrow \mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\text{mod } N} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow 1$$

The only part where exactness is not clear is the surjectivity[9]. Consider $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with integer entries such that $ad - bc = 1 + kN$. We want to find a matrix congruent to A mod N with determinant 1. Using the Smith normal form we can write $A = BDC$ where $B, C \in \mathrm{SL}_2(\mathbb{Z})$ and $D = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ with $d_1 d_2 = 1 + kN$. We put $X = \begin{pmatrix} d_1 + Nx & Ny \\ Nz & d_2 + Nw \end{pmatrix}$ and try to find integers x, y, z, w such that the matrix is in $\mathrm{SL}_2(\mathbb{Z})$. This is equivalent, after simplifying, to $k + wd_1 + xd_2 + N(xw - yz) = 0$. By Bézout we find integers x', w' such that $w'd_1 + x'd_2 = (d_1, d_2)$. Since (d_1, d_2) is a unit mod N, we find integers r, l such that $r(d_1, d_2) + k = Nl$. Thus, letting $x = rx'$ and $w = rw'$ the equation $k + wd_1 + xd_2 + N(xw - yz) = 0$ is equivalent to $l + xw - yz = 0$. We can now put $y = 1$ and $z = l + xw$. Thus given $D = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ with $d_1 d_2 = 1 + kN$ we have found D' congruent to D mod N and with determinant 1. Thus, $A' := BD'C$ is congruent to A mod N and is in $\mathrm{SL}_2(\mathbb{Z})$, proving the surjectivity in the exact sequence.

By the CRT, if $N = \prod p^{v_p}$ we have $\mathbb{Z}/N\mathbb{Z} \simeq \prod_{p|N} \mathbb{Z}/p^{v_p}\mathbb{Z}$ and thus $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_{p|N} \mathrm{SL}_2(\mathbb{Z}/p^{v_p}\mathbb{Z})$. For the cardinality of $\mathrm{SL}_2(\mathbb{Z}/p^l\mathbb{Z})$ we consider

$$1 \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p^l\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/p^l\mathbb{Z})^* \longrightarrow 1$$

where $(\mathbb{Z}/p^l\mathbb{Z})^*$ is the group of units mod p^l, of cardinality $\varphi(p^l) = (p-1)p^{l-1}$. Therefore, $\#\mathrm{SL}_2(\mathbb{Z}/p^l\mathbb{Z}) = \frac{\#\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})}{(p-1)p^{l-1}}$. To calculate the cardinality of GL_2, consider first $l = 1$. In this case $\mathbb{Z}/p\mathbb{Z}$ is a field, and it is easy to see that $\#\,\mathrm{GL}_2(k) =$

[9]See Shimura *Introduction to the arithmetic theory of automorphic functions*, Lemma 1.38, for an argument that works for SL_N

$(q^2-1)(q^2-q)$, whenever k is a finite field with cardinality q. In particular, $\#\,\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) = (p^2-1)(p^2-p)$ For $l>1$ consider the exact sequence

$$1 \longrightarrow \tilde{\Gamma}(\mathbb{Z}/p^l\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z}) \xrightarrow{\bmod p} \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow 1$$

Here $\tilde{\Gamma}(\mathbb{Z}/p^l\mathbb{Z})$ consists of matrices of the form $\begin{pmatrix} 1+pa & pb \\ pc & 1+pd \end{pmatrix}$ with entries in $\mathbb{Z}/p^l$. Therefore, $\#\tilde{\Gamma}(\mathbb{Z}/p^l\mathbb{Z}) = p^{4(l-1)}$, and

$$\#\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z}) = \#\tilde{\Gamma}(\mathbb{Z}/p^l\mathbb{Z})\#\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) = p^{4(l-1)}(p^2-1)(p^2-p)$$

and finally

$$\#\mathrm{SL}_2(\mathbb{Z}/p^l\mathbb{Z}) = \frac{\#\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})}{(p-1)p^{l-1}} = p^{3l-2}(p^2-1)$$

Recall that we are interested in the index of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. Clearly, $\Gamma_0(N)$ contains $\Gamma(N)$, and the image of $\Gamma_0(N)$ under reduction mod N (as in 19) is the group of upper triangular matrices with determinant one, of the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $a, b, d \in \mathbb{Z}/N\mathbb{Z}$ and $ad = 1 \mod N$. We can argue directly, by noting that b can be any arbitrary residue modulo N, that a must be a unit $\mod N$ and that d is determined by a, that the cardinality of this group is $N\varphi(N) = N^2\prod_{p|N}(1-p^{-1})$. Thus, we arrive at

$$[\Gamma_0(N) : \mathrm{SL}_2(\mathbb{Z})] = \frac{\#\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})}{N^2\prod_{p|N}(1-p^{-1})} = \frac{N^3\prod_{p|N}(1-p^{-2})}{N^2\prod_{p|N}(1-p^{-1})} = N\prod_{p|N}(1+p^{-1})$$

To calculate the covolume of $\mathrm{SL}_2(\mathbb{Z})$ we just need to integrate the volume form $y^{-2}dxdy$ over the fundamental domain $D := \{x+iy \mid y>1,\, y^2+x^2 \geq 1\,, -1/2 \leq x \leq 1/2\}$. We apply Fubini, integrating first over y to get

$$\mathrm{Vol}(D) = 2\int_0^{\frac{1}{2}}\left(\int_{\sqrt{1-x^2}}^{\infty} y^{-2}\,dy\right)dx = 2\int_0^{\frac{1}{2}}(1-x^2)^{-\frac{1}{2}}\,dy = 2\int_0^{\frac{\pi}{6}}d\theta = \frac{\pi}{3}$$

where we have performed the change of variables $x=\sin\theta$. Therefore, the covolume of $\Gamma_0(N)$ is

$$\frac{\pi}{3}N\prod_{p|N}(1+p^{-1})$$

In particular, the covolume of $\Gamma_0(4)$ is 2π.

While it is quite easy to construct non-compact Fuchsian groups of the first kind by just taking subgroups of $\mathrm{SL}_2(\mathbb{Z})$ determined by congruence conditions it is slightly harder to construct co-compact groups. A useful tool is the following result:

Theorem 2.1.16 (Nielsen). *Suppose $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{R})$ is non-abelian and contains only hyperbolic elements, then it acts properly discontinuous.*

Proof. Suppose that Γ is not discrete. Then we find a sequence $\gamma_k \to 1$ with $\gamma_k \neq 1$. Let σ be a fixed (hyperbolic) element of Γ. After conjugating Γ (if necessary) we can assume that σ fixes 0 and ∞ and thus is given by $\sigma = \mathrm{diag}(p, p^{-1})$ for some $p \in \mathbb{R}$. Given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ we compute the commutator

$$[\sigma, \gamma] = \sigma\gamma\sigma^{-1}\gamma^{-1} = \begin{pmatrix} 1 + (1 - q^2)bc & (q^2 - 1)ab \\ (q^{-2} - 1)cd & 1 + (1 - q^{-2})bc \end{pmatrix}.$$

We see that

$$\mathrm{tr}([\sigma, \gamma]) = 2 - (q - q^{-1})^2 bc.$$

Similar we find that

$$\mathrm{tr}([\sigma, [\sigma, \gamma]]) = 2 + (q - q^{-1})^4 abcd.$$

Of course we have

$$\gamma_k, [\sigma, \gamma_k], [\sigma, [\sigma, \gamma_k]] \to 1.$$

Note that since Γ does not contains only hyperbolic elements the (absolute values of the) traces of the commutators are all > 2. If $\gamma_k = \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix}$, we note that $b_k, c_k \to 0$ and $a_k, d_k \to 1$ as $k \to \infty$. Looking at the traces of the commutators we find that $bc \leq 0$ and $bc \geq 0$. In other words $b_k = 0$ or $c_k = 0$. In particular, we see that all γ_k share a fixed point with σ.

It can be easily seen that almost all γ_k must share the same fixed point with σ. Indeed, otherwise we find infinitely many k, l with

$$\gamma_k = \begin{pmatrix} a_k & b_k \\ 0 & d_k \end{pmatrix} \text{ and } \gamma_l = \begin{pmatrix} a_l & 0 \\ c_l & d_l \end{pmatrix}.$$

Multiplying these two matrices we see that $c_l, d_l \neq 0$ gives a contradiction to $\gamma_k\gamma_l \to 1$ as $k, l \to \infty$.

Suppose that almost all γ_k have the fixed point ∞ (the case that they all have the fixed point 0 is similar.) If we assume that 0 is not a fixed point then we have

$$\gamma_k = \begin{pmatrix} a_k & b_k \\ 0 & d_k \end{pmatrix} \text{ and } [\sigma, \gamma_k] = \begin{pmatrix} 1 & (q^2 - 1)a_k b_k \\ 0 & 1 \end{pmatrix}.$$

Thus we have found a parabolic element in Γ, which is a contradiction.

So far we have

$$\gamma_k = \begin{pmatrix} a_k & 0 \\ 0 & a_k^{-1} \end{pmatrix}$$

up to finitely many exceptions.

Since Γ is non-abelian and contains only hyperbolic elements there must be $\tau \in \Gamma$ that thus not preserve $\{0, \infty\}$. Write $\tau = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Considering the commutators $[\gamma_k, \tau]$, which tend to 1 as $k \to \infty$ one finds that $ab = 0 = cd$. This is a contradiction.

◻

Let $p \equiv 1 \bmod 4$ be prime and let n be not a quadratic residue modulo p. We claim now that the group[10]

$$\Gamma(n,p) = \left\{ \begin{pmatrix} a + b\sqrt{n} & (c + d\sqrt{n})\sqrt{p} \\ (c - d\sqrt{n})\sqrt{p} & a - b\sqrt{n} \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ a^2 - b^2 n - c^2 p + d^2 np = 1 \right\}$$

is Fuchsian of the first kind and co-compact. To see this one first checks that all elements are hyperbolic. Then Nielsen's theorem implies that $\Gamma(n,p)$ is a Fuchsian group. After checking that $\Gamma(n,p)$ has finite co-volume (i.e. a fundamental domain has finite volume) we are done. Indeed it contains no parabolic elements and hence must be co-compact.

Exercise 2, Sheet 8: For $q \in \mathbb{N}$ let $\Gamma(q) = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z}))$.

a) Show that, for a prime p and an exponent $t \in \mathbb{N}$ the quotient $\Gamma(p)/\Gamma(p^t)$ is a p-group.
b) Prove that the alternating group A_n, for $n \geq 7$ is not isomorphic to any composition factor in a composition series of $\mathrm{SL}_2(\mathbb{Z}/p^t\mathbb{Z})$.

It is well known that, if $q = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$, then

$$\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z}) \simeq \prod_{i=1}^{s} \mathrm{SL}_2(\mathbb{Z}/p_i^{t_i}\mathbb{Z})$$

In particular, the above implies that no composition factor in a composition series of $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ is isomorphic to A_n with $n \geq 7$.

c) Conclude that, if there is a normal subgroup $K \subset \mathrm{SL}_2(\mathbb{Z})$ such that $\mathrm{SL}_2(\mathbb{Z})/K \simeq A_n$ for some $n \geq 7$, then K can not contain any of the subgroups $\Gamma(q)$ with $q \in \mathbb{N}$. (Such a group K is usually called a non-congruence subgroup).

Remark 2.1.17. The exercise is also true for $n \geq 6$. However, it fails for $n = 5$, since $A_5 \simeq \mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})$. The group A_4 is not simple and $A_4 \simeq \mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z})$, in particular this last group is not simple. Finally, A_3 is cyclic of order 3 and it is a composition factor of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ (since it is the quotient of A_4 by the Klein four-group) and of $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$.

[10] This group is constructed from an order in a quaternion algebra.

Solution. For part a), observe that we need to count the number of matrices $\begin{pmatrix} 1+px & py \\ pz & 1+pw \end{pmatrix}$ with entries in $\mathbb{Z}/p^t\mathbb{Z}$ and determinant 1 modulo p^t. In particular, the values of x, y, z, w only matter modulo p^{t-1}. The condition $\det = 1$ translates to

$$\begin{aligned} &1 + px + pw + p^2xw - p^2yz \equiv 1 \bmod p^t \quad \text{if and only if} \\ &x + w + pxw - pyz \equiv 0 \bmod p^{t-1} \quad \text{if and only if} \\ &x(1+pw) \equiv pyz - w \bmod p^{t-1} \end{aligned}$$

Since $(1+pw)$ is a unit in $\mathbb{Z}/p^{t-1}\mathbb{Z}$, we can choose y, z, w freely and solve for x uniquely. Thus, $[\Gamma(p) : \Gamma(p^t)] = p^{3(t-1)}$.

Moving to part b), we take as granted that $\mathrm{PSL}_2(k)$ is simple for any field k of cardinality greater than 3 and that the group A_n is simple for $n \geq 5$. The cardinality of A_n is $n!/2$, in particular it is composite for $n > 3$. Since $\Gamma(p)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$, a composition series for $\mathrm{SL}_2(\mathbb{Z}/p^t\mathbb{Z})$ can be formed by pasting composition series for $\Gamma(p)/\Gamma(p^t)$ and for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. By part a), the composition series of $\Gamma(p)/\Gamma(p^t)$ will consist of composition factors of prime cardinality (finite p-groups are solvable). Also, for $p \geq 5$, since we have the exact sequence

$$1 \longrightarrow \{\pm \mathrm{Id}\} \longrightarrow \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z}) \longrightarrow 1$$

and $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is simple, the composition factors of $\mathrm{SL}_2(\mathbb{Z}/p^t\mathbb{Z})$ are, either of cardinality p, of cardinality 2, or $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$. Comparing these cardinalities with $n!/2 = \#A_n$, the only possibility is $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z}) \simeq A_n$. We know that the cardinality of $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is $1/2 \cdot p(p-1)(p+1)$. Therefore, if $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z}) \simeq A_n$ we must have

$$n! = p(p-1)(p+1)$$

In particular, $n!$ must be divisible by p, so necessarily $n \geq p$, and then $n! \geq p!$. Setting $n = p$, cancelling factors, we must have $(p+1) \geq (p-2)!$. This adds the restriction $p \leq 5$, and comparing $6!$ to $p(p-1)(p+1)$, we see that the above equality is impossible.

For part c), if such a K contained the principal congruence subgroup $\Gamma(q)$ for some $q \in \mathbb{N}$, then A_n would be a composition factor of $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$. Letting $q = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$, since

$$\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z}) \simeq \prod_{i=1}^{s} \mathrm{SL}_2(\mathbb{Z}/p_i^{t_i}\mathbb{Z})$$

we see that any composition factor of $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ must be a composition factor of $\mathrm{SL}_2(\mathbb{Z}/p_i^{t_i}\mathbb{Z})$ for some $1 \leq i \leq s$. By part b) this is impossible. ∎

2.2. **Multiplier Systems.** For $z \in \mathbb{C}$ we choose the argument to take values in $(-\pi, \pi]$ (i.e. $\arg(z) \in (-\pi, \pi]$). With this choice we take the principle branch of the logarithm to be

$$\log(z) = \log(|z|) + i\arg(z).$$

Further we define

$$z^s = \exp(s \log(z)).$$

We now define the quantity

$$j_g(z) = cz + d, \text{ where } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$$

The co-cycle condition

$$j_{gh}(z) = j_g(hz) j_h(z),$$

for $g, h \in \mathrm{SL}_2(\mathbb{R})$, is easy to verify.

Remark 2.2.1. Let us consider the following motivating example. Recall that in Remark 1.0.21 we have defined the Dedekind η-function. Further we used the identity

$$e_2(1, \tau) = -4\pi i \cdot \frac{d}{d\tau} \log(\eta(\tau))$$

and the transformation formula

$$e_2(c\tau + d, a\tau + b) = e_2(1, \tau) - 2\pi i \frac{c}{c\tau + d},$$

which is a special case of (7), to deduce that

$$\eta(\gamma\tau) = \epsilon_\gamma j_\gamma(\tau)^{\frac{1}{2}} \eta(\tau).$$

Here $\tau \in \mathbb{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

We deduce that

$$\epsilon_{gh} j_{gh}(\tau)^{\frac{1}{2}} = \epsilon_g \epsilon_h j_g(h\tau)^{\frac{1}{2}} j_h(\tau), \text{ for } g, h \in \mathrm{SL}_2(\mathbb{Z}).$$

The map $\mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C}^\times$, $g \mapsto \epsilon_g$ is the prototypical example of a multiplier system which we will define soon.

Before we continue we look at the following example, which should serve as a warning. Take

$$g = \begin{pmatrix} N+1 & N \\ -N & 1-N \end{pmatrix} \text{ and } h = \begin{pmatrix} 1 & 0 \\ -N & 1 \end{pmatrix}.$$

Then we see that

$$j_{gh}(z)^{\frac{1}{2}} = [\underbrace{(N^2 - 2N)z + 1 - N}_{\in \mathbb{H}}]^{\frac{1}{2}} \neq [\underbrace{\frac{-N}{-Nz+1} + 1 - N}_{\in -\mathbb{H}}]^{\frac{1}{2}} [\underbrace{-Nz + 1}_{\in -\mathbb{H}}]^{\frac{1}{2}} = j_g(hz)^{\frac{1}{2}} j_h(z)^{\frac{1}{2}}. \tag{19}$$

Indeed, both sides differ by a factor of -1.

We now define the number $\omega(g,h)$, for $g,h \in \mathrm{SL}_2(\mathbb{R})$, by

$$2\pi\omega(g,h) = -\arg(j_{gh}(z)) + \arg(j_g(hz)) + \arg(j_h(z)).$$

It can be seen that $\omega(g,h) \in \{-1,0,1\}$ and it is independent of $z \in \mathbb{H}$.

Lemma 2.2.2. *For $g,h,h' \in \mathrm{SL}_2(\mathbb{R})$ and $u = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ we have*

$$\begin{aligned}
&\omega(gh,h') + \omega(g,h) = \omega(g,hh') + \omega(h,h'),\\
&\omega(g,h) = \omega(h,g) \text{ if } gh = hg,\\
&\omega(ug,h) = \omega(g,hu) = \omega(g,h),\\
&\omega(gu,h) = \omega(g,uh),\\
&\omega(g^{-1}ug,h) + \omega(g,g^{-1}ugh) = \omega(g,h),\\
&\omega(g,u) = \omega(u,g) = 0 \text{ and}\\
&\omega(gug^{-1},g) = \omega(g,g^{-1}ug) = 0.
\end{aligned}$$

Proof. Exercise. ∎

Furthermore, if $g = \begin{pmatrix} * & * \\ 0 & d \end{pmatrix}$ with $d < 0$, then

$$\omega(g,g^{-1}) = 1.$$

Otherwise we have

$$\omega(g,g^{-1}) = 0.$$

Definition 2.2.1. For $k \in \mathbb{R}$ we define the **factor system of weight** k by setting

$$w(g,h) = e(k\omega(g,h)), \text{ with } g,h \in \mathrm{SL}_2(\mathbb{R}).$$

We note straight away that this only depends on k modulo 1. The purpose of this definition is the identity

$$w(g,h)j_{gh}(z)^k = j_g(hz)^k j_h(z)^k. \tag{20}$$

This fixes the *mistake* in (19). If we further define the slash operator $|_k g$ acting on functions $f\colon \mathbb{H} \to \mathbb{C}$ by

$$[f|_k g](z) = j_g(z)^{-k} f(gz),$$

then we obtain the composition rule

$$f|_k gh = w(g,h)[f|_k g]|_k h.$$

Now let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{R})$ be a discrete subgroup.[11]

[11] Its image in $\mathrm{PSL}_2(\mathbb{R})$ will then be a Fuchsian group as discussed earlier in this Chapter.

Definition 2.2.2. A **multiplier system of weight** k **for** Γ is a function $\vartheta\colon \Gamma \to S^1$ such that

$$\vartheta(\gamma_1\gamma_2) = w(\gamma_1, \gamma_2)\vartheta(\gamma_1)\vartheta(\gamma_2).$$

If $-1 \in \Gamma$ we additionally require that $\vartheta(-1) = e(-\frac{k}{2})$.[12]

Let us look at examples:

- The function $\vartheta(g) = \epsilon_g$ given by the transformation behavior of the Dedekind η-function is the prototype of a weight $\frac{1}{2}$ multiplier system for $\mathrm{SL}_2(\mathbb{Z})$.
- If $k \in \mathbb{Z}$, then a multiplier of weight k for Γ is simply a character of Γ. A particular explicit example can be constructed for $\Gamma_0(N)$ from a Dirichlet character χ modulo N by setting

$$\chi\colon \Gamma_0(N) \to S^1, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \chi(d).$$

  If $\chi(-1) = (-1)^k$, then this defines a weight k multiplier system for $\Gamma_0(N)$, which is also denoted by χ.

The following constructions allow us to create *new* multiplier systems from existing ones:

- If ϑ is a multiplier system of weight k for Γ and $k' \equiv k \bmod 2$, then ϑ is a multiplier system of weight k' for Γ.
- If ϑ is a multiplier system of weight k for Γ, then $\overline{\vartheta}$ is a multiplier system of weight $-k$ for Γ.
- If ϑ_1 and ϑ_2 are multiplier systems of weight k_1 (resp. k_2) for Γ, then $\vartheta_1 \cdot \vartheta_2$ is a multiplier system of weight $k_1 + k_2$ for Γ.
- If ϑ is a multiplier system of weight k for Γ and $\sigma \in \mathrm{SL}_2(\mathbb{R})$, then

$$\vartheta^\sigma(\gamma) = \vartheta(\sigma\gamma\sigma^{-1})w(\sigma\gamma\sigma^{-1}, \sigma)\overline{w(\sigma, \gamma)} \tag{21}$$

  is a multiplier system of weight k for $\sigma^{-1}\Gamma\sigma$. One verifies that

$$\vartheta^{\sigma\tau} = (\vartheta^\sigma)^\tau \text{ and } \vartheta^\gamma = \vartheta,$$

  for $\tau \in \mathrm{SL}_2(\mathbb{Z})$ and $\gamma \in \Gamma$.

Exercise 2, Sheet 3: Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be a discrete subgroup and let ϑ be a multiplier system of weight k for Γ. Further let $\sigma \in \mathrm{SL}_2(\mathbb{R})$. Show that

a) $\vartheta^\sigma(\gamma) = \vartheta(\sigma\gamma\sigma^{-1})w(\sigma\gamma\sigma^{-1}, \sigma)\overline{w(\sigma, \gamma)}$ is a multiplier system of weight k for $\sigma^{-1}\Gamma\sigma$;
b) $\vartheta^{\sigma\tau} = (\vartheta^\sigma)^\tau$ for $\sigma, \tau \in \mathrm{SL}_2(\mathbb{R})$; and
c) $\vartheta^\gamma = \vartheta$ for $\gamma \in \Gamma$.

If formulae from Lemma 2.2.2 of the lecture notes are used, then proving them is part of the exercise.

[12] It is clear that $\vartheta(-1) = \pm e(-\frac{k}{2})$ must hold. We choose the positive sign for consistency reasons. Indeed in connection with modular forms, which we will define soon, this is sensible since -1 acts trivially on $\mathbb{H}$.

Solution. For part a) we need to proof that

$$\vartheta^\sigma(\sigma^{-1}\gamma_1\gamma_2\sigma) = w(\sigma^{-1}\gamma_1\sigma, \sigma^{-1}\gamma_2\sigma)\vartheta^\sigma(\sigma^{-1}\gamma_1\sigma)\vartheta^\sigma(\sigma^{-1}\gamma_2\sigma)$$

for arbitrary $\gamma_1, \gamma_2 \in \Gamma$, where $w(g,h) := e(k\omega(g,h))$ is the factor system of weight k. Using the definition of ϑ^σ and $\vartheta(\gamma_1\gamma_2) = w(\gamma_1,\gamma_2)\vartheta(\gamma_1)\vartheta(\gamma_2)$ (since ϑ is a multiplier system of weight k), part a) is equivalent to

$$\begin{aligned} &w(\gamma_1,\gamma_2)w(\gamma_1\gamma_2,\sigma)w(\sigma,\sigma^{-1}\gamma_1\sigma)w(\sigma,\sigma^{-1}\gamma_2\sigma) \\ &\qquad = w(\gamma_1,\sigma)w(\gamma_2,\sigma)w(\sigma,\sigma^{-1}\gamma_1\gamma_2\sigma)w(\sigma^{-1}\gamma_1\sigma,\sigma^{-1}\gamma_2\sigma) \end{aligned} \tag{22}$$

Recall the first equation of Lemma 2.2.2, which we will prove below. It implies

$$w(gh,h')w(g,h) = w(g,hh')w(h,h') \tag{23}$$

for arbitrary $g,h,h' \in \mathrm{SL}_2(\mathbb{R})$. We use it three times. First, let $g = \sigma$, $h = \sigma^{-1}\gamma_1\sigma$ and $h' = \sigma^{-1}\gamma_2\sigma$. We recognize $w(g,hh')w(h,h')$ on the right hand side of (22). Using (23) and canceling some terms, (22) is equivalent to

$$w(\gamma_1,\gamma_2)w(\gamma_1\gamma_2,\sigma)w(\sigma,\sigma^{-1}\gamma_2\sigma) = w(\gamma_1,\sigma)w(\gamma_2,\sigma)w(\gamma_1\sigma,\sigma^{-1}\gamma_2\sigma) \tag{24}$$

Now let $g = \gamma_1$, $h = \gamma_2$ and $h' = \sigma$. We recognize $w(gh,h')w(g,h)$ on the left hand side of (24). Using (23) and cancelling some terms, (22) is equivalent to

$$w(\gamma_1,\gamma_2\sigma)w(\sigma,\sigma^{-1}\gamma_2\sigma) = w(\gamma_1,\sigma)w(\gamma_1\sigma,\sigma^{-1}\gamma_2\sigma) \tag{25}$$

This is equation (23) in the disguise $g = \gamma_1$, $h = \sigma$ and $h' = \sigma^{-1}\gamma_2\sigma$. Thus, part a) is proved.

For part b), unravelling the definitions (testing the equality on $\tau^{-1}\sigma^{-1}\gamma\sigma\tau$) we see that the statement is equivalent to showing

$$\mathrm{LHS} := w(\gamma,\sigma\tau)\overline{w(\sigma\tau,(\sigma\tau)^{-1}\gamma\sigma\tau)} = w(\gamma,\sigma)\overline{w(\sigma,\sigma^{-1}\gamma\sigma)}w(\sigma^{-1}\gamma\sigma,\tau)\overline{w(\tau,(\sigma\tau)^{-1}\gamma\sigma\tau)} =: \mathrm{RHS}$$

Using (23) with $g = \sigma, h = \sigma^{-1}\gamma\sigma, h' = \tau$ we see that

$$\mathrm{RHS} = w(\gamma,\sigma)w(\gamma\sigma,\tau)\overline{w(\sigma,\sigma^{-1}\gamma\sigma\tau)w(\tau,(\sigma\tau)^{-1}\gamma\sigma\tau)}$$

Using (23) again, this time with $g = \gamma, h = \sigma, h' = \sigma^{-1}\gamma\sigma\tau$ we obtain

$$\mathrm{RHS} = w(\gamma,\gamma\sigma\tau)w(\gamma\sigma,\tau)\overline{w(\gamma\sigma,\sigma^{-1}\gamma\sigma\tau)w(\tau,(\sigma\tau)^{-1}\gamma\sigma\tau)}.$$

For the LHS, we use (23) with $g = \gamma, h = \sigma\tau$ and $h' = (\sigma\tau)^{-1}\gamma\sigma\tau$ obtaining

$$\mathrm{LHS} = w(\gamma,\gamma\sigma\tau)\overline{w(\gamma\sigma\tau,(\sigma\tau)^{-1}\gamma\sigma\tau)}.$$

Comparing the last expressions for LHS and RHS, we can cancel $w(\gamma,\gamma\sigma\tau)$ and we easily recognize the remaining equality as an instance of (23) with $g = \gamma\sigma, h = \tau$ and $h' = (\sigma\tau)^{-1}\gamma\sigma\tau$. This completes the proof of part b).

Part c) is simpler. Indeed,

$$\begin{aligned}\vartheta^{\gamma_0}(\gamma) &:= \vartheta(\gamma_0\gamma\gamma_0^{-1})w(\gamma_0\gamma\gamma_0^{-1},\gamma_0)\overline{w(\gamma_0,\gamma)} = \vartheta(\gamma_0)^{-1}\theta(\gamma_0\gamma)\overline{w(\gamma_0,\gamma)}\\ &= \vartheta(\gamma)\end{aligned}$$

where we have used the definition of multiplier system twice.

To prove equality (23) from Lemma 2.2.2, recall that $w(g,h) := e(k\omega(g,h))$, and that the definition of $\omega(g,h)$ is

$$2\pi\omega(g,h) := -\arg(j_{gh}(z)) + \arg(j_g(hz)) + \arg(j_h(z)) \tag{26}$$

which does not depend on $z \in \mathbb{H}$. Plugging in this definition in equality (23), cancelling some terms and rearranging, we are left to check that

$$-\arg(j_{gh}(z))+\arg(j_g(hz))+\arg(j_h(z)) = -\arg(j_{gh}(h'z))+\arg(j_g(hh'z))+\arg(j_h(h'z)).$$

But this holds since the definition of $\omega(g,h)$ does not depend on $z \in \mathbb{H}$, and thus both sides are equal to $2\pi\omega(g,h)$. ◻

2.3. **General Modular Forms.** Let Γ be a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$, $k \in \mathbb{R}$ and ϑ a multiplier system of weight k for Γ. From now on we will assume that Γ (viewed as a subgroup of $\mathrm{PSL}_2(\mathbb{R})$) is of the first kind. In particular Γ is finitely generated (or geometrically finite) and has finite co-volume.

Definition 2.3.1. A modular form for Γ of weight k with respect to the multiplier system ϑ is a holomorphic function $f\colon \mathbb{H} \to \mathbb{C}$ such that

- $f|_k\gamma = \vartheta(\gamma)f$ for all $\gamma \in \Gamma$; and
- f is holomorphic at every cusp.

The space of all such functions will be denoted by $M_k(\Gamma,\vartheta)$.

The last condition requires some additional explanation. First, a cusp of Γ is a fixed point of a parabolic element in Γ. Note that, if Γ is geometrically finite (i.e. finitely generated), then there are only finitely many Γ-orbits of cusps. The letters $\mathfrak{a},\mathfrak{b},\dots$ are usually reserved for cusps. Given a cusp $\mathfrak{a} \in \mathbb{R}\cup\{\infty\}$ the stabilizer group $\Gamma_{\mathfrak{a}} \subseteq \mathrm{PLS}_2(\mathbb{R})$ is cyclic and infinite.[13] Thus we write

$$\Gamma_{\mathfrak{a}} = \langle\gamma_{\mathfrak{a}}\rangle.$$

There is a so called **scaling matrix** $\sigma_{\mathfrak{a}} \in \mathrm{SL}_2(\mathbb{R})$ such that

$$\sigma_{\mathfrak{a}}^{-1}\gamma_{\mathfrak{a}}\sigma_{\mathfrak{a}} = T.$$

[13] We can lift $\Gamma_{\mathfrak{a}}$ to a subgroup of $\Gamma \subseteq \mathrm{SL}_2(\mathbb{R})$. However, if $-1 \in \Gamma$, then we have to add $-\gamma_{\mathfrak{a}}$.

In particular $\sigma_{\mathfrak{a}}\infty = \mathfrak{a}$. We now compute

$$\begin{aligned}
[f|_k\sigma_{\mathfrak{a}}](Tz) &= j_{\sigma_{\mathfrak{a}}}(Tz)^{-k} f(\sigma_{\mathfrak{a}}Tz) \\
&= j_{\sigma_{\mathfrak{a}}}(Tz)^{-k} f(\gamma_{\mathfrak{a}}\sigma_{\mathfrak{a}}z) \\
&= j_{\sigma_{\mathfrak{a}}}(Tz)^{-k} j_{\gamma_{\mathfrak{a}}}(\sigma_{\mathfrak{a}}z)^k \vartheta(\gamma_{\mathfrak{a}}) f(\sigma_{\mathfrak{a}}z) \\
&= j_{\sigma_{\mathfrak{a}}}(Tz)^{-k} j_{\gamma_{\mathfrak{a}}}(\sigma_{\mathfrak{a}}z)^k j_{\sigma_{\mathfrak{a}}}(z)^k \vartheta(\gamma_{\mathfrak{a}})[f|_k\sigma_{\mathfrak{a}}](z).
\end{aligned}$$

Now we observe that since $j_T(z) = 1$ we can apply (20) twice to get

$$j_{\sigma_{\mathfrak{a}}}(Tz)^{-k} j_{\gamma_{\mathfrak{a}}}(\sigma_{\mathfrak{a}}z)^k j_{\sigma_{\mathfrak{a}}}(z)^k = j_{\sigma_{\mathfrak{a}}}(Tz)^{-k} j_T(z)^{-k} j_{\gamma_{\mathfrak{a}}\sigma_{\mathfrak{a}}}(z)^k w(\gamma_{\mathfrak{a}}, \sigma_{\mathfrak{a}}) = \frac{w(\gamma_{\mathfrak{a}}, \sigma_{\mathfrak{a}})}{w(\sigma_{\mathfrak{a}}, T)}.$$

However, by the last two properties given in Lemma 2.2.2 we have

$$w(\gamma_{\mathfrak{a}}, \sigma_{\mathfrak{a}}) = w(\sigma_{\mathfrak{a}}, T) = 1.$$

This shows that

$$[f|_k\sigma_{\mathfrak{a}}](z+1) = [f|_k\sigma_{\mathfrak{a}}](Tz) = \vartheta(\gamma_{\mathfrak{a}})[f|_k\sigma_{\mathfrak{a}}](z).$$

Writing $\vartheta(\gamma_{\mathfrak{a}}) = e(\kappa_{\mathfrak{a}})$ for $\kappa_{\mathfrak{a}} \in [0, 1)$ we find that the function

$$g(e(z)) = e(-\kappa_{\mathfrak{a}}z)[f|_k\sigma_{\mathfrak{a}}](z) \tag{27}$$

is one periodic. We say f is holomorphic at $\mathfrak{a}$ if $g(q)$ is holomorphic at 0.

Remark 2.3.1. What is happening here is that we equip the orbifold $\Gamma\backslash\mathbb{H}$ (where Γ is a Fuchsian group of the first kind) with appropriate charts at the cusps. Let us elaborate on this. Let $\pi\colon \mathbb{H} \to \Gamma\backslash\mathbb{H}$ be the canonical projection. For $z \in \mathbb{H}$ we find a disc $U_z \subseteq \mathbb{H}$ such that $\gamma U_z \cap U_z = \emptyset$ for all $\gamma \in \Gamma \setminus \Gamma_z$ and $\gamma U_z = U_z$ for $\gamma \in \Gamma_z$. Note that Γ_z is cyclic and of order $m \geq 1$. Therefore we choose $\tau_z \in \mathrm{SL}_2(\mathbb{C})$ such that $\tau_z U_z = U$, for $U = \{z\colon |z| < 1\}$. A chart is then given by $(\pi U_z), e_m\tau_z\pi^{-1})$, for $e_m(z) = z^m$. Similarly one defines charts $(\pi U_{\mathfrak{a}}, e_\infty\sigma_{\mathfrak{a}}^{-1}\pi^{-1})$. Now $e_\infty(z) = e(z)$, $\sigma_{\mathfrak{a}}$ is the scaling matrix and $U_{\mathfrak{a}}$ is a sufficiently small disc tangent to $\mathbb{R} \cup \{\infty\}$ at $\mathfrak{a}$. The role of U is played by $\mathbb{H}^Y = \{x + iy\colon y > Y\}$ for sufficiently large Y.

Note that if $g(q)$ is holomorphic at 0, then we can write down a Taylor expansion. This translates into the **Fourier expansion**

$$[f|_k\sigma_{\mathfrak{a}}](z) = e(\kappa_{\mathfrak{a}}z)\sum_{n=0}^{\infty} a_f(n, \mathfrak{a})e(nz)$$

of f at $\mathfrak{a}$. The numbers $a_f(\cdot, \mathfrak{a})$ are the Fourier coefficients of f at $\mathfrak{a}$.

Definition 2.3.2. A cusp $\mathfrak{a}$ of Γ is said to be singular for ϑ if $\vartheta(\gamma_{\mathfrak{a}}) = 1$. Further $f \in M_k(\Gamma, \vartheta)$ is called a cusp form if $a_f(0, \mathfrak{a}) = 0$ for all singular cusps of Γ. The space of all cusp forms for Γ of weight k with respect to the multiplier system ϑ is denoted by $S_k(\Gamma, \vartheta)$.

Let us give some examples that we already encountered:

(1) The Dedekind η function is a modular form of weight $\frac{1}{2}$ for $\mathrm{SL}_2(\mathbb{Z})$ with respect to ϑ_{eta}. It is a cusp form because there are no singular cusps. Indeed (up to equivalence) the only cusp of $\mathrm{SL}_2(\mathbb{Z})$ is $\mathfrak{a} = \infty$, but $\vartheta_{\mathrm{eta}}(T) = e(\frac{1}{24})$.[14]

(2) Let $k \geq 4$ be even. Recall the *numbers* $e_k(u, v)$ appearing as the constant term in the Taylor expansion of the elliptic functions

$$\mathbf{E}_k(x) = x^{-k} + e_k + \dots .$$

We claim that $E_k(z) = \frac{1}{2\zeta(k)} e_k(1, z)$ is a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$ with respect to the trivial multiplier system. To see this we compute

$$\begin{aligned}[E_k|_k\gamma](z) = j_\gamma(z)^{-k} E_k(\gamma z) &= (cz + d)^{-k} \frac{e_k(1, \gamma z)}{2\zeta(k)} \\ &= \frac{e_k(cz + d, az + b)}{2\zeta(k)} = \frac{e_k(1, \gamma z)}{2\zeta(k)} \\ &= \frac{e_k(1, z)}{2\zeta(k)} = E_k(z)\end{aligned}$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. The Fourier expansion is already computed in Lemma 1.0.9 and upon noticing that $2\zeta(k) = \frac{(2\pi)^k}{k!} B_k$ we obtain

$$E_k(z) = 1 + i^k \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) e(nz).$$

In particular these are not cusp forms.

(3) Note that

$$E_2(z) = \frac{e_2(1, z)}{2\zeta(2)} = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) e(nz) \tag{28}$$

is not a modular form of weight 2 for $\mathrm{SL}_2(\mathbb{Z})$ with trivial multiplier system. Indeed, according to (7) we have

$$[E_2|_2\gamma](z) = \frac{e_2(cz + d, az + d)}{2\zeta(2)} = E_2(z) + \frac{12}{2\pi i} \cdot \frac{c}{cz + d}.$$

But, we can compute that $f(z) = E_2(z) - N E_2(Nz)$ is a modular form of weight 2 for $\Gamma_0(N)$ with trivial multiplier system. We first note that

$$N \cdot \frac{az + b}{cz + d} = \frac{aNz + Nb}{\frac{c}{N} Nz + d}.$$

[14] For now this will be the only *exciting* multiplier system we will encounter.

Thus applying the transformation behavior of E_2 observed above we find that

$$[f|_k\gamma](z) = f(z) + \frac{12}{2\pi i} \cdot [\frac{c}{cz+d} - N \cdot \frac{\frac{c}{N}}{\frac{c}{N}Nz+d}] = f(z).$$

This is again no cusp form.

(4) To find a cusp form of integral weight we observe in the new normalization the Eisenstein series E_k (for $k \geq 4$) have constant term equal to 1. Thus if we can take the difference between two of these we get a function without constant term at ∞. However, for this function to have the right transformation behavior we have to take care of the weight:

$$\Delta(z) = \frac{E_3(z)^3 - E_6(z)^2}{1728} = e(z) + \dots.$$

This is a cusp form for $\mathrm{SL}_2(\mathbb{Z})$ of weight 12 and trivial multiplier system. Actually we have already seen a version of this function in (17) above. Indeed we get

$$(2\pi)^{12} \cdot \Delta(z) = 2^4 3^3 5^2 (20 e_4(1,z)^3 - 49 e_6(1,z)^2) = \widetilde{\Delta}.$$

Furthermore we get equality

$$\Delta(z) = \eta(z)^{24}.$$

The latter implies that $\vartheta_{\mathrm{eta}}^{24}$ is trivial and that we can write

$$\Delta(z) = e(z)\prod_{n=1}^{\infty}(1-e(nz))^{24} = \sum_{n=1}^{\infty}\tau(n)e(nz).$$

The coefficients $\tau(n)$ form a very special arithmetic function called the Ramanujan function. Of course we have $\tau(1) = 1$, but it has many more very interesting properties. Ramanujan conjectured that $\tau(n)$ is multiplicative and satisfies the bound $\tau(p) \leq 2 \cdot p^{\frac{11}{2}}$ for primes p. Both conjectures are now known, but are very deep.

(5) **Non-example:** The function

$$j(z) = \frac{E_4(z)^3}{\Delta(z)}.$$

This function transforms like a modular form of weight 0 with respect to $\mathrm{SL}_2(\mathbb{Z})$ (and trivial multiplier system), but has a simple pole at ∞. Thus it is not holomorphic at the cusps! (It anyway plays a major role in number theory.)

Exercise 3, Sheet 3: Recall that the η-multiplier ϑ_{eta} of weight $\frac{1}{2}$ for $\mathrm{SL}_2(\mathbb{Z})$ is given by the functional equation

$$\eta(\gamma z) = \vartheta_{\mathrm{eta}}(\gamma) j_\gamma(z)^{\frac{1}{2}} \eta(z) \tag{29}$$

a) Show that

$$\vartheta_{\text{eta}}(-\gamma) = e\left(\frac{1}{4}\right)\vartheta_{\text{eta}}(\gamma) \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ with } c > 0,$$
$$\vartheta_{\text{eta}}(T^m) = e\left(\frac{m}{24}\right) \text{ and}$$
$$\vartheta_{\text{eta}}(S) = i^{-\frac{1}{2}}$$

Since T and S generate $\mathrm{SL}_2(\mathbb{Z})$ this is in principle sufficient to understand the full η-multiplier. But the analysis is a bit tedious. The final result is

$$\vartheta_{\text{eta}}(\gamma) = e\left(\frac{a+d-3c}{24c} - \frac{1}{2}s(d,c)\right), \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with } c > 0. \tag{30}$$

Here $s(d,c)$ is the Dedekind sum given by

$$s(d,c) = \sum_{0 \le n < c} \frac{n}{c} \cdot \left(\frac{dn}{c} - \lfloor \frac{dn}{c} \rfloor - \frac{1}{2}\right) \tag{31}$$

This sum satisfies the reciprocity law

$$s(d,c) + s(c,d) = \frac{1}{12}\left(\frac{d}{c} + \frac{c}{d} + \frac{1}{cd} - 3\right), \text{ for coprime } c, d > 0. \tag{32}$$

b) Derive the reciprocity formula (32) modulo 2 from (29) and (30).

Solution. Recall the definition

$$\eta(\tau) = q^{\frac{1}{24}} P(q) = e\left(\frac{\tau}{24}\right) P(q) \text{ where } q = e(\tau) \text{ and } \tau \in \mathbb{H}.$$

Since $e(\tau + m) = e(\tau)$ we get $\eta(T^m\tau) = e\left(\frac{m}{24}\right)\eta(\tau)$, and comparing with (29) and using $j_{T^m}(z) = 1$ we get

$$\vartheta_{\text{eta}}(T^m) = e\left(\frac{m}{24}\right)$$

Note also that, since $-\gamma z = \gamma z$, from (29) we have

$$\vartheta_{\text{eta}}(-\gamma) = \frac{j_\gamma(z)^{\frac{1}{2}}}{j_{-\gamma}(z)^{\frac{1}{2}}}\vartheta_{\text{eta}}(\gamma)$$

Recall $j_\gamma(z) = cz + d \in \mathbb{H}$ since $c > 0$, and that the branch of the logarithm has $\arg \in (-\pi, \pi]$. Writing $\phi := \arg(cz+d) \in (0,\pi)$ we have $j_\gamma(z)^{\frac{1}{2}} = |cz+d|^{\frac{1}{2}} e^{i\frac{\phi}{2}}$. On the other hand, $\arg(-cz-d) = \arg(cz+d) - \pi \in (-\pi, 0) = \phi - \pi$ and therefore $j_{-\gamma}(z)^{\frac{1}{2}} = |cz+d|^{\frac{1}{2}} e^{i\frac{\phi}{2} - i\frac{\pi}{2}}$. Thus

$$\vartheta_{\text{eta}}(-\gamma) = \frac{j_\gamma(z)^{\frac{1}{2}}}{j_{-\gamma}(z)^{\frac{1}{2}}}\theta_{\text{eta}}(\gamma) = e^{i\frac{\pi}{2}}\vartheta_{\text{eta}}(\gamma) = e(\frac{1}{4})\vartheta_{\text{eta}}(\gamma)$$

Recall that $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, with i as fixed point, $Si = i$. Thus, plugging $\gamma = S$ and $z = i$ in (29) we see

$$\vartheta_{\mathrm{eta}}(S) = j_S(i)^{-\frac{1}{2}} = i^{-\frac{1}{2}} = e(\frac{-1}{8})$$

with the branch of the logarithm as above (we have used $j_S(z) = z$). This finishes the proof of part a).

For part b), let $c, d > 0$ coprime and choose a, b so that $ad - bc = 1$ (this is possible since $(c, d) = 1$). Write $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Applying the definition of multiplier system of weight $1/2$ to γ and S gives

$$\vartheta_{\mathrm{eta}}(\gamma S) = e\left(\frac{-\arg j_{\gamma S}(z) + \arg j_\gamma(Sz) + \arg j_S(z)}{4\pi}\right) \vartheta_{\mathrm{eta}}(\gamma)\vartheta_{\mathrm{eta}}(S)$$

for *any* $z \in \mathbb{H}$. Put $z = i$, so that $Sz = z = i$ and observe that $\arg j_S(i) = \arg(i) = \frac{\pi}{2}$. We calculate $\gamma S = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$ and therefore $j_{\gamma S}(i) = di - c$ while $j_\gamma(i) = ci + d$. Since $di - c = i(ci + d)$ and $c, d > 0$ we get (with our branch of arg) that $\arg(di - c) = \frac{\pi}{2} + \arg(ci + d)$. Therefore we arrive at

$$\vartheta_{\mathrm{eta}}(\gamma S) = \vartheta_{\mathrm{eta}}(\gamma)\vartheta_{\mathrm{eta}}(S) = \vartheta_{\mathrm{eta}}(\gamma) e\left(-\frac{1}{8}\right)$$

From formula (30) after rearranging we see

$$\frac{1}{2}\left(s(d, c) - s(-c, d)\right) = \frac{1}{24}\left(\frac{a + d}{c} + \frac{c - b}{d} - 3\right) = \frac{1}{24}\left(\frac{d}{c} + \frac{c}{d} + \frac{1}{cd} - 3\right)$$

modulo 1, where we have used $ad - bc = 1$. Using $s(-c, d) = -s(c, d)$ (apparent from the oddness of the sawtooth function in the definition (31)) and multiplying by 2 we get (32) modulo 2. $\square$

The next result gives an alternative description of the regularity condition of modular forms at the cusps.

Lemma 2.3.2. *Suppose $f\colon \mathbb{H} \to \mathbb{C}$ is holomorphic and satisfies $f|_k\gamma = \vartheta(\gamma)f$ for all $\gamma \in \Gamma$.*

(1) *$f \in M_k(\Gamma, \vartheta)$ if and only if f is of moderate growth (i.e. $|y^{\frac{k}{2}} f(x + iy)| \leq C(y^A + y^{-A})$ for constants $C, A > 0$.)*
(2) *$f \in S_k(\Gamma, \vartheta)$ if and only if $\mathrm{Im}(\cdot)^{\frac{k}{2}} f(\cdot)$ is bounded.*

Proof. We will only proof the first part and leave the second part as an exercise (see below). If Γ is co-compact, then there is nothing to show. Thus, suppose that

$\mathfrak{a}$ is a cusp of Γ. Since f is holomorphic in $\mathbb{H}$ we have the expansion

$$[f|_k\sigma_{\mathfrak{a}}](z) = \sum_{n=-\infty}^{\infty} a_f(n;\mathfrak{a})e((n+\kappa_{\mathfrak{a}})z).$$

This is noting but the Laurent expansion of g as defined in (27). The coefficients can be computed by

$$a_f(n;\mathfrak{a}) = \int_{z_0}^{z_0+1} [f|_k\sigma_{\mathfrak{a}}](z)e(-(n+\kappa_{\mathfrak{a}})z)dz,$$

for $z_0 \in \mathbb{H}$ with sufficiently large imaginary part. Note that this is independent of z_0 and of the path of integration.

Assume that f has moderate growth. We first consider the case when $\mathfrak{a} = \infty$. In this case we can choose the scaling matrix to be $\sigma_\infty = \operatorname{diag}(h, h^{-1})$ for some positive real number h. Using the moderate growth condition we obtain the estimate

$$|a_f(n;\infty)| \leq h^k \int_0^1 |f(h^2(y+ix))| \exp(2\pi(n+\kappa_{\mathfrak{a}})y)dx \leq C(f,\Gamma)y^A \exp(2\pi(n+\kappa_{\mathfrak{a}})y).$$

The crucial observation is that, for $n<0$ the right hand side goes to 0 as $y\to\infty$. This implies that $a_f(n;\infty) = 0$ for $n<0$. Second we consider another cusp $\mathfrak{a}\neq\infty$. Observe that

$$\operatorname{Im}(\sigma_{\mathfrak{a}}z) = \frac{\operatorname{Im}(z)}{|cz+d|^2} = \frac{y}{c^2y^2+(cx+d)^2} \geq C_1(c,d)\frac{1}{y+y^{-1}} \geq C_1(c,d)y^{-1},$$

for $z = x+iy$ with $x\in[0,1]$, $y>1$ and $\sigma_{\mathfrak{a}} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $c\neq 0$. Combining this with the moderate growth property we end up with

$$|[f|_k\sigma_{\mathfrak{a}}](z)| \leq C_2(f)\operatorname{Im}(\sigma_{\mathfrak{a}})^{-A}\operatorname{Im}(z)^{-\frac{k}{2}} \leq C_3(f,\mathfrak{a})y^{A-\frac{k}{2}}.$$

With this estimate at hand we can proceed as in the case of the cusp ∞.

For the opposite direction we assume that $f\in M_k(\Gamma,\vartheta)$. Note that f is bounded in any compact subset of $\mathbb{H}$. Furthermore, $[f|_k\sigma_{\mathfrak{a}}](z)\to a_f(0;\mathfrak{a})$ for $z\to\infty$. Thus $f|_k\sigma_{\mathfrak{a}}$ is bounded in a neighbourhood of ∞. By definition of the slash operator this implies that f is polynomial bounded in a neighbourhood of $\mathfrak{a}$. ◻

Exercise 1, Sheet 4: Let $f:\mathbb{H}\to\mathbb{C}$ be holomorphic and assume that $f|_k\gamma = \vartheta(\gamma)f$ for all $\gamma\in\Gamma$. Show that $f\in S_k(\Gamma,\vartheta)$ if and only if $\operatorname{Im}(\cdot)^{k/2}f(\cdot)$ is bounded.

Solution: Note that $\operatorname{Im}(\cdot)^{k/2}|f(\cdot)|$ is invariant under Γ. Indeed, by the modularity of f

$$\operatorname{Im}(\gamma z)^{k/2}f(\gamma z) = \operatorname{Im}(z)^{k/2}|cz+d|^{-k}\vartheta(\gamma)j_\gamma(z)^k f(z).$$

Since $|j_\gamma(z)| = |cz+d|$, taking absolute values we find

$$|\operatorname{Im}(\gamma z)^{k/2}f(\gamma z)| = |\operatorname{Im}(z)^{k/2}f(z)|.$$

Therefore, $g(\cdot) := \operatorname{Im}(\cdot)^{k/2} f(\cdot)$ is bounded on $\mathbb{H}$ if and only if it is bounded on a fundamental domain. The groups $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ that we are working with are discrete, finitely generated and with finite covolume. This implies that for a fundamental domain we can take a geodesic polygon with finitely many sides, such that all the vertexes (if any) that are in $\mathbb{R} \cup \{\infty\}$ correspond to inequivalent cusps of Γ. Let the finitely many inequivalent cusps be denoted by $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_\kappa$, and denote by $\Gamma_{\mathfrak{a}_i}$ the stabilizer of $\mathfrak{a}_i$ in Γ. This is an infinite cyclic group, and recall that a scaling matrix $\sigma_{\mathfrak{a}_i} \in \mathrm{PSL}_2(\mathbb{R})$ satisfies

$$\sigma_{\mathfrak{a}_i}(\infty) = \mathfrak{a}_i \quad \text{ and } \sigma_{\mathfrak{a}_i}^{-1} \Gamma_{\mathfrak{a}_i} \sigma_{\mathfrak{a}_i} = \langle T \rangle \quad \text{ where } Tz = z + 1.$$

In particular $T = \sigma_{\mathfrak{a}_i}^{-1} \gamma_{\mathfrak{a}_i} \sigma_{\mathfrak{a}_i}$ for a generator $\gamma_{\mathfrak{a}_i}$ of $\Gamma_{\mathfrak{a}_i}$.

We now solve the exercise. If $\Gamma \backslash \mathbb{H}$, then there are no cusps, so the hypothesis of the exercise imply that $f \in S_k(\Gamma, \theta)$ by definition, and $g(\cdot)$ is always bounded since it is Γ invariant and Γ has a fundamental domain $\mathcal{F}$ which is compact. From now on we assume that there are cusps for Γ. The structure of the argument will be the following

$$\begin{tikzcd}
& & f \equiv 0 \\
f \in S_k(\Gamma, \theta) \arrow[r] & \operatorname{Im}(\cdot)^{k/2} f(\cdot) \text{ is bounded} \arrow[ur, bend left, "{k<0, \text{ or } k=0, \theta \neq \theta_{\mathrm{tr}}}"] \arrow[r, "{k=0, \theta=\theta_{\mathrm{tr}}}"] \arrow[dr, bend right, "k>0"'] & f \equiv c \in \mathbb{C} \\
& & f \in S_k(\Gamma, \theta)
\end{tikzcd}$$

We will proof, in particular, that $S_k(\Gamma, \vartheta) = 0$ for $k < 0$ or $k = 0$ and $\vartheta \neq \vartheta_{\mathrm{tr}}$, and also that $S_0(\Gamma, \vartheta_{\mathrm{tr}}) = \mathbb{C}$.

Let $f \in S_k(\Gamma, \vartheta)$. The goal is to show that $g(\cdot) := \operatorname{Im}^{k/2} f(\cdot)$ is bounded on $\mathbb{H}$. Since g is Γ invariant, it is equivalent to show that g is bounded on a nice fundamental domain $\mathcal{F}$ as above. For a parameter $L > 0$ write $\mathcal{C}(L) := \{x + iy \in \mathbb{H} \mid 0 \leq x \leq 1, y > L\}$. The important property about a nice fundamental domain as described above is that, for large $L > 0$ we can express $\mathcal{F}$ as a disjoint union

$$\mathcal{F} = \left(\bigsqcup_{\text{cusps } \mathfrak{a}_i} \sigma_{\mathfrak{a}_i}(\mathcal{C}(L)) \right) \sqcup \bigsqcup \mathcal{F}_{\mathrm{comp}}(L)$$

where $\mathcal{F}_{\mathrm{comp}}(L)$ is compact in $\mathbb{H}$. We say that $\sigma_{\mathfrak{a}_i}(\mathcal{C}(L))$ is a cuspidal zone around $\mathfrak{a}_i = \sigma_{\mathfrak{a}_i}(\infty)$. By compactness, g is automatically bounded on $\mathcal{F}_{\mathrm{comp}}(L)$. For the cuspidal zones, we need to show that $g(\sigma_{\mathfrak{a}_i}(z))$ is bounded for $0 \leq x \leq 1$ and

$y > L$. We have

$$\begin{aligned} g(\sigma_{\mathfrak{a}_i} z) &= \operatorname{Im}(\sigma_{\mathfrak{a}_i} z)^{k/2} f(\sigma_{\mathfrak{a}_i} z) = \operatorname{Im}(\sigma_{\mathfrak{a}_i} z)^{k/2} j_{\sigma_{\mathfrak{a}_i}}(z)^k [f|_k \sigma_{\mathfrak{a}_i}](z) \\ &= \operatorname{Im}(\sigma_{\mathfrak{a}_i} z)^{k/2} j_{\sigma_{\mathfrak{a}_i}}(z)^k e(\kappa_{\mathfrak{a}_i} z) \sum_{n=0}^{\infty} a_f(n, \mathfrak{a}_i) e(nz) \\ &= \operatorname{Im}(\sigma_{\mathfrak{a}_i} z)^{k/2} j_{\sigma_{\mathfrak{a}_i}}(z)^k e(\kappa_{\mathfrak{a}_i} z) h_f(q; \mathfrak{a}_i) \end{aligned}$$

where $h_f(\cdot; \mathfrak{a}_i)$ is holomorphic in the disc $\{|q| < 1\}$ and, $\kappa_{\mathfrak{a}_i} \in [0, 1)$, and if $\kappa_{\mathfrak{a}_i} = 0$, then $h(q; \mathfrak{a}_i)$ has a zero at $q = 0$, so we can write $h_f(q; \mathfrak{a}_i) = q k_f(q; \mathfrak{a}_i)$ in this case, for $k_f(q; \mathfrak{a}_i)$ holomorphic in $\{|q| < 1\}$. Anyway, taking absolute values we get

$$|g(\sigma_{\mathfrak{a}_i} z)| = \begin{cases} \operatorname{Im}(z)^{k/2} |q| |k_f(q; \mathfrak{a}_i)|, & \text{if } \kappa_{\mathfrak{a}_i} = 0; \\ \operatorname{Im}(z)^{k/2} |q|^{\kappa_{\mathfrak{a}_i}} |h_f(q; \mathfrak{a}_i)|, & \text{if } 0 < \kappa_{\mathfrak{a}_i} < 1 \end{cases} \tag{33}$$

For $z = x + iy$ such that $y > L$, q remains in the closed disc $\{|q| \leq \exp(-2\pi L)\}$, which is compact inside $\{|q| < 1\}$. Therefore, in each of the cases $k_f(q; \mathfrak{a}_i)$ or $h_f(q; \mathfrak{a}_i)$ is bounded. Since On the other hand, for any $r > 0$ the expression $\operatorname{Im}(z)^{k/2} |q|^r = y^{k/2} \exp(-2\pi r y)$ is bounded for $y > L$ and, in fact, tends to 0 with exponential decay when $y \to \infty$. This proves that g is bounded on $\mathcal{F}$ as desired.

Now suppose that g is bounded. By Lemma 2.3.2 we already know that $f \in M_k(\Gamma, \theta)$. By the same calculation as above

$$g(\sigma_{\mathfrak{a}_i} z) = \operatorname{Im}(\sigma_{\mathfrak{a}_i} z)^{k/2} j_{\sigma_{\mathfrak{a}_i}}(z)^k [f|_k \sigma_{\mathfrak{a}_i}](z) = \operatorname{Im}(\sigma_{\mathfrak{a}_i} z)^{k/2} j_{\sigma_{\mathfrak{a}_i}}(z)^k e(\kappa_{\mathfrak{a}_i} z) h_f(q; \mathfrak{a}_i)$$

where h_f is holomorphic on $\{|q| < 1\}$. Suppose that $k < 0$. If $f \not\equiv$, then also $h_f \equiv 0$. If $|h_f(q_0)| = C > 0$ for some q_0 with $|q| < 1$, then by the maximum modulus theorem we know that, for any $r < 1$ such that $r > |q_0|$, there is q_r with $|q_r| = r$ such that $|h_f(q_r)| \geq C$. For any q_r we can find unique $0 \leq x < 1$ and $0 < y < \infty$ such that $q := e(z) = q_r$. Therefore, for this z we have

$$|g(\sigma_{\mathfrak{a}_i} z)| \geq y^{k/2} e(-2\pi \kappa_{\mathfrak{a}_i} y) C$$

Letting $r \to 1$, we find a sequence of points z_i with $y_i \to 0$ such that the above inequality holds. When $k < 0$ the right hand side tends to $+\infty$, which contradicts the fact that g is bounded.

In the case $k = 0$, we obtain

$$|f(\sigma_{\mathfrak{a}_i} z)| = |g(\sigma_{\mathfrak{a}_i} z)| = e(-2\pi k_{\mathfrak{a}_i} y) |h_f(q; \mathfrak{a}_i)|$$

By the maximum modulus principle, we have

$$\sup_{|q| < r} |h_f(q; \mathfrak{a}_i)| \leq \max_{|q| = r} |h_f(q; \mathfrak{a}_i)|$$

Since $e(-2\pi k_{\mathfrak{a}_i} y)$ is decreasing as a function of y we deduce that

$$\sup_{z\in\sigma_{\mathfrak{a}_i}(\mathcal{C}(L))} |f(z)| = \max_{z\in\sigma_{\mathfrak{a}_i}(\mathcal{H}(L))} |f(z)| \leq \max_{z\in\mathcal{F}_{\mathrm{comp}}(L)} |f(z)$$

where $\mathcal{H}(L) := \{z = x + iy \mid 0 \leq x \leq 1, y = L\}$, and the inequality follows from $\mathcal{H}(L) \subset \mathcal{F}_{\mathrm{comp}}(L)$. Therefore, f is a bounded holomorphic function on $\mathbb{H}$ that attains its maximum, and must be a constant by the strong maximum modulus principle. If $\vartheta(\gamma) \neq 1$ for some $\gamma \in \Gamma$, then

$$f(z) = [f|_0\gamma](z) = \vartheta(\gamma)f(z), \text{ for all } z \in \mathbb{H} \to f \equiv 0. \tag{34}$$

Finally, we assume $k > 0$. As before, we already know that $f \in M_k(\Gamma, \vartheta)$. We only need to look at singular cusps, so that $\kappa_{\mathfrak{a}_i} = 0$. We have

$$g(\sigma_{\mathfrak{a}_i} z) = \mathrm{Im}(\sigma_{\mathfrak{a}_i} z)^{k/2} j_{\sigma_{\mathfrak{a}_i}}(z)^k h_f(q; \mathfrak{a}_i)$$

where $h_f(q; \mathfrak{a}_i) = \sum_{n=0}^{\infty} a_f(n, \mathfrak{a}_i)e(nz)$ and the objective is to show that $h_f(0; \mathfrak{a}_i) = 0$. Taking absolute values

$$|g(\sigma_{\mathfrak{a}_i} z)| = \mathrm{Im}(z)^{k/2}|h_f(q; \mathfrak{a}_i)| \tag{35}$$

By hypothesis, the left hand side is bounded. When $y \to \infty$ we have $q \to 0$ and therefore $|h_f(q; \mathfrak{a}_i)| \to |h_f(0; \mathfrak{a}_i)|$. Since $k > 0$, it must be that $h_f(0; \mathfrak{a}_i) = 0$, since otherwise g would be unbounded as $y \to \infty$. Since this is true for all singular cusps and we know that $f \in M_k(\Gamma, \vartheta)$, we deduce that $f \in S_k(\Gamma, \vartheta)$, as desired. ∎

The previous lemma allows us in particular to define the so called Petersson inner product:

$$\langle f, g\rangle = \int_{\Gamma\backslash\mathbb{H}} f(z)\overline{g(z)}\,\mathrm{Im}(z)^k d\mu(z),$$

for $f, g \in S_k(\Gamma, \vartheta)$.

Remark 2.3.3. First note that the integral is defined by

$$\int_{\Gamma\backslash\mathbb{H}} h(z)d\mu(z) = \int_{\mathcal{F}} h(x + iy)\frac{dxdy}{y^2}.$$

Where $\mathcal{F}$ is some fundamental domain for Γ. To make this well defined h should be Γ-invariant. It is easy to verify that the integrand in the definition of the inner product is indeed Γ-invariant. Furthermore one directly sees that the integral is finite. This is because (under current assumptions) $\mu(\mathcal{F}) < \infty$ and $\mathrm{Im}(\cdot)^{\frac{k}{2}} f$ as well as $\mathrm{Im}(\cdot)^{\frac{k}{2}} g$ are bounded.

Lemma 2.3.4. *The space $S_k(\Gamma, \vartheta)$ equipped with $\langle\cdot, \cdot\rangle$ is a finite dimensional Hilbert space.*

Proof. It is clear that $\langle\cdot, \cdot\rangle$ defines an inner product. Once we see that $S_k(\Gamma, \vartheta)$ is a finite dimensional complex vector space completeness is also clear.

We will show that $M_k(\Gamma,\vartheta)$ is finite dimensional by reduction to a weak version of the Riemann-Roch theorem, which we now recall. Let X be a compact Riemann surface, $P_1,\dots,P_n \in X$ and let $r_1,\dots,r_n$ be positive integers. Then we consider the (complex) vector space V of meromorphic functions on X, which are holomorphic except for possible poles of order at most r_i at the points P_i (with $i=1,\dots,m$). Then the dimension of V is at most $r_1+\ldots+r_m+1$.

To apply this result be put $X = \Gamma\backslash(\mathbb{H}\cup\{\text{cusps of }\Gamma\})$. This is a compact Riemann surface. Now take $0\neq f_0 \in M_k(\Gamma,\vartheta)$, if non such function exists we are done anyway. Recall that f_0 is holomorphic on X. Let $P_1,\dots,P_m$ be the zeros of f_0 and let r_i be the order of vanishing of f_0 at P_i for $i=1,\dots,m$. (At elliptic points P_i the order of vanishing must be slightly modified but this is not essential.) We define the map

$$M_k(\Gamma,\vartheta) \ni f \mapsto \frac{f}{f_0} \in V,$$

where V is defined as above. This is an isomorphism, so that we obtain the bound

$$\dim M_k(\Gamma,\vartheta) \le r_1+\ldots+r_m+1 < \infty.$$

□

2.4. **Modular forms of integral even weight, trivial multiplier for** $\mathrm{SL}_2(\mathbb{Z})$**.** We will take a look of the very classical when $k\in 2\mathbb{N}$, $\vartheta=\vartheta_{\mathrm{tr}}$ and $\Gamma=\mathrm{SL}_2(\mathbb{Z})$.

Theorem 2.4.1. *Let $f\in M_k(\mathrm{SL}_2(\mathbb{Z}),\vartheta_{\mathrm{tr}})$ be non-zero and let $m_f(z)\in\mathbb{N}\cup\{0\}$ be the order of vanishing of f at $z\in\mathbb{H}\cup\{$ cusps of $\Gamma\}$. Further set*

$$m(z)=\begin{cases} |\overline{\Gamma_z}| & \textit{if } z\in\mathbb{H} \textit{ is an elliptic fixed point of } \mathrm{PSL}_2(\mathbb{Z}),\\ 1 & \textit{else.}\end{cases}$$

Then we have

$$\sum_{\Gamma\backslash(\mathbb{H}\cup\{\textit{cusps of }\Gamma\})} \frac{m_f(z)}{m(z)} = \frac{k}{12}.$$

Proof. For $R>0$ sufficiently large let

$$\mathcal{F}_R=\{x+iy\colon -\frac{1}{2}\le x\le\frac{1}{2},\ |x+iy|\ge 1 \text{ and } y\le R\}$$

be the truncated standard fundamental domain and let γ be the path around the boundary of $\mathcal{F}_R$. We modify this part slightly by forming little circles of radius r around the elliptic fixed points $i, \rho_\pm = \pm\frac{1}{2}+i\frac{\sqrt{3}}{2}$.

We first observe that by a theorem of Cauchy we have

$$\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}dz = \sum_{z\in\mathrm{Int}(\gamma)} m_f(z).$$

Furthermore, for all $z\in\mathrm{Int}(\gamma)$ we have $m(z)=1$.

The top piece of the integral is given by

$$\frac{1}{2\pi i}\int_{\frac{1}{2}}^{\frac{1}{2}} \frac{f'(-x+iR)}{f(-x+iR)}dx \to -m_f(\infty) \text{ as } R \to \infty.$$

Since the left and the right hand side of $\mathcal{F}_T$ are equivalent via T they cancel each other.

To compute the contribution of the arcs around the elliptic fixed points $z_0 = i, \rho_\pm$ we write

$$\frac{f'(z)}{f(z)} = \frac{m_f(z_0)}{z - z_0} + h(z)$$

for a holomorphic function h. As $r \to 0$ the contribution then approaches

$$\frac{1}{2\pi i}\int_{a_{z_0}(\gamma)} \frac{m_f(z_0)}{z - z_0} = -\mu(z_0)m_f(z_0),$$

where $a_{z_0}(\gamma)$ is the piece of the arc and $2\pi\mu(z_0)$ is the arc length. Note that

$$\mu(i) = \frac{1}{2} \text{ and } \mu(\rho_\pm) = \frac{1}{6}.$$

Finally we have to compute the contribution of bottom of the curve γ with $i, \rho_\pm$ removed. We can write this as $A \cup SA$, where A is the arc of the unit circle connecting ρ_- and i. One checks that

$$\frac{f'(Sz)}{f(Sz)}z^{-2} = \frac{k}{z} + \frac{f'(z)}{f(z)}.$$

This gives us

$$\begin{aligned}\frac{1}{2\pi i}\int_{A\cup SA} \frac{f'(z)}{f(z)}dz &= \frac{1}{2\pi i}\int_A \frac{f'(z)}{f(z)}dz - \frac{1}{2\pi i}\int_A \frac{f'(Sz)}{f(Sz)}dSz \\ &= -\frac{1}{2\pi i}\int_A \frac{k}{z}dz = \frac{k}{12}.\end{aligned}$$

Combining everything gives the desired formula and completes the proof. ◻

Note that

$$M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) \cdot M_l(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) \subseteq M_{k+l}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}).$$

This motivates us to define the (graded) ring

$$M(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \bigoplus_{k\geq 0} M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}).$$

Using Theorem 2.4.1 we can understand this ring completely. But we first make the following observations:

- If $k = 0$ we have $M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C}$. This is because by Theorem 2.4.1 we have $\sum_z m_f(z)m(z)^{-1} = 0$ for $f \neq 0$, which implies $m_f(z) = 0$ for all z. But this can only happen if f is constant.

- If $k = 2$ or odd, then $M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \{0\}$. The argument for $k = 2$ is similar to the case $k = 0$. If k is odd we observe that $-f(z) = [f|_k -1](z) = f(z)$, which is a contradiction.[15]
- If $k = 4$, then we have $M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C} \cdot E_4$. From Theorem 2.4.1 it follows that $E_4(\rho_\pm) = 0$ with $m_{E_4}(\rho_\pm) = 1$. At all other points E_4 does not vanish. Suppose now that $f \in M_4(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. Then there is $c \in \mathbb{C}$ so that $g = f - cE_4$ satisfies $m_g(\infty) \geq 1$. Applying Theorem 2.4.1 to g we find that g must be zero. In particular $f = cE_4$.
- Similarly one can show that $M_6(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C} \cdot E_6$, $M_8(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C} \cdot E_4^2$ and $M_{10}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C} \cdot E_4 E_6$.
- We have
$$M_{12}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C} \cdot E_{12} \oplus \mathbb{C} \cdot \Delta.$$
Note that $m_\Delta(\infty) = 1$, so that by Theorem 2.4.1 we see that Δ is non-zero on $\mathbb{H}$. Take $f \in M_{12}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ and define
$$g(z) = \frac{f(z) - cE_{12}(z)}{\Delta(z)}.$$
We can choose c so that $g \in M_0(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. This shows that g is constant and proves our claim.
- Inductively one obtains that
$$M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \Delta \cdot M_{k-12}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) \oplus \mathbb{C} \cdot E_k. \tag{36}$$
In particular we have
$$\dim M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{if } k \equiv 2 \bmod 12, \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{if } k \not\equiv 2 \bmod 12. \end{cases}$$

Theorem 2.4.2. *The Eisenstein series E_4 and E_6 algebraically independent over $\mathbb{C}$ and they generate $M(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ as a polynomial ring:*
$$M(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C}[E_4, E_6].$$

Proof. That $M(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ is generated by E_4 and E_6 follows directly from (36). To see that they are algebraically independent we suppose that
$$P(E_4, E_6) = 0 \text{ for } P \in \mathbb{C}[X, Y] \setminus \{0\}$$
for P with minimal degree. Note that we can assume that (after inserting the Eisenstein series) the monomials have equal weight. Now we have two cases:

- $P(E_4, E_6) = E_4^m + E_6 \cdot Q(E_4, E_6)$. But evaluating at i gives a contradiction since $E_4(i) \neq 0 = E_6(i)$.
- $P(E_4, E_6) = E_6^m + E_4 \cdot Q(E_4, E_6)$. But evaluating at $\rho_\pm$ gives a contradiction since $E_4(\rho_\pm) = 0 \neq E_6(\rho_\pm)$.

[15]Note that actually ϑ_{tr} is not a multiplier system for odd k because it does not satisfy the consistency condition.

Exercise 2, Sheet 4:

a) Show that

$$M_6(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C} \cdot E_6 \text{ and } M_8(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C} \cdot E_4^2.$$

b) Deduce that for $n \in \mathbb{N}$ one has the identity

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{0<m<n} \sigma_3(m)\sigma_3(n-m)$$

between divisor functions. (It can be used that $\frac{4i^4}{B_4} = 240$ and $\frac{8i^8}{B_8} = 480$.)

Solution. Recall that if $f \in M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ is non-zero then the following formula holds (for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, see Theorem 2.4.1)

$$\sum_{\Gamma\backslash(\mathbb{H}\cup\{\text{cusps of }\Gamma\})} \frac{m_f(z)}{m(z)} = \frac{k}{12}$$

where $m_f(z)$ is the order of the zero of f at z, and $m(z) = 1$ for all points except for $m(i) = 2$ and $m(\rho) = 3$, where $\rho = \frac{1+i\sqrt{3}}{2}$ (note that ρ and $-\rho^{-1} = \frac{-1+i\sqrt{3}}{2}$ are identified by $S \in \Gamma$). Recall that E_6 is not zero and is in $M_6(\mathrm{SL}_2(\mathbb{Z}), \theta_{\mathrm{tr}})$. Testing $(E_6|_6 S)(z) = E_6(z)$ for $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $z = i$, since $Si = i$ we obtain

$$E_6(i) = [E_6|_6 S](i) = j_S(i)^{-6} E_6(i) = i^{-6} E_6(i)$$

and thus $E_6(i) = 0$. Similarly, testing $(E_4|_4\gamma)(z) = E_4(z)$ for $z = \rho$ and $\gamma = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ we obtain, since $\gamma\rho = \rho$,

$$E_4(\rho) = [E_4|_4\gamma](\rho) = j_\gamma(\rho)^{-4} E_4(\rho) = \rho^{-4} E_4(\rho).$$

But ρ is a primitive 6-th root of unity, and thus $E_4(\rho)$. Therefore $E_4(\cdot)^2$ has a zero of order at least 2 at ρ. By the valence formula the only possibility is that:

(1) E_6 has exactly one zero in the fundamental domain, it is located at i, and it is of order 1.
(2) E_4^2 has exactly one zero in the fundamental domain, it is located at ρ and it is of order 2 (if one wants to consider ρ and $-\rho^{-1}$ as two distinct points in the fundamental domain, then one puts $m(\rho) = m(-\rho^{-1}) = 1/6$).

If we are given $f \in M_6$ we can consider $w \in \mathbb{H}$ not elliptic where E_6 does not vanish, and form $g := f - cE_6$ for some $c \in \mathbb{C}$ so that $g(w) = 0$. Then, looking at the valence formula we have

$$1 + \sum_{(\Gamma\backslash(\mathbb{H}\cup\{\text{cusps of }\Gamma\}))-\{z\}} \frac{m_g(z)}{m(z)} = 1/2,$$

which is a contradiction unless g is identically zero. The same argument works for $k = 8$ and E_4^2. This finishes the proof of part a).

For part b), note that since $E_8 \in M_8(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ we have $E_8 = cE_4^2$ for some $c \in \mathbb{C}$. Using the expansion

$$E_k(z) = 1 + ki^k B_k^{-1} \sum_{n=1}^{\infty} \sigma_{k-1}(n) e(nz)$$

we deduce $c = 1$, and then comparing coefficients we get

$$\frac{8}{B_8}\sigma_7(n) = 2\frac{4}{B_4}\sigma_3(n) + \frac{16}{B_4^2} \sum_{0<m<n} \sigma_3(m)\sigma_3(n-m).$$

Using $\frac{4}{B_4} = 240$ and $\frac{8}{B_8} = 2 \cdot 240$ we arrive at the desired identity. ◻

Exercise 3, Sheet 4: Let

$$f(z) = \sum_{n=0}^{\infty} a_f(n; \infty) e(nz) \in M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}).$$

a) Let K be an algebraic number field (i.e. a finite extension of $\mathbb{Q}$) and suppose that

$$\max\{n \in \mathbb{Z}_{\geq 0} : a_f(m, \infty) \in K \text{ for all } 0 \leq m \leq n\} \geq \dim M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) - 1.$$

Prove that all coefficients already lie in K (i.e. $a_f(n, \infty) \in K$ for all $n \in \mathbb{Z}_{\geq 0}$).

b) Show that if the Fourier coefficients $a_f(n, \infty)$ of f (at ∞) are algebraic numbers, then they are all contained in a finite extension of $\mathbb{Q}$.

Solution. Recall that a basis of $M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ can be chosen of the form $g_i := E_{k-12i}\Delta^i$ for $0 \leq i \leq \dim M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) - 1$. The point here is that the coefficients $a_{g_i}(0, \infty), \ldots, a_{g_i}(i-1, \infty)$ of g_i are 0 while the coefficient $a_{g_i}(i, \infty) = 1$ is non-zero, and all the $a_{g_i}(j, \infty)$ for $j \geq 0$ are rational. We look for the (unique) linear combination such that $f = \sum c_i g_i$. Equating the first $\dim M_k$ coefficients we arrive at a system

$$\begin{pmatrix} a_{g_0}(0,\infty) & \cdots & a_{g_{\dim M_k - 1}}(0,\infty) \\ \vdots & & \vdots \\ a_{g_0}(\dim M_k - 1, \infty) & \cdots & a_{g_{\dim M_k - 1}}(\dim M_k - 1, \infty) \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{\dim M_k - 1} \end{pmatrix} = \begin{pmatrix} a_f(0,\infty) \\ \vdots \\ a_f(\dim M_k - 1, \infty) \end{pmatrix} \tag{37}$$

Recalling that $a_{g_i}(j, \infty) = 0$ for $j < i$, and $a_{g_i}(i, \infty) = 1$, we see that the matrix lower triangular with non vanishing diagonal, and therefore invertible. Since it has rational entries, its inverse also has rational entries, and since by hypothesis the column vector a_f has entries in K we deduce that the numbers c_i are in K. Since $f = \sum c_i g_i$ and the coefficients of the g_i are all rational we deduce that f has all coefficients in K. This finishes the proof of part a).

For part b), let K be the field generated by $a_f(n,\infty)$ for $n \leq \dim M_k - 1$. By hypothesis we know that the $a_f(n,\infty)$ are algebraic, and since K is generated by a finite number of them, then K is a finite extension of $\mathbb{Q}$. Applying part a) we deduce that all coefficients lie in K, a finite extension of $\mathbb{Q}$. □

Remark 2.4.3. The exercise above can also be solved by applying Theorem 2.4.1. The idea is the same as above, but this time $\{g_i : 0 \leq i \leq \dim M_k(\mathrm{SL}_2(\mathbb{Z}), \theta_{\mathrm{tr}}) - 1\}$ is an arbitrary basis of $M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ such that all the coefficients $a_{g_i}(j,\infty)$ for $j \geq 0$ are rational[16]. As before, the key step is to show that

$$\begin{pmatrix} a_{g_0}(0,\infty) & \cdots & a_{g_{\dim M_k - 1}}(0,\infty) \\ \vdots & & \vdots \\ a_{g_0}(\dim M_k - 1,\infty) & \cdots & a_{g_{\dim M_k - 1}}(\dim M_k - 1,\infty) \end{pmatrix}$$

is invertible. This is equivalent to showing that the matrix has 0 kernel, which by the system (37) is equivalent to the assertion: if $f \in M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ and the coefficients $a_f(j,\infty) = 0$ for $0 \leq j \leq \dim M_k - 1)$, then f is identically zero. Recall the formula

$$\dim M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \begin{cases} 0, & \text{if } k \text{ odd or } k \leq 0; \\ \lfloor \frac{k}{12} \rfloor, & \text{if } k \geq 2, \text{ and } k \equiv 2 \bmod 12; \\ \lfloor \frac{k}{12} \rfloor + 1, & \text{if } k \geq 2, \text{ and } k \equiv 0, 4, 6, 8 \text{ or } 10 \bmod 12. \end{cases}$$

Now let $k \geq 4$ even (otherwise the exercise is vacuous) and suppose that $f \in M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ satisfies $a_f(j,\infty) = 0$ for $0 \leq j \leq \dim M_k - 1)$. Then f has a zero of order at least $\dim M_k$ at ∞. By the formula from Theorem 2.4.1, if $k = 12l + r$ with $r \in \{0, 4, 6, 8, 10\}$, if f is not identically zero we have

$$l + 1 + \sum_{(\Gamma\backslash(\mathbb{H}\cup\{\text{cusps of }\Gamma\}))-\infty} \frac{m_f(z)}{m(z)} = l + r/12 \tag{38}$$

Since all the summands are nonnegative, this equation cannot hold and f must be identically zero. If $r = 2$ then the equation is

$$l + \sum_{(\Gamma\backslash(\mathbb{H}\cup\{\text{cusps of }\Gamma\}))-\infty} \frac{m_f(z)}{m(z)} = l + 1/6 \tag{39}$$

Since the weights $m(z)$ are less or equal than 3 and $m_f(z)$ are nonnegative integers, this equation cannot hold either. Therefore, f is identically zero and the matrix above is invertible, as desired.

Exercise 1, Sheet 5: Let $k \in 2\mathbb{N}$ be even and let $f \in M_k\left(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}\right)$.

[16]We could use, for example, the basis consisting of the monomials $E_4^a E_6^b$ such that $4a+6b = k$, where a, b are non negative integers.

a) Determine the constant $C \in \mathbb{C}$ such that

$$\theta_k f = \frac{1}{2\pi i} f' - CE_2 f \in M_{k+2}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$$

(The resulting operator $\theta_k : M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) \to M_{k+2}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ is sometimes called Serre derivative.)

b) Find the polynomial $P \in \mathbb{C}[X, Y]$ such that $\theta_{12}\Delta = P(E_4, E_6)$.

Solution. Recall that $E_2(z) := \frac{e_2(1,z)}{2\zeta(2)}$ which transforms under $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ by

$$[E_2|_2\gamma](z) = E_2(z) + \frac{12}{2\pi i} \cdot \frac{c}{cz + d}$$

Now look at the derivative. Since $f \in M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ we have $f \circ \gamma = j_\gamma^k \cdot f$. Applying $\frac{d}{dz}$ to this relationship we get

$$(f' \circ \gamma)(z) \cdot j_\gamma^{-2} = ckj_\gamma^{k-1} f + j_\gamma^k f'$$

which is equivalent to

$$[f'|_{k+2}\gamma] = ckj_\gamma^{-1} f + f'.$$

On the other hand

$$[(E_2 f)|_{k+2}\gamma] = [E_2|_2\gamma] \cdot [f|_k\gamma] = \left(E_2 + \frac{12c}{2\pi i} j_\gamma^{-1}\right) f.$$

Putting all together

$$(\theta_k f)|_{k+2}\gamma = \frac{1}{2\pi i}(f')|_{k+2}\gamma - C(E_2 f)|_{k+2}\gamma = \frac{1}{2\pi i} f' + \frac{ck}{2\pi i} j_\gamma^{-1} f - CE_2 f - C\frac{12c}{2\pi i} j_\gamma^{-1} f$$
$$\theta_k f + (k - 12C)\frac{c}{2\pi i} j_\gamma^{-1} f.$$

Therefore, we obtain $C = k/12$. Note that, by looking at the power series development, it is clear that θ_k preserves holomorphicity at infinity, so that for $C = k/12$ the operator θ_k sends $M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ to $M_{k+2}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. Also, if $f \in S_k(\mathrm{SL}_2(\mathbb{Z}), \theta_{\mathrm{tr}})$ then it is also immediate by looking at the expansion at infinity that $\theta_k f \in S_{k+2}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. In particular, $\theta_{12}\Delta$ is a cusp form of weight 14, which has to be zero. Therefore, the polynomial of part b) is $P \equiv 0$. ⊡

2.5. **Poincaré series.** Our goal is now to construct automorphic forms for given (discrete Fuchsian group of the first kind) $\Gamma \subseteq \mathrm{SL}_2(\mathbb{R})$, weight $k \in \mathbb{R}$ and multiplier system ϑ. We can carry this out under the following assumptions that will be in place throughout this section. We assume that $k > 2$ and that $\mathfrak{a}$ is a cusp of Γ, which is singular with respect to ϑ. (Recall that $\mathfrak{a}$ comes with a scaling matrix $\sigma_\mathfrak{a}$ and a generator $\gamma_\mathfrak{a}$ of $\Gamma_\mathfrak{a}$. The condition that $\mathfrak{a}$ is singular is precisely that $\vartheta(\gamma_\mathfrak{a}) = 1$.)

Given a holomorphic function $p\colon \mathbb{H} \to \mathbb{C}$ of period 1 we define the map $\pi\colon \Gamma \times \mathbb{H} \to \mathbb{C}$ given by

$$\pi(\gamma, z) = \overline{\vartheta(\gamma) w(\sigma_{\mathfrak{a}}^{-1}, \gamma)} j_{\sigma_{\mathfrak{a}}^{-1}\gamma}(z)^{-k} p(\sigma_{\mathfrak{a}}^{-1}\gamma z).$$

We claim that $\pi(\gamma, z)$ is left $\Gamma_{\mathfrak{a}}$-invariant in the first variable (i.e. it only depends on the coset $\Gamma_{\mathfrak{a}}\gamma$). To see this let $\eta \in \Gamma_{\mathfrak{a}}$, put $\gamma' = \eta\gamma$ and observe that $\eta = \sigma_{\mathfrak{a}}\beta\sigma_{\mathfrak{a}}^{-1}$ for $\beta \in \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}$. Since p is one periodic we have

$$p(\sigma_{\mathfrak{a}}^{-1}\gamma' z) p(\beta\sigma_{\mathfrak{a}}^{-1\gamma z}) = p(\sigma_{\mathfrak{a}}^{-1\gamma z}).$$

Similarly using that $j_\beta(*) = 1$ we get

$$j_{\sigma_{\mathfrak{a}}^{-1}\gamma'}(z)^{-k} = j_{\beta\sigma_{\mathfrak{a}}^{-1}\gamma}(z)^{-k} = j_{\sigma_{\mathfrak{a}}^{-1}\gamma}(z)^{-k}.$$

Now we use that the cusp $\mathfrak{a}$ is singular with respect to ϑ and observe that

$$\vartheta(\gamma') = \vartheta(\eta\gamma) = w(\eta, \gamma)\vartheta(\gamma).$$

We had already observed earlier that

$$w(\eta, \gamma) w(\sigma_{\mathfrak{a}}^{-1}, \gamma') = w(\sigma_{\mathfrak{a}}^{-1}, \gamma).$$

Putting these observations together allows us to deduce that $\pi(\gamma', z) = \pi(\gamma, z)$ as desired.

This allows us to define the series

$$P_{\mathfrak{a},p}(z) = \sum_{\Gamma_{\mathfrak{a}}\backslash\Gamma} \pi(\gamma, z). \tag{40}$$

Before we can study convergence and other properties of $P_{\mathfrak{a},p}(z)$ we need to develop some preliminary results concerning the decomposition of translates of Γ into double cosets. To do so let $\mathfrak{a}, \mathfrak{b}, \ldots$ be a complete system of inequivalent cusps of Γ. The corresponding scaling matrices are denoted by $\sigma_{\mathfrak{a}}, \sigma_{\mathfrak{b}}, \ldots$. Let

$$U(\mathbb{Z}) = \pm \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix},$$

where we suppose for simplicity that $-1 \in \Gamma$.[17]

Lemma 2.5.1. *For any two cusps $\mathfrak{a}, \mathfrak{b}$ for Γ we have the double coset decomposition*

$$\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}} = \delta_{\mathfrak{a}\sim\mathfrak{b}} U(\mathbb{Z}) \cup \bigcup_{c>0} \bigcup_{d \ mod \ c} U(\mathbb{Z}) \begin{pmatrix} * & * \\ c & d \end{pmatrix} U(\mathbb{Z}),$$

where the union is only taken over tuples (c, d) such that $\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}$.

[17]The modifications necessary for the case when $-1 \notin \Gamma$ are straight forward.

Proof. We first consider the subset

$$\Omega_\infty = \{\tau \in \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}} \colon \tau\infty = \infty\}.$$

These are precisely the upper triangular matrices in $\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}$. Suppose $\tau \in \Omega_\infty$. Then we can write $\tau = \sigma_{\mathfrak{a}}^{-1}\gamma\sigma_{\mathfrak{b}}$. We get

$$\gamma\mathfrak{b} = \sigma_{\mathfrak{a}}\tau\sigma_{\mathfrak{b}}^{-1}\mathfrak{b} = \sigma_{\mathfrak{a}}\infty = \mathfrak{a}.$$

Thus $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent (i.e. $\mathfrak{a} \sim \mathfrak{b}$). In this case $\Omega_\infty = \mathrm{U}(\mathbb{Z})$ by definition of the scaling matrix.

Any other element in $\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}$ can we written as $\tau = \begin{pmatrix} a & * \\ c & d \end{pmatrix}$. We compute

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & * \\ c & d \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a+cm & * \\ c & d+cn \end{pmatrix}.$$

In particular, the double coset $\Omega_{d/c} = U(\mathbb{Z})\begin{pmatrix} * & * \\ c & d \end{pmatrix}U(\mathbb{Z})$ determines c uniquely and d modulo c. It is easy to observe that given $\tau \in \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}$ with lower row (c, d), then the double coset does not depend on the entries of the upper row. ◻

For applications it is often important to control the number of double cosets. We define

$$C(\mathfrak{a}, \mathfrak{b}) = \left\{ c > 0 \colon \begin{pmatrix} * & * \\ c & * \end{pmatrix} \in \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}} \right\}.$$

Let $c(\mathfrak{a}, \mathfrak{b}) = \min C(\mathfrak{a}, \mathfrak{b})$ and define $c(\mathfrak{a}) = c(\mathfrak{a}, \mathfrak{a})$. Finally pu $c_{\mathfrak{a},\mathfrak{b}} = \max(c(\mathfrak{a}), c(\mathfrak{b}))$.

Remark 2.5.2. To see that $c(\mathfrak{a})$ exists we use the the following construction of the fundamental domain $\mathcal{F}_{\mathfrak{a}}$ for $\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{a}}$. First note that $U(\mathbb{Z}) \subseteq \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{a}}$, so that we can chose our fundamental domain to be contained in the strip $P = \{z = x + iy \colon y > \text{ and } 0 \leq x \leq 1\}$. We further define

$$E = \{z \in \mathbb{H} \colon \operatorname{Im}(z) \geq \operatorname{Im}(\gamma z) \text{ for all } \gamma \in \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{a}}\}.$$

Then $\mathcal{F}_{\mathfrak{a}} = E \cap P$ is a fundamental domain. (It is sometimes called the standard polygon and the construction is due to L. R. Ford.)

The isometric circle

$$\mathcal{C}_\gamma = \{z \in \mathbb{H} \colon |j_\gamma(z)| = 1\}$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{a}} \setminus U(\mathbb{Z})$ is centered at $-\frac{d}{c}$ and has radiues $|v|^{-1}$. In particular $c(\mathfrak{a})^{-1}$ is the radius of the largest isometric circle and therefore must exist. This observation also gives the useful bound

$$c(\mathfrak{a}) = \operatorname{Vol}(\{x + iy \colon 0 < x < 1,\, y > c(\mathfrak{a})^{-1}\}) \leq \operatorname{Vol}(\mathcal{F}_{\mathfrak{a}}).$$

Concerning the numbers $c(\mathfrak{a}, \mathfrak{b})$ one can show that

$$c(\mathfrak{a}, \mathfrak{b})^2 \geq c_{\mathfrak{a},\mathfrak{b}}.$$

Lemma 2.5.3. *For any $X > 0$ we have*

$$\sum_{0<c\leq X} c^{-1}\sharp\left\{d \text{ mod } c\colon \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}\right\} \leq \frac{X}{c_{\mathfrak{a},\mathfrak{b}}}.$$

Proof. Without loss of generality we assume that $c(\mathfrak{a}) = c_{\mathfrak{a},\mathfrak{b}}$. Suppose we have two elements $\tau = \begin{pmatrix} * & * \\ c & d \end{pmatrix}$, $\tau' = \begin{pmatrix} * & * \\ c' & d' \end{pmatrix}$ in $\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}$ and with $0 < c, c \leq X$. Then we find

$$\tau'' = \tau'\tau^{-1} = \begin{pmatrix} * & * \\ c'd - cd' & * \end{pmatrix} \in \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{a}}.$$

If $c'd - cd' = 0$, then an easy computation shows that $\mathfrak{a} \sim \mathfrak{b}$ and $c' = d'$. If $c'd - cd' \neq 0$ we obtain the important inequality

$$|\frac{d'}{c'} - \frac{d}{c}| \geq \frac{c(\mathfrak{a})}{cc'} \geq \frac{c(\mathfrak{a})}{cX}. \tag{41}$$

Summing this over $0 \leq c \leq X$ and $0 \leq d \leq c$ ordered by the size of the fraction $\frac{d}{c}$ gives the result. ◻

Lemma 2.5.4. *Let $\mathfrak{a}$ be a cusp for Γ and let $z \in \mathbb{H}$ and $Y > 0$. We have*

$$\sharp\{\gamma \in \Gamma_{\mathfrak{a}}\backslash\Gamma\colon \operatorname{Im}(\sigma_{\mathfrak{a}}^{-1}\gamma z) > Y\} < 1 + \frac{10}{c(\mathfrak{a})Y}.$$

Proof. After conjugating the group we can assume without loss of generality that $\mathfrak{a} = \infty$ and $\Gamma_{\mathfrak{a}} = U(\mathbb{Z})$. The vertical strip P of width 1 (defined above for example) is a fundamental domain for $\Gamma_{\mathfrak{a}}$. Without loss of generality we can assume that z is in the standard Polygon $\mathcal{F}_{\mathfrak{a}}$ of Γ. In particular

$$|cz + d| \geq 1 \text{ for and } \gamma = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma \setminus U(\mathbb{Z}).$$

This gives the estimate

$$\operatorname{Im}(\gamma z) = \frac{y}{|cz + d| - 2} > Y.$$

Using this we obtain the three bounds

$$\begin{aligned} &y > Y, \\ &c < \frac{1}{\sqrt{yY}} \text{ and} \\ &|cx + d| < \left(\frac{y}{Y}\right)^{\frac{1}{2}}. \end{aligned}$$

Recalling (41) we can estimate the number of relevant pairs (c, d) with $C \leq c < 2C$ by

$$1 + \frac{8C}{c(\mathfrak{a})}\left(\frac{y}{Y}\right)^{\frac{1}{2}} \leq \frac{10C}{c(\mathfrak{a})}\left(\frac{y}{Y}\right)^{\frac{1}{2}} \tag{42}$$

Summing these bounds over $C = 2^{-n}(yY)^{-\frac{1}{2}}$ with $n \geq 1$ yields $\frac{10}{c(\mathfrak{a})Y}$. We add 1 to account for $\Gamma_{\mathfrak{a}}$. ∎

We can now return to studying the series defined in (40). Let us first pretend that everything converges fine and make the following computation. Given any cusp $\mathfrak{b}$ we have

$$\begin{aligned}
[P_{\mathfrak{a},p}|_k\sigma_{\mathfrak{b}}](z) &= j_{\sigma_{\mathfrak{b}}}(z)^{-k}P_{\mathfrak{a},p}(\sigma_{\mathfrak{b}}z) \\
&= j_{\sigma_{\mathfrak{b}}}(z)^{-k}\sum_{\gamma\in U(\mathbb{Z})\backslash\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}}\pi(\sigma_{\mathfrak{a}}\gamma\sigma_{\mathfrak{b}}^{-1},\sigma_{\mathfrak{b}}z) \\
&= j_{\sigma_{\mathfrak{b}}}(z)^{-k}\sum_{\gamma\in U(\mathbb{Z})\backslash\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}}\overline{\vartheta(\sigma_{\mathfrak{a}}\gamma\sigma_{\mathfrak{b}}^{-1})w(\sigma_{\mathfrak{a}}^{-1},\sigma_{\mathfrak{a}}\gamma\sigma_{\mathfrak{b}}^{-1})}j_{\gamma\sigma_{\mathfrak{b}}^{-1}}(\sigma_{\mathfrak{b}}z)^{-k}p(\gamma z) \\
&= \sum_{\gamma\in U(\mathbb{Z})\backslash\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}}\overline{\vartheta_{\mathfrak{a},\mathfrak{b}}(\gamma)}j_{\gamma}(z)^{-k}p(\gamma z), \qquad (43)
\end{aligned}$$

where

$$\vartheta_{\mathfrak{a},\mathfrak{b}}(\gamma) = \vartheta(\sigma_{\mathfrak{a}}\gamma\sigma_{\mathfrak{b}}^{-1})w(\sigma_{\mathfrak{a}}^{-1},\sigma_{\mathfrak{a}}\gamma\sigma_{\mathfrak{b}}^{-1})w(\gamma\sigma_{\mathfrak{b}}^{-1},\sigma_{\mathfrak{b}}).$$

In general this is not a multiplier system. However, if $\mathfrak{a} = \mathfrak{b}$, then $\vartheta_{\mathfrak{a},\mathfrak{a}} = \vartheta_{\mathfrak{a}}$ is the multiplier system for the conjugate group $\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{a}}$ obtained by conjugating ϑ. In particular we have

$$[P_{\mathfrak{a},p}|_k\sigma_{\mathfrak{a}}](z) = \sum_{\gamma\in U(\mathbb{Z})\backslash\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{a}}}\overline{\vartheta_{\mathfrak{a}}(\gamma)}j_{\gamma}(z)^{-k}p(\gamma z).$$

This looks a lot nicer than the original definition and many computations can be reduced to considering this form by conjugation.

Lemma 2.5.5. *Suppose that p is bounded and $k > 2$. Then the series defining $P_{\mathfrak{a},p}(z)$ converges absolutely and defines a holomorphic function on $\mathbb{H}$. Furthermore, it satisfies*

$$[P_{\mathfrak{a},p}|_k\tau](z) = \vartheta(\tau)P_{\mathfrak{a},p}(z)$$

for all $\tau \in \Gamma$.

Proof. We first check convergence. Since we are assuming that p is bounded we have to estimate

$$\sum_{\Gamma_{\mathfrak{a}}\backslash\Gamma}|j_{\sigma_{\mathfrak{a}}^{-1}\gamma}(z)^{-k}| = y^{\frac{k}{2}}\sum_{\gamma\in\Gamma_{\mathfrak{a}}\backslash\Gamma}(\mathrm{Im}(\sigma_{\mathfrak{a}}^{-1}\gamma z))^{\frac{k}{2}}.$$

To control this sum we recall that

$$\sharp\{\gamma\in\Gamma_{\mathfrak{a}}\backslash\Gamma\colon\ \mathrm{Im}(\sigma_{\mathfrak{a}}^{-1}\gamma z) > Y\} < 1 + \frac{10}{c(\mathfrak{a})Y}.$$

Convergence is immediate.

To check the transformation behaviour we can conjugate the group and assume $\mathfrak{a} = \infty$ and $\sigma_\mathfrak{a} = 1$. Take $\tau \in \Gamma$ and compute

$$\begin{aligned} P_{\mathfrak{a},p}(\tau z) &= \sum_{\gamma \in \Gamma_\mathfrak{a} \backslash \Gamma} \overline{\vartheta(\gamma)} j_\gamma(\tau z)^{-k} p(\gamma \tau z) \\ &= \sum_{\gamma \in \Gamma_\mathfrak{a} \backslash \Gamma} \overline{\vartheta(\gamma\tau^{-1})} j_{\gamma\tau^{-1}}(\tau z)^{-k} p(\gamma z). \end{aligned}$$

This follows just by a simple reordering of the sum (which is allowed now). We are done after checking that

$$\overline{\vartheta(\gamma\tau^{-1})} = \overline{w(\gamma,\tau^{-1})\vartheta(\gamma)\vartheta(\tau^{-1})} = \overline{w(\gamma,\tau^{-1})} w(\tau,\tau^{-1})\vartheta(\tau)\overline{\vartheta(\gamma)}$$

and

$$j_{\gamma\tau^{-1}}(\tau z)^{-k} = w(\gamma,\tau^{-1}) j_\gamma(z)^{-k} j_{\tau^{-1}}(\tau z)^{-k} = w(\gamma,\tau^{-1})\overline{w(\tau,\tau^{-1})} j_\tau(z)^k j_\gamma(z)^{-k}.$$

□

The next step is to check holomorphicity at the cusps. To do this we need to compute the Fourier expansion. We start by inserting Lemma 2.5.1 into (43):

$$[P_{\mathfrak{a},p}|_k\sigma_\mathfrak{b}](z) = \delta_{\mathfrak{a}\sim\mathfrak{b}} p(z) + \sum_{1 \neq \gamma \in U(\mathbb{Z}) \backslash \sigma_\mathfrak{a}^{-1}\Gamma\sigma_\mathfrak{b}/U(\mathbb{Z})} \overline{\vartheta_{\mathfrak{a},\mathfrak{b}}(\gamma)} I_\gamma(z) \tag{44}$$

where for any representative $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $c > 0$ we have

$$\begin{aligned} I_\gamma(z) &= \sum_{n\in\mathbb{Z}} j_{\gamma T^n}(z)^{-k} p(\gamma T^n z) \overline{\vartheta(\gamma_\mathfrak{b}^n)} \\ &= \sum_{n\in\mathbb{Z}} (c(z+n)+d)^{-k} \cdot p\left(\frac{a}{c} - \frac{1}{c(c(z+n)+d)}\right) \cdot e(-\kappa_\mathfrak{b} n). \end{aligned}$$

Applying Poisson summation to the n-sum yields

$$I_\gamma(z) = \sum_{n\in\mathbb{Z}} \int_\mathbb{R} (c(z+t)+d)^{-k} \cdot p\left(\frac{a}{c} - \frac{1}{c(c(z+t)+d)}\right) \cdot e(-(n+\kappa_\mathfrak{b})t) dt.$$

A change of variables leads to

$$I_\gamma(z) = \frac{1}{c} \sum_{n\in\mathbb{Z}} e((n+\kappa_\mathfrak{b})z) e((n+\kappa_\mathfrak{b})\frac{d}{c}) \cdot \int_{icy-\infty}^{icy+\infty} x^{-k} p(\frac{a}{c} - \frac{1}{cx}) e(-(n+\kappa_\mathfrak{b})\frac{x}{c}) dx.$$

Note that the integral is actually independent of the path of integration taken, so that we can replace icy by iy_0 for some $y_0 > 0$. At this point we specialize to $p(z) = e(mz)$ with $m \in \mathbb{N}$. For this choice we get

$$I_\gamma(z) = \frac{1}{c} \sum_{n\in\mathbb{Z}} e((n+\kappa_\mathfrak{b})z) e((n+\kappa_\mathfrak{b})\frac{d}{c} + m\frac{a}{c}) \cdot I(m,n;c), \tag{45}$$

where

$$I(m,n;c) = \int_{iy_0-\infty}^{iy_0+\infty} x^{-k} e\left(-\frac{m}{cx} - \frac{(n+\kappa_{\mathfrak{b}})x}{c}\right) dx.$$

This evaluates to

$$I(m,n;c) = \begin{cases} \frac{2\pi}{i^k}\left(\frac{n+\kappa_{\mathfrak{b}}}{m}\right)^{\frac{k-1}{2}} J_{k-1}\left(\frac{4\pi\sqrt{m(n+\kappa_{\mathfrak{b}})}}{c}\right) & \text{if } n+\kappa_{\mathfrak{b}}>0, \\ 0 & \text{else.} \end{cases}$$

We define the (generalized) Kloosterman sum

$$S_{\mathfrak{a},\mathfrak{b}}(m,n;c) = \sum_{\substack{d \bmod c, \\ \gamma = \begin{pmatrix} a & * \\ c & d \end{pmatrix} \in \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}}} \overline{\vartheta_{\mathfrak{a},\mathfrak{b}}(\gamma)} e\left(\frac{ma+(n+\kappa_{\mathfrak{b}})d}{c}\right). \tag{46}$$

Inserting (45) into (44) we find that

$$[P_{\mathfrak{a},p}|_k\sigma_{\mathfrak{b}}](z) = \delta_{\mathfrak{a}\sim\mathfrak{b}} e(mz) + \sum_{n=1}^{\infty} e((n+\kappa_{\mathfrak{b}})z) \sum_{c>0} \frac{1}{c} S_{\mathfrak{a},\mathfrak{b}}(m,n;c) \cdot I(m,n;c).$$

We thus have computed the Fourier expansion of the Poincaré series $P_{\mathfrak{a},p}$ at the cusp $\mathfrak{b}$. Since this is an important result let us phrase it as a theorem:

Theorem 2.5.6. *Let Γ be a Fuchsian group of the first kind, let $k \in \mathbb{R}_{>2}$ and let ϑ be a multiplier system of weight k for Γ. Put $p(z) = e(mz)$ with $m \in \mathbb{N}$ and assume that $\mathfrak{a}$ is a singular cusp. Then we have the Fourier expansion $[P_{\mathfrak{a},p}|_k\sigma_{\mathfrak{b}}](z) = e(\kappa_{\mathfrak{b}}) \sum_{n=\lfloor 1-\kappa_{\mathfrak{b}}\rfloor}^{\infty} a_{P_{\mathfrak{a},p}}(n;\mathfrak{b}) e(nz)$ with*

$$a_{P_{\mathfrak{a},p}}(n;\mathfrak{b}) = \delta_{n=m}\delta_{\mathfrak{a}\sim\mathfrak{b}} + \frac{2\pi}{i^k}\left(\frac{n+\kappa_{\mathfrak{b}}}{m}\right)^{\frac{k-1}{2}} \sum_{c>0} \frac{1}{c} S_{\mathfrak{a},\mathfrak{b}}(m,n;c) \cdot J_{k-1}\left(\frac{4\pi\sqrt{m(n+\kappa_{\mathfrak{b}})}}{c}\right),$$

where $\mathfrak{b}$ is any cusp and $S_{\mathfrak{a},\mathfrak{b}}(m,n;c)$ is the (generalized) Kloosterman sum defined in (46).

Corollary 2.5.7. *Under assumptions of Theorem 2.5.6 we have $P_{\mathfrak{a},p} \in S_k(\Gamma,\vartheta)$.*

Exercise 3, Sheet 5: Let $\Gamma = \Gamma_0(q)$ with $q = rs$ for $(r,s) = 1$. Consider the two cusps $\mathfrak{a} = \infty$ and $\mathfrak{b} = \frac{1}{r}$ with scaling matrices

$$\sigma_{\mathfrak{a}} = 1 \text{ and } \sigma_{\mathfrak{b}} = \begin{pmatrix} \sqrt{s} & 0 \\ r\sqrt{s} & \frac{1}{\sqrt{s}} \end{pmatrix}.$$

a) Let $\mathfrak{a}'$ and $\mathfrak{b}'$ be cusps of $\Gamma_0(q)$ with scalling matrices $\sigma_{\mathfrak{a}'}$ and $\sigma_{\mathfrak{b}'}$. Suppose that $\mathfrak{a} = \gamma_1\mathfrak{a}'$ and $\mathfrak{b} = \gamma_2\mathfrak{b}'$ for $\gamma_1,\gamma_2 \in \Gamma_0(q)$. Show that there are real numbers t_1, t_2 independent of n and m such that

$$S_{\mathfrak{a}',\mathfrak{b}'}(m,n;c) = e(mt_1+nt_2) S_{\mathfrak{a},\mathfrak{b}}(m,n;c)$$

b) Show that
$$S_{\mathfrak{a},\mathfrak{b}}(m,n;c) = e\left(n\frac{\overline{r}}{s}\right) S(m\overline{s},n;lr)$$
if $c = lr\sqrt{s}$ with $l \in \mathbb{N}$ and $(l,s)=1$ and otherwise the Kloosterman sum is 0. In the equation above $\overline{r}$ denotes the inverse of r modulo s, and $\overline{s}$ denotes the inverse of s modulo lr.

Solution. Part a) works for any discrete group Γ with cusps. Recall that, for two cusps $\mathfrak{a},\mathfrak{b}$ and scaling matrices $\sigma_{\mathfrak{a}},\sigma_{\mathfrak{b}}$ we define
$$\mathcal{C}_{\mathfrak{a}\mathfrak{b}} = \left\{ c>0 : \begin{pmatrix} * & * \\ c & * \end{pmatrix} \in \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}} \right\}$$
and the Kloosterman sum (for the trivial multiplier) is defined as
$$S_{\mathfrak{a},\mathfrak{b}}(m,n;c) = \sum_{\left(\begin{smallmatrix} a & * \\ c & d\end{smallmatrix}\right)\in B\backslash\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}/B} e\left(n\frac{d}{c}+m\frac{a}{c}\right)$$
where $B = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1\end{pmatrix} : n\in\mathbb{Z}\right\}$. Also, if $\Gamma_{\mathfrak{a}}$ is the stabilizer of $\mathfrak{a}$, then $\sigma_{\mathfrak{a}}^{-1}\Gamma_{\mathfrak{a}}\sigma_{\mathfrak{a}} = B$ and if $\gamma_1\in\Gamma$ with $\gamma_1\mathfrak{a}' = \mathfrak{a}$ then $\Gamma_{\mathfrak{a}'} = \gamma_1^{-1}\Gamma_{\mathfrak{a}}\gamma_1$. It follows that $\sigma_{\mathfrak{a}}^{-1}\gamma_1\sigma_{\mathfrak{a}'}\infty = \infty$ and
$$\left(\sigma_{\mathfrak{a}}^{-1}\gamma_1\sigma_{\mathfrak{a}'}\right)^{-1} B\left(\sigma_{\mathfrak{a}}^{-1}\gamma_1\sigma_{\mathfrak{a}'}\right) = \sigma_{\mathfrak{a}'}^{-1}\gamma_1^{-1}\Gamma_{a}\gamma_1\sigma_{\mathfrak{a}'} = \sigma_{\mathfrak{a}'}^{-1}\Gamma_{\mathfrak{a}'}\sigma_{\mathfrak{a}'} = B.$$
This implies that $\sigma_{\mathfrak{a}}^{-1}\gamma_1\sigma_{\mathfrak{a}'} = \left(\begin{smallmatrix} 1 & x \\ 0 & 1\end{smallmatrix}\right)$ for some $x\in\mathbb{R}$, so that $\sigma_{\mathfrak{a}'} = \gamma_1^{-1}\sigma_{\mathfrak{a}}\left(\begin{smallmatrix} 1 & x \\ 0 & 1\end{smallmatrix}\right)$. Similarly $\sigma_{\mathfrak{b}}^{-1}\gamma_2\sigma_{\mathfrak{b}'} = \left(\begin{smallmatrix} 1 & y \\ 0 & 1\end{smallmatrix}\right)$ and thus $\sigma_{\mathfrak{b}'} = \gamma_1^{-1}\sigma_{\mathfrak{b}}\left(\begin{smallmatrix} 1 & y \\ 0 & 1\end{smallmatrix}\right)$ for some $y\in\mathbb{R}$. It follows that
$$\sigma_{\mathfrak{a}'}^{-1}\Gamma\sigma_{\mathfrak{b}'} = \begin{pmatrix} 1 & -x \\ 0 & 1\end{pmatrix}\sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}\begin{pmatrix} 1 & y \\ 0 & 1\end{pmatrix}.$$
Therefore, there is a bijection that sends the double coset $B\backslash\sigma_{\mathfrak{a}^{-1}}\Gamma\sigma_{\mathfrak{b}}/B$ represented by $\left(\begin{smallmatrix} a & * \\ c & d\end{smallmatrix}\right)$ to the double coset of $B\backslash\sigma_{\mathfrak{a}'}^{-1}\Gamma\sigma_{\mathfrak{b}'}/B$ represented by $\left(\begin{smallmatrix} a-cx & * \\ c & d+cy\end{smallmatrix}\right)$ (recall that in the double coset the entries a,d are defined modulo c). Therefore, looking at the definition of the Kloosterman sum we see
$$S_{\mathfrak{a}',\mathfrak{b}'}^{\sigma_{\mathfrak{a}'},\sigma_{\mathfrak{b}'}}(m,n;c) = e(-mx+ny)S_{\mathfrak{a},\mathfrak{b}}^{\sigma_{\mathfrak{a}},\sigma_{\mathfrak{b}}}(m,n;c)$$
In particular, the absolute value of the Kloosterman sum is well-defined for equivalent cusps (and any choice of scaling matrix). This finishes the proof of part a).

For part b) we compute
$$\begin{pmatrix} a & b \\ qc & d\end{pmatrix}\begin{pmatrix} \sqrt{s} & 0 \\ r\sqrt{s} & \frac{1}{\sqrt{s}}\end{pmatrix} = \begin{pmatrix} \sqrt{s}(a+rb) & \frac{b}{\sqrt{s}} \\ \sqrt{s}(qc+dr) & \frac{d}{\sqrt{s}}\end{pmatrix} = \begin{pmatrix} \sqrt{s}x & \frac{y}{\sqrt{s}} \\ \sqrt{s}ru & \frac{v}{\sqrt{s}}\end{pmatrix}$$
where a,b,c,d are integers with $ad-qbc=1$ and x,y,u,v are also integers. Since $u = sc+d$ and $(d,c)=1$ we deduce that $(u,c)=1$. On the other direction if we

start with a matrix $\begin{pmatrix} \sqrt{s}x & \frac{y}{\sqrt{s}} \\ \sqrt{s}ru & \frac{v}{\sqrt{s}} \end{pmatrix}$ with $xv - ruy = 1$, multiply by on the right by $\sigma_{\mathfrak{b}}^{-1}$ and check if the resulting matrix belongs to $\Gamma_0(q)$ we get

$$\begin{pmatrix} \sqrt{s}x & \frac{y}{\sqrt{s}} \\ \sqrt{s}ru & \frac{v}{\sqrt{s}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{s}} & 0 \\ -r\sqrt{s} & \sqrt{s} \end{pmatrix} = \begin{pmatrix} x - yr & y \\ r(u-v) & v \end{pmatrix}$$

This matrix belongs to $\Gamma_0(q)$ if and only if $u \equiv v \bmod(s)$, which by the determinant condition is automatically a unit $\bmod(s)$. Therefore

$$\Gamma_0(q)\sigma_{\mathfrak{b}} = \left\{ \begin{pmatrix} \sqrt{s}x & \frac{y}{\sqrt{s}} \\ \sqrt{s}ru & \frac{v}{\sqrt{s}} \end{pmatrix} \mid x, y, u, v \in \mathbb{Z} \ , \ xv - yur = 1 \ , \ u \equiv v \bmod s \ , \ (u, s) = 1 \right\}.$$

Fix $u \in \mathbb{Z}$ with $(u, s) = 1$. Note that, by the determinant condition, v determines x modulo ur. Also, multiplying by elements of B on the right and left we observe that in a double coset v is determined only modulo qu, and since we must have $v \equiv u$ mod , and $q = rs$ with $(r, s) = 1$, by the chinese remainder theorem the map $\begin{pmatrix} \sqrt{s}x & \frac{y}{\sqrt{s}} \\ \sqrt{s}ru & \frac{v}{\sqrt{s}} \end{pmatrix} \mapsto v \bmod ru$ is injective from double cosets $B\backslash\Gamma\sigma_{\mathfrak{b}}/B$ with fixed u, to residues modulo ru. The image of the map are exactly the units modulo ru. Indeed, given such a unit ϵ, using that $(ru, s) = 1$, we can find an integer v such that $v \equiv \epsilon \bmod ru$ and $v \equiv u \bmod s$. Then, we let x be an integer representing the inverse of ϵ modulo ru and we let y the unique integer such that $xv - yur = 1$. The matrix with these entries is in $\Gamma_0(q)\sigma_{\mathfrak{b}}$ with the entry v as desired. Therefore, the corresponding Kloosterman sum is

$$S_{\mathfrak{a},\mathfrak{b}}(m, n; \sqrt{s}ru) = \sum_{\substack{v \equiv u \bmod(s) \\ v \text{ a unit } \bmod(urs)}} e\left(\frac{nv + m\overline{v}s}{qu}\right)$$

where $\overline{v}$ is the inverse of v modulo ru. Let $\overline{s}$ be an integer representing the inverse of s modulo ur and $\overline{u}, \overline{r}$ be integers representing the inverses of u, r respectively, modulo s. We can parametrize v in the Kloosterman sum as $v = d\overline{s}s + u\overline{u}\overline{r}ur$ where d moves in the units modulo ur. Also, $\overline{v}$ is represented by $\overline{d}\overline{s}s$. Therefore,

$$\begin{aligned} S_{\mathfrak{a},\mathfrak{b}}(m, n; \sqrt{s}ru) &= \sum_{d \in (\mathbb{Z}/(ru)\mathbb{Z})^\times} e\left(\frac{nd\overline{s}s + nu\overline{u}\overline{r}ur + m\overline{d}\overline{s}ss}{rsu}\right) \\ &= \sum_{d \in (\mathbb{Z}/(ru)\mathbb{Z})^\times} e\left(\frac{nu\overline{u}\overline{r}}{s}\right) e\left(\frac{n\overline{s}d + m\overline{d}\overline{s}}{ru}\right) = e\left(\frac{n\overline{r}}{s}\right) S(m\overline{s}, n; ru). \end{aligned}$$

This is what we wanted to show. ∎

It is not obvious that the Poincaré series are non-trivial in general. However, using the explicit form of the Fourier coefficients one can produce estimates that ensure that the Poincaré series are non-zero for large enough k. This means that we have constructed some non-trivial cusp forms in quite some generality.

Lemma 2.5.8. *Let Γ be a subgroup of $PSL_2(\mathbb{R})$ that is discrete, finitely generated and such that Vol$(\Gamma\backslash\mathbb{H}) < \infty$. Let $m \in \mathbb{N}$ and consider a cusp $\mathfrak{a}$ of Γ. Then there is a large enough $k_0 > 2$ such that for any weight $k \geq k_0$ and any multiplier system ϑ for Γ (of weight k) the Poincaré series $P_{\mathfrak{a},p}$ of weight k associated to θ and $p(z) = e(mz)$ is nonzero.*

Proof. We use Theorem 2.5.6 to write

$$(P_{\mathfrak{a},p}|_k\sigma_{\mathfrak{a}})(z) = e(\kappa_{\mathfrak{a}}z)\sum_{n=\lfloor 1-\kappa_{\mathfrak{a}}\rfloor}^{\infty} a_{P_{\mathfrak{a},p}}(n;\mathfrak{a})e(nz)$$

where

$$a_{P_{\mathfrak{a},p}}(n;\mathfrak{a}) = \delta_{n=m} + \frac{2\pi}{i^k}\left(\frac{n+\kappa_{\mathfrak{a}}}{m}\right)^{\frac{k-1}{2}}\sum_{c>0}\frac{1}{c}S_{\mathfrak{a},\mathfrak{a}}(m,n;c)J_{k-1}\left(\frac{4\pi\sqrt{m(n+\kappa_{\mathfrak{a}})}}{c}\right)$$

In particular, for $n = m$ this has the form $1+\mathcal{E}$ and we want to show that for large k the stuff $\mathcal{E}$ is less than 1 in absolute value. It is important here that $\kappa_{\mathfrak{a}} \in [0,1)$, in particular it is bounded. Recall that we have a bound

$$\sum_{0<c\leq X}\frac{1}{c}|S_{\mathfrak{a},\mathfrak{a}}(m,n;c)| \leq c(a)^{-1}X$$

where $c(a)$ is the minimum moduli of the cusp a. Also, we have a power series expansion (valid for example for $\mathrm{Re}(z) > 0$)

$$J_{k-1}(z) = \left(\frac{z}{2}\right)^{k-1}\sum_{r=0}^{\infty}(-1)^r\frac{\left(\frac{1}{4}z^2\right)^r}{r!\Gamma(k+r)}.$$

For $k \geq 1$ we can bound trivially (this is a very bad bound when z is large but it is enough for our purposes)

$$|J_{k-1}(z)| \leq 2^{1-k}\frac{|z|^{k-1}}{\Gamma(k)}\exp\left(\frac{|z|^2}{4}\right).$$

In particular, since we fixed $m = n$, $\kappa_{\mathfrak{a}} \leq 1$ and the moduli satisfy $c \geq c(a)$ we see that $\frac{4\pi\sqrt{m^2+m\kappa_{\mathfrak{a}}}}{c}$ is bounded. Therefore

$$J_{k-1}\left(\frac{4\pi\sqrt{m^2+m\kappa_{\mathfrak{a}}}}{c}\right) \leq A(2\pi\sqrt{m^2+m\kappa_{\mathfrak{a}}})^{k-1}c^{1-k}\Gamma(k)^{-1}$$

for some $A > 0$ (we have disposed of the bad term $\exp(|z|^2/4)$ noticing that it is bounded, since $z = \frac{4\pi\sqrt{m^2+m\kappa_{\mathfrak{a}}}}{c}$ remains bounded). Therefore

$$|\sum_{c>0}\frac{1}{c}S_{\mathfrak{a},\mathfrak{a}}(m,n;c)J_{k-1}\left(\frac{4\pi\sqrt{m(n+\kappa_{\mathfrak{a}})}}{c}\right)| \leq \frac{A(2\pi)^{k-1}(2m^2)^{\frac{k-1}{2}}}{\Gamma(k)}\sum_{c>0}c^{-k}|S_{\mathfrak{a},\mathfrak{a}}(m,n;c)|.$$

Using the trivial bound (47) and integrating by parts we get

$$\sum_{c>0} c^{-k}|S_{\mathfrak{a},\mathfrak{a}}(m,n;c)| \leq \frac{2k-3}{k-2}c(\mathfrak{a})^{1-k}$$

(note that $k>2$). One can also obtain this bound dyadically, by individually estimating the contributions of $2^n c(\mathfrak{a}) \leq c < 2^{n+1}c(a)$ and summing over $i \geq 0$ (this gives a worse constant $\frac{2}{1-2^{2-k}}$, but it is the same for our purposes). Putting it all together, we obtain

$$\begin{aligned} a_{P_{\mathfrak{a},p}}(m;\mathfrak{a}) &= 1 + \frac{2\pi}{i^k}\left(\frac{m+\kappa_{\mathfrak{a}}}{m}\right)^{\frac{k-1}{2}} \sum_{c>0}\frac{1}{c}S_{\mathfrak{a},\mathfrak{a}}(m,m;c)J_{k-1}\left(\frac{4\pi\sqrt{m(m+\kappa_{\mathfrak{a}})}}{c}\right) \\ &= 1 + O\left(\left(1+\frac{1}{m}\right)^{\frac{k-1}{2}} \frac{(2\pi)^{k-1}(2m^2)^{\frac{k-1}{2}}}{\Gamma(k)}\frac{2k-3}{k-2}c(\mathfrak{a})^{1-k}\right). \end{aligned} \tag{47}$$

Using the Stirling formula for the Gamma function

$$\Gamma(k) \sim \sqrt{2\pi}e^{-k}k^{k-1/2} \text{ as } k \to \infty$$

one sees that the error in (47) tends to 0 when $k \to \infty$. Therefore, since one of the Fourier coefficients of $P_{\mathfrak{a},p}$ is not zero, it must be that $P_{\mathfrak{a},p}$ is a non-zero cusp form of weight k and multiplier ϑ. □

The Poincaré series also satisfy the following interesting property:

Theorem 2.5.9. *Let Γ be a Fuchsian group of the first kind, let $k \in \mathbb{R}_{>2}$ and let ϑ be a multiplier system of weight k for Γ. Put $p(z) = e(mz)$ with $m \in \mathbb{N}$ and assume that $\mathfrak{a}$ is a singular cusp. Then, for $f \in S_k(\Gamma,\vartheta)$ we have*

$$\langle f, P_{\mathfrak{a},p}\rangle = \frac{\Gamma(k-1)}{(4\pi m)^{k-1}} \cdot a_f(m;\mathfrak{a}).$$

Proof. Without loss of generality we can assume that $\mathfrak{a} = \infty$ and $\sigma_{\mathfrak{a}} = 1$. We simply compute

$$\begin{aligned} \langle f, P_{\mathfrak{a},p}\rangle &= \int_{\Gamma\backslash\mathbb{H}} \mathrm{Im}(z)^k f(z)\overline{P_{\mathfrak{a},p}(z)}d\mu(z) \\ &= \int_{\Gamma\backslash\mathbb{H}} \sum_{\gamma\in U(\mathbb{Z})\backslash\Gamma} \mathrm{Im}(z)^k \underbrace{f(z)\vartheta(\gamma)\overline{j_\gamma(z)}^{-k}}_{=|j_\gamma(z)|^{-2k}f(\gamma z)}\overline{e(m\gamma z)}d\mu(z) \\ &= \int_{\Gamma\backslash\mathbb{H}} \sum_{\gamma\in U(\mathbb{Z})\backslash\Gamma} \mathrm{Im}(\gamma z)^k f(\gamma z)\overline{e(m\gamma z)}d\mu(z). \end{aligned}$$

Recall that the integral $\int_{\Gamma\backslash\mathbb{H}} \ldots d\mu(z)$ is understood to be an integral over a suitable fundamental domain $\mathcal{F}$ of Γ. Interchanging sum and integral as well as a change of variables then yields

$$\langle f, P_{\mathfrak{a},p}\rangle = \sum_{\gamma\in U(\mathbb{Z})\backslash\Gamma}\int_{\gamma\mathcal{F}}\operatorname{Im}(z)^k f(z)\overline{e(mz)}d\mu(z) = \int_{U(\mathbb{Z})\backslash\mathbb{H}}\operatorname{Im}(z)^k f(z)\overline{e(mz)}d\mu(z).$$

Inserting the Fourier expansion of f (at $\mathfrak{a}=\infty$) makes it easy to compute the remaining integral:

$$\langle f, P_{\mathfrak{a},p}\rangle = \sum_{n=1}^{\infty} a_f(n;\mathfrak{a})\int_0^1 e(x(n-m))dx\int_0^\infty y^{k-2}e^{-2\pi(n+m)y}dy.$$

The x-integral evaluates to $\delta_{m=n}$ and recognising the y-integral as a Γ-function gives the desired result. ◻

We can now establish the following very strong formula, which will later play a crucial role in applications.

Theorem 2.5.10 (Petersson Formula)**.** *Let Γ be a Fuchsian group of the first kind, let $k\in\mathbb{R}_{>2}$ and let ϑ be a multiplier system of weight k for Γ. For two singular cusps $\mathfrak{a},\mathfrak{b}$ of Γ we have*

$$\frac{\Gamma(k-1)}{(4\pi\sqrt{mn})^{k-1}}\cdot\sum_{f\in\mathcal{O}}\overline{a_f(m;\mathfrak{a})}\cdot a_f(n;\mathfrak{b})$$
$$= \delta_{m=n}\delta_{\mathfrak{a}\sim\mathfrak{b}} + 2\pi i^{-k}\sum_{c>0}c^{-1}S_{\mathfrak{a},\mathfrak{b}}(m,n;c)J_{k-1}(\frac{4\pi\sqrt{mn}}{c}),$$

where $\mathcal{O}$ is an orthonormal basis of $S_k(\Gamma,\vartheta)$.

Remark 2.5.11. Note that there are no convergence issues on the right hand side of the formula, since $S_k(\Gamma,\vartheta)$ is finite dimensional. See Lemma 2.3.4 above.[18]

Proof. Let $p(z)=e(mz)$ and $p'(z)=e(nz)$. Then we first write

$$P_{\mathfrak{a},p}(z) = \sum_{f\in\mathcal{O}}\langle P_{\mathfrak{a},p}, f\rangle f(z) = \frac{\Gamma(k-1)}{(4\pi m)^{k-1}}\sum_{f\in\mathcal{O}}\overline{a_f(m;\mathfrak{a})}\cdot f(z).$$

This way we can compute

$$\langle P_{\mathfrak{a},p}, P_{\mathfrak{b},p'}\rangle = \frac{\Gamma(k-1)}{(4\pi m)^{k-1}}\sum_{f\in\mathcal{O}}\overline{a_f(m;\mathfrak{a})}\cdot\langle f, P_{\mathfrak{b},p'}\rangle = \frac{\Gamma(k-1)^2}{(4^2\pi^2 mn)^{k-1}}\sum_{f\in\mathcal{O}}\overline{a_f(m;\mathfrak{a})}\cdot a_f(n;\mathfrak{b}).$$

On the other hand we have

$$\langle P_{\mathfrak{a},p}, P_{\mathfrak{b},p'}\rangle = \frac{\Gamma(k-1)}{(4\pi m)^{k-1}}a_{P_{\mathfrak{a},p}}(n;\mathfrak{b}).$$

Evaluating $a_{P_{\mathfrak{a},p}}(n;\mathfrak{b})$ using Theorem 2.5.6 and combining the two expressions for $\langle P_{\mathfrak{a},p}, P_{\mathfrak{b},p'}\rangle$ gives the desired result. ◻

[18]This was not discussed in the lecture and added there afterwards for completeness.

Example 2.5.12. For our amusement we can apply the Petersson formula in the following special situation. Take $k = 12$, $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and $\vartheta = \vartheta_{\mathrm{tr}}$. Recall that $S_{12}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C} \cdot \Delta$ so that we can take $\mathcal{O} = \{\Delta/\langle\Delta,\Delta\rangle^{\frac{1}{2}}\}$. On the other hand the essentially only choice of (singular) cusps is $\mathfrak{a} = \mathfrak{b} = \infty$ and in this case the Kloosterman sum takes the shape

$$S(m,n;c) = S_{\infty,\infty}(m,n;c) = \sum_{\substack{d \bmod c,\\ (c,d)=1}} e\left(\frac{n\overline{d}+md}{c}\right),$$

where $d \cdot \overline{d} \equiv 1 \bmod c$. Thus the Petersson formula for $m = 1$ and $n \in \mathbb{N}$ reads

$$\frac{\Gamma(11)}{(4\pi)^{11}} \cdot n^{-\frac{11}{2}} \cdot \frac{\tau(n)}{\langle\Delta,\Delta\rangle} = \delta_{n=1} + 2\pi \sum_{c\in\mathbb{N}} \frac{S(1,n;c)}{c} J_{11}\left(\frac{4\pi\sqrt{n}}{c}\right).$$

Is this formula helpful in understanding the properties of $\tau(n)$?

Exercise 2, Sheet 5: Let $\Delta = \sum_{n=1}^{\infty} \tau(n)e(nz) \in S_{12}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ be the Ramanujan Δ-function. Show that

$$\tau(m)\tau(n) = \sum_{d|(m,n)} d^{11}\tau\left(\frac{mn}{d^2}\right) \tag{48}$$

Manual:

i) Use the Petersson Formula (i.e. Theorem 2.5.9 of the lecture notes) to write down an expression for $\tau(n)\tau(m)$ in terms of Kloosterman sums and J-Bessel functions.

ii) Manipulate the resulting right hand side using the identities[19]

$$S(m,n;c) = \sum_{d|(c,m,n)} dS(mnd^{-2}, 1; cd^{-1}) \tag{49}$$

and

$$\delta_{m=n} = \sum_{d|(m,n)} \delta_{1=\frac{mn}{d^2}} \tag{50}$$

Solution. By the Petersson Formula (Theorem 2.5.10), since $S_{12}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ is one dimensional and $\Delta \neq 0$, we have

$$\tau(m)\tau(n) = \frac{(4\pi\sqrt{mn})^{11}}{\Gamma(11)} \|\Delta\|_{L^2}^2 \left(\delta_{m=n} + 2\pi \sum_{c>0} c^{-1} S(m,n;c) J_{11}\left(\frac{4\pi\sqrt{mn}}{c}\right)\right) \tag{51}$$

[19] A brief elementary proof of Selberg's identity (49) can be found in the note *Selberg's identity for Kloosterman sums* by G. Harcos and G. Károlyi.

Since $\tau(1)=1$, in particular

$$d^{11}\tau(\frac{mn}{d^2}) = \frac{(4\pi\sqrt{mn})^{11}}{\Gamma(11)}\|\Delta\|_{L^2}^2 \left(\delta_{\frac{mn}{d^2}=1} + 2\pi\sum_{c>0} c^{-1}S\left(\frac{mn}{d^2},1;c\right)J_{11}\left(\frac{4\pi\sqrt{mn}}{cd}\right)\right)$$

for any $d|(m,n)$. It is now clear that the part involving delta functions in (48) follows immediately from identity (50). On the other hand, we can use (49) to rewrite the sum of Kloosterman sums in a different way

$$\begin{aligned}\sum_{c=1}^{\infty} c^{-1}S_{a,b}(m,n;c)J_{11}\left(\frac{4\pi\sqrt{mn}}{c}\right) &= \sum_{c=1}^{\infty}\sum_{d|(m,n,c)}\frac{d}{c}S\left(\frac{mn}{d^2},1;\frac{c}{d}\right)J_{11}\left(\frac{4\pi\sqrt{\frac{mn}{d^2}}}{\frac{c}{d}}\right)\\ &= \sum_{d|(m,n)}\sum_{r=1}^{\infty} r^{-1}S\left(\frac{mn}{d^2},1;r\right)J_{11}\left(\frac{4\pi\sqrt{\frac{mn}{d^2}}}{r}\right)\end{aligned}$$

where we have changed variables $c=rd$. Therefore,

$$\begin{aligned}\tau(m)\tau(n) &= \frac{(4\pi\sqrt{mn})^{11}}{\Gamma(11)}\|\Delta\|_{L^2}^2\sum_{d|(m,n)}\left(\delta_{1=\frac{mn}{d^2}} + 2\pi\sum_{r=1}^{\infty} r^{-1}S\left(\frac{mn}{d^2},1;r\right)J_{11}\left(\frac{4\pi\sqrt{\frac{mn}{d^2}}}{r}\right)\right)\\ &= \sum_{d|(m,n)} d^{11}\tau\left(\frac{mn}{d^2}\right)\end{aligned}$$

as desired. ∎

Exercise 3, Sheet 8: For a fixed prime p we consider the space $L^2(\mathbb{Z}/p\mathbb{Z})$ of p-periodic functions from $\mathbb{Z}$ to $\mathbb{C}$. We equip $\mathbb{Z}/p\mathbb{Z}$ with the Haar probability measure so that the inner product is given by

$$\langle G,H\rangle = \frac{1}{p}\sum_{n \bmod p} G(n)\overline{H(n)}, \text{ for } G,H\in L^2(\mathbb{Z}/p\mathbb{Z}).$$

For $G\in L^2(\mathbb{Z}/p\mathbb{Z})$ we define the normalized Fourier transform by

$$\hat{G}(h) = \frac{1}{\sqrt{p}}\sum_{n \bmod p} G(n)e\left(\frac{hn}{p}\right).$$

Further we set

$$\check{G}(n) = \frac{1}{\sqrt{p}}\sum_{\substack{h \bmod p\\ (h,p)=1}} \hat{G}(h)e\left(\frac{\overline{h}n}{p}\right).$$

a) Let $(a,q)=1$ and set $K(n)=\frac{1}{\sqrt{p}}S(1,an;p)$. Compute $\hat{K}$ and show that

$$\check{K}(n) = \begin{cases}\frac{p-1}{\sqrt{p}} & \text{if } n\equiv a \bmod p,\\ -\frac{1}{\sqrt{p}} & \text{else.}\end{cases}$$

b) Determine the kernel of the map $\check{(\cdot)} : L^2(\mathbb{Z}/p\mathbb{Z}) \to L^2(\mathbb{Z}/p\mathbb{Z})$ and show that $\check{(\cdot)}$ is self-inverse on $\ker\left(\check{(\cdot)}\right)^{\perp}$.

Solution. For part a), we compute directly

$$\hat{K}(h) = \frac{1}{p} \sum_{n \bmod p} \sum_{\substack{d \bmod p \\ (d,p)=1}} e\left(\frac{dan + \overline{d}}{p}\right) e\left(\frac{hn}{p}\right) = \frac{1}{p} \sum_{\substack{d \bmod p \\ (h,p)=1}} e\left(\frac{\overline{d}}{p}\right) \sum_{n \bmod p} e\left(\frac{n(da+h)}{p}\right).$$

The inner sum is 0 unless $da + h = 0$ modulo p. Since a, d are invertible we have two options. If $h = 0$ then the inner sum is always 0 and $\hat{K}(h) = 0$. Otherwise, $da+h = 0$ modulo p exactly for $d = -\overline{a}h$, and we find $\hat{K}(h) = e\left(\frac{-a\overline{h}}{p}\right)$. Therefore, we have

$$\check{K}(n) = \frac{1}{\sqrt{p}} \sum_{\substack{h \bmod p \\ (h,p)=1}} e\left(\frac{(n-a)\overline{h}}{p}\right).$$

Since $\sum_{i=1}^{p-1} e\left(\frac{ai}{p}\right) = p-1$ or -1 according to whether a is 0 or not modulo p, part a) is clear.

For part b), observe that $G \mapsto \hat{G}$, which we will denote by $\mathcal{F}(G)$, is the Fourier transform, which is an isometry in $L^2(\mathbb{Z}/p\mathbb{Z})$ whose inverse is given by

$$\mathcal{F}^{-1}(G)(n) := \frac{1}{\sqrt{p}} \sum_{h \bmod p} G(h) e\left(\frac{-hn}{p}\right).$$

Denote by $P : L^2(\mathbb{Z}/p\mathbb{Z}) \to L^2(\mathbb{Z}/p\mathbb{Z})$ the map $P(f)(n) = f(n)$ if $n \not\equiv 0$ and $P(f) = 0$ otherwise. If $\delta \in L^2(\mathbb{Z}/p\mathbb{Z})$ is the function described by $\delta(0) = \sqrt{p}$ and $\delta(n) = 0$ for $n \not\equiv 0$ modulo n, then P is the orthogonal projection onto the orthogonal complement of P. Let $H := \langle\delta\rangle^{\perp}$. Clearly, $\langle\delta\rangle$ is the kernel of P, and P acts like the identity on H. Also, consider the isometric involution described by $S(f)(0) = f(0)$ and $S(f)(n) = f(-\overline{n})$ for $n \not\equiv 0$ modulo p. We have $S^2 = \mathrm{Id}$, and it follows that $S \circ P$ is self-inverse on H. The map $\check{(\cdot)}$ described in the exercise is precisely $\mathcal{F}^{-1} \circ S \circ P \circ \mathcal{F}$. Therefore,

$$\begin{aligned}
&\ker\left(\check{(\cdot)}\right) = \mathcal{F}^{-1}(\langle\delta\rangle) = \langle \mathrm{const}_1 \rangle, \\
&\mathcal{F}^{-1}(H) = \langle \mathrm{const}_1 \rangle)^{\perp} = \{f \in L^2(\mathbb{Z}/p\mathbb{Z}) : \sum_{n \bmod p} f(n) = 0\}
\end{aligned}$$

and $\check{(\cdot)}$ is self-inverse on the subspace $\mathcal{F}^{-1}(H)$. □

Remark 2.5.13. To check that $\mathcal{F}$ and $\mathcal{F}^{-1}$ are inverse isometries, simply observe that $\mathcal{F}(\sqrt{p}\delta_n) = e\left(\frac{\cdot n}{p}\right)$ and $\mathcal{F}^{-1}\left(e\left(\frac{\cdot n}{p}\right)\right) = \sqrt{p}\delta_n$, and check that the sets $\{\sqrt{p}\delta_n\}_{n \bmod p}$ and $\left\{e\left(\frac{\cdot n}{p}\right)\right\}_{n \bmod p}$ are orthonormal basis.

Exercise 4 (Bonus), Sheet 7: The goal of this exercise is to verify

$$E_{1,\chi_{-4}}(z) := \frac{1}{4} + \sum_{n=1}^{\infty}\left(\sum_{d|n}\chi_{-4}(d)\right)e(nz) \in M_1(\Gamma_0(4),\chi_{-4}). \tag{52}$$

We start by defining

$$\mathbf{E}_{1,\chi_{-4}}(z,s) = \sum_{\substack{(0,0)\neq(c,d)\in\mathbb{Z}^2\\ 4|c}} \frac{\chi_{-4}(d)}{cz+d}\cdot|cz+d|^{-2s}, \tag{53}$$

for $\mathrm{Re}(s) > \frac{1}{2}$.

a) Modify the argument leading to Theorem 2.5.6 of the lecture notes to compute the Fourier expansion of $\mathbf{E}_{1,\chi_{-4}}(z,s)$ at ∞.

b) Show that $\mathbf{E}_{1,\chi_{-4}}(z,s)$ has an analytic continuation to $\mathrm{Re}(s) = 0$. This allows us to define $\mathbf{E}_{1,\chi_{-4}}(z,0)$. Here it can be used that the Dirichlet L-function $L(s,\chi_{-4})$ defined by $\sum_{n\in\mathbb{N}}\chi_{-4}(n)n^{-s}$ when $\mathrm{Re}(s) > 1$ has an analytic continuation to $s \in \mathbb{C}$.

c) Relate $E_{1,\chi_{-4}}(z)$ to $\mathbf{E}_{1,\chi_{-4}}(z,s)$ and deduce (52). It can be used that $L(0,\chi_{-4}) = \frac{1}{2}$ and $L(1,\chi_{-4}) = \frac{\pi}{4}$.

Solution. We can write

$$\begin{aligned}\mathbf{E}_{1,\chi_{-4}}(z,s) = 2L(1+2s,\chi_{-4}) &+ 2\sum_{c=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{1}{(4cz+4n+1)|4cz+4n+1|^{2s}}\\ &- 2\sum_{c=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{1}{(4cz+4n+3)|4cz+4n+3|^{-2s}}\end{aligned} \tag{54}$$

We want to apply Poisson summation formula to the function

$$f_{w,s}(x) := \frac{1}{(w+x)|w+x|^{2s}}$$

for certain choices of $w = u+iv \in \mathbb{H}p$. First we calculate the Fourier transform

$$\begin{aligned}\hat{f}_{w,s}(\alpha) &:= \int_{\mathbb{R}}\frac{e(-\alpha t)}{(u+iv+t)|u+iv+t|^{2s}}\,dt = e(\alpha u)\int_{\mathbb{R}}\frac{e(-\alpha t)}{(iv+t)|iv+t|^{2s}}\,dt\\ &= e(\alpha u)v^{-2s}\int_{\mathbb{R}}\frac{e(-\alpha vt)}{(i+t)|i+t|^{2s}} = e(\alpha u)v^{-2s}\left(\int_{\mathbb{R}}\frac{te(-\alpha vt)}{(t^2+1)^{s+1}}\,dt - i\int_{\mathbb{R}}\frac{e(-\alpha vt)}{(t^2+1)^{s+1}}\,dt\right)\\ &= e(\alpha u)v^{-2s}\left(-i\frac{\pi\alpha v}{s}\int_{\mathbb{R}}\frac{e(-\alpha vt)}{(t^2+1)^{s}}\,dt - i\int_{\mathbb{R}}\frac{e(-\alpha vt)}{(t^2+1)^{s+1}}\,dt\right).\end{aligned}$$

This is Basset's integral, which is very important for the spectral theory of automorphic forms. It is related to the modified K-Bessel function in the following way:

$$\Gamma(s)\int_{\mathbb{R}}\frac{e(\beta t)}{(1+t^2)^s}\,dt = \int_{\mathbb{R}}\int_0^\infty\left(\frac{x}{t^2+1}\right)^s e^{2\pi i\beta t}e^{-x}\,\frac{dx}{x}\,dt = \int_0^\infty x^{s-1}e^{-x}\int_{\mathbb{R}}e^{2\pi i\beta t}e^{-t^2x}\,dt\,dx$$
$$= \sqrt{\pi}\int_0^\infty x^{s-\frac{3}{2}}e^{-x}e^{-\frac{\pi^2\beta^2}{x}}\,dx.$$

When $\beta=0$ we arrive at

$$\int_{\mathbb{R}}\frac{dt}{(1+t^2)^s} = \sqrt{\pi}\frac{\Gamma(s-1/2)}{\Gamma(s)}.$$

When $\beta\neq 0$, we change variables $x=\pi|\beta|t$ obtaining

$$\int_{\mathbb{R}}\frac{e(\beta t)}{(1+t^2)^s}\,dt = \frac{\pi^s\beta^{s-1/2}}{\Gamma(s)}\int_0^\infty x^{s-3/2}e^{-\pi\beta(x+\frac{1}{x})}\,dx = 2\frac{\pi^s|\beta|^{s-1/2}}{\Gamma(s)}K_{s-1/2}(2\pi|\beta|)$$

where one can take as definition

$$K_s(z) = \frac{1}{2}\int_0^\infty x^{s-1}e^{-\frac{z}{2}(x+\frac{1}{x})}\,dx$$

for $\mathrm{Re}(z)>0$ and $s\in\mathbb{C}$. This is the modified Bessel function of the second kind of order s and argument z. Although at first we need $\mathrm{Re}(s)>\frac{1}{2}$ for the computations above to be valid, we observe that $K_s(z)$ is an entire function of s for fixed z. Also, note that

$$K_s(z) = K_{-s}(z)$$

as follows immediately from making the change of variables $x\mapsto x^{-1}$ in the integral defining $K_s(z)$. In order to perform the analytic continuation of $\mathbf{E}_{1,\chi_{-4}}(z,s)$ in the variable s we will need uniform bounds for $K_s(z)$ where $a\le\mathrm{Re}(s)\le b$ and $\mathrm{Re}(z)\ge c$. We show that there is a constant $C=C(a,b,c)$ such that

$$|K_s(z)|\le Ce^{-\mathrm{Re}(z)}$$

for all such s and z. Let $0<\epsilon<c/2$, and find C big enough such that $\max(x^{b-1},x^{-a-1})\le Ce^{\epsilon x}$ for $x\ge 1$. Then, using $x+1/x\ge 2$ for $x>0$ we obtain

$$|K_s(z)|\le\frac{1}{2}\int_1^\infty x^{b-1}e^{-\frac{\mathrm{Re}(z)}{2}(x+\frac{1}{x})}\,dx+\frac{1}{2}\int_1^\infty x^{-a-1}e^{-\frac{\mathrm{Re}(z)}{2}(x+\frac{1}{x})}\,dx$$
$$\le Ce^{-\mathrm{Re}(z)}\int_1^\infty e^{-\frac{\mathrm{Re}(z)}{2}(x+\frac{1}{x}-2)+\epsilon x}\,dx\le Ce^{-\mathrm{Re}(z)}\int_1^\infty e^{-\frac{c}{2}(x+\frac{1}{x}-2)+\epsilon x}\,dx$$
$$\le C\frac{e^{-\frac{c}{2}+\epsilon}}{c/2-\epsilon}e^{-\mathrm{Re}(z)}\le C_1e^{-\mathrm{Re}(z)}$$

as desired. Coming back to the Fourier transform of $f_{w,s}$ for $w = u + iv$, we can write

$$\widehat{f_{w,s}}(\alpha) = -2e(\alpha u)v^{-2s}\left(\frac{\pi\alpha v}{s}\frac{\pi^s|\alpha v|^{s-1/2}}{\Gamma(s)}K_{s-1/2}(2\pi|\alpha v|) + i\frac{\pi^{s+1}|\alpha v|^{s+1/2}}{\Gamma(s+1)}K_{s+1/2}(2\pi|\alpha v|)\right)$$

for $\alpha \neq 0$, and

$$\widehat{f_{w,s}}(0) = -i\sqrt{\pi}v^{-2s}\frac{\Gamma(s+1/2)}{\Gamma(s+1)}$$

for $\alpha = 0$. Applying Poisson summation formula to $f_{w,s}$ for $w = cz + 1/4$ we get

$$\begin{aligned}
&\sum_{n\in\mathbb{Z}}\frac{1}{(4cz+4n+1)|4cz+4n+1|^{2s}} \\
&= 4^{-2s-1}\sum_{n\in\mathbb{Z}}\frac{1}{(cz+1/4+n)|cz+1/4+n|^{2s}} = 4^{-2s-1}\sum_{n\in\mathbb{Z}}\widehat{f_{w,s}}(n) \\
=& -i4^{-2s-1}\sqrt{\pi}(cy)^{-2s}\frac{\Gamma(s+1/2)}{\Gamma(s+1)} - 2\cdot 4^{-2s-1}\sum_{0\neq n\in\mathbb{Z}}e(n(cx+1/4))(cy)^{-2s} \\
&\quad\times\left[i\frac{\pi ncy}{s}\frac{\pi^s|ncy|^{s-1/2}}{\Gamma(s)}K_{s-1/2}(2\pi|ncy|) + i\frac{\pi^{s+1}|ncy|^{s+1/2}}{\Gamma(s+1)}K_{s+1/2}(2\pi|ncy|)\right]
\end{aligned}$$

Similarly

$$\begin{aligned}
&\sum_{n\in\mathbb{Z}}\frac{1}{(4cz+4n+3)|4cz+4n+3|^{2s}} = 4^{-2s-1}\sum_{n\in\mathbb{Z}}\frac{1}{(cz+3/4+n)|cz+3/4+n|^{2s}} \\
&= -i4^{-2s-1}\sqrt{\pi}(cy)^{-2s}\frac{\Gamma(s+1/2)}{\Gamma(s+1)} - 2\cdot 4^{-2s-1}\sum_{0\neq n\in\mathbb{Z}}e(n(cx+3/4))(cy)^{-2s}\times \\
&\left[i\frac{\pi ncy}{s}\frac{\pi^s|ncy|^{s-1/2}}{\Gamma(s)}K_{s-1/2}(2\pi|ncy|) + i\frac{\pi^{s+1}|ncy|^{s+1/2}}{\Gamma(s+1)}K_{s+1/2}(2\pi|ncy|)\right].
\end{aligned}$$

Recalling (54), we arrive at

$$\begin{aligned}
\mathbf{E}_{1,\chi_{-4}}(z,s) = 2L(1+2s,\chi_{-4}) - 4^{-2s}\sum_{c=1}^{\infty}\sum_{0\neq n\in\mathbb{Z}}\left(e\left(\frac{n}{4}\right) - e\left(\frac{3n}{4}\right)\right)(cy)^{-2s}\times \\
\left[i\frac{\pi ncy}{s}\frac{\pi^s|ncy|^{s-1/2}}{\Gamma(s)}K_{s-1/2}(2\pi|ncy|) + i\frac{\pi^{s+1}|ncy|^{s+1/2}}{\Gamma(s+1)}K_{s+1/2}(2\pi|ncy|)\right]e(ncx).
\end{aligned}$$

Note that for fixed $y > 0$ the double series converges absolutely since $\mathrm{Re}(s) > 1/2$, and because of our bound for K_s. Writing $m = cn$ can rewrite the double sum as

$$\mathbf{E}_{1,\chi_{-4}}(z,s) = 2L(1+2s,\chi_{-4}) - 4^{-2s}y^{-2s}\sum_{0\neq m\in\mathbb{Z}}^{\infty}\sum_{c|m} c^{-2s}\left(e\left(\frac{m}{4c}\right) - e\left(\frac{3m}{4c}\right)\right)\times$$
$$\left[i\frac{\pi m y}{s}\frac{\pi^s|my|^{s-1/2}}{\Gamma(s)}K_{s-1/2}(2\pi|my|) + i\frac{\pi^{s+1}|my|^{s+1/2}}{\Gamma(s+1)}K_{s+1/2}(2\pi|my|)\right]e(mx).$$

Now, because of our bound for K_s, and the fact that $L(s,\chi_{-4})$ and $\frac{1}{s\Gamma(s)} = \frac{1}{\Gamma(s+1)}$ are entire functions, we deduce that $\mathbf{E}_{1,\chi_{-4}}(z,\cdot)$ has an analytic continuation to $\mathbb{C}$. Evaluating this continuation at $s = 0$ and using $K_{1/2}(\cdot) = K_{-1/2}(\cdot)$ we see that

$$\mathbf{E}_{1,\chi_4}(z,0) = 2L(1,\chi_{-4}) - \sum_{0\neq m\in\mathbb{Z}}^{\infty}\sum_{c|m}\left(e\left(\frac{m}{4c}\right) - e\left(\frac{3m}{4c}\right)\right)\times$$
$$\left[i\,\mathrm{sgn}(m)\pi\sqrt{|m|y}K_{1/2}(2\pi|my|) + i\pi\sqrt{|m|y}K_{1/2}(2\pi|my|)\right]e(mx) \quad (55)$$
$$= 2L(1,\chi_{-4}) - 2\pi i\sum_{m=1}^{\infty}\sum_{c|m}\left(e\left(\frac{m}{4c}\right) - e\left(\frac{3m}{4c}\right)\right)\sqrt{my}K_{1/2}(2\pi my)e(mx)$$

For holomorphicity at infinity we need to look at $K_{1/2}(2\pi my)$ more closely. Let $\mathrm{Re}(z) > 0$. Then

$$\begin{aligned}K_{1/2}(z) &= \frac{1}{2}\int_0^\infty \frac{1}{\sqrt{x}}e^{-\frac{z}{2}(x+1/x)}\,dx = \frac{e^{-z}}{2}\int_0^\infty \frac{1}{\sqrt{x}}e^{-\frac{z}{2}(\sqrt{x}-\frac{1}{\sqrt{x}})^2}\,dx\\ &= e^{-z}\int_0^\infty e^{-\frac{z}{2}(u-1/u)^2}\,du = e^{-z}\int_{\mathbb{R}}\left(\frac{1}{2}+\frac{t}{2\sqrt{t^2+4}}\right)e^{-\frac{z}{2}t^2}\,dt\\ &= e^{-z}\frac{1}{2}\frac{\sqrt{2\pi}}{\sqrt{z}}\int_{\mathbb{R}}e^{-\pi x^2}\,dx = \frac{\sqrt{\pi}}{\sqrt{2z}}e^{-z}\end{aligned}$$

where the square root is the principal branch. We have used the change of variables $u = \frac{t+\sqrt{t^2+4}}{2}$ that maps $\mathbb{R}$ bijectively onto $(0,\infty)$. Coming back to $\mathbf{E}_{1,\chi_{-4}}(z,0)$, we have

$$\begin{aligned}\mathbf{E}_{1,\chi_{-4}}(z,0) &= 2L(1,\chi_{-4}) - \pi i\sum_{m=1}^{\infty}\sum_{c|m}\left(e\left(\frac{m}{4c}\right) - e\left(\frac{3m}{4c}\right)\right)e^{-2\pi m y}e(mx)\\ &= 2L(1,\chi_{-4}) - \pi i\sum_{m=1}^{\infty}\sum_{c|m}\left(e\left(\frac{m}{4c}\right) - e\left(\frac{3m}{4c}\right)\right)e(mz).\end{aligned}$$

To evaluate the sum over divisors, observe that

$$\sum_{c|m}\left(e\left(\frac{m}{4c}\right)-e\left(\frac{3m}{4c}\right)\right)=\sum_{d|m}\left(e\left(\frac{d}{4}\right)-e\left(\frac{3d}{4}\right)\right).$$

If d is even, then expression in the bracket is 0. When $d\equiv 1 \bmod 4$, the expression is $2i$, and when $d\equiv 3 \bmod 4$, the expression is $-2i$. Therefore,

$$\mathbf{E}_{1,\chi_{-4}}(z,0)=2L(1,\chi_{-4})+2\pi\sum_{m=1}^{\infty}\left(\sum_{d|m}\chi_{-4}(d)\right)e(mz).$$

Finally, using that $L(1,\chi_{-4})=\pi/4$ we arrive at

$$\mathbf{E}_{1,\chi_{-4}}(z,0)=2\pi\left(\frac{1}{4}+\sum_{m=1}^{\infty}\left(\sum_{d|m}\chi_{-4}(d)\right)e(mz)\right)=2\pi E_{1,\chi_{-4}}(z).$$

The only thing left to prove is that $\mathbf{E}_{1,\chi_{-4}}(z,0)\in M_1(\Gamma_0(4),\chi_{-4})$. Observe that

$$\begin{aligned}\mathbf{E}_{1,\chi_{-4}}(z,s) &:= \sum_{\substack{(0,0)\neq(c,d)\in\mathbb{Z}^2\\ 4|c}}\frac{\chi_{-4}(d)}{cz+d}\cdot|cz+d|^{-2s}=\zeta(1+2s)\sum_{\substack{(c,d)=1\\ 4|c}}\frac{\chi_{-4}(d)}{cz+d}\cdot|cz+d|^{-2s}\\ &=\zeta(1+2s)\sum_{\gamma\in B\backslash\Gamma_0(4)}j_\gamma(z)^{-1}|j_\gamma(z)|^{-2s}\chi_{-4}(\gamma).\end{aligned}$$

Therefore, applying the slash operator for $\delta\in\Gamma_0(4)$

$$\begin{aligned}[\mathbf{E}_{1,\chi_{-4}}(\cdot,s)|_1\delta](z) &= \zeta(1+2s)\sum_{\gamma\in B\backslash\Gamma_0(4)}j_\delta(z)^{-1}j_\gamma(\delta z)^{-1}|j_\gamma(\delta z)|^{-2s}\chi_{-4}(\gamma)\\ &=|j_\delta(z)|^{2s}\chi_{-4}(\delta)\mathbf{E}_{1,\chi_{-4}}(z,s)\end{aligned}$$

where we have used that $\chi_{-4}=\chi_{-4}^{-1}$. The relation above holds for $\mathrm{Re}(s)>1/2$. Fixing z and $\delta\in\Gamma_0(4)$ and looking at both sides as holomorphic functions on s, by analytic continuation we get

$$[\mathbf{E}_{1,\chi_{-4}}(\cdot,0)|_1\delta](z)=\chi_{-4}(\delta)\mathbf{E}_{1,\chi_{-4}}(z,0) \tag{56}$$

and the same holds for $E_{1,\chi_{-4}}(\cdot)$. Finally, we need to show holomorphicity at all the cusps. These can be done by mimicking the proof of Theorem 2.5.6, finding the expansion at at a different cusp and performing the analytic continuation on s. However, there is a fast way of concluding from facts we have learned from the course. Recall Lemma 2.3.2, which says that if $E_{1,\chi_{-4}}(\cdot)$ is holomorphic and satisfies $[E_{1,\chi_{-4}}|\gamma]=\chi_{-4}(\gamma)E_{1,\chi_{-4}}$, then $E_{1,\chi_{-4}}(\cdot)\in M_1(\Gamma_0(4),\chi_{-4})$ if and only if $|y^{k/2}f(x+iy)|\leq C(y^A+y^{-A})$ for some $C,A>0$. Since it is holomorphic at ∞, it is clear that $|E_{1,\chi_{-4}}(z)| \le C$ for some $C > 0$ and all $\mathrm{Im}(z) \ge 1$. For $\mathrm{Im}(z) \le 1$ observe that, for any $1 > \epsilon > 0$ and $y \le 1/(2\pi)$, we have

$$\begin{aligned} 4|E_{1,\chi_{-4}}(z)| &\le 1 + 4\sum_{n=1}^{\infty} \sigma_0(n)\exp(-2\pi ny) \le 1 + C_1 \sum_{n=1}^{\infty} n^{\epsilon}\exp(-2\pi ny) \\ &\le 1 + C_1 \lceil \frac{1}{\pi y} \rceil^{1+\epsilon} + C_1(2\pi y)^{-1-\epsilon} \cdot 2\pi y \sum_{n=\lceil \frac{1}{\pi y}\rceil}^{\infty} (2\pi yn)^{\epsilon}\exp(-2\pi yn) \\ &\le 1 + C_1 \lceil \frac{1}{\pi y} \rceil^{1+\epsilon} + C_1(2\pi y)^{-1-\epsilon} \int_1^{\infty} x^{\epsilon} e^{-x}\, dx \le C(1 + y^{-1-\epsilon}) \end{aligned}$$

where we have used $\sigma_0(n) \le Cn^{\epsilon}$ for a constant depending on ϵ, and we have bounded the series by the corresponding integral, using that $x^{\epsilon}e^{-x}$ is decreasing for $x \ge \epsilon$. Therefore, $E_{1,\chi_{-4}}$ is polynomially bounded, and we conclude that it must be in $M_1(\Gamma_0(4), \chi_{-4})$, as desired. ◻

3. Intermezzo: Theta Series

We consider the following space of matrices

$$\begin{aligned} \mathcal{SP}_k = \{A \in \mathrm{Mat}_{k\times k}(\mathbb{Z}) \mid A > 0, \text{ symmetric} \\ \text{and the diagonal entries of } A \text{ are even}\}, \end{aligned}$$

where $k \in \mathbb{N}$. Given $A \in \mathcal{SP}_k$ we can write $A = B^tB$ for a real matrix B. There is a minimal $N_A \in \mathbb{N}$ such that $N_A \cdot A^{-1} \in \mathcal{SP}_k$. This integer is called the level of A. To $A \in \mathcal{SP}_k$ we can associate the quadratic form

$$Q_A(\mathbf{x}) = \frac{1}{2}\mathbf{x}^tA\mathbf{x} = \frac{1}{2}A[\mathbf{x}].$$

Let $P_l(\mathbf{x}) = P(x_1, \ldots, x_k)$ be a homogeneous polynomial of degree l. We call P_l harmonic, if

$$\Delta P_l = 0,$$

where $\Delta = \frac{\partial^2}{\partial x_1^2} + \ldots + \frac{\partial^2}{\partial x_k^2}$. We denote the space of homogeneous harmonic polynomials of degree l by $\mathcal{H}_l$. Since for $P_l \in \mathcal{H}_l$ we can write

$$P_l(\mathbf{x}) = |\mathbf{x}|^l P_l(\frac{x}{|x|})$$

it is completely determined by its values on

$$S^{k-1} = \{\mathbf{x} \in \mathbb{R}^n \colon |x| = 1\} = \mathrm{SO}(k)/\mathrm{SO}(k-1).$$

Thus $\mathcal{H}_l$ is isomorphic to

$$\mathcal{E}_l = \{P|_{S^{k-1}} \colon P \in \mathcal{H}_l\}.$$

The importance of these function spaces lies in the decomposition

$$L^2(S^{k-1}) = \overline{\bigoplus_{l\in\mathbb{N}\cup\{0\}} \mathcal{E}_l}.$$

where S^{k-1} is equipped with the rotation invariant measure

$$d\mu(\theta) = \frac{1}{2}\pi^{-\frac{k}{2}}\Gamma(\frac{k}{2}) \prod_{1\le j<k} \sin(\theta)_j^{j-1} d\theta_j$$

in coordinates

$$x_1 = \sin(\theta_{k-1})\cdots\sin(\theta_2)\sin(\theta_1),\ x_2 = \sin(\theta_{k-1})\cdots\sin(\theta_2)\cos(\theta_1),\\ \ldots, x_{k-1} = \sin(\theta_{k-1})\cos(\theta_{k-1}),\ x_k = \cos(\theta_{k-1})$$

with $0 \le \theta_1 < 2\pi$ and $0 \le \theta_j < \pi$ if $1 < j < k$. This is nothing but the spectral expansion (Friedrichs extension) of the Laplacian $\Delta_{S^{k-1}}$ acting on (smooth functions in) $L^2(S^{k-1})$. Indeed one easily checks that

$$\Delta_{S^{k-1}} P_l = -l(l+k-2)P_l \text{ for } P_l \in \mathcal{E}_l.$$

Here the $\Delta_{S^{k-1}}$ is the Laplace-Beltrami operator on the (positively curved) Riemannian manifold S^{k-1}, but for our purposes it suffices to know that it arises by writing

$$\Delta = \frac{\partial^2}{\partial r^2} + \frac{k-1}{r}\frac{\partial}{\partial r} + \frac{1}{r^2}\Delta_{S^{k-1}}$$

in polar coordinates.

Definition 3.0.1. Let $A \in \mathcal{SP}_k$, P_l be a harmonic polynomial, $z \in \mathbb{H}$ and $\mathbf{r}$ of the congruence

$$A\mathbf{r} \equiv 0 \mod N_A.$$

Then we define the (generalised) theta series

$$\theta_{P_l,Q_A}(z,\mathbf{r}) = \sum_{\mathbf{n}\in\mathbb{Z}^k} P_l\left(B(n+N^{-1}\mathbf{r})\right) e\left(\frac{1}{2}A[n+N^{-1}\mathbf{r}]z\right).$$

There are (at least) two obvious things to note:

- $\theta_{P_l,Q_A}(z,-\mathbf{r}) = (-1)^l\theta_{P_l,Q_A}(z,\mathbf{r})$; and
- $\theta_{P_l,Q_A}(z,\mathbf{r})$ depends only on $\mathbf{r}$ modulo N_A.
- $\theta_{P_l,Q_A}(z,\mathbf{r}) = N_A^{-l}\sum_{\mathbf{m}\equiv l \bmod N_A} P_l(B\mathbf{m})e(\frac{1}{2N_A^2}A[\mathbf{m}]z)$.

We are now going to study the transformation behavior under the action of $\mathrm{SL}_2(\mathbb{Z})$ on z. Recall that this group is generated by

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Lemma 3.0.1.
$$\left[\theta_{P_l,Q_A}(\cdot,\mathbf{r})|_{\frac{k}{2}+l}T\right](z) = e\left(\frac{1}{2N^2}\mathbf{r}^t A\mathbf{r}\right)\theta_{P_l,Q_A}(z,\mathbf{r}).$$

Proof. This follows directly form the definition of θ_{P_l,Q_A}. ◻

We now prove a kind of functional equation which is crucial for our further analysis.

Lemma 3.0.2. *Under current assumptions we have*

$$\sum_{\mathbf{m}\in\mathbb{Z}^k} P_l(B(\mathbf{m}+\mathbf{x}))e\left(\frac{1}{2}A[\mathbf{m}+\mathbf{x}]z\right) = \frac{i^{-l}(i/z)^{\frac{k}{2}+l}}{\sqrt{|\det(A)|}}\sum_{\mathbf{m}\in\mathbb{Z}^k} P_l(B^{-t}\mathbf{m})e\left(-\frac{1}{2z}A^{-1}[\mathbf{m}]+\mathbf{m}^t\mathbf{x}\right)$$

For $l=0$ the proof is a straight forward application of Poisson summation and the direct evaluation of the Gaussian integral. In most modern expositions one deduces the general case by applying suitable integral operators. However, we will use a proof given by Eichler in 1973.

Proof. We set
$$f(\mathbf{x}) = \sum_{\mathbf{m}\in\mathbb{Z}^k} P_l(B(\mathbf{m}+\mathbf{x}))e\left(\frac{1}{2}A[\mathbf{m}+\mathbf{x}]z\right).$$
Since the sum converges absolute and uniformly (for fixed $z\in\mathbb{H}$) f determines a continuous function with period 1 in each argument. Thus we obtain the Fourier expansion
$$f(\mathbf{x}) = \sum_{\mathbf{n}\in\mathbb{Z}^k} c_{\mathbf{n}}e(\mathbf{n}^t\mathbf{x}) \tag{57}$$
with coefficients
$$\begin{aligned} c_{\mathbf{n}} &= \int_0^1\dots\int_0^1 f(\mathbf{x})e(-\mathbf{n}^t\mathbf{x})dx_1\dots dx_k \\ &= \sum_{\mathbf{m}\in\mathbb{Z}^k}\int_0^1\dots\int_0^1 P_l(B(\mathbf{m}+\mathbf{x}))e\left(\frac{1}{2}(\mathbf{m}+\mathbf{x})^tA(\mathbf{m}+\mathbf{x})z-\mathbf{n}^t\mathbf{x}\right)dx_1\dots dx_k \\ &= \int_{\mathbb{R}}\dots\int_{\mathbb{R}} P_l(B\mathbf{x})e\left(\frac{1}{2}\mathbf{x}^tA\mathbf{x}z-\mathbf{n}^t\mathbf{x}\right)dx_1\dots dx_k. \end{aligned}$$
Since the integrand is holomorphic we can make the change of variables $\mathbf{x}-z^{-1}A^{-1}\mathbf{n}\mapsto\mathbf{x}$ and shift the contour back to the real line. Thus we obtain
$$c_{\mathbf{n}} = e(-\frac{1}{2}\mathbf{n}^tA^{-1}\mathbf{n}z^{-1})\int_{\mathbb{R}}\dots\int_{\mathbb{R}} P_l(B\mathbf{x}+z^{-1}B^{-t}\mathbf{n})e\left(\frac{1}{2}\mathbf{x}^tA\mathbf{x}z\right)dx_1\dots dx_k.$$

By holomorphicity in z it is enough to compute the integral for $z = iy$ with $y > 0$. We make the change of variables $\sqrt{y}B\mathbf{x} \mapsto \mathbf{x}$, which yields

$$c_{\mathbf{n}} = \frac{e(-\frac{1}{2}\mathbf{n}^tA^{-1}\mathbf{n}z^{-1})}{y^{\frac{k}{2}+l}\det(B)} \int_{\mathbb{R}} \cdots \int_{\mathbb{R}} P_l(\sqrt{y}\mathbf{x} - iB^{-t}\mathbf{n}) e\left(\frac{i}{2}\mathbf{x}^t\mathbf{x}\right) dx_1 \dots dx_k.$$

At this point we spectrally expand

$$P_l(\sqrt{y}\mathbf{x} - iB^{-t}\mathbf{n}) = (-i)^l P_l(B^{-t}\mathbf{n}) + \sum_{\deg(Q)>0} b_Q Q(\mathbf{x})$$

in harmonic polynomials Q, which are orthogonal with respect to integration over the unit sphere. We now switch to polar coordinates. Note that by orthogonality we have

$$\int_{S^{k-1}} Q(\mathbf{x})d\mathbf{x} = 0$$

for all Q with $\deg(Q) > 0$. We arrive at

$$c_{\mathbf{n}} = \mathrm{Vol}(S^{k-1})\frac{(-i)^l(i/z)^{\frac{k}{2}+l}}{\det(B)} e(-\frac{1}{2}\mathbf{n}^tA^{-1}\mathbf{n}z^{-1})P_l(B^{-t}\mathbf{n}) \int_0^\infty e^{-\pi r^2} r^{k-1} dr.$$

Inserting this formula for the Fourier coefficients in (57) completes the proof. ∎

Corollary 3.0.3. *We have*

$$\theta_{P_l,Q_A}(-z^{-1},\mathbf{r}) = \frac{i^{-l}(-iz)^{\frac{k}{2}+l}}{\sqrt{|\det(A)|}} \sum_{A\mathbf{l}\equiv 0 \ mod \ N_A} \psi(\mathbf{r},\mathbf{l})\theta_{P_l,Q_A}(z,\mathbf{l}),$$

for $\psi(\mathbf{r},\mathbf{l}) = e\left(\frac{\mathbf{l}^tA\mathbf{r}}{N_A^2}\right)$.

Proof. There is a one to one correspondence between $\mathbf{m} \in \mathbb{Z}^{2k}$ and $\mathbf{n} \in \mathbb{Z}^{2k}$ such that $A\mathbf{n} \equiv 0 \bmod N_A$, which is explicitly given by $\mathbf{n} = N_A A^{-1}\mathbf{m}$. Using the previous lemma with $\mathbf{x} = N_A^{-1}\mathbf{r}$ we find

$$\theta_{P_l,Q_A}(-z^{-1},\mathbf{r}) = \frac{i^k(-z)^{\frac{k}{2}+l}}{\sqrt{|\det A|}} \sum_{\substack{\mathbf{n}\in\mathbb{Z}^k,\\ A\mathbf{n}\equiv 0 \bmod N_A}} P_l(B\mathbf{n}N_A^{-1}) e\left(\frac{\mathbf{n}^tA\mathbf{n}}{2N_A^2}z + \frac{\mathbf{n}^tA\mathbf{r}}{N_A^2}\right).$$

The result follows directly from rearranging te $\mathbf{n}$-sum. ∎

Exercise 3, Sheet 6:

a) Suppose $A \in \mathcal{SP}_k$ and $A^{-1} \in \mathcal{SP}_k$. Show that k is even. (Recall that $\mathcal{SP}_k$ is the set of positive definite symmetric integral matrices with even diagonal.)
b) Show that there is $A \in \mathcal{SP}_k$ such that $\theta_{1,Q_A}(z) \in M_{\frac{k}{2}}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ if and only if $k \equiv 0 \bmod 8$.

Solution. For part a), we simply look at the trace. Let B, C be symmetric matrices. Then

$$\begin{aligned}\mathrm{Tr}(BC) &= \sum_i (BC)_i^i = \sum_i B_i^i C_i^i + \sum_{i<j} B_j^i C_i^j + \sum_{i>j} B_j^i C_i^j \\ &= \sum_i B_i^i C_i^i + \sum_{i<j} B_j^i C_i^j + \sum_{i>j} B_i^j C_j^i \\ &= \sum_i B_i^i C_i^i + 2\sum_{i<j} B_j^i C_i^j\end{aligned} \tag{58}$$

where the symmetry of B, C is used in the third equality. The last equality follows by swapping the indexes i, j. If, in addition, one of B, C has even diagonal, we deduce that $\mathrm{Tr}(BC)$ is even. Also, if $BC = \mathrm{Id}$ then $\mathrm{Tr}(BC) = k$. Therefore, if A is a symmetric matrix such that both A and A^{-1} have integer entries and one of them is in $\mathcal{SP}_k$, then k is even.

For part b), assume that there is $A \in \mathcal{SP}_k$ such that $\theta_{1,Q_A}(z) \in M_{\frac{k}{2}}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. Since θ_{tr} is a multiplier system only for even integers, this implies immediately that $k/2$ is an even integer. Also, recall Corollary 3.0.3, which states that

$$\theta_{P_l,Q_A}(-z^{-1}, \mathbf{r}) = \frac{i^{-l}(-iz)^{\frac{k}{2}+l}}{\sqrt{|\det(A)|}} \sum_{A\mathbf{l}\equiv 0 \bmod N_A} \psi(\mathbf{r}, \mathbf{l})\theta_{P_l,Q_A}(z, \mathbf{l}).$$

In our case, $l = 0$, $P_l = 1$ and $\mathbf{r} \equiv 0 \bmod N_A$, which implies $\psi(\mathbf{r}, \mathbf{l}) = 1$. Therefore, for we deduce

$$z^{k/2}\theta_{1,Q_A}(z) = [\theta_{1,Q_A}|_{\frac{k}{2}} S](-z^{-1}) = \theta_{1,Q_A}(-z^{-1}) = \frac{(-iz)^{\frac{k}{2}}}{\sqrt{\det(A)}} \sum_{A\mathbf{l}\equiv 0 \bmod N_A} \theta_{1,Q_A}(z, \mathbf{l})$$

where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and we used the hypothesis that $\theta_{1,Q_A} \in M_{\frac{k}{2}}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. Canceling the power of z,

$$\theta_{1,Q_A}(z) = \frac{(-i)^{k/2}}{\sqrt{\det(A)}} \sum_{A\mathbf{l}\equiv 0 \bmod N_A} \theta_{1,Q_A}(z, \mathbf{l}) \tag{59}$$

Recall the definition

$$\theta_{1,Q_A}(z, \mathbf{l}) = \sum_{\mathbf{n}\in\mathbb{Z}^k} e\left(\frac{1}{2}A[\mathbf{n} + N_A^{-1}\mathbf{l}]z\right)$$

and observe that, since A is positive definite, $\theta_{1,Q_A}(z, \mathbf{l})$ has a nonzero constant coefficient iff $\mathbf{l} \equiv 0 \bmod N_A$, in which case the coefficient is 1. Therefore, comparing constant coefficients in (59) we deduce

$$(-i)^{k/2} = \sqrt{\det(A)}$$

which implies $\det(A) = 1$ and $k \equiv 0 \bmod 8$.

For the other direction, note that if we are given $A_1 \in \mathcal{SP}_k$ and $A_2 \in \mathcal{SP}_l$ and we define $A_1 \oplus A_2$ by

$$A_1 \oplus A_2 = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

then $\theta_{1,Q_{A_1 \oplus A_2}}(z) = \theta_{1,Q_{A_1}}(z)\theta_{1,Q_{A_2}}(z)$. In particular, if $\theta_{1,Q_{A_1}}(z) \in M_{\frac{k}{2}}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ and $\theta_{1,Q_{A_2}}(z) \in M_{\frac{l}{2}}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$, then $\theta_{1,Q_{A_1 \oplus A_2}}(z) \in M_{\frac{k+l}{2}}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. This shows that it is enough to consider $k = 8$. Assume that we can find $A \in \mathcal{SP}_8$ with $\det(A) = 1$. Then $A\mathbf{l} \equiv 0 \bmod N_A$ if and only if $\mathbf{l} \equiv 0 \bmod N_A$ and Corollary 3.0.3 gives

$$\theta_{1,Q_A}(-z^{-1}) = z^4 \theta_{1,Q_A}(z) \quad \text{ that is } \quad [\theta_{1,Q_A}|_{12}S] = \theta_{1,Q_A}.$$

From the definition of θ_{1,Q_A} it is immediate that $\theta_{1,Q_A}(z+1) = \theta_{1,Q_A}(z)$ (see the remarks after Definition 3.0.1). Therefore, since T and S generate $\mathrm{SL}_2(\mathbb{Z})$, we deduce $\theta_{1,Q_A} \in M_4(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ in this case. An example of such a matrix is given by

$$A = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 4 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

Writing f_r for the principal minor of size $r \times r$, we have $f_1 = 2$, $f_2 = 3$, $f_3 = 4$, $f_4 = 5$, $f_5 = 6$, $f_6 = 7$ and finally $f_7 = 4f_6 - 4f_5 = 4$ and $\det(A) = f_8 = 2f_7 - f_6 = 1$. Note that all the principal minors are positive, and consequently A is positive definite. Therefore, $\theta_{1,Q_A} \in M_4(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ as desired.[20] ◻

Remark 3.0.4. Let A be a symmetric matrix of size k, with k odd. Suppose that A has integer entries, which are even on the diagonal. We claim that $\det(A)$ is even. Reducing modulo 2, $B := \overline{A}$ is an antisymmetric matrix of odd size k, that is $B^t = -B$. We need to see $\det(B) = 0$ in this case. Let X be the *generic* antisymmetric matrix of odd size k. To describe it, we introduce variables $x_{i,j}$ for every pair $1 \le i < j \le k$. Then X is the antisymmetric matrix of size k with entries in the polynomial ring $\mathbb{Z}[x_{i,j}]$, and such that the entry of X at row i and column j equals $x_{i,j}$ (for $i < j$). Since $X^t = -X$ we deduce

$$\det(X) = \det(X^t) = \det(-X) = (-1)^k \det(X) = -\det(X)$$

[20]Observe that, for such an A, necessarily $\theta_{1,Q_A} = E_4$, since $M_4(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C}E_4$.

which implies $\det(X) = 0$ (since the ring $\mathbb{Z}[x_{i,j}]$ does not have characteristic 2). Now consider the ring homomorphism $f : \mathbb{Z}[x_{i,j}] \to \mathbb{Z}/2\mathbb{Z}$ that agrees with reduction mod 2 on $\mathbb{Z}$ and sends the indeterminate $x_{i,j}$ to $B_{i,j}$, the entry at row i and column j of B. Then, since the determinant is a polynomial on the entries, $\det(B) = f(\det(X)) = 0$, as desired.

Note the following consequence of the above: if A is a symmetric matrix of even size, with integer entries which are even on the diagonal, and $|\det(A)| = 1$, then A^{-1} has even entries on the diagonal. The reason is that the entry of A^{-1} at row i and column j is given by $\det(A)^{-1}(-1)^{i+j}C_{j,i}$, where $C_{j,i}$ is the determinant of the matrix that results from A after removing row j and column i. In particular, when $i = j$ this is a symmetric matrix of odd size with even entries in the diagonal, and we can apply the paragraph above to conclude that $C_{i,i}$ is even. This can be applied to $A \in \mathcal{SP}_{8k}$ such that $\det(A) = 1$, deducing that $N_A = 1$ in this case.

Let us define
$$\mathcal{G} = \{\mathbf{r} \bmod N_A \colon A\mathbf{r} \equiv 0 \bmod N_A\}.$$

Lemma 3.0.5. *$\mathcal{G}$ is a finite abelian group with*
$$\sharp\mathcal{G} = \det(A).$$

Proof. The group structure (with respect to addition) is obvious. Further, we note that the fundamental parallelogram given by $A \cdot [0,1]^k$ has volume $\det(A)$ and has integral vertices. Thus $\sharp(A \cdot [0,1]^k \cap \mathbb{Z}^k) = \det(A)$. On the other hand we see that the matrix $N_A^{-1}A$ maps $[0,N]^k$ to $A \cdot [0,1]^k$. Furthermore vectors $\mathbf{r} \in [0,N_A]^k$ with $A\mathbf{r} \equiv 0 \bmod N_A$ are precisely those that map to integral elements of $A \cdot [0,1]^k$. Thus the count above concludes the argument. ∎

Example 3.0.6. If $A = \operatorname{diag}(a_1,\dots,a_k)$, then $\mathcal{G} = \mathbb{Z}/a_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/a_k\mathbb{Z}$.

Note that the (symmetric) bilinear form $(\mathbf{x},\mathbf{y})_A = \mathbf{x}^tA\mathbf{y}$ is non-degenerate. Therefore, every character of $\mathcal{G}$ is given by
$$\mathbf{r} \mapsto \psi(\mathbf{r},\mathbf{l}) = e(\frac{1}{N_A^2}\mathbf{l}^tA\mathbf{r})$$
for some $\mathbf{l} \in \mathcal{G}$. We have symmetry $\psi(\mathbf{r},\mathbf{l}) = \psi(\mathbf{l},\mathbf{r})$ and orthogonality
$$\sum_{\mathbf{l}\in\mathcal{G}} \psi(\mathbf{r},\mathbf{l}) = \begin{cases} \det(A) & \text{if } \mathbf{r} \equiv 0 \bmod N_A, \\ 0 & \text{else.} \end{cases}$$

We now want to compute the transformation behavior of $\theta_{P_l,Q_A}(z,\mathbf{r})$ for general $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. This is of course possible since we understand what T and S do (which generate $\mathrm{SL}_2(\mathbb{Z})$), but the computation is cumbersome to carry out in general. Suppose
$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

If $d = 0$, then $\gamma = \pm T^a S$ and everything is easy. Thus we assume $d > 0$. (If $d < 0$ we can work with $-\gamma$ instead. The computation uses a neat trick. We start by considering

$$\gamma' = \gamma S = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}.$$

Note that

$$d\gamma' z = b - (dz - c)^{-1}.$$

Thus we can write

$$\begin{aligned}
\theta_{P_l,Q_A}(\gamma' z, \mathbf{r}) &= N_A^{-l} \sum_{\mathbf{m} \equiv \mathbf{r} \bmod N_A} P_l(B\mathbf{m}) e\left(\frac{1}{2N_A^2} A[\mathbf{m}] \left(\frac{b}{d} - \frac{1}{d(dz-c)}\right)\right) \\
&= N_A^{-l} \sum_{\substack{\mathbf{g} \bmod dN_A, \\ \mathbf{g} \equiv \mathbf{r} \bmod N_A}} e\left(\frac{bA[\mathbf{g}]}{2dN_A^2}\right) \cdot \sum_{\mathbf{m} \equiv \mathbf{g} \bmod dN_A} P_l(B\mathbf{m}) e\left(\frac{dA[\mathbf{m}]}{2(dN_A)^2} \cdot \frac{-1}{dz-c}\right) \\
&= d^{\frac{l}{2}} \sum_{\substack{\mathbf{g} \bmod dN_A, \\ \mathbf{g} \equiv \mathbf{r} \bmod N_A}} e\left(\frac{bA[\mathbf{g}]}{2dN_A^2}\right) \cdot \theta_{P_l,Q_{dA}}\left(\frac{-1}{dz-c}, \mathbf{g}\right).
\end{aligned}$$

By Corollary 3.0.3 we have

$$\theta_{P_l,Q_{dA}}\left(\frac{-1}{dz-c}, \mathbf{g}\right) = d^{\frac{l}{2}} \frac{(i(c-dz))^{\frac{k}{2}+l}}{i^l \det(dA)^{\frac{1}{2}}} \sum_{\substack{\mathbf{l} \bmod dN_A, \\ A\mathbf{l} \equiv 0 \bmod N_A}} \psi(\mathbf{g}, \mathbf{l}) \theta_{P_l,Q_{dA}}(dz - c, \mathbf{l}).$$

Note that $\det(dA) = d^k \det(A)$ and $cA[\mathbf{m}] \equiv cA[\mathbf{l}] \bmod 2dN_A^2$. Thus we get

$$\theta_{P_l,Q_A}(\gamma' z, \mathbf{r}) = N_A^{-l} \frac{(i(c-dz))^{\frac{k}{2}+l}}{i^l d^{\frac{k}{2}} \det(A)^{\frac{1}{2}}} \sum_{\substack{\mathbf{l} \bmod dN_A, \\ A\mathbf{l} \equiv 0 \bmod N_A}} \varphi(\mathbf{r}, \mathbf{l}) \cdot \sum_{\mathbf{m} \equiv \mathbf{l} \bmod dN_A} P_l(B\mathbf{m}) e\left(\frac{A[\mathbf{m}]}{2N_A^2} z\right),$$

where

$$\varphi(\mathbf{r}, \mathbf{l}) = \sum_{\substack{\mathbf{g} \bmod dN_A, \\ g \equiv \mathbf{r} \bmod N_A}} e\left(\frac{bA[\mathbf{g}] + 2ad\mathbf{l}^t A\mathbf{g} + acdA[\mathbf{g}]}{2dN_A^2}\right).$$

We claim that $\varphi(\mathbf{r}, \mathbf{l})$ depends only on $\mathbf{l} \bmod N_A$ (instead of dN_A). Indeed we first change $\mathbf{g}$ to $\mathbf{g} + c\mathbf{l}$ and observe that

$$\varphi(\mathbf{r}, \mathbf{l}) = \underbrace{e\left(\frac{2a\mathbf{l}^t A\mathbf{r} - acA[\mathbf{l}]}{2N_A^2}\right)}_{e\left(-\frac{acA[\mathbf{l}]}{2N_A^2}\right)\psi(a\mathbf{r}, \mathbf{l})} \varphi(\mathbf{r} - c\mathbf{l}, 0). \tag{60}$$

Thus we can write

$$\theta_{P_l,Q_A}(\gamma' z, \mathbf{r}) = i^{-l} d^{-\frac{k}{2}} \det(A)^{-\frac{1}{2}} (i(c-dz))^{\frac{k}{2}+l} \cdot \sum_{\mathbf{h}' \in \mathcal{G}} \varphi(\mathbf{r}, \mathbf{h}') \theta_{P_l,Q_A}(z; \mathbf{h}').$$

Now we recall that $\gamma z = \gamma'(-1/z)$. Thus

$$\begin{aligned}\theta_{P_l,Q_A}(\gamma z,\mathbf{r}) &= \theta_{P_l,Q_A}(\gamma'(-1/z),\mathbf{r})\\ &= i^{-l}d^{-\frac{k}{2}}\det(A)^{-\frac{1}{2}}(\frac{i}{z}(cz+d))^{\frac{k}{2}+l}\cdot\sum_{\mathbf{h}'\in\mathcal{G}}\varphi(\mathbf{r},\mathbf{h}')\theta_{P_l,Q_A}(-\frac{1}{z};\mathbf{h}').\end{aligned}$$

We can apply Corollary 3.0.3 again to the right hand side. This gives

$$\theta_{P_l,Q_A}(\gamma z,\mathbf{r}) = i^{-2l}d^{-\frac{k}{2}}\det(A)^{-1}(cz+d)^{\frac{k}{2}+d}\cdot\sum_{\mathbf{l}\in\mathcal{G}}\Phi(\mathbf{r},\mathbf{l})\theta_{P_l,Q_A}(z;\mathbf{l}),$$

where

$$\Phi(\mathbf{r},\mathbf{l}) = \sum_{\mathbf{h}'\in\mathcal{G}}\varphi(\mathbf{r},\mathbf{h}')\cdot\psi(\mathbf{h}',\mathbf{l}).$$

Note that in order to identify the co-cycle we used that[21]

$$(\frac{i}{z}(cz+d))^{\frac{k}{2}+l}\cdot(-iz)^{\frac{k}{2}+l} = (cz+d)^{\frac{k}{2}+l}.$$

Our remaining task is to analyze $\Phi(\mathbf{r},\mathbf{l})$. To do so we assume that $N_A \mid c$ (i.e. $\gamma\in\Gamma_0(N_A)$). This allows us to conclude that for $A\mathbf{l}\equiv 0 \bmod N_A$ we have $A[\mathbf{l}]\equiv 0 \bmod 2N_A$. Inserting this in (60) we get

$$\varphi(\mathbf{r},\mathbf{l}) = \psi(a\mathbf{r},\mathbf{l})\varphi(\mathbf{r},0).$$

The point is that we can use orthogonality of characters to compute

$$\begin{aligned}\Phi(\mathbf{r},\mathbf{l}) &= \sum_{\mathbf{h}'\in\mathcal{G}}\varphi(\mathbf{r},\mathbf{h}')\cdot\psi(\mathbf{h}',\mathbf{l})\\ &= \varphi(\mathbf{r},0)\sum_{\mathbf{h}'\in\mathcal{G}}\psi(a\mathbf{r},\mathbf{h}')\cdot\psi(\mathbf{h}',\mathbf{l}) = \begin{cases}\varphi(\mathbf{r},0)\det(A) & \text{if } \mathbf{l}\equiv -a\mathbf{h} \bmod N_A,\\ 0 & \text{else.}\end{cases}\end{aligned}$$

Before we perform the last steps let us state what we are aiming to prove:

Proposition 3.0.7. *For $\gamma = \begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma_0(N_A)$ with $d>0$ and $d\equiv 1 \bmod 2$ we have*

$$\theta_{P_l,Q_a}(\gamma z,\mathbf{r}) = G(c,d)\cdot e\left(\frac{abA[\mathbf{r}]}{2N_A^2}\right)\cdot(cz+d)^{\frac{k}{2}+l}\cdot\theta_{P_l,Q_A}(z,a\cdot\mathbf{r}),$$

where

$$G(c,d) = d^{-\frac{k}{2}}\sum_{\mathbf{x} \bmod d} e\left(-2c\frac{A[\mathbf{x}]}{d}\right).$$

[21] This is checked by recalling that $d>0$ and considering the distinct cases $c<0$, $c=0$ and $c>0$.

Proof. So far we have obtained

$$\theta_{P_l,Q_A}(\gamma z,\mathbf{r}) = \varphi(\mathbf{r},0)d^{-\frac{k}{2}} \cdot (cz+d)^{\frac{k}{2}+l} \cdot \underbrace{i^{2l}\theta_{P_l,Q_A}(z,-a\mathbf{r})}_{=\theta_{P_l,Q_A}(z,a\mathbf{r})}.$$

Recall that

$$\varphi(\mathbf{r},0) = \sum_{\substack{\mathbf{g} \bmod dN_A,\\ \mathbf{g}\equiv r \bmod N_A}} e\left(\frac{bA[\mathbf{g}]}{2dN_A^2}\right).$$

Since $ad = 1+bc \equiv 1 \bmod N_A$ we can write $\mathbf{g} = ad\mathbf{r} + \mathbf{x}N_A$ for $\mathbf{x} \bmod d$. We obtain

$$\varphi(\mathbf{r},0) = e\left(\frac{a^2bdA[\mathbf{r}]}{2N_A^2}\right)\sum_{\mathbf{x} \bmod d} e(\frac{bA[\mathbf{x}]}{2d}) = e\left(\frac{abA[\mathbf{r}]}{2N_A^2}\right)\sum_{\mathbf{x} \bmod d} e(-\frac{2cA[\mathbf{x}]}{d}).$$

In the last step we have used the assumption that $d \equiv 1 \bmod 2$ in order to make the change of variables $\mathbf{x}$ to $2c\mathbf{x}$. ◻

Essentially the last task is to evaluate the Gauß sums $G(c,d)$. We first treat the one dimensional case. To do se we define the Legendre symbol by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \equiv y^2 \bmod p, \\ -1 & \text{else} \end{cases} \tag{61}$$

for odd primes p and $(n,p)=1$. This is extended to all $d \equiv 1 \bmod 2$ and $(n,d)=1$ by

$$\left(\frac{n}{d}\right) = \left(\frac{n}{p_1}\right)^{r_1}\cdots\left(\frac{n}{p_s}\right)^{r_s},$$

where $d = p_1^{r_1}\cdots p_s^{r_s}$ is the prime factorization of d. This is the Jacobi-symbol.

Lemma 3.0.8. *For $d \in \mathbb{N}$ with $d \equiv 1 \bmod 2$ and for c with $(c,d)=1$ we have*

$$g(c,d) := \sum_{x \bmod d} e(c\frac{x^2}{d}) = \left(\frac{c}{d}\right)\epsilon_d\sqrt{d},$$

where

$$\epsilon_d = \left(\frac{-1}{d}\right)^{\frac{1}{2}} = \begin{cases} 1 & \text{if } d \equiv 1 \bmod 4, \\ i & \text{if } d \equiv -1 \bmod 4. \end{cases}$$

Proof. We first execute several reduction steps.

Suppose that $d = qr^2$ where q is square-free. Then we can write $x \bmod d$ as $x = u + qrv$ where $u \bmod qr$ and $v \bmod r$. We obtain

$$g(c,d) = \sum_{u \bmod qr} e\left(\frac{cu^2}{d}\right)\sum_{v \bmod r} e\left(\frac{2cuv}{r}\right).$$

By character orthogonality we can execute the v-sum and obtain

$$g(c,d) = r \sum_{\substack{u \bmod qr,\\ u\equiv 0 \bmod r}} e\left(\frac{cu^2}{d}\right) = r\cdot g(c,q).$$

Thus we can restrict to square-free d.

For d square-free we have

$$\sharp\{x \bmod d\colon x^2 \equiv y \bmod d\} = \prod_{p\mid d}\left(1+\left(\frac{y}{p}\right)\right) = \sum_{q\mid d}\left(\frac{y}{q}\right).$$

Inserting this into the Gauß sum yields

$$g(c,d) = \sum_{q\mid d}\sum_{y \bmod d}\left(\frac{y}{q}\right) e\left(\frac{cy}{d}\right).$$

By character orthogonality the inner sum vanishes unless $q=d$. So that

$$g(c,d) = \sum_{y \bmod d}\left(\frac{y}{d}\right) e(\frac{cy}{d}) = \left(\frac{c}{d}\right) g(1,d).$$

Next suppose $d=q_1q_2$ with $(q_1,q_2)=1$ and square-free. Then, using the Chinese Remainder Theorem we can write

$$\mathbb{Z}/d\mathbb{Z} \cong \mathbb{Z}/q_1\mathbb{Z}\times\mathbb{Z}/q_2\mathbb{Z}.$$

This gives

$$g(1,d) = \sum_{x \bmod q_1}\sum_{y \bmod q_2} e(\frac{(q_2x+q_1y)^2}{d}) = g(q_2,q_1)\cdot g(q_1,q_2).$$

Note that by quadratic reciprocity we have[22]

$$\left(\frac{q_1}{q_2}\right)\left(\frac{q_2}{q_1}\right) = (-1)^{(q_1-1)(q_2-1)/4} = \frac{\epsilon_{q_1q_2}}{\epsilon_{q_1}\cdot\epsilon_{q_2}}.$$

Thus it remains to be seen that $g(1,p)=\epsilon_p\cdot\sqrt{p}$, where p is prime.[23]

We give an argument due to Schur (1921). Define the matrix

$$B = \left(e(\frac{nk}{p})\right)_{0\le n,k\le p-1}.$$

[22]Here it is important that q_1 and q_2 are both positive and odd. Note that a standard proof of this actually uses the sign of the Gauß sum that we are trying to compute. But there are other arguments, so that our proof is not cyclic. For example one can Artins general Reciprocity Theorem to derive quadratic reciprocity.

[23]To see that $|g(p,1)|=\sqrt{p}$ is relatively easy. Indeed we can simply compute

$$|g(1,p)|^2 = \sum_{x,y \bmod p} e(\frac{(x-y)(x+y)}{p}) = \sum_{x \bmod p} e(x^2/p)\sum_{y \bmod p} e(2xy/p).$$

Since p is odd the y-sum vanishes unless $x=0$. But for $x=0$ it contributes p and we are done.

Of course we have

$$\mathrm{Tr}(B) = g(1,p) = \epsilon_p \cdot \sqrt{p}.$$

And we want to determine the sign ϵ_p. By character orthogonality we compute

$$B^2 = \left(\sum_{v=0}^{p-1} e(\frac{v(n+k)}{p}) \right)_{0 \le n,k \le p-1} = \begin{pmatrix} p & 0 & \cdots & 0 \\ 0 & 0 & \cdots & p \\ \vdots & \vdots & \iddots & \vdots \\ 0 & p & \cdots & 0 \end{pmatrix}.$$

In particular $B^4 = p^2 \cdot \mathbf{1}_p$. Thus the fourth power of an eigenvalues of B must be p^2. Thus we write the eigenvalues as $\lambda_v \cdot \sqrt{p}$ with $\lambda_v^4 = 1$. Put $m_r = \sharp\{v \colon \lambda_v = i^r\}$. Then we must have

$$\epsilon_p = \lambda_0 + \cdots + \lambda_{p-1} = m_0 - m_2 + i \cdot (m_1 - m_3).$$

The eigenvalues of B^2 are $\pm p$ and it is easy to compute the dimension of the respective eigenspaces. This gives the constraints

$$m_0 + m_2 = \frac{p+1}{2} \text{ and } m_1 + m_3 = \frac{p-1}{2}.$$

Since we already know that $|\epsilon_p| = 1$ we are left with two cases. First, $m_0 = m_2$ and $m_1 - m_3 = \pm 1$. In this case it easy to see that $p \equiv -1 \bmod 4$. Second, $m_0 - m_2 = \pm 1$ and $m_1 = m_3$. In this case $p \equiv 1 \bmod 4$. So far we have seen that

$$\epsilon_p = \pm 1 \cdot \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4, \\ i & \text{if } p \equiv -1 \bmod 4. \end{cases}$$

We still have to pin down the remaining sign, which turns out to be quite complicated. We claim that $\det(B) = i^{\binom{p}{2}} p^{\frac{p}{2}}$. With this at hand we can proceed as follows. Indeed we gain the new identity

$$i^{m_1+2m_2+3m_3} p^{m_0+m_1+m_2+m_3} = \det(B) = i^{\binom{p}{2}} p^{\frac{p}{2}}.$$

Looking at the i powers we find that

$$m_1 + 2m_2 + 3m_3 \equiv 2m_2 + m_1 - m_3 \equiv \frac{p(p-1)}{2} \bmod 4$$

Suppose we have $p \equiv 1 \bmod 4$. Recall that in this case we already know that $m_0 - m_2 = \pm 1$ and $m_1 = m_3$. We compute

$$\pm 1 = m_0 - m_2 = m_0 + m_2 - 2m_2 = \frac{p+1}{2} - 2m_2 - m_1 + m_3 \equiv \frac{p+1}{2} - \frac{p(p-1)}{2} \bmod 4.$$

Since we have $p \equiv 1 \bmod 4$ we find that $\pm 1 \equiv 1 \bmod 4$. This determines the sign. The case of $p \equiv 3 \bmod 4$ is similar and we omit it.

However we should still compute the determinant. Since B is a Vandermonde matrix we have

$$\det(B) = \prod_{0\leq n<k\leq p-1} (e(\frac{k}{p}) - e(\frac{n}{p})) = \prod_{0\leq n<k\leq p-1} e(\frac{k+n}{2p})(e(\frac{k-n}{2p}) - e(-\frac{k-n}{2p}))$$
$$= i^{\binom{p}{2}} \cdot \prod_{0\leq n<k\leq p-1} e(\frac{k+n}{2p}) \cdot \prod_{0\leq n<k\leq p-1} (2\sin(\frac{\pi(k-n)}{p})).$$

The first product is easily computed to be

$$\prod_{0\leq n<k\leq p-1} e(\frac{k+n}{2p}) = i^{(p-1)^2} = 1.$$

The second product is positive. Thus we find that $\det(B) = i^{\binom{p}{2}} \cdot K$ for something positive. But we already know that $C = |\det(B)|) = p^{\frac{p}{2}}$. This concludes the proof. ⧉

We are now ready to compute the multi-dimensional version:

Lemma 3.0.9. *Suppose $d \in \mathbb{N}$ with $(d, 2c\det(A)) = 1$. Then we have*

$$G(c,d) = \left(\frac{\det(A)}{d}\right)\left(\overline{\epsilon_d}\left(\frac{2c}{d}\right)\right)^k.$$

Proof. Since d is odd we find an integral matrix V such that

$$V^tAV \equiv M \bmod d$$

for $M = \mathrm{diag}(a_1, \dots, a_k)$. (This follows from the exercise below.) Note that we still have $(\det(V), d) = 1$. At this point we change variables $\mathbf{x}$ to $V\mathbf{y}$ in the sum defining $G(c,d)$. Note that we have

$$A[\mathbf{x}] \equiv M[\mathbf{y}] \equiv \sum_{i=1}^k a_i y_i^2 \bmod d.$$

We get

$$G(c,d) = d^{-\frac{k}{2}} \prod_{i=1}^k g(-2ca_i, d).$$

We are done after inserting the evaluation of the one dimensional Gauß sums obtained above. Note that we have $m_1 \cdots m_k \equiv \det(A)\det(V)^2 \bmod d$. ⧉

Exercise 2, Sheet 6: Let $A \in \mathrm{Mat}_{k\times k}(\mathbb{Z})$ be a symmetric matrix and let d be an odd integer. Show that A can be diagonalized modulo d, i.e. there exists a matrix $M \in \mathrm{GL}_k(\mathbb{Z}/d\mathbb{Z})$ such that M^tAM is congruent to a diagonal matrix modulo d.

Solution. Write $d = \prod_p p^{i_p}$. The Chinese remainder theorem says that

$$\mathbb{Z}/d\mathbb{Z} \simeq \prod_p \mathbb{Z}/p^{i_p}\mathbb{Z}$$

From this isomorphism we obtain

$$M_k(\mathbb{Z}/d\mathbb{Z}) \simeq \prod_p M_k(\mathbb{Z}/p^{i_p}\mathbb{Z})$$

and looking at the group of units

$$\mathrm{GL}_k(\mathbb{Z}/d\mathbb{Z}) = (M_k(\mathbb{Z}/d\mathbb{Z}))^\times \simeq \prod_p \left(M_k(\mathbb{Z}/p^{i_p}\mathbb{Z})\right)^\times = \prod_p \mathrm{GL}_k(\mathbb{Z}/p^{i_p})$$

These observations reduce the problem to the case $d = p^n$ for some $n \geq 1$, so that we work with matrices in the ring $\mathbb{Z}/p^n\mathbb{Z}$. Consider a symmetric matrix $A \in M_k(\mathbb{Z}/p^n\mathbb{Z})$, which we can assume to be nonzero. Let $r := \min_{1\leq i,j\leq k}(v_p(A_{i,j}))$ be the minimal valuation of all the entries of A. If $v_p(A_{i,i}) = r$ for some $1 \leq i \leq k$, we can swap rows and columns to assume $v_p(A_{1,1}) = r$. Otherwise, after swapping some pair of rows and columns we can assume that $v_p(A_{1,j_0}) = r$ for some $j_0 \geq 2$, but that $v_p(A_{i,i}) > r$ for all $1 \leq i \leq k$. Then, letting $P = \mathrm{Id} + E_{j_0,1} \in \mathrm{SL}_k(\mathbb{Z}/p^n\mathbb{Z})$ we see that $(P^tAP)_{1,1} = A_{1,1} + 2A_{1,j_0} + A_{j_0,j_0}$, and then $v_p(A_{1,1} + 2A_{1,j_0} + A_{j_0,j_0})$[24] $= v_p(A_{1,j_0}) = \min_{1\leq i,j\leq k}(v_p(A_{i,j}))$.

Now we can assume that $v_p(A_{i,j}) \geq r = v_p(A_{1,1})$ for all $1 \leq i, j \leq r$. Therefore, for any $j \geq 2$ there exists $c_j \in \mathbb{Z}/p^k\mathbb{Z}$ such that $A_{1,j} = c_jA_{1,1}$. Considering $P = \mathrm{Id} - \sum_{j=2}^k c_jE_{1,j} \in \mathrm{SL}_k(\mathbb{Z}/p^n\mathbb{Z})$, we observe that

$$P^tAP = \begin{pmatrix} A_{1,1} & 0 \\ 0 & B \end{pmatrix}$$

for a symmetric matrix $B \in M_{k-1}(\mathbb{Z}/p^n\mathbb{Z})$. Proceeding inductively, we can find $P \in \mathrm{SL}_k(\mathbb{Z}/p^n\mathbb{Z})$ such that P^tAP is diagonal, as desired. Note that the algorithm actually gives $P^tAP = \mathrm{diag}(d_1, \dots, d_n)$ where $d_i \mid d_{i+1}$ for $1 \leq i \leq k-1$. □

Remark 3.0.10. The conclusion of the exercise does not hold if d is even. For a counterexample, we let $A \in M_k(\mathbb{Z}/d\mathbb{Z})$ be a nonzero symmetric matrix with all diagonal entries equal to 0, and the rest of the entries satisfying $2A_{i,j} = 0$ for all $1 \leq i, j \leq k$. Then, we see that

$$x^tAx = 0 \text{ for all } x \in (\mathbb{Z}/d\mathbb{Z})^k$$

As a consequence, for any $P \in \mathrm{GL}_k(\mathbb{Z}/d\mathbb{Z})$, the diagonal entries of P^tAP are all zero. If this matrix was diagonal, it would be identically zero, and then A would also be identically zero, contrary to hypothesis.

[24]We use that p is odd to guarantee that $v_p(2) = 0$.

We extend the Jacobi Symbol from $d > 0$ odd to all odd d by requiring

$$\left(\frac{c}{d}\right) = \frac{c}{|c|}\left(\frac{c}{-d}\right) \text{ if } c \neq 0.$$

We also set

$$\left(\frac{0}{d}\right) = \begin{cases} 1 & \text{if } d = \pm 1, \\ 0 & \text{else.} \end{cases}$$

We can now combine everything:

Proposition 3.0.11. *Let $A \in \mathcal{SP}_k$ and let P_l be a harmonic polynomial. Suppose that $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ with $N_A \mid c$ and $d \equiv 1 \bmod 2$. Then for any $\mathbf{r} \in \mathcal{G}$ we have*

$$[\theta_{P_l,Q_A}(\cdot, \mathbf{r})|_{\frac{k}{2}+l}\gamma](z) = e\left(\frac{abA[\mathbf{r}]}{2N_A^2}\right)\vartheta_{th}(\gamma)\theta_{P_l,Q_A}(z, a\mathbf{r}),$$

where

$$\vartheta_{th}(\gamma) = \left(\frac{\det(A)}{d}\right)\left(\overline{\epsilon_d}\left(\frac{2c}{d}\right)\right)^k.$$

Proof. The case $c = 0$ is easy. For $d > 0$ we can apply Proposition 3.0.7 together with the evaluation of the Gauß sum given in Lemma 3.0.9. The case $d < 0$ is ok due to our modification of the Jacobi symbol. ∎

Remark 3.0.12. It can be seen that the (generalized) theta functions $\theta_{P_l,Q_A}(z, \mathbf{r})$ for $\mathbf{r} \in \mathcal{G}$ are modular forms for the principal congruence subgroup

$$\Gamma(4N_A) = \ker[\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/4N_A\mathbb{Z})].$$

Indeed for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(4N_A)$ the transformation behavior simplifies to

$$[\theta_{P_l,Q_A}(\cdot, \mathbf{r})|_{\frac{k}{2}+l}\gamma](z) = \left(\frac{2c}{d}\right)^k \theta_{P_l,Q_A}(z, \mathbf{r}).$$

Furthermore these are cusp-forms as soon as P_l is not constant.

We are mostly interested in the case of $\theta_{P_l,Q_A}(z) = \theta_{P_l,Q_A}(z, \mathbf{0})$.

Theorem 3.0.13. *Let $A \in \mathcal{SP}_k$ and P_l be a harmonic polynomial. Then*

$$\theta_{P_l,Q_A}(z) \in M_{\frac{k}{2}+l}(\Gamma_0(2N_A), \vartheta_{th}).$$

If $l > 0$, then $\theta_{P_l,Q_A}(z)$ is a cusp form.

Proof. The transformation behavior follows directly from our earlier considerations. (Note that since $(d, c) = 1$ it must be odd.) It remains to check the regularity conditions at the cusps. This is done as follows. First we note that every cusp of $\Gamma_0(2N_A)$ can be translated to ∞ using a matrix in $\mathrm{SL}_2(\mathbb{Z})$. (This is different from the scaling matrix, but good enough!) However, as we have seen above acting on $\theta_{P_l,Q_A}(z)$ by an element of $\mathrm{SL}_2(\mathbb{Z})$ gives us a linear combination of the (generalized) theta functions $\theta_{P_l,Q_A}(z,\mathbf{r})$ where $\mathbf{r}$ runs through $\mathcal{G}$. Thus it suffices to check that all $\theta_{P_l,Q_A}(z,\mathbf{r})$ are holomorphic at infinity. Vanishing at the cusps is similarly easy to see when $l>0$. This is because $P_l(0)=0$ as soon as P_l is non-constant. ◻

Things simplify when k is even. Indeed in this case we have

$$\vartheta_{\mathrm{th}}(\gamma)=\chi_{D_A}(\gamma)=\left(\frac{D_A}{d}\right) \text{ with } D_A=(-1)^{\frac{k}{2}}\det(A).$$

This is simply a character.

Theorem 3.0.14. *Let $A\in\mathcal{SP}_k$ for even k and let P_l be a harmonic polynomial of even degree l. Suppose that $N_A>1$. Then*

$$\theta_{P_l,Q_A}(z)\in M_{\frac{k}{2}+l}(\Gamma_0(N_A),\chi_{D_A}).$$

Furthermore, if $l>0$, then $\theta_{P_l,Q_A}(z)$ is a cusp form.

Proof. Essentially everything is clear except for the transformation behavior in the case when

$$\gamma=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma_0(N_A)$$

with d even. If such a γ exist, then $2\nmid N_A$ and $2\nmid\det(A)$. In this case one sees that

$$D_A=(-1)^{\frac{k}{2}}\det(A)\equiv 1 \bmod 4.$$

In particular $\chi_{D_A}(d)$ depends only on d mod N_A. Thus we can do the following trick. Let

$$\gamma'=\gamma T=\begin{pmatrix} a & a+b\\ c & c+d\end{pmatrix}.$$

Our transformation law applies to this matrix. Indeed we get

$$[\theta_{P_l,Q_A}|_{\frac{k}{2}+l}\gamma](z)=[\theta_{P_l,Q_A}|_{\frac{k}{2}+l}\gamma'](z-1)=\chi_{D_A}(d+c)\theta_{P_l,Q_A}(z-1)=\chi_{D_A}(d)\theta_{P_l,Q_A}(z).$$

◻

Remark 3.0.15. Note that we can ask if the statement of the theorem above remains true when $A\in\mathcal{SP}_k$ and $\det(A)=N_A=1$. In this case k must be even and we can ask about the transformation behavior of $\theta_{P_l,Q_A}(z)$ with respect to $\mathrm{SL}_2(\mathbb{Z})$. For this we need to consider the action of matrices with vanishing lower right entry (for example S). This can be established by means of Corollary 3.0.3.

Recall that a Dirichlet character $\chi:\mathbb{Z}\to\mathbb{C}^\times$ modulo N arises as follows. We start with a character $\chi:(\mathbb{Z}/N\mathbb{Z})^\times$, also denoted by χ, in the usual sense. Then we put

$$\chi(k)=\begin{cases}\chi(k \bmod N) & \text{if } (k,N)=1,\\ 0 & \text{else.}\end{cases}$$

To a Dirichlet character modulo N we associate the Gauß sum

$$\tau(\chi) = \sum_{x \bmod N} \chi(x) e\left(\frac{x}{N}\right).$$

An example of a Dirichlet character modulo 4 is

$$\chi_{-4}(d) = \begin{cases} 1 & \text{if } d \equiv 1 \bmod 4, \\ -1 & \text{if } d \equiv 3 \bmod 4, \\ 0 & \text{if } 2 \mid d. \end{cases} \tag{62}$$

Exercise 1, Sheet 6: Let χ be a non-trivial Dirichlet character modulo p, where p is an odd prime. Write $\chi(-1) = (-1)^\rho$ for $\rho \in \{0, 1\}$ and

$$\theta_\chi(z) = \sum_{n \in \mathbb{Z}} \chi(n) n^\rho e(n^2 z)$$

a) Show that

$$\theta_\chi\left(-\frac{1}{2pz}\right) = i^{-\rho} \frac{\tau(\chi)}{\sqrt{p}} (-iz)^{\rho + \frac{1}{2}} \theta_{\chi^{-1}}\left(\frac{z}{2p}\right) \tag{63}$$

b) Find $M \in \mathbb{N}$ (depending on p) and a multiplier system ϑ such that $\theta_\chi \in M_{\rho + \frac{1}{2}}(\Gamma_0(M), \vartheta)$.

Solution. We will apply Corollary 3.0.3 with $A = 2p$, $N_A = 4p$ and $P_\rho = x^\rho$, where $\rho \in \{0, 1\}$. From Definition 3.0.1 we have

$$\begin{aligned} \theta_{x^\rho, Q_A}(z, 4k) &= \sum_{n \in \mathbb{Z}} \left(\sqrt{2p}\left(n + \frac{4k}{4p}\right)\right)^\rho e\left(\frac{1}{2} 2p \left(n + \frac{4k}{4p}\right)^2 z\right) \\ &= \left(\frac{2}{p}\right)^{\rho/2} \sum_{n \in \mathbb{Z}} (pn + k)^\rho e\left((pn + k)^2 \frac{z}{p}\right). \end{aligned}$$

It follows that

$$\theta_\chi(z) = \left(\frac{p}{2}\right)^{\rho/2} \sum_{k \bmod p} \chi(k) \theta_{x^\rho, Q_A}(pz, 4k) \tag{64}$$

Similarly, we have

$$\begin{aligned} \theta_{x^\rho, Q_A}(z, 2k) &= \sum_{n \in \mathbb{Z}} \left(\sqrt{2p}\left(n + \frac{2k}{4p}\right)\right)^\rho e\left(\frac{1}{2} 2p \left(n + \frac{2k}{4p}\right)^2 z\right) \\ &= (2p)^{-\rho/2} \sum_{n \in \mathbb{Z}} (2pn + k)^\rho e\left((2pn + k)^2 \frac{z}{4p}\right) \end{aligned}$$

and we also have the expression

$$\theta_\chi(z) = (2p)^{\rho/2} \sum_{k \bmod 2p} \chi(k) \theta_{x^\rho, Q_A}(4pz, 2k) \tag{65}$$

From Corollary 3.0.3 we obtain the identity

$$\theta_{x^\rho,Q_A}(-z^{-1},4k) = \frac{i^{-\rho}(-iz)^{\frac{1}{2}+\rho}}{\sqrt{2p}} \sum_{l \bmod 2p} e\left(\frac{4k2p2l}{16p^2}\right)\theta_{x^\rho,Q_A}(z,2l)$$
$$= \frac{i^{-\rho}(-iz)^{\frac{1}{2}+\rho}}{\sqrt{2p}} \sum_{l \bmod 2p} e\left(\frac{kl}{p}\right)\theta_{x^\rho,Q_A}(z,2l).$$

Applying the identity for any k modulo p and using the expression (64) we obtain

$$\theta_\chi\left(-\frac{1}{2pz}\right) = \left(\frac{p}{2}\right)^{\rho/2} \sum_{k \bmod p} \chi(k)\theta_{x^\rho,Q_A}\left(-\frac{1}{2z},4k\right)$$
$$= \left(\frac{p}{2}\right)^{\rho/2} \frac{i^{-\rho}(-2iz)^{\frac{1}{2}+\rho}}{\sqrt{2p}} \sum_{k \bmod p}\sum_{l \bmod 2p} \chi(k)e\left(\frac{kl}{p}\right)\theta_{x^\rho,Q_A}(2z,2l)$$
$$= \left(\frac{p}{2}\right)^{\rho/2} \frac{i^{-\rho}(-2iz)^{\frac{1}{2}+\rho}}{\sqrt{2p}} \sum_{l \bmod 2p}\left(\sum_{k \bmod p} \chi(k)e\left(\frac{kl}{p}\right)\right)\theta_{x^\rho,Q_A}(2z,2l).$$

If $(l,p)=1$, we can change variables, writing $k=\bar{l}x$ in the inner sum, to obtain

$$\sum_{k \bmod p} \chi(k)e\left(\frac{kl}{p}\right) = \chi^{-1}(l)\tau(\chi) \tag{66}$$

If p divides l the inner sum is $\sum_{k \bmod p}\chi(k)$, which equals 0 since χ is primitive. Since $\chi^{-1}(l)=0$, equation (66) also holds in this case. Thus, we arrive at

$$\theta_\chi\left(-\frac{1}{2pz}\right) = \left(\frac{p}{2}\right)^{\rho/2} \frac{i^{-\rho}(-2iz)^{\frac{1}{2}+\rho}}{\sqrt{2p}}\tau(\chi) \sum_{l \bmod 2p} \chi^{-1}(l)\theta_{x^\rho,Q_A}(2z,2l)$$
$$= \left(\frac{p}{2}\right)^{\rho/2} \frac{i^{-\rho}(-2iz)^{\frac{1}{2}+\rho}}{\sqrt{2p}}\tau(\chi)(2p)^{-\rho/2}\theta_{\chi^{-1}}\left(\frac{z}{2p}\right)$$
$$= \frac{i^{-\rho}(-iz)^{\frac{1}{2}+\rho}}{\sqrt{p}}\tau(\chi)\theta_{\chi^{-1}}\left(\frac{z}{2p}\right)$$

where we used the expression (65) for χ^{-1} in the second line. This finishes the proof of part a).

For part b) we will apply Proposition 3.0.7 using the expression (64). Let $\gamma \in \Gamma_0(4p^2)$, which we can write as $\gamma = \begin{pmatrix} a & b \\ 4p^2c & d \end{pmatrix}$. We see that

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 4p^2c & d \end{pmatrix} = \begin{pmatrix} a & pb \\ 4pc & d \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

Letting $\gamma_1 := \begin{pmatrix} a & pb \\ 4pc & d \end{pmatrix}$, and using $j_\gamma(z) = j_{\gamma_1}(pz)$ we obtain formally

$$\begin{aligned}
[\theta_{x^\rho,Q_A}(p\cdot,4k)|_{\frac{1}{2}+\rho}\gamma](z) &= j_\gamma(z)^{-\frac{1}{2}+\rho} j_{\gamma_1}(pz)^{\frac{1}{2}+\rho}[\theta_{x^\rho,Q_A}(\cdot,4k)|_{\frac{1}{2}+\rho}\gamma_1](pz) \\
&= [\theta_{x^\rho,Q_A}(\cdot,4k)|_{\frac{1}{2}+\rho}\gamma_1](pz)
\end{aligned}$$

Applying Proposition 3.0.7 to $\theta_{x^\rho,Q_A}(\cdot,4k)$ and $\gamma_1 \in \Gamma_0(4p)$ we arrive at

$$\begin{aligned}
[\theta_{x^\rho,Q_A}(p\cdot,4k)|_{\frac{1}{2}+\rho}\gamma](z) &= [\theta_{x^\rho,Q_A}(\cdot,4k)|_{\frac{1}{2}+\rho}\gamma_1](pz) \\
&= e\left(\frac{apb2p(4k)^2}{32p^2}\right)\theta_{\text{th}}(\gamma_1)\theta_{x^\rho,Q_A}(pz,4ak) \qquad (67) \\
&= \theta_{\text{th}}(\gamma_1)\theta_{x^\rho,Q_A}(pz,4ak).
\end{aligned}$$

Using expression (64) and the fact that $(a,p)=1$, we obtain

$$[\theta_\chi(\cdot)|_{\frac{1}{2}+\rho}\gamma](z) = \left(\frac{p}{2}\right)^{\rho/2} \sum_{k \bmod p} \chi(k)\theta_{\text{th}}(\gamma_1)\theta_{x^\rho,Q_A}(pz,4ak) = \theta_{\text{th}}(\gamma_1)\chi^{-1}(a)\theta_\chi(z).$$

Therefore, $\theta_\chi \in M_{\frac{1}{2}+\rho}(\Gamma_0(4p^2),\vartheta)$ where the multiplier system ϑ is defined as

$$\vartheta(\gamma) := \theta_{\text{th}}(\gamma_1)\chi^{-1}(a)$$

for $\gamma \in \Gamma_0(4p^2)$ and γ_1 and a defined as above. ◻

Remark 3.0.16. Let Q_8 be the quadratic form

$$Q_8(\mathbf{x}) = \frac{1}{2}A[\mathbf{x}] = \frac{1}{2}\sum_{r=1}^{8} x_r^2 + \frac{1}{2}\left(\sum_{r=1}^{8} x_r\right)^2 - x_1x_2 - x_2x_8.$$

Then there is a harmonic polynomial P_8 such that

$$\theta_{P_8,Q_8}(z) = \Delta(z).$$

Proof. For now take P to be some harmonic polynomial. If $\deg(P)=0$, in other words $P=c$, then

$$\theta_{P,Q_8}(z) = cE_4(z).$$

On the other hand if $\deg(P)>0$, then $\theta_{P,Q_8}(z)$ is cuspidal. In particular, if $0 < \deg(P) < 8$, then $\theta_{P,Q_8}(z) = 0$ since there are no cusp forms of the corresponding weight and level. Furthermore, if $\deg(P)=8$ then $\theta_{P,Q_8}(z) \in \mathbb{C}\Delta$. Thus it suffices to find P for which $\theta_{P,Q_8}(z) \neq 0$.

Next let us note the following triviality

$$\theta_{P,Q_8}(z) = \sum_{n\geq 0} B_P(n)e(nz) \text{ for } B_p(n) = \sum_{\substack{\mathbf{x}\in\mathbb{Z}^8,\\ Q_8(\mathbf{x})=n}} P(B\mathbf{x}).$$

This of course implies

$$\theta_{P+\tilde{P},Q_8}(z) = \theta_{P,Q_8}(z) + \theta_{\tilde{P},Q_8}(z)$$

On the other hand, our discussion above implies

$$B_p(n) = \begin{cases} 240 \cdot c \cdot \sigma_3(n) & \text{if } P = c, \\ 0 & \text{if } 1 \leq \deg(P) < 8. \end{cases}$$

We make the Ansatz

$$P_8(B\mathbf{x}) = \tilde{P}_8(u)[Q_8(\alpha) \cdot Q_8(\mathbf{x})]^4 \text{ for } u = \frac{\mathbf{x}^t A_{Q_8}\alpha}{2\sqrt{Q_8(\mathbf{x})Q_8(\alpha)}}$$

and some $\alpha \in \mathbb{Z}^8$ to be specified soon. Here $\tilde{P}_8$ is a certain even Polynomial of degree 8. We can write

$$\tilde{P}_8(u) = u^8 + \sum_{\rho=1}^{7} c_\rho H_\rho(u) - w_8,$$

for Legendre-like-Polynomials H_ρ of degree ρ.[25] Since P_8 is orthogonal to the constant function one determines $w_8 = 2^{-7}$.

Using our remarks above we compute

$$\begin{aligned} B_{P_8}(n) &= (Q_8(\alpha) \cdot n)^4 \sum_{Q_8(\mathbf{x})=n} (u^8 - w_8) \\ &= 2^{-8} \sum_{Q_8(\mathbf{x})=n} [\mathbf{x}^t A_{Q_8}\alpha]^8 - 2^{-7} \cdot 240 \cdot \sigma_3(n)(Q_8(\alpha) \cdot n)^8. \end{aligned}$$

To see that our generalised theta function does not vanish we only need to look at the first Fourier coefficient. We now choose α such that $Q_8(\alpha) = 1$. Thus we get

$$2^8 B_8(1) = \underbrace{\sum_{Q_8(\mathbf{x})=1} \left[\mathbf{x}^t A_{Q_8}\alpha\right]^8}_{\geq 2\cdot(2Q_8(\alpha))^8} - 2^5 \cdot 15 \geq 2^9 - 2^5 \cdot 15 = 2^5(16-15) = 2^5 > 0.$$

In the first step we used that the $\mathbf{x}$ sum includes $\mathbf{x} = \alpha, -\alpha$ and we drop all the rest by positivity. Thus we have seen that $B_8(1) \geq \frac{1}{8}$ which implies non-vanishing.[26] ◻

[25] If we were working in 3 variables these would really be just Legendre polynomials. However, in our case they are determined (up to constant) by their property of being polynomials of degree ρ and by the differential equation

$$(1-u^2)H_\rho'' - 7uH_\rho' + \rho(6+\rho)H_\rho = 0.$$

[26] Working more precisely one can get $B_8(1) = \frac{9}{16}$ on the nose.

4. Satz II: Quadratic Forms

In this section we illustrate basic applications of modular forms to quadratic forms via theta functions. Here we are interested in the specific case of positive definite quadratic forms with integral coefficients:

$$Q(\mathbf{x}) = \sum_{i<j} a_{ij}x_ix_j + \frac{1}{2}\sum_i a_{ii}x_i^2 = \frac{1}{2}\mathbf{x}^\top A\mathbf{x} = \frac{1}{2}A[\mathbf{x}]. \tag{68}$$

In particular A is a symmetric positive definite matrix with integral entries and even diagonal (i.e. $A \in \mathcal{SP}k$). Let k be the rank of Q (i.e. $A \in M_{k\times k}(\mathbb{Z})$). Then we are interested in studying problems surrounding the diophantine equation

$$Q(\mathbf{m}) = n \text{ for } \mathbf{m} \in \mathbb{Z}^k \text{ and } n \in \mathbb{N}.$$

For $k = 2$ this can be approached using algebraic number theory. On the other hand, if k is sufficiently large analytic tools such as the circle method turn out to be very powerful. Another possibility, which we will pursue here, relies on the modularity of theta functions.

The maybe most famous example is the proof of Jacobi's four square theorem using modular forms. Set

$$r_4(n) = \sharp\{\mathbf{x} \in \mathbb{Z}^4 \colon n = x_1^2 + x_2^2 + x_3^2 + x_4^2\}.$$

Then

$$\sum_{n\geq 0} r_4(n)e(nz) = \theta_{1,Q_A}(z),$$

where $A = \mathrm{diag}(2,2,2,2)$. In particular $N_A = 4$ so that

$$\theta_{1,Q_A}(z) \in M_2(\Gamma_0(4), \vartheta_{\mathrm{tr}}).$$

We have two candidates of modular forms in $M_2(\Gamma_0(4), \vartheta_{\mathrm{tr}})$:

$$\begin{aligned} E_{2,2}(z) &= E_2(z) - 2E_2(2z) \in M_2(\Gamma_0(2), \vartheta_{\mathrm{tr}}) \subseteq M_2(\Gamma_0(4), \vartheta_{\mathrm{tr}}) \text{ and} \\ E_{2,4}(z) &= E_2(z) - 4E_2(4z) \in M_2(\Gamma_0(4), \vartheta_{\mathrm{tr}}). \end{aligned}$$

Since we know the Fourier expansion of E_2 at ∞ (see (28)) we can write down the expansions of $E_{2,a}$ with $a = 2, 4$ at ∞:

$$E_{2,a} = (1-a) - 24\sum_{n\in\mathbb{N}} \left[\sigma_1(n) - \delta_{a|n}\cdot a\cdot\sigma_1(n/a)\right] e(nz).$$

We see that they are linearly independent so that

$$2 \leq \dim M_2(\Gamma_0(4), \vartheta_{\mathrm{tr}}).$$

We claim that the dimension actually equals 2. To show this we derive the following general result.

Lemma 4.0.1. *Suppose $\Gamma \subseteq SL_2(\mathbb{Z})$ is of finite index, then*

$$\dim M_k(\Gamma, \vartheta_{tr}) \leq \frac{k}{12} \cdot [SL_2(\mathbb{Z})\colon \Gamma] + 1.$$

Proof. We let $d = \dim M_k(\Gamma, \vartheta_{\mathrm{tr}})$. Then we observe that there is $f \in M_k(\Gamma, \vartheta_{\mathrm{tr}})$ with $m_f(\infty) \geq d-1$. (This is a problem in linear algebra, since we can build linear combinations eliminating at least the first $d-1$ Fourier coefficients.) Now write $\mu = [\mathrm{SL}_2(\mathbb{Z})\colon \Gamma]$ and find representatives

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i=1}^{\mu} \Gamma \cdot \gamma_i.$$

This allows us to construct the function

$$g(z) = \prod_{i=1}^{\mu} [f|_k\gamma_i](z) \in M_{k\cdot\mu}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}).$$

By Theorem 2.4.1 we conclude that

$$d - 1 \leq m_f(\infty) \leq m_g(\infty) \leq \frac{k\mu}{12}.$$

$\square$

Since $[\mathrm{SL}_2(\mathbb{Z})\colon \Gamma_0(4)] = 6$[27] we have $\dim M_4(\Gamma_0(4), \vartheta_{\mathrm{tr}}) \leq 2$. Thus we have seen that

$$M_4(\Gamma_0(4), \vartheta_{\mathrm{tr}}) = \mathbb{C} \cdot E_{2,2} + \mathbb{C} \cdot E_{2,4}.$$

One can even show that $S_4(\Gamma_0(4), \vartheta_{\mathrm{tr}}) = \{0\}$ (**Exercise**) but this is not relevant at the moment.

Exercise 1, Sheet 7: Show that $S_2(\Gamma_0(4), \vartheta_{\mathrm{tr}}) = 0$.

Solution. Let $f \in S_2(\Gamma_0(4), \vartheta_{\mathrm{tr}})$ and consider

$$g(z) := \prod_{\gamma \in \Gamma_0(4)\backslash \mathrm{SL}_2(\mathbb{Z})} (f|_2\gamma)(z).$$

Recall that $[\Gamma_0(4) : \mathrm{SL}_2(\mathbb{Z})] = 6$. Also, it is clear from the definitions that $[(f_1 \cdot f_2)|_{k+l}\gamma] = [f_1|_k\gamma] \cdot [f_2|_l\gamma]$ for $k, l \in \mathbb{R}$ and $\gamma \in \mathrm{SL}_2(\mathbb{R})$. Using this remark, we let $\delta \in \mathrm{SL}_2(\mathbb{Z})$ and observe that

$$g|_{12}\delta = \prod_{\gamma \in \Gamma_0(4)\backslash \mathrm{SL}_2(\mathbb{Z})} ([f|_2\gamma]|_2\delta) = \prod_{\gamma \in \Gamma_0(4)\backslash \mathrm{SL}_2(\mathbb{Z})} [f|_2\gamma\delta] = g$$

since right multiplication by δ permutes the right cosets of $\Gamma_0(4)$ in $\mathrm{SL}_2(\mathbb{Z})$. This proves that $g \in M_{12}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. Since f is a cusp form, for each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the function $f|_2\gamma$ vanishes at infinity, so in fact $g \in S_{12}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. We now show

[27] One can show by writing down general systems of representatives that $[\mathrm{SL}_2(\mathbb{Z})\colon \Gamma_0(N)] = N \cdot \prod_{p|N}(1 + p^{-1})$. This is the content of Proposition 4.1.7 below.

that $g \equiv 0$.

Given $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, recall that stabilizer of the cusp $\gamma\infty$ is $\Gamma_0(4) \cap \gamma U(\mathbb{Z})\gamma^{-1} = \gamma\left(\gamma^{-1}\Gamma_0(4)\gamma \cap U(\mathbb{Z})\right)\gamma^{-1}$. Since $\Gamma_0(4)$ contains $\Gamma(4)$, which is normal of finite index in $\mathrm{SL}_2(\mathbb{Z})$, we deduce that

$$\gamma^{-1}\Gamma_0(4)\gamma \cap U(\mathbb{Z}) = \langle T^{d_\gamma}\rangle$$

for a unique positive integer d_γ, where $T = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$. It follows that $[f|_2\gamma](z)$ has period d_γ, since $\gamma T^{d_\gamma}\gamma^{-1} \in \Gamma_0(4)$ and therefore

$$[f|_2\gamma]|_2 T^{d_\gamma} = [f|_2(\gamma T^{d_\gamma}\gamma^{-1})]|_2\gamma = f|_2\gamma.$$

Since $f|_2\gamma$ is holomorphic, zero at infinity and has period d_γ, we can write

$$[f|_2\gamma](z) = q^{d_\gamma^{-1}} h_\gamma\left(q^{d_\gamma^{-1}}\right)$$

for a holomorphic function h_γ on the unit disc, where $q := e(z)$ and $q^r := e(rz)$ for any real r. Therefore, we deduce

$$g(z) = q^{\sum_{\gamma\in\Gamma_0(4)\backslash\mathrm{SL}_2(\mathbb{Z})}\frac{1}{d_\gamma}} \prod_{\gamma\in\Gamma_0(4)\backslash\mathrm{SL}_2(\mathbb{Z})} h_\gamma(q^{\frac{1}{d_\gamma}}).$$

On the other hand, we know that $g(z)$ is holomorphic on q. After observing that all d_γ are positive and that $d_{\mathrm{Id}} = 1$ we deduce that g has a zero of order at least 2 at infinity. Since $S_{12}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ is spanned by Δ, which has a simple zero at infinity, we conclude that $g \equiv 0$. By the identity principle, we deduce that $f \equiv 0$, as desired. ◻

Remark 4.0.2. Another way to do the exercise is as follows. First, recall that

$$M_2(\Gamma_0(4), \vartheta_{\mathrm{tr}}) = \mathbb{C}E_{2,2} + \mathbb{C}E_{2,4}$$

where $E_{2,N}(z) := E_2(z) - NE_2(Nz)$. The Eisenstein series E_2 has an expansion at infinity

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)e(nz).$$

It is not a modular form, but satisfies instead

$$E_2\left(\frac{az+b}{cz+d}\right) = (cz+d)^2E_2(z) + \frac{12c}{2\pi i}(cz+d)$$

for $ad - bc = 1$, $a, b, c, d \in \mathbb{Z}$. Using this transformation law one sees that $E_{2,N} \in M_2(\Gamma_0(N), \vartheta_{\mathrm{tr}})$ and, in particular, $E_{2,2}, E_{2,4} \in M_2(\Gamma_0(4), \vartheta_{\mathrm{tr}})$. Also, we have expansions

$$E_{2,N}(z) = 1 - N - 24\sum_{n=1}^{\infty}\left(\sigma_1(n) - N\delta_{N|n}\sigma_1\left(\frac{n}{N}\right)e(nz)\right).$$

If $f \in S_2(\Gamma_0(4), \vartheta_{\mathrm{tr}})$ we can write $f = aE_{2,2} + bE_{2,4}$. Since f is cuspidal, looking at the constant coefficient in the expansion we deduce $a = -3b$. Now we look at $\mathfrak{a} = 0$, which is a cusp inequivalent to ∞. Consider $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Since $f \in S_2(\Gamma_0(4), \vartheta_{\mathrm{tr}})$, we must have $[f|_2 S](z) \to 0$ when $\mathrm{Im}(z) \to \infty$. Using the transformation behaviour for E_2, we calculate

$$\begin{aligned}[NE_2(N\cdot)|_2 S](z) &= Nz^{-2}E_2\left(-\frac{N}{z}\right) = Nz^{-2}E_2\left(\frac{-1}{\frac{z}{N}}\right) = Nz^{-2}\left(\frac{z}{N}\right)^2 E_2\left(\frac{z}{N}\right) + Nz^{-2}\frac{12}{2\pi i}\frac{z}{N} \\ &= \frac{1}{N}E_2\left(\frac{z}{N}\right) + \frac{12}{2\pi i z}.\end{aligned}$$

Therefore, we have

$$[E_{2,N}|_2 S](z) = E_2(z) - \frac{1}{N}E_2\left(\frac{z}{N}\right)$$

and we obtain

$$[f|_2 S](z) = (a+b)E_2(z) - \frac{a}{2}E_2\left(\frac{z}{2}\right) - \frac{b}{4}E_2\left(\frac{z}{4}\right).$$

Looking at the constant term of the expansion at infinity, we deduce $2a = 3b$, which together with $a = -3b$ implies $a = b = 0$, so $f \equiv 0$ as desired.

We return to studying the representation numbers of the sum of four squares. By looking at $r_4(0) = 1$ and $r_4(1) = 8$ we see that

$$\theta_{1,Q_A}(z) = -\frac{1}{3} \cdot E_{2,4}.$$

Comparing coefficients in the corresponding Fourier expansions gives the following theorem:

Theorem 4.0.3 (Jacobi's four square theorem)**.** *We have*

$$r_4(n) = \sharp\{\mathbf{x} \in \mathbb{Z}^4 \colon n = x_1^2 + \ldots + x_4^2\} = 8 \cdot [\sigma_1(n) - 4 \cdot \delta_{4|n} \cdot \sigma_1(n/4)].$$

For educational purposes we can rewrite this as follows:

$$r_4(n) = n \cdot 8\frac{2 + (-1)^n}{2^{v_2(n)}} \cdot \prod_{p \text{ odd}} \frac{1 - p^{-v_p(n)-1}}{1 - p^{-1}}.$$

We have used that $\sigma_1(mn) = \sum_{d|mn} d = \sigma_1(m)\sigma_1(n)$ for $(m,n) = 1$ and

$$\sigma_1(p^k) = p^k \sum_{s=0}^{k} p^{-s} = p^k \cdot \frac{1 - p^{-k-1}}{1 - p^{-1}}.$$

Furthermore we have written $n = \prod_p p^{v_p(n)}$, thus $v_p(n)$ (the p-adic valuation of n) is the exponent of p in the prime factor decomposition of n. After recalling that

$$\frac{\pi^2}{6} = \zeta(2) = \sum_{n \in \mathbb{N}} n^{-2} = \prod_p (1 - p^{-2})^{-1}$$

we can further write this as

$$r_4(n) = \underbrace{\pi^2 n}_{=\delta_\infty(n,A)} \cdot \underbrace{\left(\frac{2+(-1)^n}{2^{v_2(n)}}\right)}_{=\delta_2(n,A)} \cdot \prod_{p \text{ odd}} \underbrace{\frac{1-p^{-v_p(n)-1}}{1-p^{-1}}(1-p^{-2})}_{=\delta_p(n,A)}.$$

To explain this yoga we give now the proper definitions of the *local densities* $\delta_*(n,A)$ and verify that they agree with the formulae given above.

We start with $\delta_\infty(n,A)$. For general $A \in \mathcal{SP}_k$ we define

$$\delta_\infty(n,A) = \lim_{U \to \{n\}} \frac{\mathrm{Vol}(Q_A^{-1}(U))}{\mathrm{Vol}(U)},$$

where the volumes are computed with respect to the Lebesgue measure and the limit is taken over neighborhoods of $\{n\}$ in $\mathbb{R}$. Let us compute this for $A = \mathrm{diag}(2,2,2,2)$:

$$\begin{aligned}\delta_\infty(n,A) &= \lim_{\epsilon \to 0} \frac{1}{2\epsilon} \int_{\mathbb{R}^4} \mathbb{1}_{\{|\mathbf{x}|^2 - n \in (-\epsilon,\epsilon)\}}(\mathbf{x}) d\mathbf{x} \\ &= \lim_{\epsilon \to 0} \frac{1}{2\epsilon} \int_{\mathbb{R}} \int_0^\pi \int_0^\pi \int_0^{2\pi} r^3 \mathbb{1}_{\{r^2 - n \in (-\epsilon,\epsilon)\}}(r) \sin^2(\theta_1)\sin(\theta_2) d\theta_3 d\theta_2 d\theta_1 dr \\ &= \lim_{\epsilon \to 0} \frac{1}{2\epsilon} 2\pi \cdot 2 \cdot \frac{\pi}{2} \cdot \frac{1}{4}[(n+\epsilon)^2 - (n-\epsilon)^2] = \pi^2 \cdot n.\end{aligned}$$

This agrees with the factor found in the representation of $r_4(n)$ given above. The computations suggests that in general we have

$$\delta_\infty(n,A) = \frac{(2\pi)^{\frac{k}{2}}}{\Gamma(k/2)} \det(A)^{-\frac{1}{2}} n^{\frac{k}{2}-1}. \tag{69}$$

Recall that $\mathbb{Z}_p = \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$ equipped with the pro-finite topology. The quotient field $\mathbb{Q}_p$ is a locally compact field and thus features a Haar measure (with respect to addition). Thus we can define

$$\delta_p(n,A) = \lim_{U \to \{n\}} \frac{\mathrm{Vol}(Q_A^{-1}(U))}{\mathrm{Vol}(U)},$$

where U runs over a a system of neighborhoods of n in $\mathbb{Q}_p$ and the volume is taken with respect to the Haar measure. Using that $\mathrm{Vol}(p^r\mathbb{Z}_p) = p^{-r}$ and that $n + p^r\mathbb{Z}_p$ are open (compact) neighborhoods of n it is easy to see that one can rewrite this as

$$\lim_{r \to \infty} \frac{1}{p^{r(k-1)}} \sharp\{\mathbf{x} \in (\mathbb{Z}/p^r\mathbb{Z})^k \colon Q_A(\mathbf{x}) \equiv n \bmod p^r\}. \tag{70}$$

We claim that this agrees with the factors we have found for $A = \mathrm{diag}(2,2,2,2)$. Indeed for odd p we can compute

$$\begin{aligned}
&\frac{1}{p^{3r}}\sharp\{\mathbf{x}\in(\mathbb{Z}/p^r\mathbb{Z})^k\colon Q_A(\mathbf{x})\equiv n \bmod p^r\}\\
&\quad= p^{-4r}\sum_{d \bmod p^r}\ \sum_{x_1,x_2,x_3,x_4 \bmod p^r} e(\frac{d}{p^r}(x_1^2+x_2^2+x_3^2+x_4^2-n))\\
&\quad= p^{-4r}\sum_{a|p^r}\ \sum_{\substack{d \bmod p^r,\\ (p,d)=1}} e(-\frac{dn}{p^r})\left(\sum_{x \bmod p^r} e(\frac{d}{p^r}x^2)\right)^4)\\
&\quad= \sum_{a|p^r} a^{-2}\sum_{\substack{d \bmod p^r,\\ (p,d)=1}} e(-\frac{dn}{p^r}).
\end{aligned}$$

The d-sum is a so called Ramanujan sum. It evaluates to

$$\sum_{\substack{d \bmod p^r,\\ (p,d)=1}} e(-\frac{dn}{p^r}) = \sum_{b|(n,a)} b\cdot\mu(a/b).$$

where μ is the Möbius function. Recall that the Möbius function is multiplicative and satisfies

$$\mu(p^s)=\begin{cases}1 & \text{if } s=0,\\ -1 & \text{if } s=1,\\ 0 & \text{else.}\end{cases}$$

on prime powers. In total we have

$$\frac{1}{p^{3r}}\sharp\{\mathbf{x}\in(\mathbb{Z}/p^r\mathbb{Z})^k\colon Q_A(\mathbf{x})\equiv n \bmod p^r\} = \sum_{a|p^r} a^{-2}\sum_{b|(n,a)} b\cdot\mu(a/b).$$

If $(n,p)=1$ it is straight forward that this evaluates to

$$\frac{1}{p^{3r}}\sharp\{\mathbf{x}\in(\mathbb{Z}/p^r\mathbb{Z})^k\colon Q_A(\mathbf{x})\equiv n \bmod p^r\} = (1-p^{-2})$$

for all $r\geq 1$. If $(n,p)>1$, then we suppose that $r\geq v_p(n)+1$. In this case we get

$$\begin{aligned}
\frac{1}{p^{3r}}\sharp\{\mathbf{x}\in(\mathbb{Z}/p^r\mathbb{Z})^k\colon Q_A(\mathbf{x})\equiv n \bmod p^r\} &= 1+\sum_{s=1}^{v_p(n)} p^{-2s}(p^s-p^{s-1}) - p^{-v_p(n)-2}\\
&= 1+p^{-1}-p^{-v_p(n)-1}-p^{-v_p(n)-2}\\
&= (1-p^{-v_p(n)-1})(1+p^{-1})\\
&= \frac{1-p^{-v_p(n)-1}}{1-p^{-1}}(1-p^{-2}).
\end{aligned}$$

Thus we have interpreted Jacobi's formula for $r_4(n)$ as a product of local density which can be *defined* as local volumes.

- The product $\prod_p \delta_p(n, A)$ converges absolutely as soon as $k \geq 4$. The situation for $k = 2, 3$ is more tricky.
- For general integral quadratic forms $Q = Q_A$ one would hope for an asymptotic

$$r_Q(n) = \delta_\infty(n, A) \cdot \prod_p \delta_p(n, A) \cdot (1 + o_Q(1))$$

  to hold. Under favorable circumstances this can be shown using the circle method and furnishes a local to global principle.

In the next subsection we will see what can be said in general. But before we include a elementary proof of Lagrange's four square theorem as an exercise.

Exercise 1, Sheet 1: The goal of this exercise is to give an elementary proof of Lagrange's four square theorem:

a) Show that for every $p > 2$ there is $1 \leq m < p$ so that

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

with $x_1, x_2, x_3, x_4 \in \mathbb{Z}_{\geq 0}$.

b) Show that every prime p is representable as a sum of four squares (of non-negative integers).

c) Show that every integer n can be written as a sum of four squares of non-negative integers.

Solution. For part a), note that the subsets of $\mathbb{Z}_p$ defined by $A := \{x^2 \mid x \in \mathbb{Z}_p\}$ and $B := \{1-y^2 \mid y \in \mathbb{Z}_p\}$ have both cardinality $\frac{p+1}{2}$, and therefore must intersect. Thus $x^2 = -1 - y^2 \mod p$ has a solution. By modifying $x \mapsto -x$ and/or $y \mapsto -y$ if necessary, we can choose representatives with $0 \leq x, y \leq \frac{p-1}{2}$. Therefore

$$x^2 + y^2 + 1 = mp \quad \text{with} \quad 1 \leq m \leq \frac{p-1}{2}$$

For part b) the classical argument by descent runs as follows. For a prime $p > 2$ as above let $m \geq 1$ be the smallest positive integer such that mp is a sum of four squares. By part a) we know $1 \leq m_p \leq \frac{p-1}{2}$. The goal is to show $m = 1$. For the sake of contradiction, suppose that $m > 1$ and consider the integers y_i congruent to x_i modulo m and such that $(1-m)/2 \leq y_i \leq m/2$. We have

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mr$$

for a certain $0 \leq r \leq m$. If $r = 0$, then all x_i are divisible by m, which contradicts $\sum x_i^2 = mp$ with p a prime strictly greater than m. Similarly, if $r = m$ then

$y_i = m/2$ for all i which gives $x_i = \frac{m}{2}(2t_i+1)$ for some $t_i \geq 0$ and therefore

$$mp = x_1^2+x_2^2+x_3^2+x_4^2 = m^2\frac{(2t_1+1)^2+(2t_2+1)^2+(2t_3+1)^2+(2t_4+1)^2}{4} = m^2k$$

for some $k \geq 0$. In this case $m \mid p$ again, which is a contradiction to $m > 1$ and $p > m$ prime. Therefore, we must have $1 \leq r \leq m-1$. Now we use the Euler identity

$$\begin{aligned} pm^2r &= (x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) \\ &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 + (x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 \\ &+ (x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2 + (x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2 \\ &=: z_1^2+z_2^2+z_3^2+z_4^2. \end{aligned}$$

By the choice of y_i it is clear that each z_2, z_3, z_4 are divisible by m. To see that m also divides z_1 note that

$$z_1 \equiv x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 \mod m$$

by hypothesis. Therefore, considering $z_i' = z_i/m$ we find an expression for pr as a sum of four squares. As $1 \leq r < m$, we have a contradiction to the minimality of m.

For part c) we simply express n as a product of primes and use part b) and the Euler identity inductively. ∎

Exercise 3, Sheet 7: Let

$$r_2(n) = \#\{x_1, x_2 \in \mathbb{Z} : n = x_1^2 + x_2^2\}.$$

Use the fact

$$E_{1,\chi_{-4}}(z) := \frac{1}{4} + \sum_{n=1}^{\infty}\left(\sum_{d\mid n}\chi_{-4}(d)\right)e(nz) \in M_1(\Gamma_0(4), \chi_{-4})$$

from (52) to show that

$$r_2(n) = 4\left(\sum_{\substack{d\mid n \\ d\equiv 1 \bmod 4}} 1 - \sum_{\substack{d\mid n \\ d\equiv 3 \bmod 4}} 1\right).$$

Solution. Consider the quadratic form Q_A associated to $A := \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ and form the theta function

$$\theta_{1,Q_A}(z) = \sum_{\mathbf{n}\in\mathbb{Z}^2} e\left(\frac{1}{2}A[\mathbf{n}]z\right) = \sum_{n\geq 0} r_2(n)e(nz)$$

where the second equality follows from the definitions of A and $r_2(\cdot)$. Clearly $A \in \mathcal{SP}_k$ and $4A^{-1} \in \mathcal{SP}_k$. Therefore, we can apply Theorem 3.0.14, with $k = 2$

and $N_A = 4$, to deduce that $\theta_{1,Q_A} \in M_1(\Gamma_0(4), \chi_{D_A})$. Here $D_A = -\det(A) = -4$ and

$$\chi_{D_A}(\gamma) = \left(\frac{-4}{d}\right) = \chi_{-4}(d)$$

where $\gamma = \left(\begin{smallmatrix} a & b \\ 4c & d \end{smallmatrix}\right) \in \Gamma_0(4)$. Since $r_2(0) = 1$, we observe that

$$g(z) := \theta_{1,Q_A}(z) - 4E_{1,\chi_{-4}}(z) \in M_1(\Gamma_0(4), \chi_{-4})$$

with a zero at ∞. Since χ_{-4} is a quadratic character, we see

$$g(z)^2 \in M_2(\Gamma_0(4), \theta_{\mathrm{tr}})$$

with a zero at ∞ of order at least 2. Proceeding as in exercise 1 we can consider

$$h(z) := \prod_{\gamma \in \Gamma_0(4) \backslash \mathrm{SL}_2(\mathbb{Z})} [g^2|_2\gamma] \in M_{12}(\mathrm{SL}_2(\mathbb{Z}))$$

It follows that h has a zero of order at least 2 at ∞. Since $S_{12}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ is spanned by Δ, with a zero of order 1 at ∞, we deduce that $h \equiv 0$. By the identity principle this implies $g \equiv 0$. That is,

$$\sum_{n \geq 0} r_2(n) e(nz) = 1 + 4 \sum_{n=1}^{\infty} \left(\sum_{d|n} \chi_{-4}(d) \right) e(nz).$$

Comparing coefficients and using the definition of $\chi_{-4}(\cdot)$, we are done. ◻

Bonus Exercise: Prove the following formula

$$r_8(m) := |\{(n_1, \ldots, n_8) \in \mathbb{Z}^8 : n_1^2 + \ldots + n_8^2 = m\}| = 16 \sum_{d|m} (-1)^{m-d} d^3 \tag{71}$$

Solution. Letting $A_8 := \mathrm{diag}(2,2,2,2,2,2,2,2)$, we recognize

$$\theta_{1,Q_8}(z) := \sum_{\mathbf{n} \in \mathbb{Z}^8} e\left(\frac{1}{2} A_8[\mathbf{n}] z\right) = \sum_{m \geq 0} r_8(m) e(mz)$$

Also, recall that $\theta(z) := \sum_{n \in \mathbb{Z}} e(n^2 z) \in M_{\frac{1}{2}}(\Gamma_0(4), \vartheta_{\mathrm{th}})$, where ϑ_{th} is a multiplier that takes values in μ_4, the group of roots of unity of order dividing 4. Therefore, $\vartheta_{\mathrm{th}}^4 = \vartheta_{\mathrm{tr}}$. Since we recognize that

$$\theta_{1,Q_8} = \theta^8$$

we deduce that $\theta_{1,Q_8} \in M_4(\Gamma_0(4), \vartheta_{\mathrm{tr}})$. Let $E_4 \in M_4(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ be the usual Eisenstein series of weight 4 for $\mathrm{SL}_2(\mathbb{Z})$. We claim that

$$M_4(\Gamma_0(4), \vartheta_{\mathrm{tr}}) = \mathbb{C}E_4 \oplus \mathbb{C}E_4(2\cdot) \oplus \mathbb{C}E_4(4\cdot).$$

Since $E_4(2\cdot) = \iota_{1,2}(E_4)$ and $E_4(4\cdot) = \iota_{1,4}(E_4)$, we know that these are modular forms of weight 4 for $\Gamma_0(4)$. Looking at the Fourier expansion at ∞ we see

$$E_4(z) = 1 + 240\sum_{m=1}^{\infty}\sigma_3(m)e(mz)$$
$$E_4(2z) = 1 + 240\sum_{m=1}^{\infty}\delta_{2|m}\sigma_3\left(\frac{m}{2}\right)e(mz)$$
$$E_4(4z) = 1 + 240\sum_{m=1}^{\infty}\delta_{4|m}\sigma_3\left(\frac{m}{4}\right)e(mz).$$

Therefore, if $f = aE_4 + bE_4(2\cdot) + cE_4(4\cdot)$, we have, for $m \geq 1$

$$a_f(m;\infty) = 240\left(a\sigma_3(m) + b\delta_{2|m}\sigma_3\left(\frac{m}{2}\right) + c\delta_{4|m}\sigma_3\left(\frac{m}{4}\right)\right).$$

In particular, if $f = 0$, taking $m = 1$ we deduce $a = 0$, then taking $m = 2$ we deduce $b = 0$, and finally taking $m = 4$ we see $c = 0$. Therefore, the modular forms $E_4, E_4(2\cdot)$ and $E_4(4\cdot)$ are linearly independent. On the other hand, recall from Lemma 4.0.1 that for a finite index subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ we have

$$\dim M_k(\Gamma, \vartheta_{\mathrm{tr}}) \leq \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] + 1.$$

In our case, $k = 4$ and $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(4)] = 6$. Therefore, we deduce $\dim M_4(\Gamma_0(4), \vartheta_{\mathrm{tr}}) \leq 3$. Together with the paragraph above we arrive at the conclusion that

$$M_4(\Gamma_0(4), \vartheta_{\mathrm{tr}}) = \mathbb{C}E_4 \oplus \mathbb{C}E_4(2\cdot) \oplus \mathbb{C}E_4(4\cdot) \tag{72}$$

In particular, there exist unique $a, b, c \in \mathbb{C}$ such that $\theta_{1,Q_8} = aE_4 + bE_4(2\cdot) + cE_4(4\cdot)$. Looking at (72) and taking $m = 1$ and $m = 2$, together with the equation for the constant coefficient, we arrive at the following system

$$a + b + c = 1$$
$$240a = r_8(1)$$
$$240\sigma_3(2)a + 240b = r_8(2).$$

Since $r_8(1) = 16$ and $r_8(2) = 4\binom{8}{2} = 112$, we deduce

$$a = \frac{1}{15}, \quad b = -\frac{2}{15}, \quad c = \frac{16}{15}.$$

Since $240 = 15 \cdot 16$, we see from (72) that

$$r_8(m) = 16\left(\sigma_3(m) - 2\delta_{2|m}\sigma_3\left(\frac{m}{2}\right) + 16\delta_{4|m}\sigma_3\left(\frac{m}{4}\right)\right)$$

If m is odd, this agrees with (71). If $m = 2^k m_0$ with m_0 odd and $k \geq 1$, we need to prove

$$r_8(m) = 16\left(\sum_{\substack{d|m \\ d \text{ even}}} d^3 - \sum_{\substack{d|m \\ d \text{ odd}}} d^3\right) = 16(-1+\sum_{r=1}^{k} 2^{3r}) \sum_{d|m_0} d^3 = 16(-1+\sum_{r=1}^{k} 2^{3r})\sigma_3(m_0)$$

When $k = 1$, we know that

$$r_8(m) = 16(\sigma_3(m) - 2\sigma_3(m_0)) = 16(\sigma_3(2)\sigma_3(m_0) - 2\sigma_3(m_0)) = 16(-1+8)\sigma_3(m_0)$$

as desired, where we use that $\sigma_3(m_1m_2) = \sigma_3(m_1)\sigma_3(m_2)$ when $(m_1, m_2) = 1$ and that $\sigma_3(2) = 9$. When $k \geq 2$, we have

$$\begin{aligned}
r_8(m) &= 16(\sigma_3(2^k m_0) - 2\sigma_3(2^{k-1}m_0) + 16\sigma_3(2^{k-2}m_0)) \\
&= 16(1 + \sum_{r=1}^{k} 2^{3r} - 2\sum_{r=0}^{k-1} 2^{3r} + 2^4 \sum_{r=0}^{k-2} 2^{3r})\sigma_3(m_0) \\
&= 16(1 + \sum_{r=1}^{k} 2^{3r} - 2 - \sum_{r=1}^{k-1} 2^{3r+1} + \sum_{r=1}^{k-1} 2^{3r+1})\sigma_3(m_0) \\
&= 16(-1 + \sum_{r=1}^{k} 2^{3r})\sigma_3(m_0)
\end{aligned}$$

as desired. ◻

4.1. **The General Theory of Quadratic Forms.** We start by develop some of the general theory of quadratic forms. Throughout let Q be a positive definite quadratic form with integral coefficients of rank k. We associate the matrix A as in (68).

Definition 4.1.1. We define the discriminant of Q by

$$D = \begin{cases} (-1)^{\frac{k}{2}} \det(A) & \text{if } k \text{ is even,} \\ \frac{(-1)^{\frac{k+1}{2}}}{2} \det(A) & \text{if } k \text{ is odd.} \end{cases}$$

Remark 4.1.1. This makes sense because for A as above show that

$$\det(A) \equiv \begin{cases} (-1)^{\frac{k}{2}} \bmod 4 & \text{if } k \text{ is even,} \\ 0 \bmod 2 & \text{if } k \text{ is odd.} \end{cases}$$

Exercise 2, Sheet 7: Let $A \in \mathcal{SP}_k$, and let N_A denote the level of A (i.e. the smallest positive integer N such that $N \cdot A^{-1} \in \mathcal{SP}_k$).

a) Show that if a prime p divides $\det(A)$, then p divides N_A.

Now suppose that k is even and assume that $2 \nmid \det(A)$.

b) Show that $(-1)^{k/2} \det(A) \equiv 1 \bmod 4$.

c) Conclude that $\chi_{D_A}(d) = \left(\frac{(-1)^{k/2}\det(A)}{d}\right)$ depends only on d modulo N_A.

Solution. For part a), suppose that p does not divide N_A. Denote by $\overline{B}$ the reduction of the matrix B modulo p. Then A and $N_A \cdot A^{-1}$ are two matrices with integer entries such that $\overline{A} \cdot \overline{N_A \cdot A^{-1}} = N_A \cdot \mathrm{Id}$, which is invertible modulo p. Therefore, $\overline{A}$ is a unit in $M_{k\times k}(\mathbb{Z}/p\mathbb{Z})$ which implies that $\det(\overline{A}) = \overline{\det(A)}$ is a unit in $\mathbb{Z}/p\mathbb{Z}$. Equivalently, p does not divide $\det(A)$.

Now suppose that k is even and that $\det(A)$ is not divisible by 2. We will work modulo 4. Since the entries of A are integers, and the entries in the diagonal are even, there must be an index $2 \le j \le k$ such that a_j^1 is odd (otherwise $\det(A)$ would be even). Interchanging rows and columns 2 and j (this corresponds to multiplying A by a transposition matrix on both the left and the right, which does not change the determinant), we can assume that a_2^1 is odd. We can write

$$\overline{A} = \begin{pmatrix} P & X \\ X^t & Q \end{pmatrix} \quad P = \begin{pmatrix} 2a & b \\ b & 2a \end{pmatrix} \quad X \in M_{2\times(k-2)}(\mathbb{Z}/4\mathbb{Z}),\ Q \in M_{(k-2)\times(k-2)}(\mathbb{Z}/4\mathbb{Z})$$

and the diagonal entries of Q are even. Since b is odd, we see that $\det(A) = -1 \bmod 4$. In particular it is invertible. It is easy to see that

$$\begin{pmatrix} P & X \\ X^t & Q \end{pmatrix} = \begin{pmatrix} I & 0 \\ X^tP^{-1} & I \end{pmatrix}\begin{pmatrix} P & 0 \\ 0 & Q - X^tP^{-1}X \end{pmatrix}\begin{pmatrix} I & P^{-1}X \\ 0 & I \end{pmatrix}$$

Since P^{-1} has even entries in the diagonal, we deduce the same thing for the $(k-2)\times(k-2)$ symmetric matrix $X^tP^{-1}X$, and therefore also for $Q - X^tP^{-1}X$. Clearly $\overline{\det(A)} = \det(P)\det(Q - X^tP^{-1}X)$. Since $\det(P) = -1 \bmod 4$, we can proceed inductively with $Q - X^tP^{-1}X$ to deduce $(-1)^{k/2}\det(A) \equiv 1 \bmod 4$, as desired.

For part c), assume that d is odd. Write $d = (-1)^\epsilon \prod_p p^{i_p}$ and $\det(A) = \prod_q q^{j_q}$, where the primes are all odd. Using the definitions and the law of quadratic reciprocity we calculate

$$\left(\frac{(-1)^{k/2}\det(A)}{d}\right) = (-1)^{\frac{k}{2}\epsilon}\left(\frac{(-1)^{k/2}\det(A)}{|d|}\right) = (-1)^{\frac{k}{2}\epsilon}\prod_p \left(\frac{(-1)^{k/2}\det(A)}{p}\right)^{i_p}$$

$$= (-1)^{\frac{k}{2}\epsilon}\prod_p (-1)^{\frac{k}{2}\frac{(p-1)i_p}{2}}\prod_{p,q}\left(\frac{q}{p}\right)^{i_pj_q} = (-1)^{\frac{k}{2}\epsilon}(-1)^{\frac{k}{2}\sum_p \frac{p-1}{2}i_p}\prod_{p,q}\left(\frac{p}{q}\right)^{i_pj_q}\prod_{p,q}(-1)^{i_pj_q\frac{(p-1)(q-1)}{4}}$$

$$= (-1)^{\frac{k}{2}\epsilon}(-1)^{\left(\sum_p \frac{p-1}{2}i_p\right)\cdot\left(\frac{k}{2}+\sum_q \frac{q-1}{2}j_q\right)}\left(\frac{|d|}{\det(A)}\right) = (-1)^{\frac{k}{2}\epsilon}\left(\frac{|d|}{\det(A)}\right)$$

$$= \left(\frac{(-1)^\epsilon}{\det(A)}\right)\left(\frac{|d|}{\det(A)}\right) = \left(\frac{d}{\det(A)}\right) = \prod_q \left(\frac{d}{q}\right)^{j_q}.$$

In the fifth equality we use that $(-1)^{k/2}\det(A) \equiv 1 \bmod 4$ to deduce that $k/2 + \sum_q \frac{q-1}{2} j_q$ is even. Since the last expression only depends on d modulo primes that divide $\det(A)$, and since every such prime divides N_A by part (a), we deduce that $\chi_{D_A}(d)$ only depends on d modulo N_A, as desired. ⊡

Remark 4.1.2. There is another way to prove part a) which gives a bit more information. Let $N_A = p^u n$ and $\det(A) = p^v m$ where $(nm, p) = 1$. Let $\operatorname{adj}(A)$ be the adjugate matrix to A, so that $A \operatorname{adj}(A) = \det(A) I_k$ holds. Then,

$$N_A A^{-1} = \frac{N_A}{\det(A)} \operatorname{adj}(A) = p^{u-v} \frac{n_0}{m_0} \operatorname{adj}(A) \in M_k(\mathbb{Z}).$$

We deduce that the p-valuation of each entry of $\operatorname{adj}(A)$ is at least $v-u$. Therefore

$$v_p(\det(\operatorname{adj}(A))) \geq k(v-u).$$

On the other hand, from $A \operatorname{adj}(A) = \det(A) I_k$ it follows that $\det(\operatorname{adj}(A)) = \det(A)^{k-1}$. We arrive at

$$(k-1)v \geq k(v-u), \quad \text{equivalently,} \quad v \leq ku.$$

Therefore, if $v > 0$ we must have $u > 0$, as desired.

Definition 4.1.2. Two quadratic forms Q_1 and Q_2 (of equal rank) are equivalent (over $\mathbb{Z}$) if there is $U \in \mathrm{GL}_k(\mathbb{Z})$ such that

$$A_1 = U^\top A_2 U.$$

Remark 4.1.3. We can view Q as above as a quadratic form over any ring R containing $\mathbb{Z}$. Equivalence over R is then defined by the obvious modification of the definition above.

Definition 4.1.3. The group of automorphs of Q is defined by

$$O(Q) = \{U \in M_k(\mathbb{Z}) \colon U^\top A U = A\}.$$

This is a finite group and we write $\sharp O(Q) = o(Q)$.

The numbers D and $o(Q)$ are invariants of classes of equivalent forms. We write

$$r(n, Q) = \sharp\{\mathbf{m} \in \mathbb{Z}^r \colon Q(\mathbf{m}) = n\}$$

for the representation number of n by Q. (Since Q is assumed to be positive definite this is a finite number.)

Definition 4.1.4. Two positive definite integral quadratic forms Q_1 and Q_2 are said to be in the same genus (i.e. $Q_2 \in \operatorname{gen}(Q_1)$ or $Q_1 \in \operatorname{gen}(Q_2)$) if they are equivalent over $\mathbb{Z}_p$ for all primes p.

Remark 4.1.4. Note that since both Q_1 and Q_2 are positive definite they are automatically equivalent over $\mathbb{R}$.

Exercise 1, Sheet 8: Give an example of two integral quadratic forms that lie in the same genus but not in the same equivalence class (over $\mathbb{Z}$). Both assertions should be proved.

Solution. We will prove that setting

$$A_1 = \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 1 & 0 \\ 0 & pq \end{pmatrix}$$

for distinct odd primes p, q the matrices are in the same genus iff p is a square modulo q and q is a square modulo p. By quadratic reciprocity, this implies that one of them is congruent to 1 modulo 4. First of all, it is evident that the quadratic forms are not equivalent over $\mathbb{Z}$, since A_2 represents 1 but A_1 does not (using positivity of x^2). To see that they are in the same genus, we recall the following version of Hensel's lemma:

Proposition 4.1.5. *Let r be a prime (including $r = 2$) and let $f(X) \in \mathbb{Z}_r[X]$ be a polynomial with p-adic integers as coefficients. Suppose that there is $x_0 \in \mathbb{Z}_r$ such that $v_r(f(x_0)) > 2v_r(f'(x_0))$. Then, there is $x \in \mathbb{Z}_r$ with $f(x) = 0$ and $v_r(x - x_0) \geq v_r(f(x_0)) - v_r(f'(x_0))$.*

Proof. See Serre's *A course in arithmetic*, page 14. ∎

Now consider an odd prime r distinct from p and q. We assert that equation $pX^2 + qY^2 = 1$ has non-trivial solution mod r. Indeed, considering the two sets $A := \{1 - px^2 \mid x \in \mathbb{Z}/r\mathbb{Z}\}$ and $B := \{qy^2 \mid y \in \mathbb{Z}/r\mathbb{Z}\}$, they have cardinality $(r + 1)/2$, so they must intersect. Lifting to $\mathbb{Z}_r$ that means there are $x_0, y_0 \in \mathbb{Z}_r$ such that $px_0^2 + qy_0^2 = 1 \bmod r$. One of x_0, y_0 has to be a unit, say x_0. Then, considering $f(X) := pX^2 + qy_0^2 - 1$, we have $f(x_0) = 0 \bmod r$ and $f'(x_0) = 2px_0^2$ is a unit. We can apply Hensel's lemma and find $x \in Z_p$ and $y = y_0$ such that $px^2 + qy^2 = 1$. It is an easy matter to check that, for $P = \begin{pmatrix} x & -qy \\ y & px \end{pmatrix}$ we have $\det(P) = 1$ and

$$P^t A_1 P = \begin{pmatrix} x & y \\ -qy & px \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix} \begin{pmatrix} x & -qy \\ y & px \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & pq \end{pmatrix}$$

So far, no conditions on p and q were needed. Now let's see what happens at $\mathbb{Z}_p$. For A_1 and A_2 to be equivalent over $\mathbb{Z}_p$, in particular they need to represent the same numbers. For A_1 to represent 1, we need there needs to exist a solution to $pX^2 + qY^2 = 1$ in $\mathbb{Z}_p$. Reducing modulo p, it is necessary that q is a square modulo p. This condition is also sufficient, since then the polynomial $f(Y) := qY^2 - 1$ has a solution y_0 modulo p with $f'(y_0) = 2qy_0 \in \mathbb{Z}_p^\times$, so that a true zero $y \in \mathbb{Z}_p^\times$ exists. That is, $y^2 = q^{-1}$. As before, considering $P = \begin{pmatrix} 0 & -y^{-1} \\ y & 0 \end{pmatrix}$ we find $P^t A_1 P = A_2$. The same argument works over $\mathbb{Z}_q$. In particular, for A_1 and A_2 to be equivalent over both $\mathbb{Z}_p$ and $\mathbb{Z}_q$ it is necessary and sufficient that p is a square mod q and vice versa. By quadratic reciprocity, at least one of the primes will have to be congruent to 1 mod 4.

Suppose that $q \equiv 1$ modulo 4. As before, for A_1 and A_2 to be equivalent over $\mathbb{Z}_2$ it is necessary and sufficient that A_1 represents 1 (if this holds we apply the same change variables as before). We need to find a solution to $pX^2 + qY^2 = 1$ in $\mathbb{Z}_2$. Working modulo 8 we have two cases. If $q \equiv 1 \bmod 8$, then $f(Y) := qY^2 - 1$ has $v_2(f(1)) \geq 3$ and $v_2(f'(1)) = 1$, so by Hensel's lemma there exists $y \in \mathbb{Z}_2^\times$ with $qy^2 = 1$. Therefore $(0, y)$ is a solution to $pX^2 + qY^2 = 1$ as desired. On the other hand, if $q \equiv 5 \bmod 8$, we consider $f(Y) := qY^2 - 1 - 4p$. As before, $v_2(f(1)) \geq 3$ and $v_2(f'(1)) = 1$, so by Hensel's lemma there exists y such that $(2, y)$ is a solution to $pX^2 + qY^2 = 1$, as desired. Some examples can be, letting $q = 5, p = 11$ or $q = 17, p = 13$. ⧉

Of course two forms that are equivalent over $\mathbb{Z}$ are automatically in the same genus. It turns out that the genus can be decomposed into finitely many equivalence classes:

$$\operatorname{gen}(Q) = \bigsqcup_i [Q_i].$$

We define the genus mass by

$$m(\operatorname{gen}(Q)) = \sum_i o(Q_i)^{-1}.$$

We also define the weighted sum

$$r(n, \operatorname{gen}(Q)) = m(\operatorname{gen}(Q))^{-1} \sum_i \frac{r(n, Q_i)}{o(Q_i)}.$$

We have the following important theorem:

Theorem 4.1.6 (Minkowski-Siegel-Smith)**.** *Let Q be a positive definite integral quadratic for. Then we have*

$$r(m, gen(Q)) = \delta_\infty(n, A) \cdot \prod_p \delta_p(n, A).$$

where $A \in SP_k$ such that $Q = Q_A$ and the local densities are defined in (69) and (70).

We omit the proof and return to the theory that involves modular forms (more directly). To do so we need to understand the spaces $M_{\frac{k}{2}}(\Gamma_0(2N_A), \vartheta_{th})$ where $A \in \mathcal{SP}_k$ better.

Proposition 4.1.7. *A set of representatives of $\Gamma_0(N)\backslash SL_2(\mathbb{Z})$ is given by*

$$\begin{pmatrix} * & * \\ u & v \end{pmatrix} \text{ for } v \mid N,\ (u, v) = 1 \text{ and } u \bmod \frac{N}{v}.$$

In particular

$$[SL_2(\mathbb{Z})\colon \Gamma_0(N)] = N \prod_{p|N}(1+p^{-1}).$$

Furthermore, an exhaustive set of inequivalent cusps for $\Gamma_0(N)$ *is given by*

$$\frac{u}{v} \text{ with } v \mid N,\ (u,v)=1 \text{ and } u \bmod (v, N/v).$$

Proof. We write

$$\underbrace{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}}_{\in\Gamma_0(N)} \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{\in \mathrm{SL}_2(\mathbb{Z})} = \begin{pmatrix} * & * \\ \gamma a + \delta c & \gamma b + \delta d \end{pmatrix} = \begin{pmatrix} * & * \\ u & v \end{pmatrix}.$$

We first observe that (d,N) is invariant under right multiplication by elements in $\Gamma_0(N)$. Furthermore, choosing γ and δ appropriately allows us to ensure that $v=(d,N)\mid N$. Note that all possible solutions

$$\gamma' b + \delta' d = v$$

are of the form $\delta' = \delta - bt$ and $\gamma' = \gamma + dt$. Since we need $N \mid \gamma'$ to hold we need to assume that $t \equiv 0 \bmod N/v$. This is however the only restriction. Note that we have $u' = \gamma' a + \delta' c = u + t$. Thus we can choose u freely modulo N/v. It is clear from the argument that we have found our set of representatives. To compute the index is now straight forward and we omit the computation.

Since $\Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ all cusps are equivalent to ∞ over $\mathbb{Z}$. Write

$$\tau = S \cdot \begin{pmatrix} * & * \\ u & v \end{pmatrix}^{-1} = \begin{pmatrix} u & * \\ v & * \end{pmatrix}.$$

In particular we have $\tau\infty = \frac{u}{v}$ with $(u,v)=1$ and $v \mid N$. We now simply check when such fractions are equivalent:

$$\frac{u'}{v'} = \underbrace{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}}_{\in\Gamma_0(N)} \frac{u}{v}.$$

From $v' = \gamma u + \delta v$ we obtain $v \mid v'$. Similarly we also have $v' \mid v$ so that $v' = v$ and $\delta \equiv 1 \bmod N/v$. We conclude by observing that

$$u' = \alpha u + \beta v \equiv \alpha u \equiv \delta u \equiv u \bmod (v, N/v).$$

$\square$

Example 4.1.8. For example $\Gamma_0(4)$ has (up to equivalence) the three cusps ∞, 0 and $\frac{1}{2}$.

Since in general it is important to know if a cusp is singular (with respect to $\vartheta_{\rm th}$) for example we will compute the stabilizers in detail. Given a cusp $\mathfrak{a} = \frac{u}{v}$ as above we have

$$\tau_{\mathfrak{a}} = \begin{pmatrix} u & * \\ v & * \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ with } \tau_{\mathfrak{a}}\infty = \mathfrak{a}.$$

We must have

$$\tau_{\mathfrak{a}}^{-1}\Gamma_{\mathfrak{a}}\tau_{\mathfrak{a}} \subseteq \Gamma_{\infty}.$$

Thus we can recover

$$\Gamma_{\mathfrak{a}} = \tau_{\mathfrak{a}}\Gamma_{\infty}\tau_{\mathfrak{a}}^{-1} \cap \Gamma_0(N) = \left\{ \pm \begin{pmatrix} 1-muv & mu^2 \\ -mv^2 & 1+muv \end{pmatrix} : mv^2 \equiv 0 \bmod N \right\}.$$

Thus m ranges over all integers divisible by $m_{\mathfrak{a}} = N/(N, v^2)$. Thus $\Gamma_{\mathfrak{a}}$ is generated by

$$\gamma_{\mathfrak{a}} = \begin{pmatrix} 1-m_{\mathfrak{a}}uv & m_{\mathfrak{a}}u^2 \\ -m_{\mathfrak{a}}v^2 & 1+m_{\mathfrak{a}}uv \end{pmatrix}.$$

Note that in particular a real scaling matrix is given by

$$\sigma_{\mathfrak{a}} = \tau_{\mathfrak{a}} \cdot \begin{pmatrix} \sqrt{m_{\mathfrak{a}}} & 0 \\ 0 & \frac{1}{\sqrt{m_{\mathfrak{a}}}} \end{pmatrix}.$$

To each singular cusp $\mathfrak{a}$ of $\Gamma_0(N)$ we attach the (generalized) Eisenstein series

$$E_{\mathfrak{a}}(z) = \sum_{\gamma \in \Gamma_{\mathfrak{a}}\backslash\Gamma} \overline{\vartheta_{\rm th}(\gamma)}\overline{w(\sigma_{\mathfrak{a}}^{-1},\gamma)} j_{\sigma_{\mathfrak{a}}^{-1}\gamma}(z)^{-\frac{k}{2}} \tag{73}$$

For $k > 4$ this converges and we have $E_{\mathfrak{a}}(z) \in M_{\frac{k}{2}}(\Gamma_0(N), \vartheta_{\rm th})$. Note that $E_{\mathfrak{a}} = P_{\mathfrak{a},\mathbf{1}}$ where the Poincaré series was defined in (40) for $p = \mathbf{1}$ being constantly one. For another singular cusp $\mathfrak{b}$ the same procedure that we used to compute the Fourier expansion of Poincaré series yields

$$[E_{\mathfrak{a}}|_{\frac{k}{2}}\sigma_{\mathfrak{b}}](z) = \delta_{\mathfrak{a}=\mathfrak{b}} + \sum_{n=1}^{\infty} \eta_{\mathfrak{a},\mathfrak{b}}(n)e(nz), \tag{74}$$

where

$$\eta_{\mathfrak{a},\mathfrak{b}}(n) = \left(\frac{2\pi}{i}\right)^{\frac{k}{2}} \frac{n^{\frac{k}{2}-1}}{\Gamma(\frac{k}{2})} \sum_{c>0} c^{-k} S_{\mathfrak{a},\mathfrak{b}}(0,n;c).$$

Remark 4.1.9. We leave it as an exercise to check that for $N = 1$, $4 \mid k$ and $\vartheta_{th} = \vartheta_{\rm tr}$ one recovers the correct Fourier coefficients of the Eisenstein series $E_{\frac{k}{2}}$ from $\eta_{\infty,\infty}(n)$.

Exercise 1, Sheet 9: Recall that the Ramanujan sum was defined by

$$c_q(d) = \sum_{\substack{x \bmod q \\ (x,q)=1}} e\left(\frac{dx}{q}\right)$$

It evaluates to

$$c_q(d) = \sum_{y|(q,d)} \mu\left(\frac{q}{y}\right) y \tag{75}$$

where μ is the Möbius function given by

$$\zeta(s)^{-1} = \sum_{n=1}^{\infty} \mu(n) n^{-s} \tag{76}$$

for $\mathrm{Re}(s) > 1$.

Let $k \geq 4$ be even, let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and take $\mathfrak{a} = \infty$. Recall the definition of the Eisenstein series $E_{\mathfrak{a}} \in M_k(\mathrm{SL}_2(\mathbb{Z}), \theta_{\mathrm{tr}})$ and its Fourier expansion.

a) Evaluate the Fourier coefficients

$$\eta_{\infty,\infty}(n) = \left(\frac{2\pi}{i}\right)^k \frac{n^{k-1}}{\Gamma(k)} \sum_{c>0} c^{-k} S_{\infty,\infty}(0, n; c)$$

as explicit as possible.

b) Conclude that the Fourier expansion of $E_{\mathfrak{a}}$ agrees with the one of the classical Eisenstein series E_k.

Solution. Clearly, $S_{\infty,\infty}(0, n; c) = c_c(n)$. Using (75), (76) and letting $d = cy$ we get

$$\sum_{c=1}^{\infty} c^{-k} c_c(n) = \sum_{c=1}^{\infty} \sum_{y|(c,n)} c^{-k} \mu\left(\frac{c}{y}\right) y = \sum_{y|n} \sum_{d=1}^{\infty} (dy)^{-k} \mu(d) y = \zeta(k)^{-1} \sum_{y|n} y^{1-k}$$
$$= \zeta(k)^{-1} \sum_{d|n} \left(\frac{n}{d}\right)^{1-k} = n^{1-k} \sigma_{k-1}(n) \zeta(k)^{-1}.$$

It follows that,

$$\eta_{\infty,\infty}(n) = \left(\frac{2\pi}{i}\right)^k \frac{1}{\Gamma(k)\zeta(k)} \sigma_{k-1}(n).$$

Then we use one of the identities for the Bernoulli numbers, $2\zeta(k) = \frac{(2\pi)^k}{k!} B_k = \frac{(2\pi)^k}{k\Gamma(k)} B_k$. From this, it follows that

$$\eta_{\infty,\infty}(n) = \left(\frac{2\pi}{i}\right)^k \frac{2k}{(2\pi)^k} \frac{\sigma_{k-1}(n)}{B_k} = i^k \frac{2k}{B_k} \sigma_{k-1}(n).$$

Since this expression agrees with the n-th Fourier coefficient of E_k, we are finished. ◻

Remark 4.1.10. We explain how the identities (75) and (76) are proved. We say that a function $f : \mathbb{Z}_{>0} \to \mathbb{C}$ is multiplicative if $f(nm) = f(n)f(m)$ for coprime positive integers. For example, $f = \phi$, the Euler totient function, is multiplicative. Given two functions $f, g : \mathbb{Z}_{>0} \to \mathbb{C}$ we define its convolution as

$$(f * g)(n) = \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right).$$

Convolution is commutative and associative, and the function δ_1 is the identity. Furthermore, the convolution of two multiplicative functions is multiplicative. Indeed, if n, m are coprime and $d \mid nm$ then we can write uniquely $d = d_1 d_2$ where $d_1 \mid n$ and $d_2 \mid m$. Therefore,

$$\begin{aligned}(f * g)(nm) &= \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right) = \sum_{d_1 \mid n} \sum_{d_2 \mid m} f(d_1 d_2) g\left(\frac{nm}{d_1 d_2}\right) \\ &= \left(\sum_{d_1 \mid n} f(d_1) g\left(\frac{n}{d_1}\right)\right)\left(\sum_{d_2 \mid m} f(d_2) g\left(\frac{m}{d_2}\right)\right).\end{aligned}$$

Recall that the Möbius function μ is the multiplicative function defined on power of primes as $\mu(1) = 1$, $\mu(p) = -1$ and $\mu(p^n) = 0$ for $n \geq 2$. Also, define id_d as $\mathrm{id}_d(n) = n$ if $n \mid d$, and zero otherwise. This function is clearly multiplicative, and the identity (75) is equivalent to proving $c_{\cdot}(d) := (\mu * \mathrm{id}_d)(\cdot)$. Observe also that if d is fixed and $q = nm$ coprime, then since $x \in (\mathbb{Z}/(nm)\mathbb{Z})^\times$ can be expressed as $x = rm\overline{m} + sn\overline{n}$ for unique $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $s \in (\mathbb{Z}/m\mathbb{Z})^\times$, we deduce

$$\begin{aligned}c_{nm}(d) &= \sum_{\substack{x \bmod nm \\ (x,nm)=1}} e\left(\frac{dx}{q}\right) = \sum_{\substack{r \bmod n \\ (r,n)=1}} \sum_{\substack{s \bmod m \\ (r,n)=1}} e\left(\frac{d\overline{m}r}{n}\right) e\left(\frac{d\overline{n}s}{n}\right) \\ &= c_n(\overline{m}d) c_m(\overline{n}d) = c_n(d) c_m(d)\end{aligned}$$

where the last equality follows since $(\overline{n}, m) = (\overline{m}, n) = 1$. Since all functions are multiplicative, to check $c_{\cdot}(d) := (\mu * \mathrm{id}_d)(\cdot)$ we can restrict to prime powers. Let p a prime and $d = p^n d_0$ with $(d_0, p) = 1$. Then it is very simple to check

$$(\mu * \mathrm{id}_d)(p^a) = \begin{cases} 1, & \text{if } a = 0; \\ p^a - p^{a-1}, & \text{if } 0 < a \leq n; \\ -p^n, & \text{if } a = n+1; \\ 0, & \text{if } a \geq n+2 \end{cases}$$

We need to prove that these formulae also hold for $c_{p^a}(d)$. For $a = 0$ it is clear. For $a > 0$ we evaluate the sum as

$$c_{p^a}(d) = \sum_{\substack{x \bmod p^a \\ (x,q)=1}} e\left(\frac{d_0 x}{p^{a-n}}\right) = \sum_{x \bmod p^a} e\left(\frac{d_0 x}{p^{a-n}}\right) - \sum_{y \bmod p^{a-1}} e\left(\frac{d_0 y}{p^{a-n-1}}\right) \tag{77}$$

Then the formula follows by character orthogonality. This proves (75). We move to (76). To any arithmetic function $f : \mathbb{Z}_{>0} \to \mathbb{C}$ we can associate the Dirichlet L-function L_f defined as

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

If $|f(n)| \leq Cn_0^{\sigma}$, then the series converges absolutely on $\mathrm{Re}(s) > \sigma_0 + 1$ and defines an holomorphic function there. If f is multiplicative, we have the product decomposition

$$L_f(s) = \prod_{p \text{ prime}} \left(1 + \sum_{n=1}^{\infty} \frac{f(p)}{p^{ns}}\right).$$

Also, if $f = g * h$ then one checks that

$$L_{g*h}(s) = \sum_{n=1}^{\infty} \sum_{d|n} \frac{g(d)h\left(\frac{n}{d}\right)}{n^s} = \sum_{d=1}^{\infty} \sum_{c=1}^{\infty} \frac{g(d)}{d^s} \frac{h(c)}{c^s} = L_g(s)L_h(s).$$

This is valid in the domain where both Dirichlet series are absolutely convergent. When $g = \mathrm{cons}_1$, defined as $\mathrm{const}_1(n) = 1$ for all n, we have $L_{\mathrm{const}_1}(s) = \zeta(s)$. It is immediate to check that $\mathrm{const}_1 * \mu = \delta_1$, for example by looking at power of primes, and since $L_{\delta_1}(s) \equiv 1$ we deduce

$$\zeta(s)L_{\mu}(s) \equiv 1$$

as desired.

Definition 4.1.5. For $k \geq 5$ we define the Eisenstein space by

$$E_{\frac{k}{2}}(\Gamma_0(N), \vartheta_{\mathrm{th}}) = \langle E_{\mathfrak{a}} | \mathfrak{a} \text{ singular} \rangle.$$

Remark 4.1.11. Since the Petersson inner product $\langle f, g \rangle$ is defined as soon as f or g is cuspidal it makes sense to speak of $S_{\frac{k}{2}}(\Gamma_0(N), \vartheta_{\mathrm{th}})^{\top} \subset M_{\frac{k}{2}}(\Gamma_0(N), \vartheta_{\mathrm{th}})$. It turns out that

$$S_{\frac{k}{2}}(\Gamma_0(N), \vartheta_{\mathrm{th}})^{\top} = E_{\frac{k}{2}}(\Gamma_0(N), \vartheta_{\mathrm{th}}). \tag{78}$$

In any case we write[28]

$$\theta_{1,Q_A}(z) = E_{Q_A}(z) + F_{Q_A}(z),$$

where

$$E_{Q_A}(z) \in E_{\frac{k}{2}}(\Gamma_0(N), \vartheta_{\mathrm{th}}) \text{ and } F_{Q_A}(z) \in S_{\frac{k}{2}}(\Gamma_0(N), \vartheta_{\mathrm{th}}).$$

If $k \geq 5$ we can decompose

$$E_{Q_A}(z) = \sum_{\mathfrak{a} \text{ singular}} \varphi_{\mathfrak{a}}(Q_A) E_{\mathfrak{a}}(z).$$

[28]This makes sense for all k when we use the identification (78). If we want to make use of the explicit construction of the $E_{\mathfrak{a}}$, then we need to assume that $k \geq 5$.

By construction of $E_{\mathfrak{a}}$ we obviously have

$$\varphi_{\mathfrak{a}}(Q_a) = \lim_{y\to\infty}[\theta_{1,Q_A}|_{\frac{k}{2}}\sigma_{\mathfrak{a}}](z) = a_{\theta_{1,Q_A}}(0;\mathfrak{a}).$$

In particular one can in principle compute the Eisenstein part $E_{Q_A}(z)$ of θ_{1,Q_A} rather explicitly.

Example 4.1.12. Let us consider the $Q_A = x_1^2 + \ldots + x_s^2$. Then we have

$$\theta_{1,Q_A}(z) = \theta(z)^s,$$

where

$$\theta(z) = \sum_{n\in\mathbb{Z}} e(n^2 z) \in M_{\frac{1}{2}}(\Gamma_0(4), \vartheta_{\mathrm{th}})$$

is the standard theta function. (Applying our theorem for the automorphy of theta functions directly might give level 8 at first, but one can extend the theta multiplier ϑ_{th} to $\Gamma_0(4)$ in this case.) As noted above $\Gamma_0(4)$ as 3 cusps:

$\mathfrak{a}$	$m_{\mathfrak{a}}$	$\gamma_{\mathfrak{a}}$	singular for ϑ_{th}
1	4	$\begin{pmatrix} -3 & 4 \\ -4 & 5 \end{pmatrix}$	Yes
$\frac{1}{2}$	1	$\begin{pmatrix} -1 & 1 \\ -4 & 3 \end{pmatrix}$	No
$\frac{1}{4}$	1	$\begin{pmatrix} -3 & 1 \\ -16 & 5 \end{pmatrix}$	Yes

We obtain

$$\varphi_1(Q_A) = i^{-\frac{s}{2}},\ \varphi_{\frac{1}{2}}(Q_A) = 0 \text{ and } \varphi_{\frac{1}{4}}(Q_A) = 1.$$

This can be seen as follows. First note that the cusp $\frac{1}{4}$ is equivalent to ∞ and $\theta(z) \to 1$ as $z \to \infty$. (This is also obvious from the Fourier expansion at infinity, since 0 is represented exactly once.) On the other hand $\frac{1}{2}$ is non-singular and thus θ has by default no zeroth Fourier coefficient at $\frac{1}{2}$. It follows that the same is true for (integral) powers of θ. Finally, the value at the cusp 1, which is equivalent to 0, can be computed from the transformation behavior directly.

For $s = 2, 4, 6, 8$ the cuspidal part $F_{Q_A}(z)$ turns out to be zero. In particular one will obtain formulae for the representation numbers $r_s(n)$ that closely resembles Jacobi's Four Square Theorem. However, as soon as $s \geq 10$ the cuspidal part contributes non-trivially. For example one can see that

$$r_{10}(n) = \underbrace{\frac{64}{5}\sum_{d|n}\chi_4(n/d)d^4 + \frac{4}{5}\sum_{d|n}\chi_4(d)d^4}_{=a_{E_{Q_A}}(n,\infty)} + \underbrace{\frac{8}{5}\sum_{\substack{z\in\mathbb{Z}[i],\\ \mathrm{Nr}(z)=n}} z^4}_{=a_{F_{Q_A}}(n,\infty)}.$$

For larger (even) s the formula become even more complicated. Note that the case of odd s is in general more complicated due to the complications introduced from half integral weight forms.

We come to the following incredible fact, which in hindsight might be quite natural:

Theorem 4.1.13 (Siegel). *Let Q_A be a positive definite quadratic from of rank k (i.e. $A \in \mathcal{SP}_k$). Then we have*

$$E_{Q_A}(z) = \theta_{gen(Q_A)}(z),$$

where

$$\theta_{gen(Q_A)}(z) = 1 + \sum_{n=1}^{\infty} r(n, gen(Q_A))e(nz) = m(Q_A)^{-1} \sum_i o(Q_i)^{-1} \theta_{1,Q_i}(z).$$

Proof. Using the transformation properties of the theta functions θ_{1,Q_i} (where $\mathrm{gen}(Q) = \bigsqcup_i [Q_i]$) with respect to $\mathrm{SL}_2(\mathbb{Z})$ we see that the numbers $\varphi_{\mathfrak{a}}(Q_i)$ are genus invariant. In particular

$$E_{Q_A}(z) - \theta_{\mathrm{gen}(Q_A)}(z) \in S_{\frac{k}{2}}(\Gamma_0(2N_A), \vartheta_{\mathrm{th}}).$$

We will skip the argument that the difference is actually zero.[29] ∎

Remark 4.1.14. This result has vast generalizations usually named Siegel-Weil formulae. Note that most modern proofs will look very different and usually involve Weil-representations (i.e. oscillatory representations) as a replacement for theta functions. Siegel's original formulation is quite different from what we have stated above: *Für gerades $m > 0$ lässt sich $F(\mathfrak{S}, \tau)$ homogen linear mit constanten Coefficienten zusammensetzen aus den $(4S)$-ten Teilwerten der $(\frac{m}{2} - 2)$-ten Ableitung der mit den Perioden 1, τ gebildeten elliptischen $\wp$-Function.*[30]

Recall that by the Minkowski-Siegel-Smith Theorem the genus representation numbers are given in terms of local densities. Therefore, comparing coefficients gives

$$r(n, Q_A) = \delta_\infty(n, A) \cdot \prod_p \delta_p(n, A) + a_{F_{Q_A}}(n, \infty).$$

Thus as soon as we can produce strong enough bounds for the Fourier coefficients of cusp forms we get a good handle on the numbers $r(n, Q_A)$. (Of course this also requires some lower bounds on the local densities.) This motivates the study of upper bounds for Fourier coefficients of cusp forms.

Exercise 2, Sheet 9:

a) Show that there are $A_1, A_2 \in \mathcal{SP}_{24}$ with $\det(A_1) = \det(A_2) = 1$ and $c_1, c_2 \in \mathbb{C}$ so that $0 \neq c_1\theta_{1,Q_{A_1}} + c_2\theta_{1,Q_{A_2}} \in \mathbb{C} \cdot \Delta$.

[29] One way to see this is a nice trick using Hecke operators.

[30] In our notation $\tau = z \in \mathbb{H}$, $m = k$, $\mathfrak{S} = A$ is an integral positive definite symmetric matrix, $S = \det(\mathfrak{S})$ and $F(\mathfrak{S}, \tau) = \theta_{\mathrm{gen}(Q_A)}(\tau)$.

b) Show that for any $k \in \mathbb{N}$ the space $M_{4k}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ can be spanned by theta functions θ_{1,Q_A} with $A \in \mathcal{SP}_{8k}$ and $\det(A) = 1$.

Solution. Recall the quadratic form of Remark 3.0.16. This was defined as

$$Q_8(x) = \frac{1}{2}A[x] = \frac{1}{2}\sum_{r=1}^{8} x_r^2 + \frac{1}{2}\left(\sum_{r=1}^{8} x_r\right)^2 - x_1x_2 - x_2x_8.$$

We observe that $A \in \mathcal{SP}_8$ and $\det(A) = 1$ (this can be computed directly, or else can be constructed as in Serre *A course in Arithmetic* page 51). Therefore, $\theta_{1,Q_A} \in M_4(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = \mathbb{C}E_4$, and comparing the constant coefficient we get

$$\theta_{1,Q_A} = E_4 \tag{79}$$

Consider now the direct sum $B := A \oplus A \oplus A$. We observe that $\theta_{1,Q_B} = \theta_{1,Q_A}^3 \in M_{12}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. Therefore, we can write

$$E_4^3 = \theta_{1,Q_B} = aE_{12} + b\Delta$$

for unique $a, b \in \mathbb{C}$. By comparing the constant coefficient, it follows that $a = 1$. Recall that

$$E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \quad \text{and} \quad E_{12}(z) = 1 + \frac{24\cdot 2730}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n.$$

Comparing the coefficient of q, we calculate $b = 720 - \frac{24\cdot 2730}{691}$, in particular $b \neq 0$. Note that since $a = 1$, for the Eisenstein part of θ_{1,Q_B} we have $E_{Q_B} = E_{12}$. From theorem 4.1.10, we obtain $E_{Q_B} = \theta_{\mathrm{gen}(Q_A)}$, where

$$\theta_{\mathrm{gen}(Q_B)} = m(Q_B)^{-1}\sum_i o(Q_i)^{-1}\theta_{1,Q_i}$$

is an average of theta functions over the genus of B. Since this average equals E_{12}, which is different from θ_{1,Q_B} (since $b \neq 0$) we deduce that the genus of B is composed not only of B, and that there is C in the genus of B with $\theta_{1,Q_C} \neq \theta_{1,Q_B}$. Since C is locally isomorphic to B, one can deduce that $C \in \mathcal{SP}_{24}$ with $\det(C) = 1$. Indeed, $\det(C) > 0$ since B and C are equivalent over $\mathbb{R}$, and if $\det(C) > 1$ we would have $p \mid \det(C)$ for some prime, but then B and C would not be equivalent over $\mathbb{Z}_p$, a contradiction. Looking at the constant coefficient, we deduce that $\theta_{1,Q_B} - \theta_{1,Q_C} = c\Delta$ for some $c \neq 0$, which is what we wanted.

For part b), recall that $\theta_{1,Q_{A\oplus B}} = \theta_{1,Q_A}\cdot\theta_{1,Q_B}$. Consider the direct sum $\mathcal{L} := \oplus_{k\geq 0}L_{4k}$ of vector spaces L_{4k}, where $L_{4k} \subset M_{4k}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ is the subspace spanned by theta functions θ_{1,Q_A} with $A \in \mathcal{SP}_{8k}$ and $\det(A) = 1$. Then this direct sum is closed under multiplication, and is thus a subring of $\mathcal{M} = \bigoplus_{k\geq 0} M_{4k}$. We know that $\theta_{1,Q_A} = E_4$, $\theta_{1,Q_A}^2 = E_8$ and $c^{-1}(\theta_{1,Q_B} - \theta_{1,Q_C}) = \Delta$. Therefore, $L_{4r} = M_{4r}$ for $0 \leq r \leq 3$. Recall that

$$M_{4r+12} = \mathbb{C}E_{4r+12} \oplus \Delta M_{4r}.$$

Considering any $A \in \mathcal{S}_{8k+24}$ with $\det(A) = 1$, we have

$$\theta_{1,Q_A} = E_{4r+12} + c\Delta f_{4r}$$

for some $c \in \mathbb{C}$ and $f_{4r} \in M_{4k}$. By induction we can assume $M_{4k} = L_{4k}$, and since $\Delta \in L_{12}$ and $\mathcal{L}$ is closed under multiplication and linear combinations, we deduce $E_{4r+12} \in L_{4k+12}$. By the direct sum decomposition above, this shows that $L_{4k+12} = M_{4k+12}$, and we finish by induction. ◻

Remark 4.1.15. A direct way of proving part a) follows from Serre *A course in Arithmetic*, page 51. We will assume that the reader already has had a look at that page. For each $k \geq 1$, Serre constructs a free abelian group of rank $8k$, denoted by Γ_{8k}, together with a certain positive definite symmetric bilinear form $(\cdot) : \Gamma_{8k} \times \Gamma_{8k} \to \mathbb{Z}$ such that $v \cdot v \in 2\mathbb{Z}$ for all $v \in \Gamma_{8k}$ and such that the map

$$\Phi_{8k} : \Gamma_{8k} \to \mathrm{Hom}_{\mathbb{Z}}(\Gamma_{8k}, \mathbb{Z}) \quad v \mapsto \Phi_{8k}(v) := (w \mapsto \Phi_{8k}(v)(w) = v \cdot w)$$

is an isomorphism. This is the coordinate free version of the following statement: whenever we choose a $\mathbb{Z}$-basis v_i of Γ_{8k}, then the matrix A_{8k}, with $(A_{8k})_{i,j} = v_i \cdot v_j$, satisfies $|\det(A_{8k})| = 1$. Since A_{8k} is positive definite, it must be $\det(A_{8k}) = 1$. Therefore, we have $A_{8k} \in \mathcal{S}_{8k}$ and $\det(A_{8k}) = 1$, so that letting $Q_{8k}(x) = \frac{1}{2}x^t Ax$, we have $\theta_{1,Q_{8k}} \in M_{4k}(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. In particular, for $k = 1$ we have $\theta_{1,Q_8} = E_4$ as in part a), and for $k = 2$ we have $\theta_{1,Q_{16}} = E_8 = \theta_{1,Q_6}^2$. We will prove that $\theta_{1,Q_{24}} \neq E_4^3$. For this, it is enough to calculate the coefficient of q in the expansion at infinity. Equivalently, we need to calculate the representation number of 2 for Γ_{24}, that is, the number of $v \in \Gamma_{8k}$ such that $v \cdot v = 2$. Serre describes Γ_{8k} as the abelian group of vectors $v = (x_i) \in \mathbb{Q}^{8k}$ such that

$$2x_i \in \mathbb{Z},\ x_i - x_j \in \mathbb{Z},\ \sum_{i=1}^{8k} x_i \in 2\mathbb{Z}$$

and the bilinear product is just the restriction of the usual euclidean product. Suppose $v \cdot v = 2$. We have $v = \left(\frac{y_i}{2}\right)$ where $y_i \in \mathbb{Z}$ and all have the same parity. If they were all odd we would have $v \cdot v \geq 24/4 = 6 > 2$, a contradiction. Therefore, we can write $v = \sum_i a_i e_i$ where e_i is the canonical basis and $a_i \in \mathbb{Z}$. Since $\sum a_i^2 = 2$, we see that the only possibility is that $|a_i| = 1$ for two indices, and $a_j = 0$ otherwise. Therefore, the solutions to $v \cdot v$ in Γ_{8k} are

$$v = \pm e_i \pm e_j\, (i \neq j)$$

which gives a total of $4\binom{24}{2} = 2 \cdot 24 \cdot 23$ choices. Since the q coefficient of E_4^3 equals 720, we deduce that

$$\theta_{1,Q_{24}} = E_4^3 + (2 \cdot 24 \cdot 23 - 3 \cdot 240)\Delta = E_4^3 + 24 \cdot 16\Delta$$

In particular, $\theta_{1,Q_{24}} \neq E_4^3 = \theta_{1,Q_8}^3$, as desired.

Bonus Exercise: Prove the following formula

$$r_6(m) := \sharp\{(n_1,\ldots,n_6)\in\mathbb{Z}^6 : n_1^2+\ldots+n_6^2 = m\} = 16\sum_{d|m}\chi_{-4}\left(\frac{m}{d}\right)d^2 - 4\sum_{d|m}\chi_{-4}(d)d^2.$$

Solution. As before, introduce $A_6 := \operatorname{diag}(2,2,2,2,2,2)$ and

$$\theta_{1,Q_6}(z) = \sum_{\mathbf{n}\in\mathbb{Z}^6} e\left(\frac{1}{2}A_8[\mathbf{n}]z\right) = \sum_{m\geq 0} r_6(m)e(mz)$$

and observe that $\theta_{1,Q_6} = \theta^6$. This time the multiplier $\vartheta_{\mathrm{th}}^6$ is not trivial on $\Gamma_0(4)$. Recall that

$$\vartheta_{\mathrm{th}}\left(\begin{pmatrix} a & b \\ 4c & d\end{pmatrix}\right) = \left(\frac{4c}{d}\right)\overline{\epsilon_d} \quad \text{where} \quad \epsilon_d := \begin{cases} 1, & \text{if } d\equiv 1 \bmod 4; \\ i, & \text{if } d\equiv 3 \bmod 4\end{cases}$$

Therefore, $\vartheta_{\mathrm{th}}^6$ is the multiplier χ_{-4}, defined as

$$\chi_{-4}\left(\begin{pmatrix} a & b \\ 4c & d\end{pmatrix}\right) = \chi_{-4}(d) := \begin{cases} 1, & \text{if } d\equiv 1 \bmod 4; \\ -1, & \text{if } d\equiv 3 \bmod 4\end{cases}$$

Therefore, $\theta_{1,Q_6}\in M_3(\Gamma_0(4),\chi_{-4})$. To apply our usual strategy we need to find a basis of this finite dimensional vector space. First, we claim that $\dim M_3(\Gamma_0(4),\chi_{-4}) = 2$. For the upper bound, we apply an identical argument to that of the proof of Lemma 4.0.1. For the sake of contradiction, suppose that $\dim M_3(\Gamma_0(4),\chi_{-4})\geq 3$. Then, by forming a linear combination we can find a non-zero $0\neq f\in M_3(\Gamma_0(4),\chi_{-4})$ with a zero of order at least 2 at ∞. Then $0\neq f^2\in M_6(\Gamma_0(4),\theta_{\mathrm{tr}})$ has a zero of order at least 4 at infinity. Therefore, the product

$$g := \prod_{\gamma\in\Gamma_0(4)\backslash \mathrm{SL}_2(\mathbb{Z})} [f^2|_6\gamma] \in M_{36}(\mathrm{SL}_2(\mathbb{Z}),\vartheta_{\mathrm{tr}}) \tag{80}$$

is a modular form of weight 36 for $\mathrm{SL}_2(\mathbb{Z})$ with a zero of order at least 4 at infinity. Applying the formula of Theorem 2.4.1, we deduce that g is identically zero, a contradiction. Therefore, $\dim M_3(\Gamma_0(4),\chi_{-4})\leq 2$. On the other hand, $\Gamma_0(4)$ has three cusps. In the notation of Example 4.1.8, they are represented by $1, 1/2$ and $1/4$. The cusps represented by 1 and $1/4$ are singular for ϑ_{th}, therefore also singular for $\chi_{-4} = \vartheta_{\mathrm{th}}^2$. On the other hand, the stabilizer of the cusp $1/2$ is generated by

$$\gamma_{\frac{1}{2}} = \begin{pmatrix} -1 & 1 \\ -4 & 3\end{pmatrix}$$

so that

$$\chi_{-4}\left(\gamma_{\frac{1}{2}}\right) = \chi_{-4}(3) = -1 \tag{81}$$

Therefore, the cusp $1/2$ is nonsingular for χ_{-4}. We arrive at the conclusion that for the multiplier χ_{-4} the group $\Gamma_0(4)$ has two inequivalent singular cusps. Therefore, the space $\mathcal{E}_3(\Gamma_0(4),\chi_{-4})$ of Definition 4.1.5 has dimension 2, and after noting that the cusp $1/4$ is equivalent to ∞ and the cusp 1 is equivalent to 0, we deduce that

$$M_3(\Gamma_0(4),\chi_{-4}) = \mathbb{C}E_\infty \oplus \mathbb{C}E_0 \tag{82}$$

where $E_{\mathfrak{a}}$ is the generalized Eisenstein series associated to a singular cusp as in (73). The Fourier expansion of these series at ∞ is given in (74), so that

$$E_\infty(z) = 1 + \sum_{n=1}^{\infty} \eta_{\infty,\infty}(n) e(nz) \quad \text{and} \quad E_0(z) = \sum_{n=1}^{\infty} \eta_{0,\infty}(n) e(nz)$$

where

$$\eta_{\infty,\infty}(n) = \left(\frac{2\pi}{i}\right)^3 \frac{n^2}{2} \sum_{c>0} c^{-3} S^{\chi_{-4}}_{\infty,\infty}(0,n;c)$$

$$\text{and } \eta_{0,\infty}(n) = \left(\frac{2\pi}{i}\right)^3 \frac{n^2}{2} \sum_{c>0} c^{-3} S^{\chi_{-4}}_{0,\infty}(0,n;c).$$

We have modified the notation for the Kloosterman sums slightly, to avoid confusion with the classical Kloosterman sums. We start by analysing $S^{\chi_{-4}}_{\infty,\infty}(0,n;c)$. These are nonzero only for $c = 2^r c_0$, where $r \geq 2$ and $(c_0, 2) = 1$, and in that case they are defined by

$$S^{\chi_{-4}}_{\infty,\infty}(0,n;c) = \sum_{d \in (\mathbb{Z}/c\mathbb{Z})^\times} \chi_{-4}(d) e\left(\frac{nd}{c}\right).$$

Suppose that $c = c_1 c_2$ with $4 \mid c_1$ and $(c_1, c_2) = 1$. Let $\overline{c_1}$, $\overline{c_2}$ be integers representing the inverse of c_1 modulo c_2 and of c_2 modulo c_1 respectively. We can write any $d \in (\mathbb{Z}/c\mathbb{Z})^\times$ uniquely as $d = d_1\overline{c_2}c_2 + d_2\overline{c_1}c_1$, where d_1, d_2 range over representatives of $(\mathbb{Z}/c_1\mathbb{Z})^\times$ and $(\mathbb{Z}/c_2\mathbb{Z})^\times$ respectively. Since $4 \mid c_1$ and $\chi_{-4}(d)$ only depends on d modulo 4, we see that

$$\begin{aligned} S^{\chi_{-4}}_{\infty,\infty}(0,n;c) &= \sum_{d \in (\mathbb{Z}/c\mathbb{Z})^\times} \chi_{-4}(d) e\left(\frac{nd}{c}\right) = \sum_{\substack{d_1 \in (\mathbb{Z}/c_1\mathbb{Z})^\times \\ d_2 \in (\mathbb{Z}/c_2\mathbb{Z})^\times}} \chi_{-4}(d_1) e\left(\frac{nd_1\overline{c_2}}{c_1}\right) e\left(\frac{nd_2\overline{c_1}}{c_2}\right) \\ &= \chi_{-4}(c_2)\left(\sum_{d_1 \in (\mathbb{Z}/c_1\mathbb{Z})^\times} \chi_{-4}(d_1) e\left(\frac{nd_1}{c_1}\right)\right)\left(\sum_{d_2 \in (\mathbb{Z}/c_2\mathbb{Z})^\times} e\left(\frac{nd_2}{c_2}\right)\right) \\ &= \chi_{-4}(c_2) S^{\chi_{-4}}_{\infty,\infty}(0,n;c_1) S_{\infty,\infty}(0,n;c_2) \end{aligned}$$

where $S_{\infty,\infty}(0,n;c)$ is the Ramanujan sum as in (75). In particular, writing $c = 2^r c_0$ for $(c_0, 2) = 1$, we have

$$S^{\chi_{-4}}_{\infty,\infty}(0,n;2^r c_0) = \chi_{-4}(c_0) S^{\chi_{-4}}_{\infty,\infty}(0,n;2^r) \sum_{y \mid (c_0,n)} \mu\left(\frac{c_0}{y}\right) y.$$

Write $n = 2^s n_0$ where $(n_0, 2) = 1$. Observe that we can write $d \in (\mathbb{Z}/2^r\mathbb{Z})^\times$ as $d = 1 + 4x$ or $d = 3 + 4x$ for a unique $x \in \mathbb{Z}/2^{r-2}\mathbb{Z}$. Therefore,

$$\begin{aligned} S^{\chi_{-4}}_{\infty,\infty}(0, 2^s n_0; 2^r) &= \sum_{x \bmod 2^{r-2}} e\left(\frac{n_0}{2^{r-s}}\right) e\left(\frac{n_0 x}{2^{r-s-2}}\right) - \sum_{x \bmod 2^{r-2}} e\left(\frac{3n_0}{2^{r-s}}\right) e\left(\frac{n_0 x}{2^{r-s-2}}\right) \\ &= \left(e\left(\frac{n_0}{2^{r-s}}\right) - e\left(\frac{3n_0}{2^{r-s}}\right)\right) \sum_{x \bmod 2^{r-2}} e\left(\frac{n_0 x}{2^{r-s-2}}\right). \end{aligned}$$

By character orthogonality, the sum vanishes unless $r \leq s + 2$, in which case it equals 2^{r-2}. On the other hand, if $r \leq s + 1$ the first factor vanishes. The only remaining case is $r = s + 2$, where it is easily checked that

$$S^{\chi_{-4}}_{\infty,\infty}(0, 2^s n_0; 2^{s+2}) = 2^{s+1}\chi_{-4}(n_0)i.$$

Therefore, when calculating $\eta_{\infty,\infty}(n)$ where $n = 2^s n_0$, we restrict to $c = 2^{s+2}c_0$ and employ the above formulas, we obtain

$$\begin{aligned} \eta_{\infty,\infty}(n) &= \left(\frac{2\pi}{i}\right)^3 \frac{n^2}{2} \sum_{c_0 \text{ odd}} 2^{-3(s+2)} c_0^{-3} 2^{s+1} \chi_{-4}(n_0) i \chi_{-4}(c_0) \sum_{y|(c_0,n)} \mu\left(\frac{c_0}{y}\right) y \\ &= -\frac{\pi^3}{8} n_0^2 \chi_{-4}(n_0) \sum_{y|n_0} y^{-2}\chi_{-4}(y) \sum_{d \text{ odd}} \frac{\chi_{-4}(d)\mu(d)}{d^3}. \end{aligned}$$

Recall that $L(s, \chi_{-4}\mu)L(s, \chi_{-4}) = 1$, where

$$L(s, f) = \sum_{d=1}^{\infty} \frac{f(d)}{d^s}$$

In particular, the inner sum above equals $L(3, \chi_{-4})^{-1}$ and we have

$$\begin{aligned} \eta_{\infty,\infty}(n) &= -\frac{\pi^3}{8L(3, \chi_{-4})} \sum_{y|n_0} \left(\frac{n_0}{y}\right)^2 \chi_{-4}\left(\frac{n_0}{y}\right) = -\frac{\pi^3}{8L(3, \chi_{-4})} \sum_{d|n_0} d^2\chi_{-4}(d) \\ &= -\frac{\pi^3}{8L(3, \chi_{-4})} \sum_{d|n} d^2\chi_{-4}(d) = -4\sum_{d|n} d^2\chi_{-4}(d) \end{aligned}$$

where we use that $\chi_{-4}(d)$ is 0 for even d and that $L(3, \chi_{-4})$ is an special value of an L-function that can be calculated explicitly as $L(3, \chi_{-4}) = \frac{\pi^3}{32}$. We have done half the work, and now we need to calculate the coefficients $\eta_{0,\infty}(n)$, which involve the Kloosterman sums $S^{\chi_{-4}}_{0,\infty}(0, n; c)$. According to equation (46), these are given by

$$S^{\chi_{-4}}_{0,\infty}(0, n; c) = \sum_{\gamma = \begin{pmatrix} a & * \\ c & d \end{pmatrix} \in U(\mathbb{Z})\backslash\sigma_0^{-1}\Gamma_0(4)/U(\mathbb{Z})} \overline{\theta_{0,\infty}(\gamma)} e\left(\frac{nd}{c}\right) \tag{83}$$

In our case, since the weight is integral, one can check that the factor $\theta_{0,\infty}(\gamma)$ reduces to $\chi_{-4}(\sigma_0\gamma)$. Also, in the definition above σ_0 is a scalling matrix for the cusp 0, and we can choose $\sigma_0 = \begin{pmatrix} 0 & -\frac{1}{2} \\ 2 & 0 \end{pmatrix}$ We calculate

$$\sigma_0^{-1}\begin{pmatrix} x & y \\ 4z & w \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{2} \\ -2 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ 4z & w \end{pmatrix} = \begin{pmatrix} 2z & w/2 \\ -2x & -2y \end{pmatrix} =: \gamma$$

Since x is odd, we see that $S_{0,\infty}^{\chi_{-4}}(0, n; c)$ is nonzero only for $c = 2c_0$, where $(c_0, 2) = 1$. Also, y is determined modulo x above, and if γ is as above, $\chi_{-4}(\sigma_0\gamma) = \chi_{-4}(w)$. Since $xw - 4yz = 1$, we have $w = \overline{x} = x \bmod 4$. Therefore, writing $c_0 = -x$ we get $\chi_{-4}(\sigma_0\gamma) = -\chi_{-4}(c_0)$. Putting these considerations together, we arrive at

$$S_{0,\infty}^{\chi_{-4}}(0, n; 2c_0) = -\chi_{-4}(c_0)\sum_{d\in(\mathbb{Z}/c_0\mathbb{Z})^\times} e\left(\frac{nd}{c_0}\right) = -\chi_{-4}(c_0)\sum_{y|(c_0,n)} \mu\left(\frac{c_0}{y}\right) y.$$

Inserting this into the definition of $\eta_{0,\infty}(n)$ we have

$$\begin{aligned}
\eta_{0,\infty}(n) &= \left(\frac{2\pi}{i}\right)^3 \frac{n^2}{2}\sum_{c_0 \text{ odd}} -\chi_{-4}(c_0)c_0^{-3}2^{-3}\sum_{y|(c_0,n)}\mu\left(\frac{c_0}{y}\right) y \\
&= -i\pi^3\frac{n^2}{2}\sum_{y|n_0}\chi_{-4}(y)y^{-2}\sum_{d_0 \text{ odd}}\frac{\mu(d_0)\chi_{-4}(d_0)}{d_0^3} \\
&= -i\frac{\pi^3}{2L(3,\chi_{-4})}\sum_{y|n}\chi_{-4}(y)\left(\frac{n}{y}\right)^2 = -16i\sum_{d|n}\chi_{-4}\left(\frac{n}{d}\right)d^2.
\end{aligned}$$

We now have all we need to finish the exercise. Let $\theta_{1,Q_6} = aE_\infty + bE_0$ for unique $a, b \in \mathbb{C}$. Looking at the constant coefficient we deduce $a = 1$, and from $12 = r_6(1) = \eta_{\infty,\infty}(1) + b\eta_{0,\infty}(1) = -4 - 16ib$ we deduce[31] $b = i$. Therefore,

$$r_6(n) = 16\sum_{d|n}\chi_{-4}\left(\frac{n}{d}\right)d^2 - 4\sum_{d|n}\chi_{-4}(d)d^2.$$

Remark 4.1.16. The argument above actually gives the value of $L(3, \chi_{-4})$. Note that by our reasoning we have

$$\eta_{\infty,\infty}(n) = -\frac{\pi^3}{8L(3,\chi_{-4})}\sum_{d|n}\chi_{-4}(d)d^2 \quad \text{and} \quad \eta_{0,\infty}(n) = -i\frac{\pi^3}{2L(3,\chi_{-4})}\sum_{d|n}\chi_{-4}\left(\frac{n}{d}\right)d^2.$$

[31] Observe that, in the notation of Example 4.1.12, for $s = 6$, we have $a = \varphi_{1/4}(Q_{A_6}) = 1$ and $b = \varphi_1(Q_{A_6}) = i$, as expected.

Looking at the constant coefficient of the equation $\Theta_{1,Q_6} = aE_\infty + bE_0$ we deduce $a = 1$ as before. Using $r_6(1) = 12$ and $r_6(2) = 4\binom{6}{2} = 60$ we obtain

$$12 = -\frac{\pi^3}{8L(3,\chi_{-4})} - i\frac{\pi^3}{2L(3,\chi_{-4})}b \quad \text{and} \quad 60 = -\frac{\pi^3}{8L(3,\chi_{-4})} - i\frac{2\pi^3}{L(3,\chi_{-4})}b$$

where we have used $\sum_{d|2}\chi_{-4}\left(\frac{2}{d}\right)d^2 = 4$. These two equations imply $b = i$ and $L(3,\chi_{-4}) = \frac{\pi^3}{32}$, as desired.

4.2. **Kloosterman sums and bounds for Fourier coefficients of cusp forms.** In this section we will establish basic upper bounds for the Fourier coefficients of cusp forms using the Petersson formula Theorem 2.5.10. An essential ingredient will be a good understanding of the Kloosterman sums $S_{\mathfrak{a},\mathfrak{b}}(m,n;c)$ defined in (46). Directly from the definition we obtain the bound

$$\sum_{0<c\leq X} c^{-1}|S_{\mathfrak{a},\mathfrak{b}}(m,n;c)| \leq \sum_{0<c\leq X} c^{-1}\sharp\left\{d \bmod c\colon \begin{pmatrix} * & * \\ c & d\end{pmatrix} \in \sigma_{\mathfrak{a}}^{-1}\Gamma\sigma_{\mathfrak{b}}\right\} \leq \frac{X}{c_{\mathfrak{a},\mathfrak{b}}}. \tag{84}$$

In the last step we have applied Lemma 2.5.3. Putting $X = c$ yields the weak bound

$$|S_{\mathfrak{a},\mathfrak{b}}(m,n;c)| \leq \frac{c^2}{c_{\mathfrak{a},\mathfrak{b}}}.$$

Note that another crucial ingredient will be a satisfying bound for the J-Bessel function. This is a classical well studied function and it is easy to locate the estimate

$$J_k(x) \leq C_k \cdot \min(x^k, x^{-\frac{1}{2}}), \tag{85}$$

where $C_k > 0$ is some constant depending on k.

Remark 4.2.1. Applying Petersson's formula (Theorem 2.5.10) with $\mathfrak{a} = \mathfrak{b}$ and $m = n$ yields

$$\sum_{f\in\mathcal{O}} |a_f(m;\mathfrak{a})|^2 = \frac{(4\pi m)^{k-1}}{\Gamma(k-1)}\left(1 + 2\pi i^{-k}\sum_{c>0} c^{-1}S_{\mathfrak{a},\mathfrak{b}}(m,m;c)J_{k-1}(\frac{4\pi m}{c})\right),$$

Applying (85) and (84) allows us to estimate[32]

$$\sum_{f\in\mathcal{O}} |a_f(m;\mathfrak{a})|^2 \leq C_{\mathfrak{a},k,\epsilon}m^{k+\epsilon} \tag{86}$$

for any $\epsilon > 0$ (where $C_{\mathfrak{a},k,\epsilon} > 0$ is a constant depending on $\mathfrak{a}$, k and ϵ). This implies $|a_f(m;\mathfrak{a})| \leq C_{\mathfrak{a},k,\epsilon}m^{\frac{k}{2}+\epsilon}$, for $f \in S_k(\Gamma,\vartheta)$. We consider this to be the trivial bound. (There are different ways to see this.)

[32]For example one can do so by splitting the c-sum at $4\pi m$, apply a dyadic dissection to the infinite part and use partial summation.

While in general the Kloosterman sums $S_{\mathfrak{a},\mathfrak{b}}(m,n;c)$ can be very complicated the situation gets a bit better when we are dealing with the Hecke congruence subgroups. With our application to quadratic forms in mind we need to consider Kloosterman sums for $\Gamma_0(2N)$ attached to the theta multiplier ϑ_{th}. One finds that in this case

$$S_{\vartheta_{\mathrm{th}}}(m,n;c) := S_{\infty,\infty}(m,n;c) = \delta_{2N|c}\cdot \sum_{\substack{x \bmod c,\\ (x,c)=1}} \overline{\epsilon_x}^k \left(\frac{\det(A)2^kc^k}{x}\right)\cdot e\left(\frac{mx+n\overline{x}}{c}\right).$$

(Recall that $\overline{x}$ denotes the inverse of x modulo c.)

For Kloosterman sums with theta multiplier we have the following improvement over the trivial bound (86):

Theorem 4.2.2. *For $f\in S_{\frac{k}{2}}(\Gamma_0(2N),\vartheta_{th})$ with $k\geq 5$ we have*

$$|a_f(m;\infty)| \leq C_{f,\epsilon}m^{\frac{k}{4}-\frac{1}{4}+\epsilon}. \tag{87}$$

For all $\epsilon>0$ and some positive constant $C_{f,\epsilon}$ possibly depending on f (in particular on k and N) and ϵ.

Proof. We start by proving a little auxiliary estimate:

$$\frac{1}{r}\sum_{a \bmod r}|S_{\vartheta_{\mathrm{th}}}(am,am;r)|^2 \leq 4(m,r)r\sigma_0(r). \tag{88}$$

We can of course assume that $2N \mid r$, since otherwise the statement is trivial. Compute

$$\begin{aligned}&\frac{1}{r}\sum_{a \bmod r}|S_{\vartheta_{\mathrm{th}}}(am,am;r)|^2 \\ &= \frac{1}{r}\sum_{a \bmod r}\sum_{\substack{x_1,x_2 \bmod r,\\ (x_1x_2,r)=1}} \overline{\epsilon_{x_1}}^k\epsilon_{x_2}^k\left(\frac{\det(A)2^kc^k}{x_1}\right)\left(\frac{\det(A)2^kc^k}{x_2}\right)\cdot e\left(\frac{am(x_1-x_2)+am(\overline{x}_1-\overline{x_2})}{c}\right)\end{aligned} \tag{89}$$

Executing the a sum detects the condition

$$m(x_1+\overline{x}_1)\equiv m(x_2+\overline{x}_2) \bmod r.$$

Thus we get

$$\begin{aligned}&\frac{1}{r}\sum_{a \bmod r}|S_{\vartheta_{\mathrm{th}}}(am,am;r)|^2 \\ &\qquad\leq \sharp\{x_1,x_2 \bmod r\colon (x_1x_2,r)=1 \text{ and } m(x_1-x_1)(x_1x_2-1)\equiv 0 \bmod r\}.\end{aligned}$$

The claim follows by counting solutions.

Starting from (88) we can derive some useful estimates. Define

$$\mathcal{A}(Q,R) = \sum_{q\leq Q} \sum_{\substack{r\leq R,\\ (r,q)=1}} |S_{\vartheta_{\rm th}}(\overline{q}m,\overline{q}m;r)|^2,$$

$$\mathcal{B}(Q,R) = \sum_{q\leq Q} \sum_{\substack{r\leq R,\\ (r,q)=1}} |S_{\vartheta_{\rm th}}(m,m;qr)|,$$

$$\mathcal{C}(Q,R) = \sum_{q\leq Q} \sum_{r\leq R} |S_{\vartheta_{\rm th}}(m,m;qr)| \text{ and}$$

$$\mathcal{D}(Q,R) = \sum_{q\leq Q} \sum_{r\leq R} (qr)^{-1}|S_{\vartheta_{\rm th}}(m,m;qr)|.$$

We first estimate

$$\begin{aligned}\mathcal{A}(Q,R) &\leq \sum_{r\leq R}(\frac{Q}{r}+1)\sum_{a \bmod r}|S_{\vartheta_{\rm th}}(am,am;r)|^2\\ &\leq \sum_{r\leq R} 3(Q+r)(m,r)r\sigma_0(r) \leq 4\sigma_0(m)R^2(Q+R)\log(4R).\end{aligned}$$

Next we observe that

$$|S_{\vartheta_{\rm th}}(m,m;qr)| = |\tilde{S}_{\vartheta_{\rm th}}(\overline{q}m,\overline{q}m;r)S_{\vartheta_{\rm th}}(\overline{r}m,\overline{r}m;q)|$$

as long as $(q,r)=1$. Here $\tilde{S}_{\vartheta_{\rm th}}$ is a Kloosterman sum with slightly modified multiplier.[33] Note however that the argument arriving at (88) was insensitive to the exact form of the multiplier. Thus we can use Cauchy-Schwarz to estimate

$$\mathcal{B}(Q,R) \leq \mathcal{A}(Q,R)^{\frac{1}{2}}\tilde{\mathcal{A}}(Q,R)^{\frac{1}{2}} \leq 4\sigma_0(m)QR(Q+R)\log(4QR).$$

Further we have

$$\mathcal{C}(Q,R) \leq \sum_{a\leq Q}\sum_{b\leq R}\mathcal{B}(Q/a,R/b) \leq 4\sigma_0(m)QR(Q+R)\log(4QR)^2.$$

Finally using partial summation we arrive at

$$\mathcal{D}(Q,R) \leq \tau(m)(Q+R)\log(4QR)^3. \tag{90}$$

We can now proceed with the main part of the proof. First, without loss of generality we assume that $f\in S_{\frac{k}{2}}(\Gamma_0(2N),\vartheta_{\rm th})$ has Petersson norm one (i.e. $\langle f,f\rangle = 1$). Then for each q with $2N \mid q$ we have

$$S_{\frac{k}{2}}(\Gamma_0(2N),\vartheta_{\rm th}) \subseteq S_{\frac{k}{2}}(\Gamma_0(q),\vartheta_{\rm th}).$$

Thus f is also an element in the (potentially) bigger space of cusp forms for $\Gamma_0(q)$ (with respect to the theta multiplier). Note however that the Petersson norm

[33] We leave it as an exercise to work out the precise factorization properties. This requires quadratic reciprocity and the Chinese remainder theorem.

rescales when we change underlying group. Thus in the new space the norm of f is now $[\Gamma_0(2N)\colon\Gamma_0(q)]^{\frac{1}{2}}$. Applying Petersson's formula (i.e. Theorem 2.5.10) we obtain

$$\frac{\Gamma(\frac{k}{2}-1)}{(4\pi m)^{\frac{k}{2}-1}}\frac{|a_f(m;\infty)|^2}{[\Gamma_0(2N)\colon\Gamma_0(q)]} \leq 1+2\pi i^{-\frac{k}{2}}\sum_{c\equiv 0 \bmod q} c^{-1}S_{\vartheta_{\mathrm{th}}}(m,m,c)J_{\frac{k}{2}-1}(\frac{4\pi m}{c}).$$

Put $m(Q)=\sum_{\substack{Q<q\leq 2Q,\\ q\equiv 0 \bmod 2N}}[\Gamma_0(2N)\colon\Gamma_0(q)]$. Summing both sides over $Q<q\leq Q$ with $q\equiv 2 \bmod N$ we get

$$\begin{aligned} &m(Q)m^{-\frac{k}{2}+1}|a_f(m;\infty)|^2 \\ &\qquad\qquad \leq C_k\left(Q+\sum_{Q<q\leq 2Q}\sum_{r=1}^{\infty}(rq)^{-1}\left|S_{\vartheta_{\mathrm{th}}}(m,m,rq)J_{\frac{k}{2}-1}\left(\frac{4\pi m}{rq}\right)\right|\right).\end{aligned}$$

We break the r-sum up into dyadic pieces $R<r\leq 2R$. Using the estimate (85) we get

$$\sum_{Q<q\leq 2Q}\sum_{r=1}^{\infty}(rq)^{-1}\left|S_{\vartheta_{\mathrm{th}}}(m,m,rq)J_{\frac{k}{2}-1}\left(\frac{4\pi m}{rq}\right)\right| \leq Q+\min\left(\frac{(RQ)^{\frac{1}{2}}}{m^{\frac{1}{2}}},\frac{m}{QR}\right)\mathcal{D}(Q,R).$$

This can be effectively bounded using our Kloosterman sum estimate (90) above. The worst case for the resulting inequality appears to be $R=mQ^{-1}$. Thus we get the bound

$$m(Q)m^{-\frac{k}{2}+1}|a_f(m;\infty)|^2 \leq C_{k,\epsilon}(Q+mQ^{-1})m^{\epsilon}.$$

Choosing $Q=m^{\frac{1}{2}}$ and observing that $m(Q)$ is bounded from below yields the desired result. ◻

Remark 4.2.3. The theorem above is only half of the truth. Indeed it is conjectured that the better bound

$$|a_f(m;\infty)| \leq C_{f,\epsilon}\cdot m^{\frac{k}{2}-\frac{1}{2}+\epsilon}, \tag{91}$$

holds for all $f\in S_{\frac{k}{2}}(\Gamma_0(2N),\vartheta_{\mathrm{th}})$ with $k\geq 1$ that are not contained in a certain subspace of theta functions.[34] If k is even, then this actually follows from a deep result due to Deligne resolving the Ramanujan Petersson conjecture for integral weight modular forms.

4.3. **Representation numbers and equidistribution.** We are now ready to apply the theory that was developed in this section to quadratic forms. The first application concerns representation numbers of quadratic forms:

[34]For these theta functions the bound is known to be false, but they can only exist for odd k (i.e. $k/2\notin\mathbb{Z}$).

Theorem 4.3.1. *Let Q_A be a positive definite integral quadratic form in $k \geq 5$ variables (i.e. $A \in \mathcal{SP}_k$). Then we have*

$$r(n, Q_A) = \frac{(2\pi)^{\frac{k}{2}} n^{\frac{k}{2}-1}}{\Gamma(k/2)\sqrt{\det(A)}} \cdot \prod_p \delta_p(n, A) + O_{f,\epsilon}(n^{\frac{k}{4}-\frac{1}{4}+\epsilon}).$$

Proof. We consider the theta series $\theta_{1,Q_A}(z) \in M_{\frac{k}{2}}(\Gamma_0(2N_A), \vartheta_{\mathrm{th}})$ write it as

$$\theta_{1,Q_A}(z) = E_{Q_A}(z) + F_{Q_A}(z).$$

According to Siegel's Theorem (i.e. Theorem 4.1.13) we have $E_{Q_A}(z) = \theta_{\mathrm{gen}(Q_A)}(z)$. Thus, by comparing Fourier coefficients at infinity we have

$$r(n, Q_A) = r(n, \mathrm{gen}(Q_A)) + a_{F_{Q_A}}(n; \infty).$$

Since $F_{Q_A}(z) \in S_{\frac{k}{2}}(\Gamma_0(2N_A), \vartheta_{\mathrm{th}})$ and $k \geq 5$ we can use the bound (87) to obtain

$$r(n, Q_A) = r(n, \mathrm{gen}(Q_A)) + O_{n,\epsilon}(n^{\frac{k}{4}-\frac{1}{4}+\epsilon}).$$

We conclude by applying Theorem 4.1.6 to write

$$r(n, \mathrm{gen}(Q_A)) = \delta_\infty(n, A) \cdot \prod_p \delta_p(n, A).$$

Recall that according to (69) we have $\delta_\infty(n, A) = \frac{(2\pi)^{\frac{k}{2}} n^{\frac{k}{2}-1}}{\Gamma(k/2)\sqrt{\det(A)}}$. ◻

Some comments are in order. First, note that the same result can be obtained using the circle method. Second, if k is even, then a better error term can be achieved using the stronger bound (91) for the Fourier coefficients of cusp forms. Finally, the result is only meaningful if the local densities $\delta_p(n, A)$ are sufficiently well understood. In the setting of the theorem above this is no problem. Indeed, it can be shown that for $k \geq 5$ one has

$$C_A \leq \prod_p \delta_p(n, A) \leq C'_A \text{ for } C_A, C'_A > 0 \tag{92}$$

as long there is $\mathbf{x} \in \mathbb{Z}^k$ such that

$$Q_A(\mathbf{x}) \equiv n \bmod 2^7 \det(A)^3.$$

Before moving on we will briefly comment on quadratic forms in few variables:

- If $k = 2$, then the approach above would naturally lead to the study of modular forms of weight one. However, the product of local densities does not converge absolutely in this case. More classically this case can be approached using the connection between positive definite binary quadratic forms and class numbers of imaginary quadratic fields.

- The case $k = 3$ is very interesting but also very complicated. On the algebraic side it becomes necessary to introduce the so called spinor genus. Similarly the analytic theory has its complications. A detailed discussion would ge beyond the scope of these notes.
- If $k = 4$ everything works essentially as above. The only difference is that we can not apply (87) directly. Instead, since 4 is obviously even, one can use the Ramanujan type bound (91). (For weight $2 = \frac{4}{2}$ this estimate was actually established before Deligne by Eichler precisely for this purpose.) Finally, also the treatment of $\delta_2(n, A)$ is slightly more complicated.

We come to our second application. The goal is to show that the integral solutions to $Q_A(\mathbf{x}) = n$ are distributed in the ellipsoid

$$\mathcal{E}_A(n) = \{\mathbf{x} \in \mathbb{R}^k \colon Q_A(\mathbf{x}) = n\}.$$

We abbreviate $\mathcal{E}_A(1) = \mathcal{E}_A$. Given a (sufficiently nice) domain $\Omega \subseteq \mathcal{E}_A$ we consider

$$r_\Omega(n, Q_A) = \sharp\{\mathbf{x} \in \mathbb{Z}^k \colon Q_A(\mathbf{x}) = n \text{ and } \frac{\mathbf{x}}{\sqrt{n}} \in \Omega\}.$$

If n runs through a sequence of integers n with $r(n, Q) \neq 0$, then one expects that

$$r_\Omega(n, Q_A) \sim \mathrm{Vol}(\Omega) \cdot r(n, Q).$$

In this situation we say that the integral points on $Q(\mathbf{x}) = n$ are equidistributed with respect to the invariant measure on $\mathcal{E}_A$.

Theorem 4.3.2. *Let Q_A be a positive definite integral quadratic form in $k \geq 5$ variables (i.e. $A \in \mathcal{SP}_k$). Let $n \to \infty$ run through a sequence of integers such that the congruence*

$$Q_A(\mathbf{x}) \equiv n \ mod\ 2^7 \det(A)^3 \tag{93}$$

has a solution $\mathbf{x} \in \mathbb{Z}^k$. Then the integral points on $Q(\mathbf{x}) = n$ are equidistributed with respect to the invariant measure on $\mathcal{E}_A$. We even have the quantitative statement

$$r_\Omega(n, Q_A) = \mathrm{Vol}(\Omega) \cdot r(n, Q) + O_{Q_A,\Omega,\epsilon}(n^{\frac{k-1}{4}+\epsilon}) \tag{94}$$

where the error term is significantly smaller than the main term.

Proof. We start by observing that it suffices to consider

$$r_f(n, Q_A) = \sum_{Q_A(\mathbf{x})=n} f(\frac{m}{\sqrt{n}}) \text{ for } f \in \mathcal{C}^\infty(\mathcal{E}_A)$$

instead of $r_\Omega(n, Q_A)$. This is a standard approximation argument. Furthermore, since the functions

$$\{\mathbf{x} \mapsto P_l(A\mathbf{x}) \colon P_l \text{ harmonic polynomial of degree } l\} \tag{95}$$

form a complete orthogonal system in $L^2(\mathcal{E}_A)$ it suffices to consider $r_f(n, Q_A)$ for such f.

We first treat the case when f is the constant function (i.e. $f(\mathbf{x}) = 1$). In this case we obviously have

$$r_f(n, Q_A) = r(n, Q_A)$$

and there is nothing to do.

Second, if $f(\mathbf{x}) = P_l(A\mathbf{x})$ for $l \geq 1$, then $n^{\frac{l}{2}} r_f(n, Q_A)$ is the Fourier coefficient of $\theta_{P_l,Q_A}(z) \in S_{\frac{k}{2}+l}(\Gamma_0(2N_A), \vartheta_{\text{th}})$. In particular, applying (87) gives

$$r_f(n, Q_A) = O_{f,Q_A,\epsilon}(n^{\frac{k}{4}-\frac{1}{4}+\epsilon})$$

in this case.

The two cases considered above give (94). To see that the main term is really a main term we recall that

$$r(n, Q_A) = \delta_\infty(n, A) \cdot \prod_p \delta_p(n, A) + O_{Q_A,\epsilon}(n^{\frac{k}{4}-\frac{1}{4}+\epsilon}).$$

According to our assumption (93) the product of local densities is bounded from below by $C_A \cdot n^{\frac{k}{2}-1}$. Since $k \geq 5$ the latter is significantly bigger than the error term. ◻

The assumption $k \geq 5$ can be easily relaxed to include the case $k = 4$. The case $k = 3$ on the other hand is way more complicated. Here a version of the equidistribution statement remains true, but it is a deep theorem due to Duke.

5. Satz III: Hecke Operators

In many ways Hecke operators are the bridge between arithmetic and (complex) analysis. A modern theory of modular forms without Hecke operators is unthinkable.

Part of Hecke's motivation to introduce these operators comes from the general question which we will explain now.[35] Given a sequence $(a_n)_{n\in\mathbb{N}}$ of interesting numbers (for example $a_n = r(n, Q_A)$ with $A \in \mathcal{SP}_k$) we can do two natural[36] things. First, we can associate the Dirichlet series

$$D(s) = \sum_{n\in\mathbb{N}} \frac{a_n}{n^s}.$$

Under some mild growth conditions on the numbers a_n this will converge in some right half plane and define a holomorphic function there. Second, we can associate

$$f(z) = \sum_{n=1}^{\infty} a_n e(nz).$$

[35] This is of course my own interpretation of what Hecke wrote. Unfortunately I do not really know what Hecke was thinking.

[36] At least from the point of view of an analytic number theorist such as Hecke.

Again this defines a function on $\mathbb{H}$ as soon as the numbers a_n are well behaved.[37] Formally, ignoring convergence issues for now, we can relate these two objects by taking the Mellin transform

$$[\mathfrak{M}f](s) = \int_0^\infty f(iy)y^s \frac{dy}{y} = \sum_{n=1}^\infty a_n \int_0^\infty e^{-2\pi n y} y^{s-1} dy = (2\pi)^{-s}\Gamma(s)D(s).$$

Thus morally $f(z)$ and $D(s)$ are two sides of the same coin. In particular, properties of f should be reflected by corresponding properties of D and vice versa.

Of special interest are Dirichlet series with Euler product:

$$D(s) = \sum_{p \text{ prime}} \sum_{k=1}^\infty a_{p^k} p^{-ks}.$$

Such a product representations holds (in the region of absolute convergence) precisely when $a_{nm} = a_n a_m$ for $(n,m) = 1$ (i.e. when the coefficients a_n are multiplicative). Examples are given by

- If $a_n = 1$ for all $n \in \mathbb{N}$, then the corresponding Dirichlet series is precisely the Riemann zeta function $D(s) = \zeta(s)$ with the product representation

  $$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} \text{ for } \operatorname{Re}(s) > 1,$$

  which is the mother of all Euler products.
- If $a_n = \frac{1}{8} r_4(n)$, then

$$\begin{aligned} D(s) = \frac{1}{8} \sum_{n=1}^\infty r_4(n) n^{-1} &= \sum_{n=1}^\infty \sigma_1(n) n^{-s} - \sum_{n=1}^\infty \sigma_1(n)(4n)^{-s} \\ = (1 - 4^{1-s})\zeta(s)\zeta(1-s) &= \frac{1+2^{1-s}}{1-2^{-s}} \cdot \prod_{p \text{ odd prime}} (1 - (1+p)p^{-s} + pp^{-2s})^{-1} \\ &\qquad \text{for } \operatorname{Re}(s) > 2 \end{aligned}$$

  where we used Jacobi's Four Square Theorem.
- For arbitrary $A \in \mathcal{SP}_k$ and $a_n = r(n, Q_A)$ there is **no** reason to expect that $D(s)$ has an Euler Product.

In general we would like to decompose a Dirichlet series $D(s)$ into pieces with Euler product:

$$D(s) = b_1 D_1(s) + \ldots + b_r D_r(s), \tag{96}$$

where $D_i(s)$ are associated to multiplicative sequences $(a_n^{(i)})_{n \in \mathbb{N}}$. Even more, we would like to do this by decomposing $f(z)$ in a *purely function theoretic way*. This

[37] Note that for general a_n there is no reason to expect that this is actually (related to) a modular form. But in our example $a_n = r(n, Q)$ we have $f(z) = \theta_{1,Q}(z) - 1$.

goal is achieved by the theory of Hecke Operators as soon as the sequence a_n can be described via Fourier coefficients of modular forms.[38]

We now give a basic example where the decomposition (96) of $D(s)$ is classically well known. Re-interpreting this decomposition on the function theoretic side (i.e. for $f(z)$) will lead us to some very suggestive operators.

Let $D < -4$ be a fundamental discriminant (i.e. $D \equiv 1 \bmod 4$ square-free or $D = 4D'$ with $D' \equiv 2, 3 \bmod 4$ square-free). Then D is the discriminant of the imaginary quadratic number field $K = \mathbb{Q}(\sqrt{D})$. Let $\mathcal{O}_K$ be the ring of integers in K. Since we are assuming $D < -4$ we have $\sharp\mathcal{O}_K^\times = \{\pm 1\}$. We denote the ideal class group of K by $\mathcal{C}_K$. This is a finite abelian group and we define the class number of K by $h_K = \sharp\mathcal{C}_K$. Given an integral ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ we write $[\mathfrak{a}]$ for the corresponding class in $\mathcal{C}_K$.

The Dedekind zeta function of K is defined as

$$\zeta_K(s) = \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} [\sharp\mathcal{O}_K/\mathfrak{a}]^{-s} = \sum_{n=1}^{\infty} \underbrace{\sharp\{\mathfrak{a} \subseteq \mathcal{O}_K \colon \sharp\mathcal{O}_K/\mathfrak{a} = n\}}_{=a_K(n)} n^{-s}.$$

It makes sense to consider the partial zeta functions

$$\zeta_K(s, [\mathfrak{b}]) = \sum_{\substack{\mathfrak{a}\subseteq\mathcal{O}_K,\\ [\mathfrak{a}]=[\mathfrak{b}]}} [\sharp\mathcal{O}_K/\mathfrak{a}]^{-s} = \sum_{n=1}^{\infty} \underbrace{\sharp\{\mathfrak{a} \subseteq \mathcal{O}_K \colon \sharp\mathcal{O}_K/\mathfrak{a} = n,\ [\mathfrak{a}] = [\mathfrak{b}]\}}_{=a_K(n,[\mathfrak{b}])} n^{-s}.$$

Of course we have $\zeta_K(s) = \sum_{[\mathfrak{b}]\in\mathcal{C}_K} \zeta_K(s, [\mathfrak{b}])$. All these zeta functions are holomorphic in some right half plane and posses a meromorphic continuation to the complex plane. While $\zeta_K(s)$ has an Euler Product similar to the one of the Riemann Zeta Function, the partial zeta functions are not eulerian in general.

To each ideal class $[\mathfrak{a}] \in \mathcal{C}_K$ we can associate a integral positive definite binary quadratic form

$$Q_{\mathfrak{a}}(x, y) = \frac{\mathrm{Nr}_{K|\mathbb{Q}}(\alpha x + \beta y)}{\sharp\mathcal{O}_K/\mathfrak{a}} \text{ where } \mathfrak{a} = \mathbb{Z}\alpha + \mathbb{Z}\beta$$

of discriminant D. Similarly we can take an integral positive definite binary quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ of discriminant D and associate the ideal class $[\mathfrak{a}_Q] \in \mathcal{C}_K$ given by

$$\mathfrak{a}_Q = \mathbb{Z} + \frac{b + \sqrt{D}}{2a} \cdot \mathbb{Z}.$$

This gives us a bijection between the ideal class group $\mathcal{C}_K$ of K and the set of equivalence classes of positive definite integral binary quadratic forms of discriminant D. Under this correspondence we have

$$r(n, Q) = 2 \cdot a_K(n, [\mathfrak{a}_Q]).$$

[38] Of course such sequences a_n form only a small sample of all interesting sequences, but a sufficiently interesting one.

In particular, if $D_Q(s)$ denotes the Dirichlet series associated to the sequence $(\frac{1}{2}r(n,Q))_{n\in\mathbb{N}}$, then we have

$$D_Q(s) = \zeta_K(s, [\mathfrak{a}_Q]).$$

On the other hand, we have

$$f_Q(z) = \frac{1}{2} + \frac{1}{2}\sum_{n\in\mathbb{N}} r(n,Q)e(nz) = \frac{1}{2}\cdot\theta_{1,Q}(z) \in M_1(\Gamma_0(D), \chi_D).$$

On the level of Dirichlet series it is well known how to expand the partial zeta functions into Dirichlet Series with Euler Product. To do so we take a character $\chi \in \widehat{\mathcal{C}_K}$ (i.e. a homomorphism $\chi\colon \mathcal{C}_K \to S^1$) and associate

$$D_\chi(s) = \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \chi([\mathfrak{a}])(\sharp\mathcal{O}_K/\mathfrak{a})^{-s}.$$

(One could also write $D_\chi(s) = \zeta_K(s,\chi)$, but non of this is standard notation!) Using elementary facts on the splitting behavior of primes in the extension $K|\mathbb{Q}$ one obtains the Euler Product

$$D_\chi(s) = \prod_{p \text{ prime}} (1 - \lambda_\chi(p)p^{-s} + \chi_D(p)p^{-2s})^{-1},$$

with

$$\lambda_\chi(p) = \begin{cases} \chi([\mathfrak{p}]) + \chi(\mathfrak{p})^{-1} & \text{if } (p)_{\mathcal{O}_K} = \mathfrak{p}\cdot\mathfrak{p}', \\ 0 & \text{if } (p)_{\mathcal{O}_K} = \mathfrak{p} \text{ and} \\ \chi(\mathfrak{p}) & \text{if } (p)_{\mathcal{O}_K} = \mathfrak{p}^2. \end{cases}$$

Note that the functions $D_\chi(s)$ also have a meromorphic continuation and satisfy a functional equation. In particular, if $\chi = \mathbf{1}$ is the trivial character, then we have $D_{\mathbf{1}}(s) = \zeta_K(s)$.

Using character orthogonality we write

$$D_Q(s) = \frac{1}{h_K}\sum_{\chi\in\widehat{\mathcal{C}_K}} \chi([\mathfrak{a}]_Q)^{-1} D_\chi(s).$$

This achieves our goal to decompose D_Q into eulerian Dirichlet Series. But the procedure is somehow unsatisfying because in general there will be no (abelian) group like $\mathcal{C}_K$ in the background that allows us to play this trick. Thus we will take a closer look at what happens on the modular side. We define the functions

$$f_\chi(z) = \frac{h}{2}\delta_{\chi=\mathbf{1}} + \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \chi([\mathfrak{a}])e(\sharp\mathcal{O}_K/\mathfrak{a}\cdot z).$$

These are of course precisely the functions on $\mathbb{H}$ that correspond to the Dirichlet series D_χ with Euler Product! Then we have $f_\chi(z) \in M_1(\Gamma_0(D), \chi_D)$. Indeed we can compute

$$f_\chi(z) = \sum_{[\mathfrak{b}]\in\mathcal{C}_K} \chi([\mathfrak{b}])\zeta_K(s,[\mathfrak{b}]) = \sum_{[\mathfrak{a}_Q]\in\mathcal{C}_K} \chi([\mathfrak{a}_Q]) f_Q(z).$$

This shows that $f_\chi(z)$ is a linear combination of the classical theta functions $f_Q(z) = \frac{1}{2}\theta_{1,Q}(z)$. Of course we also have

$$f_Q(z) = \frac{1}{h}\sum_{\chi\in\widehat{\mathcal{C}_K}} \chi([\mathfrak{a}_Q])^{-1} f_\chi(z).$$

For a (rational) prime p with $(p)_{\mathcal{O}_K} = \mathfrak{p}\cdot\mathfrak{p}'$ we make the following ad-hoc[39] observation:

$$\begin{aligned}\sum_{\substack{\mathfrak{a}\subseteq\mathcal{O}_K,\\ [\mathfrak{a}]=[\mathfrak{b}]\\ \sharp\mathcal{O}_K/\mathfrak{a}\equiv 0 \bmod p}} (\sharp\mathcal{O}_K/\mathfrak{a})^{-s} &= \sum_{\substack{\mathfrak{a}\subseteq\mathcal{O}_K,\\ [\mathfrak{a}]=[\mathfrak{b}]\\ \mathfrak{p}\mid\mathfrak{a}}} (\sharp\mathcal{O}_K/\mathfrak{a})^{-s} + \sum_{\substack{\mathfrak{a}\subseteq\mathcal{O}_K,\\ [\mathfrak{a}]=[\mathfrak{b}]\\ \mathfrak{p}'\mid\mathfrak{a}}} (\sharp\mathcal{O}_K/\mathfrak{a})^{-s} - \sum_{\substack{\mathfrak{a}\subseteq\mathcal{O}_K,\\ [\mathfrak{a}]=[\mathfrak{b}]\\ (p)_{\mathcal{O}_K}\mid\mathfrak{a}}} (\sharp\mathcal{O}_K/\mathfrak{a})^{-s}\\ &= p^{-s}\zeta_K(s,[\mathfrak{b}\mathfrak{p}]) + p^{-s}\zeta_K(s,[\mathfrak{b}\mathfrak{p}']) - p^{-2s}\zeta_K(s,[\mathfrak{b}]).\end{aligned}$$

Rewriting this (and treating the cases $(p)_{\mathcal{O}_K} = \mathfrak{p}$ and $(p)_{\mathcal{O}_K} = \mathfrak{p}^2$ similarly) yields

$$\begin{aligned}&\chi_D(p)p^{-s}\zeta_K(s,[\mathfrak{b}]) + p^s \sum_{\substack{\mathfrak{a}\subseteq\mathcal{O}_K,\\ [\mathfrak{a}]=[\mathfrak{b}]\\ \sharp\mathcal{O}_K/\mathfrak{a}\equiv 0 \bmod p}} (\sharp\mathcal{O}_K/\mathfrak{a})^{-s}\\ &\qquad = \begin{cases} \zeta_K(s,[\mathfrak{b}\mathfrak{p}]) + \zeta_K(s,[\mathfrak{b}\mathfrak{p}']) & \text{if } (p)_{\mathcal{O}_K} = \mathfrak{p}\mathfrak{p}',\\ 0 & \text{if } (p)_{\mathcal{O}_K} = \mathfrak{p} \text{ and}\\ \zeta_K(s,[\mathfrak{b}\mathfrak{p}]) & \text{if } (p)_{\mathcal{O}_K} = \mathfrak{p}^2.\end{cases}\end{aligned} \tag{97}$$

Write $\mathfrak{b} = \mathfrak{a}_Q$. Note that the left hand side of (97) consists only of data *that is known* by f_Q. Thus we would like to interpret it as the Fourier coefficient of a function associated to f_Q. To do se we first write

$$\begin{aligned}&\chi_D(p)p^{-s}\zeta_K(s,[\mathfrak{b}]) + p^s \sum_{\substack{\mathfrak{a}\subseteq\mathcal{O}_K,\\ [\mathfrak{a}]=[\mathfrak{b}]\\ \sharp\mathcal{O}_K/\mathfrak{a}\equiv 0 \bmod p}} (\sharp\mathcal{O}_K/\mathfrak{a})^{-s}\\ &\qquad = \sum_{n=1}^{\infty} \left(\chi_D(p)\delta_{p\mid n} a_K(n/p,[\mathfrak{a}_Q]) + a_K(pn,[\mathfrak{a}_Q])\right) n^{-s}\\ &\qquad = \frac{\chi_D(p)}{2}\sum_{n=1}^{\infty}\delta_{p\mid n} r(n,Q)n^{-s} + \frac{1}{2p}\sum_{l=0}^{p-1}\sum_{n=1}^{\infty} e(\frac{nl}{p}) r(n,Q)(n/p)^{-s}.\end{aligned}$$

[39]Recall that we are trying do decompose the Dirichlet series $\zeta(s,[\mathfrak{b}])$ into pieces with Euler product. Thus it makes sense to test how this function changes when a divisibility condition is introduced.

The coefficients of the Dirichlet series in the last line are easily recognized as the Fourier coefficients of

$$[T_p f_Q](z) := \chi_D(p) f_Q(pz) + \frac{1}{p}\sum_{l=0}^{p-1} f\left(\frac{z+l}{p}\right).$$

If we now also set $\mathfrak{b}\mathfrak{p} = \mathfrak{a}_{Q_1}$ and $\mathfrak{b}\mathfrak{p}' = \mathfrak{a}_{Q_2}$, then (97) translates into

$$[T_p f_Q](z) = \begin{cases} f_{Q_1}(z) + f_{Q_2}(z) & \text{if } (p)\mathcal{O}_K = \mathfrak{p}\mathfrak{p}', \\ 0 & \text{if } (p)\mathcal{O}_K = \mathfrak{p} \text{ and} \\ f_{Q_1}(z) & \text{if } (p)\mathcal{O}_K = \mathfrak{p}^2. \end{cases}$$

In particular the operator T_p acts on the space

$$T(D) = \langle f_Q \colon Q \text{ with discriminant } D\rangle_{\mathbb{C}} \subseteq M_1(\Gamma_0(D), \chi_D).$$

It turns out that the functions $\{f_\chi \colon \chi \in \widehat{\mathcal{C}_K}\}$ form a basis of $T(D)$. Even more the functions f_χ are eigenfunctions of all the operators T_p:

$$[T_p f_\chi](z) = \lambda_\chi(p) \cdot f_\chi(z).$$

Therefore, we recover the functions f_χ, which correspond to the eulerian Dirichlet series D_χ, by simultaneously diagonalizing the family $\{T_p \colon p \text{ prime}\}$ of linear operators on $T(D)$. Note that the operators T_p are ultimately defined without any reference to binary quadratic forms (or ideal classes). Thus they are purely function theoretic objects. In particular they provide us with a more satisfying *explanation* of the decomposition (96) for D_Q, which might generalize beyond the example of binary quadratic forms.

In general we **guess** that the operators T_p for $(p, N) = 1$ defined by

$$[T_p f](z) = p^{k-1}\chi(p) f(pz) + \frac{1}{p}\sum_{l=0}^{p-1} f\left(\frac{z+l}{p}\right) \tag{98}$$

define a nice family of (linear) operators on $S_k(\Gamma_0(N), \chi)$. Here $k, N \in \mathbb{N}$ and χ is a Dirichlet character modulo N. We will now develop a general theory of Hecke operators to make this more precise.

5.1. **Double co-sets and Hecke algebras.** We start with some general definitions and observations. Throughout this section G is a general group (but we can keep $G = \mathrm{GL}_2^+(\mathbb{R}) = \{g \in \mathrm{GL}_2(\mathbb{R}) \colon \det(g) > 0\}$ in the back of our head).

Definition 5.1.1. Let G be a group with two subgroups $\Gamma_1, \Gamma_2 \subseteq G$. Then Γ_1 and Γ_2 are said to be commensurable if

$$[\Gamma_1 \colon \Gamma_1 \cap \Gamma_2] < \infty \text{ and } [\Gamma_2 \colon \Gamma_1 \cap \Gamma_2] < \infty.$$

We write $\Gamma_1 \sim \Gamma_2$.

It can be seen that the relation $\Gamma_1 \sim \Gamma_2$ defines an equivalence relation on subgroups of G.

Definition 5.1.2. For a subgroup $\Gamma \subseteq G$ of a group G we define the commensurator $\widetilde{\Gamma}$ of Γ in G by

$$\widetilde{\Gamma} = \{g \in G \colon g\Gamma g^{-1} \text{ is commensurable with } \Gamma\}.$$

The commensurator $\widetilde{\Gamma}$ of a subgroup Γ turns out to be a subgroup of G. Note that $\widetilde{\Gamma}$ heavily depends on the ambient group G. One can also see that $\Gamma_1 \sim \Gamma_2$ implies $\widetilde{\Gamma}_1 = \widetilde{\Gamma}_2$.

Example 5.1.1. If $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup and $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, then Γ and $\alpha^{-1}\Gamma\alpha$ are commensurable.

Proof. Since Γ is a congruence subgroup there is q such that

$$\Gamma(q) = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})) \subseteq \Gamma.$$

It suffices to show that there is q' such that $\Gamma(q') \subseteq \alpha^{-1}\Gamma\alpha$. Indeed this implies that $\Gamma(qq') \subseteq \Gamma \cap \alpha^{-1}\Gamma\alpha$ and $\Gamma(qq')$ has finite index in Γ and $\alpha^{-1}\Gamma\alpha$.

To see the claim we can take q' such that $q'\alpha^{-1}\tau\alpha \in \mathrm{Mat}_{2\times 2}(q\mathbb{Z})$ for all $\tau \in \mathrm{Mat}_{2\times 2}(\mathbb{Z})$. Then $\alpha\Gamma(q')\alpha^{-1} \subseteq \Gamma(q) \subseteq \Gamma$ so that $\Gamma(q') \subseteq \alpha^{-1}\Gamma\alpha$. ◻

Exercise 3, Sheet 9: Let G be a group. For two subgroups Γ_1, Γ_2 recall what it means for Γ_1 and Γ_2 to be commensurable. Further, recall the definition of the commensurator $\tilde{\Gamma}_1$ of Γ_1 in G.

a) Show that being commensurable defines an equivalence relation on subgroups of G.
b) Let $\Gamma \subset G$ be a subgroup. Show that $\tilde{\Gamma}$, the commensurator of Γ in G, is a subgroup of G.
c) Let $G = \mathrm{GL}_2^+(\mathbb{R})$ and let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Compute the commensurator of Γ in G.

Solution. For a), the only nontrivial part is transitivity. That is, if $\Gamma_1 \sim \Gamma_2$ and $\Gamma_2 \sim \Gamma_3$ then we need to show that $\Gamma_1 \sim \Gamma_3$. The assumptions are that $\Gamma_1 \cap \Gamma_2 \backslash \Gamma_1$, $\Gamma_1 \cap \Gamma_2 \backslash \Gamma_2$, $\Gamma_2 \cap \Gamma_3 \backslash \Gamma_2$ and $\Gamma_2 \cap \Gamma_3 \backslash \Gamma_3$ are finite sets. We claim that the natural inclusion $\Gamma_1 \cap \Gamma_2 \hookrightarrow \Gamma_2$ induces an injection

$$\Gamma_1 \cap \Gamma_2 \cap \Gamma_3 \backslash \Gamma_1 \cap \Gamma_2 \hookrightarrow \Gamma_2 \cap \Gamma_3 \backslash \Gamma_2.$$

Indeed, if $\gamma_1, \gamma_2 \in \Gamma_1 \cap \Gamma_2$ satisfy $\gamma_1\gamma_2^{-1} \in \Gamma_2 \cap \Gamma_3$, then automatically, $\gamma_1\gamma_2^{-1} \in \Gamma_1 \cap \Gamma_2 \cap \Gamma_3$ from which $\Gamma_1 \cap \Gamma_2 \cap \Gamma_3\gamma_1 = \Gamma_1 \cap \Gamma_2 \cap \Gamma_3\gamma_2$. We also need the observation that, if $K \subset H$ is finite index and $H \subset G$ is also finite index, then $K \subset G$ is finite index. This follows by considering $H = \bigsqcup Kh_i$ and $G = \bigsqcup Hg_j$ and noticing that $G = \bigsqcup Kh_ig_j$, so that in fact $[K : G] = [K : H][H : G]$. Putting together the two observations, we get that $\Gamma_1 \cap \Gamma_2 \cap \Gamma_3$ is of finite index in Γ_1 as well as in Γ_3, which means that $\Gamma_1 \sim \Gamma_3$, as desired.

For part b), we employ the following observation: if H is finite index in G and $\theta : G \to \theta(G)$ is an isomorphism, then $\theta(H)$ is finite index in $\theta(G)$. As a consequence, if $\Gamma_1 \sim \Gamma_2$ and θ is an automorphism of G, then $\theta(\Gamma_1) \sim \theta(\Gamma_2)$. Let $g \in \tilde{\Gamma}$. Then $g\Gamma g^{-1} \cap \Gamma$ is a subgroup of finite index in both Γ and $g\Gamma g^{-1}$. Applying the automorphism $x \mapsto g^{-1}xg$, we obtain that $\Gamma \cap g^{-1}\Gamma g$ is of finite index in both $g^{-1}\Gamma g$ and Γ, showing that $g \in \tilde{\Gamma}$ iff $g^{-1} \in \tilde{\Gamma}$. Also, if $g_1, g_2 \in \tilde{\Gamma}$, then $\Gamma \sim g_1\Gamma g_1^{-1}$ and $\Gamma \sim g_2\Gamma g_2^{-1}$. Applying $x \mapsto g_1xg_1^{-1}$ to this last equivalence, we obtain $g_1\Gamma g_1^{-1} \sim g_1g_2\Gamma g_2^{-1}g_1^{-1}$. By transitivity, we arrive at $\Gamma \sim g_1g_2\Gamma g_2^{-1}g_1^{-1}$, that is, $g_1g_2 \in \tilde{\Gamma}$.

For part c), we show that $\tilde{\Gamma} = Z(G)\,\mathrm{GL}_2^+(\mathbb{Q})$, where $Z(G)$ is the subgroup of real valued scalar matrices. It is shown in example 5.1.1 of the lectures that $\mathrm{GL}_2^+(\mathbb{Q}) \subset \tilde{\Gamma}$, and it is clear that $Z(G) \subset \tilde{\Gamma}$ as well, since conjugating by a scalar matrix leaves every matrix fixed. For the opposite direction, assume that $g \in \tilde{\Gamma}$. We will show that $gM_2(\mathbb{Q})g^{-1} = M_2(\mathbb{Q})$.

We need the following observation: if $H \subset \Gamma = \mathrm{SL}_2(\mathbb{Z})$ is of finite index, then $\mathbb{Q}[H] = \mathbb{Q}[\Gamma] = M_2(\mathbb{Q})$, where we write $\mathbb{Q}[H]$ for the subalgebra of $M_2(\mathbb{C})$ generated by the elements of H over $\mathbb{Q}$. Indeed, suppose $H \subset \Gamma$ is of finite index and let $g \in \Gamma$. We have an induced action on cosets $H\gamma \mapsto H\gamma g$, and since the set of cosets is finite, there is a power of g that acts like the identity, say g^N. In particular, $Hg^N = H$, so that $g^N \in H$. Letting $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ respectively, we see that there are positive integers N, M such that

$$T^N = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in H \quad \text{and} \quad U^M = \begin{pmatrix} 1 & 0 \\ M & 1 \end{pmatrix} \in H$$

Considering $T^N - U^M = Ne_{1,2} - Me_{2,1}$ and also $T^N - U^{-M} = Ne_{1,2} + Me_{2,1}$, we deduce that $e_{1,2}, e_{2,1} \in \mathbb{Q}[H]$. Also, we have

$$T^NU^M = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ M & 1 \end{pmatrix} = \begin{pmatrix} 1+NM & N \\ M & 1 \end{pmatrix} \in H$$

and therefore $\mathrm{diag}(1+NM, 1) \in \mathbb{Q}[H]$. Similarly, $\mathrm{diag}(1, 1+NM) \in \mathbb{Q}[H]$, from which it follows that $e_{1,1}, e_{2,2} \in \mathbb{Q}[H]$. Putting all together, we have proved that $\mathbb{Q}[H] = \mathbb{Q}[\Gamma] = M_2(\mathbb{Q})$.

Now, consider $g \in \tilde{\Gamma}$. We know that $g\Gamma g^{-1} \cap \Gamma$ is a finite index subgroup of Γ and of $g\Gamma g^{-1}$. From the first fact, we deduce that $\mathbb{Q}[g\Gamma g^{-1} \cap \Gamma] = M_2(\mathbb{Q})$. After applying $x \mapsto g^{-1}xg$, since $g^{-1}\left(g\Gamma g^{-1} \cap \Gamma\right) g$ is of finite index in Γ as well, we have $\mathbb{Q}[g^{-1}\left(g\Gamma g^{-1} \cap \Gamma\right) g] = M_2(\mathbb{Q})$. But since $g^{-1}\mathbb{Q}[H]g = \mathbb{Q}[g^{-1}Hg]$ for any subgroup $H \subset G$, we deduce that $g^{-1}M_2(\mathbb{Q})g = M_2(\mathbb{Q})$, as desired.

Finally, using that $ge_{1,1}g^{-1}, ge_{1,2}g^{-1}, ge_{2,1}g^{-1}$ and $ge_{2,2}g^{-1}$ are all in $M_2(\mathbb{Q})$, we obtain $x_ix_j/\det(g) \in \mathbb{Q}$, for any choice $x_i, x_j \in \{a,b,c,d\}$, the entries of g. After dividing each entry by the square root of the determinant we can assume that $\det(g) \in \mathbb{Q}$, so $x_ix_j \in \mathbb{Q}$ for any choice $x_i, x_j \in \{a,b,c,d\}$. Suppose, for example, that $a \neq 0$. Then after multiplying g by a we arrive at a matrix with rational entries, as desired. ∎

Lemma 5.1.2. *Let $\Gamma_1, \Gamma_2 \subseteq G$ be two commensurable subgroup of a group, let $\alpha \in \widetilde{\Gamma}_1$ (i.e. Γ and $\alpha^{-1}\Gamma\alpha$ are commensurable). Then we can write*

$$\Gamma_1\alpha\Gamma_2 = \bigsqcup_{i=1}^{r} \Gamma_2\alpha\gamma_i = \bigsqcup_{j=1}^{s} \delta_j\alpha\Gamma_2,$$

where $(\gamma_i)_{i=1,\ldots,r}$ (resp. $(\delta_j)_{j=1,\ldots,s}$) is a full set of representatives for $(\Gamma_2 \cap \alpha^{-1}\Gamma_1\alpha)\backslash\Gamma_2$ (resp. $\Gamma_1/(\Gamma_1 \cap \alpha^{-1}\Gamma_2\alpha)$).

Proof. This is elementary. One first notes that each right coset of Γ_1 in $\Gamma_1\alpha\Gamma_2$ can be written as

$$\Gamma_1\alpha\gamma \subseteq \Gamma_1\alpha\Gamma_2 \text{ for } \gamma \in \Gamma_2.$$

Now $\Gamma_1\alpha\gamma = \Gamma_1\alpha\gamma'$ if and only if $\gamma'\gamma^{-1} \in \Gamma_2 \cap \alpha{-}1\Gamma_1\alpha$. One concludes by noting that since $\alpha^{-1}\Gamma_1\alpha \sim \Gamma_1 \sim \Gamma_2$ the index $[\Gamma_2\colon \Gamma_2 \cap \alpha^{-1}\Gamma_1\alpha]$ is finite. ∎

We now fix a semigroup $\Delta \subseteq G$. By $\mathcal{C}(\Delta)$ we denote the collection of mutually commensurable subgroups $\Gamma \subseteq G$ such that

$$\Gamma \subseteq \Delta \subseteq \widetilde{\Gamma}.$$

Further let R be a commutative ring with identity. (For concreteness we could take $R = \mathbb{Z}$, but there is no harm in working more generally for now.) For $\Gamma_1, \Gamma_2 \in \mathcal{C}(\Delta)$ we put

$$\mathcal{H}_R(\Gamma_1, \Gamma_2; \Delta) = \langle \Gamma_1\alpha\Gamma_2 \colon \alpha \in \Delta \rangle_R.$$

This is the free R-module generated by the double co-sets $\Gamma_1\alpha\Gamma_2$ with $\alpha \in \Delta$. In particular, elements are formal sums of the form

$$\eta = \sum_{\alpha \in \Delta} c_\alpha \cdot \Gamma_1\alpha\Gamma_2,$$

where $c_\alpha \in R$ is zero for all but finitely many α.

The degree of a double co-set $\Gamma_1\alpha\Gamma_2$ is defined to be the number of right Γ_1 co-sets contained in it:

$$\deg(\Gamma_1\alpha\Gamma_2) = [\Gamma_2 \colon \Gamma_2 \cap \alpha^{-1}\Gamma_1\alpha].$$

We extend the degree to a map $\deg\colon \mathcal{H}_R(\Gamma_1, \Gamma_2; \Delta) \to R$ by setting

$$\deg(\eta) = \sum_{\alpha} c_\alpha \cdot \deg(\Gamma_1\alpha\Gamma_2).$$

Given an R-module M and suppose that $\Delta \subseteq G$ acts on M from the right:

$$M \times \Delta \ni (m, \alpha) \mapsto m \cdot \alpha \in M.$$

(This action should of course satisfy $m \cdot 1 = m$ and $m \cdot (\alpha_1 \alpha_2) = (m \cdot \alpha_1) \cdot \alpha_2$.) For $\Gamma \in \mathcal{C}(\Delta)$, we can define the submodule

$$M^\Gamma = \{m \in M \colon m \cdot \gamma = m \text{ for all } \gamma \in \Gamma\}.$$

On this space we can define the action of a double co-set as follows. Take $\Gamma_1 \alpha \Gamma_2 = \bigsqcup_{i=1}^d \Gamma \alpha_i$ and define

$$m | \Gamma_1 \alpha \Gamma_2 = \sum_{i=1}^d m \cdot \alpha_i.$$

We extend this linearly to an action $m|\eta$ for $\eta \in \mathcal{H}_R(\Gamma_1, \Gamma_2; \Delta)$.

Lemma 5.1.3. *Let $m \in M^{\Gamma_1}$ and $\eta \in \mathcal{H}_R(\Gamma_1, \Gamma_2; \Delta)$. Then operation $m|\eta$ is well defined and we have $m|\eta \in M^{\Gamma_2}$.*

Proof. Clear. $\square$

Given $\Gamma_1, \Gamma_2, \Gamma_3 \in \mathcal{C}(\Delta)$ and $\eta_1 \in \mathcal{H}_R(\Gamma_1, \Gamma_2; \Delta)$ and $\eta_2 \in \mathcal{H}_R(\Gamma_2, \Gamma_3; \Delta)$ we want to define the product $\eta_1 \cdot \eta_2 \in \mathcal{H}_R(\Gamma_1, \Gamma_3; \Delta)$. Of course it suffices to define the product on double co-sets $\Gamma_1 \alpha \Gamma_2$ and $\Gamma_2 \beta \Gamma_3$ with $\alpha, \beta \in \Delta$ and then extend it linearly. We put

$$(\Gamma_1 \alpha \Gamma_2)(\Gamma_2 \beta \Gamma_3) = \sum_{\gamma \in \Delta} c_\gamma \Gamma_1 \gamma \Gamma_3,$$

where

$$c_\gamma = \sharp\{(i,j) \colon \Gamma_1 \alpha_i \beta_j = \Gamma_1 \gamma\}. \tag{99}$$

Remark 5.1.4. Let $M = R(\Gamma_1 \backslash \Delta)$ be the free R-module generated by right Γ_1 co-sets $\Gamma_1 \alpha$ with $\alpha \in \Delta$. The semigroup Δ acts on M in the obvious way by right multiplication. Furthermore, we can embed

$$\mathcal{H}_R(\Gamma_1, \Gamma_2; \Delta) \to R(\Gamma_1 \backslash \Delta), \Gamma_1 \alpha \Gamma_2 = \bigsqcup_i \Gamma_1 \alpha_i \mapsto \sum_i \Gamma_1 \alpha_i.$$

Using this embedding we have the identification

$$\mathcal{H}_R(\Gamma_1, \Gamma_2; \Delta) = R(\Gamma_1 \backslash \Delta)^{\Gamma_2}.$$

We compute

$$\begin{aligned}(\Gamma_1 \alpha \Gamma_2) | (\Gamma_2 \beta \Gamma_3) &= \sum_{i=1}^r \Gamma_1 \alpha_i | (\Gamma_2 \beta \Gamma_3) \\ &= \sum_{i=1}^r \sum_{j=1}^s \Gamma_1 \alpha_i \beta_j \\ &= \sum_\gamma c_\gamma \cdot \Gamma_1 \gamma \in R(\Gamma_1 \backslash \Delta)^{\Gamma_3}.\end{aligned}$$

Now, for each $\gamma \in \Delta$ we write

$$\Gamma_1\gamma\Gamma_3 = \bigsqcup_{k=1}^{\deg(\Gamma_1\gamma\Gamma_3)} \Gamma_1\gamma_k$$

and we note that $c_{\gamma_k} = c_\gamma$. Thus we can write

$$(\Gamma_1\alpha\Gamma_2)|(\Gamma_2\beta\Gamma_3) = \sum_{\Gamma_1\gamma\Gamma_3} c_\gamma \sum_{k=1}^{\deg(\Gamma_1\gamma\Gamma_3)} \Gamma_1\gamma_k = \sum_\gamma c_\gamma \Gamma_1\gamma\Gamma_3 \in \mathcal{H}_R(\Gamma_1, \Gamma_2; \Delta).$$

In the last equality we have reversed the identification between $\mathcal{H}_R(\Gamma_1, \Gamma_2; \Delta)$ and $R(\Gamma_1\Delta)^{\Gamma_3}$. Thus we find

$$(\Gamma_1\alpha\Gamma_2) \cdot (\Gamma_2\beta\Gamma_3) = (\Gamma_1\alpha\Gamma_2)|(\Gamma_2\beta\Gamma_3).$$

Thus we have defined a bilinear pairing

$$\mathcal{H}_R(\Gamma_1, \Gamma_2; \Delta) \times \mathcal{H}_R(\Gamma_2, \Gamma_3; \Delta) \to \mathcal{H}_R(\Gamma_1, \Gamma_3; \Delta),\ (\eta_1, \eta_2) \mapsto \eta_1 \cdot \eta_2$$

and under the identification $\mathcal{H}_R(\Gamma_1, \Gamma_i; \Delta) = R(\Gamma_1\backslash\Delta)^{\Gamma_i}$ (with $i = 2, 3$) we get

$$\eta_1 \cdot \eta_2 = \eta_1|\eta_2.$$

We directly obtain that $(\eta_1 \cdot \eta_2) \cdot \eta_3 = \eta_1 \cdot (\eta_2 \cdot \eta_3)$.

Lemma 5.1.5. *Given* $\Gamma_1\alpha\Gamma_2$ *and* $\Gamma_2\beta\Gamma_3$ *as above. Then we have*

$$c_\gamma \cdot \deg(\Gamma_1\gamma\Gamma_3) = \sharp\{(i, j) \colon \Gamma_1\alpha_i\beta_j\Gamma_3 = \Gamma_1\gamma\Gamma_3\}.$$

Proof. Suppose $\Gamma_1\gamma\Gamma_3 = \bigsqcup_{k=1}^t \Gamma_1\gamma_k$. In particular, $\deg(\gamma) = t$. Then we have $\Gamma_1\alpha_i\beta_j\Gamma_4 = \Gamma_1\gamma\Gamma_3$ if and only if $\Gamma_1\alpha_i\beta_j = \Gamma_1\gamma_k$ for exactly one $1 \leq k \leq t$. We conclude by observing that

$$\begin{aligned}\sharp\{(i, j) \colon \Gamma_1\alpha_i\beta_j\Gamma_3 = \Gamma_1\gamma\Gamma_3\} &= \sum_{k=1}^t \sharp\{(i, j) \colon \Gamma_1\alpha_i\beta_j = \Gamma_1\gamma_k\} \\ &= t \cdot \sharp\{(i, j) \colon \Gamma_1\alpha_i\beta_j = \Gamma_1\gamma\} = t \cdot c_\gamma.\end{aligned}$$

∎

Lemma 5.1.6. *If* $\eta_1 \in \mathcal{H}_R(\Gamma_1, \Gamma_2; \Delta)$ *and* $\eta_2 \in \mathcal{H}_R(\Gamma_2, \Gamma_3; \Delta)$*, then*

$$\det(\eta_1 \cdot \eta_2) = \deg(\eta_1) \cdot \deg(\eta_2).$$

Proof. It is sufficient to check this for generators $\Gamma_1\alpha\Gamma_2$ and $\Gamma_2\beta\Gamma_3$ of the respective algebras. We compute

$$\begin{aligned}\deg(\Gamma_1\alpha\Gamma_2 \cdot \Gamma_2\beta\Gamma_3) &= \sum_\gamma c_\gamma \deg(\Gamma_1\gamma\Gamma_3) \\ &= \sum_\gamma \sharp\{(i, j) \colon \Gamma_1\alpha_i\beta_j\Gamma_3 = \Gamma_1\gamma\Gamma_3\} \\ &= \sharp\{(i, j)\} = \deg(\Gamma_1\alpha\Gamma_2) \cdot \deg(\Gamma_2\alpha\Gamma_3).\end{aligned}$$

Definition 5.1.3. We call
$$\mathcal{H}(\Gamma;\Delta)=\mathcal{H}_{\mathbb{Z}}(\Gamma,\Gamma;\Delta)$$
the Hecke algebra of Γ (over $\mathbb{Z}$) with respect to Δ.

Remark 5.1.7. If $\Delta\subseteq\Delta'$ and $\Gamma\in\mathcal{C}(\Delta')$, then $\mathcal{H}(\Gamma,\Delta)$ is a subalgebra of $\mathcal{H}(\Gamma;\Delta')$.

Proposition 5.1.8. *Let $\alpha\in\widetilde{\Gamma}$ and suppose that*[40]
$$\Gamma\alpha\Gamma=\bigsqcup_{i=1}^{d}\Gamma\alpha_i=\bigsqcup_{j=1}^{d}\beta_j\Gamma.$$
Then we can find representatives δ_i that simultaneously work for left and right co-sets:
$$\Gamma\alpha\Gamma=\bigsqcup_{i=1}^{d}\Gamma\delta_i=\bigsqcup_{i=1}^{d}\delta_i\Gamma.$$

Proof. We claim that $\Gamma\alpha_i\cap\beta_j\Gamma\neq\emptyset$ for all tuples (i,j). Indeed assuming the contrary we find indices i and j such that
$$\Gamma\alpha_i\subseteq\bigsqcup_{k\neq j}\beta_k\Gamma.$$
This implies
$$\Gamma\alpha\Gamma=\Gamma\alpha_i\Gamma=\bigsqcup_{k\neq j}\beta_k\Gamma,$$
which is a contradiction.

With the claim established we can simply replace α_i and β_i by some $\delta_i\in\Gamma\alpha_i\cap\beta_i\Gamma\neq\emptyset$. □

For us an involution on Δ is a map $(\cdot)^\iota\colon\Delta\to\Delta$ such that
$$(\alpha\beta)^\iota=\beta^\iota\alpha^\iota\text{ and }\alpha^{\iota\iota}=\alpha.$$

Theorem 5.1.9 (Gelfand's Trick)**.** *Suppose there is an involution $\iota\colon\Delta\to\Delta$ such that*
$$\Gamma^\iota=\Gamma\textit{ and }\Gamma\alpha^\iota\Gamma=\Gamma\alpha\Gamma\textit{ for all }\alpha\in\Delta.$$
Then $\mathcal{H}_R(\Gamma;\Delta)$ is commutative.

Proof. Let $\alpha,\beta\in\Delta$. We first write
$$\Gamma\alpha\Gamma=\bigsqcup_{i=1}^{d}\Gamma\alpha_i$$

[40] The point in this assumption is that in both expansions we need the same number of representatives.

and we observe that by assumption on ι we have

$$\Gamma\alpha\Gamma = \Gamma\alpha^\iota\Gamma = (\Gamma\alpha\Gamma)^\iota = \bigsqcup_{i=1}^d \alpha_i^\iota\Gamma.$$

Thus the assumption of the previous proposition is satisfied and we can pick α_i such that

$$\Gamma\alpha\Gamma = \bigsqcup_{i=1}^d \Gamma\alpha_i = \bigsqcup_{i=1}^d \alpha_i\Gamma.$$

Similarly we can write

$$\Gamma\beta\Gamma = \bigsqcup_{i=1}^d \Gamma\beta_i = \bigsqcup_{i=1}^d \beta_i\Gamma.$$

Recall that

$$\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \sum_\gamma c_\gamma \Gamma\gamma\Gamma.$$

Now we compute

$$\begin{aligned} c_\gamma &= \sharp\{(i,j)\colon \Gamma\alpha_i\beta_j = \Gamma\gamma\} \\ &= \frac{1}{\deg(\Gamma\gamma\Gamma)}\sharp\{(i,j)\colon \Gamma\alpha_i\beta_j\Gamma = \Gamma\gamma\Gamma\} \\ &= \frac{1}{\deg(\Gamma\gamma\Gamma)}\sharp\{(i,j)\colon \Gamma\beta_j^\iota\alpha_i^\iota\Gamma = \Gamma\gamma\Gamma\} \\ &= \sharp\{(i,j)\colon \Gamma\beta_j^\iota\alpha_i^\iota = \Gamma\gamma\} =: c'_\gamma \end{aligned} \tag{100}$$

Combining everything we get

$$\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \sum_\gamma c_\gamma \cdot \Gamma\gamma\Gamma = \sum_\gamma c'_\gamma \cdot \Gamma\gamma\Gamma = \Gamma\beta^\iota\Gamma \cdot \Gamma\alpha^\iota\Gamma = \Gamma\beta\Gamma \cdot \Gamma\alpha\Gamma.$$

This completes the proof. ∎

Example 5.1.10. Let $\Gamma = \mathrm{SL}_n(\mathbb{Z})$, $G = \mathrm{GL}_n^+(\mathbb{Q})$ and

$$\Delta = \{\alpha \in \mathrm{Mat}_{n\times n}(\mathbb{Z})\colon \det(\alpha) > 0\}.$$

Then we have the involution $\alpha \mapsto \alpha^t$. This obviously leaves Γ invariant. Furthermore, by the elementary divisor theorem we can write

$$\Gamma\alpha\Gamma = \Gamma\alpha_d\Gamma$$

for some diagonal matrix $\alpha_d = \mathrm{diag}(d_1, \ldots, d_n)$ with $d_i \in \mathbb{N}$ so that $d_i \mid d_{i+1}$. We check

$$\Gamma\alpha^t\Gamma = (\Gamma\alpha\Gamma)^t = (\Gamma\alpha_d\Gamma)^t = \Gamma\alpha_d^t\Gamma = \Gamma\alpha_d\Gamma = \Gamma\alpha\Gamma.$$

Thus we can apply Gelfand's Trick to show that $\mathcal{H}(\Gamma, \Delta)$ is commutative.

Exercise 1, Sheet 10: Let $\Gamma_1, \Gamma_2 \subset \mathrm{SL}_2(\mathbb{R})$ be two discrete subgroups of finite co-volume. Let $k \in \mathbb{R}$ and let ϑ_i be a multiplier system for Γ_i of weight k (with $i = 1, 2$). On the intersection $\Lambda = \Gamma_1 \cap \Gamma_2$ the product

$$\xi(\gamma) = \vartheta_1(\gamma)\vartheta_2(\gamma)^{-1}$$

defines a character and we assume that the kernel $E = \ker(\xi) \subset \Lambda$ has finite index in Γ_2.

a) Let $f \in M_k(\Gamma_1, \vartheta_1)$. Show that

$$g(z) = \sum_{\alpha \in E\backslash\Gamma_2} \vartheta_2(\alpha)^{-1}[f \mid_k \alpha](z)$$

is well-defined and that we have $g \in M_k(\Gamma_2, \vartheta_2)$.

b) Show that if $[\Lambda : E] > 1$, then $g = 0$.

Solution. To see that g is well-defined, let $\beta = \epsilon\alpha$, where $\epsilon \in E$. Observe that $[f|_k\epsilon\alpha] = [[f|_k\epsilon]|_k\alpha]w_k(\epsilon, \alpha)$, where w_k is the factor system of weight k; see Definition 2.2.1. Also, by definition of multiplier system of weight k we have $\vartheta_2(\epsilon\alpha) = \vartheta_2(\epsilon)\vartheta_2(\alpha)w_k(\epsilon, \alpha)$. Since $f \in M_k(\Gamma_1, \vartheta_1)$ we have $[f|_k\epsilon] = \vartheta_1(\epsilon)f$, and from the definition of E, $\vartheta_1(\epsilon) = \vartheta_2(\epsilon)$. These observations justify the following calculation:

$$\begin{aligned}
\vartheta_2(\epsilon\alpha)^{-1}[f|_k\epsilon\alpha] &= \vartheta_2(\epsilon\alpha)^{-1}\vartheta_2(\alpha)\vartheta_2(\alpha)^{-1}[[f|_k\epsilon]|_k\alpha]w_k(\epsilon, \alpha) \\
&= \vartheta_2(\epsilon\alpha)^{-1}\vartheta_2(\alpha)\vartheta_2(\alpha)^{-1}\vartheta_1(\epsilon)w_k(\epsilon, \alpha)[f|_k\alpha] \\
&= \vartheta_2(\epsilon\alpha)^{-1}\vartheta_2(\alpha)\vartheta_2(\alpha)^{-1}\vartheta_2(\epsilon)w_k(\epsilon, \alpha)[f|_k\alpha] \\
&= \vartheta_2(\alpha)^{-1}[f|_k\alpha].
\end{aligned}$$

Therefore, g is well-defined. To show that $g \in M_k(\Gamma_2, \vartheta_2)$, observe that multiplying on the right by $\gamma \in \Gamma_2$ permutes the right cosets $E\backslash\Gamma_2$. We get

$$\begin{aligned}
g(z) &= \sum_{\alpha \in E\backslash\Gamma_2} \vartheta_2(\alpha\gamma)^{-1}[f|_k\alpha\gamma](z) = \sum_{\alpha \in E\backslash\Gamma_2} \vartheta_2(\alpha)^{-1}\vartheta_2(\alpha)\vartheta_2(\alpha\gamma)^{-1}[[f|_k\alpha]|_k\gamma]w_k(\alpha, \gamma) \\
&= \vartheta_2(\gamma)^{-1}[g|_k\gamma]
\end{aligned}$$

as desired (we have used that $\vartheta_2(\alpha\gamma) = \vartheta_2(\alpha)\vartheta_2(\gamma)w_k(\alpha, \gamma)$, valid since ϑ_2 is a multiplier system of weight k for Γ_2).

For part b), let $\gamma \in \Lambda = \Gamma_1 \cap \Gamma_2$. we calculate

$$\begin{aligned}
[g|_k\gamma] &= \sum_{\alpha \in E\backslash\Gamma_2} \vartheta_2(\alpha)^{-1}[[f|_k\alpha]|_k\gamma] = \sum_{\alpha \in E\backslash\Gamma_2} \vartheta_2(\alpha)^{-1} w_k(\alpha,\gamma)^{-1}[f|_k\alpha\gamma] \\
&= \sum_{\alpha \in E\backslash\Gamma_2} \vartheta_2(\alpha)^{-1} w_k(\alpha,\gamma)^{-1} w_k(\gamma,\gamma^{-1}\alpha\gamma)[[f|_k\gamma]|_k\gamma^{-1}\alpha\gamma] \\
&= \vartheta_1(\gamma) \sum_{\alpha \in E\backslash\Gamma_2} \vartheta_2(\alpha)^{-1} w_k(\alpha,\gamma)^{-1} w_k(\gamma,\gamma^{-1}\alpha\gamma)[f|_k\gamma^{-1}\alpha\gamma].
\end{aligned}$$

Now, observe that $x \mapsto \gamma^{-1}x\gamma$ is an automorphism of Γ_2, and since $\gamma \in \Lambda = \Gamma_1 \cap \Gamma_2$, this conjugation normalizes E. Therefore, $\alpha \mapsto \gamma^{-1}\alpha\gamma$ induces a bijection of $E\backslash\Gamma_2$. Also, we have the identities

$$\vartheta_2(\alpha\gamma) = \vartheta_2(\alpha)\vartheta_2(\gamma)w_k(\alpha,\gamma) \quad \text{and} \quad \vartheta_2(\alpha\gamma) = \vartheta_2(\gamma)\vartheta_2(\gamma^{-1}\alpha\gamma)w_k(\gamma,\gamma^{-1}\alpha\gamma)$$

which imply

$$\vartheta_2(\alpha)^{-1} w_k(\alpha,\gamma)^{-1} w_k(\gamma,\gamma^{-1}\alpha\gamma)\vartheta_2(\gamma^{-1}\alpha\gamma) = 1.$$

Therefore, we arrive at

$$\begin{aligned}
[g|_k\gamma] &= \vartheta_1(\gamma) \sum_{\alpha \in E\backslash\Gamma_2} \vartheta_2(\alpha)^{-1} w_k(\alpha,\gamma)^{-1} w_k(\gamma,\gamma^{-1}\alpha\gamma)[f|_k\gamma^{-1}\alpha\gamma] \\
&= \vartheta_1(\gamma) \sum_{\alpha \in E\backslash\Gamma_2} \vartheta_2(\gamma^{-1}\alpha\gamma)^{-1}[f|_k\gamma^{-1}\alpha\gamma] \\
&= \vartheta_1(\gamma) g.
\end{aligned}$$

Finally, if $[\Lambda : E] > 1$, we can choose $\gamma \in \Lambda$ such that $\vartheta_1(\gamma) \neq \vartheta_2(\gamma)$, and then

$$\vartheta_1(\gamma)g = [g|_k\gamma] = \vartheta_2(\gamma)g$$

which implies $g \equiv 0$. ◻

Exercise 3, Sheet 10: Let G be a finite group and let $H \subset G$ be a subgroup. Let π be an irreducible representation of G on some (finite dimensional) $\mathbb{C}$-vector space V. In particular, we have the action

$$v \cdot g := \pi(g^{-1})v \text{ for } g \in G \text{ and } v \in V.$$

Thus we have an action of $\mathcal{H}_{\mathbb{C}}(H,G)$ on V^H given by $v|\eta$, where $v \in V$ and $\eta \in \mathcal{H}_{\mathbb{C}}(H,G)$. (See Lemma 5.1.3.)

a) Realize the Hecke algebra as $\mathrm{End}_G(\mathbb{C}[H\backslash G])$.
b) Prove that the following are equivalent:
   i) The Hecke algebra $\mathcal{H}_{\mathbb{C}}(H,G)$ is commutative.
   ii) Every irreducible representation contains up to scalars at most one H-fixed vector.

Solution. Recall Frobenius Reciprocity: If (U,σ) and (V,τ) are representations of H and G respectively, then

$$\mathrm{Hom}_G(V, \mathrm{Ind}_H^G(U)) \simeq \mathrm{Hom}_H(V|_H, U).$$

By $\mathrm{Ind}_H^G(U)$ we mean a *induced representation*, with underlying space

$$\mathrm{Ind}_H^G(U) := \{f : G \to U \mid f(hg) = \sigma(h)f(g) \text{ for all } h \in H, g \in G\}.$$

The action of G on $\mathrm{Ind}_H^G(U)$ is by right translation. That is, we have

$$(g \cdot f)(x) = f(xg) \text{ for } f \in \mathrm{Ind}_H^G(U), x, g \in G.$$

The bijection in Frobenius reciprocity is defined as follows. To $\Phi \in \mathrm{Hom}_G(V, \mathrm{Ind}_H^G(U))$ we associate $\phi \in \mathrm{Hom}_H(V|_H, U)$ such that $\phi(v) := \Phi(v)(1)$. In the other direction, to $\phi \in \mathrm{Hom}_H(V|_H, U)$ we associate $\Phi \in \mathrm{Hom}_G(V, \mathrm{Ind}_H^G(U))$ such that $\Phi(v)(g) := \phi(gv)$. It is a simple computation (although a bit tedious) to check that the two maps above are inverse to each other and have the desired transformation behaviour. We will be concerned with $\mathbb{C}[H\backslash G] := \mathrm{Ind}_H^G(1)$, where 1 is the trivial one-dimensional representation of H. Therefore,

$$\mathbb{C}[H\backslash G] = \{f : G \to \mathbb{C} \mid f(hg) = f(g) \text{ for all } h \in H, g \in G\}.$$

By Frobenius reciprocity we have a bijection

$$\mathrm{Hom}_G(W, \mathbb{C}[H\backslash G]) \simeq \mathrm{Hom}_H(W_H, 1) \tag{101}$$

for any G-representation W. We want to see that $\mathrm{End}_G(\mathbb{C}[H\backslash G]) \simeq \mathbb{C}(H,G)$. There is a canonical basis of $\mathbb{C}[H\backslash G]$, consisting of the characteristic functions δ_{Hg}. The action of G on this basis is described as $x \cdot \delta_{Hg} = \delta_{Hgx^{-1}}$. Also, $\Phi \in \mathrm{End}_G(\mathbb{C}[H\backslash G])$ is uniquely determined by $\Phi(\delta_H)$, since $\Phi(\delta_{Hg}) = \Phi(g^{-1}\delta_H) = g^{-1}\Phi(\delta_H)$. Write

$$\Phi(\delta_H) = \sum_{g \in H\backslash G} a_{Hg}\delta_{Hg}.$$

Since H fixes δ_H, we must have

$$\sum_{g \in H\backslash G} a_{Hg}\delta_{Hg} = \Phi(\delta_H) = \Phi(h\cdot\delta_H) = \sum_{g \in H\backslash G} a_{Hg} h\cdot\delta_{Hg} = \sum_{g \in H\backslash G} a_{Hg}\delta_{Hgh^{-1}} = \sum_{g \in H\backslash G} a_{Hgh}\delta_{Hg}.$$

It follows that $a_{Hg} = a_{Hgh}$ for any $h \in H$, and thus we can write

$$\Phi(\delta_H) = \sum_{g \in H\backslash G/H} a_{HgH}\delta_{HgH}.$$

Reciprocally, any such expression corresponds to a well-defined endomorphism of $\mathbb{C}[H\backslash G]$. Indeed, we only need to check that the expression $\Phi(\delta_{Hg}) := g^{-1} \cdot \Phi(\delta_H)$ is well-defined. To see this, note that $Hg = Hx$ implies $xg^{-1} \in H$, which stabilizes $\Phi(\delta_H)$. We check that

$$g^{-1} \cdot \Phi(\delta_H) = x^{-1}\left(\cdot(xg^{-1}) \cdot \Phi(\delta_H)\right) = x^{-1}\Phi(\delta_H).$$

Therefore, we have established a bijection of $\mathcal{H}_{\mathbb{C}}(H,G)$ with $\mathbb{C}[H\backslash G]$, which sends the double coset HgH to $\Phi_g \in \mathbb{C}[H\backslash G]$ defined by $\Phi_g(\delta_{Hx}) := \delta_{HgHx}$. To see that this bijection respects multiplication, let $g, x \in G$ arbitrary and consider the endomorphisms $\Phi_g, \Phi_x \in \mathrm{End}(\mathbb{C}[H\backslash G])$ such that $\Phi_g(\delta_H) = \delta_{HgH} = \sum \delta_H g_i$ and $\Phi_x(\delta_H) = \sum \delta_{Hx_j}$, where the sums are over the cosets $Hg_i \subset HgH$ and the cosets $Hx_j \subset HxH$ respectively. Composing the endomorphisms,

$$\begin{aligned}\Phi_x(\Phi_g(\delta_H)) = \Phi_x(\sum_i \delta_{Hg_i}) = \sum_i g_i^{-1} \cdot \Phi_x(\delta_H) = \sum_i g_i^{-1} \sum_j \delta_{Hx_j} \\ = \sum_{i,j} \delta_{Hx_jg_i} = \sum_{y \in H\backslash G/H} d_y \delta_{HyH}\end{aligned}$$

where $d_y = \#\{(i,j) : Hx_jg_i = Hy\}$. This is the same coefficient as c_γ in the definition of the multiplication of the Hecke algebra (see (99)). This shows that $\mathcal{H}(H,G) \simeq \mathrm{End}(\mathbb{C}[H\backslash G])$, as desired.

For part b), we need several basic facts from the representation theory of finite groups. Recall that representations of finite groups over a field of characteristic 0 are completely reducible. That is, given a representation (V, σ) of G we can write $V \simeq \oplus W_i^{d_i}$ where (W_i, τ_i) is irreducible and the decomposition is unique. Recall also Schur's lemma, which says that, for two irreducible G-representations W_1 and W_2, we have

$$\mathrm{Hom}_G(W_1, W_2) \simeq \begin{cases} \mathbb{C}, & \text{if } W_1 \simeq W_2; \\ 0, & \text{otherwise.} \end{cases}$$

From Schur's lemma, we see that

$$V = \bigoplus W_i^{d_i} \longrightarrow \mathrm{End}_G(V) \simeq M_{d_i \times d_i}(\mathbb{C}).$$

In particular, the Hecke algebra $\mathcal{H}_{\mathbb{C}}(H,G) \simeq \mathrm{End}_G(\mathbb{C}[H\backslash G])$ is commutative if and only if each G-irreducible representation appears with multiplicity at most 1 in $\mathrm{End}_G(\mathbb{C}[H\backslash G])$. By Frobenius reciprocity,

$$\mathrm{Hom}_G(W, \mathbb{C}[H\backslash G]) \simeq \mathrm{Hom}_H(W_H, 1) \tag{102}$$

for any G representation W. If $\mathbb{C}[H\backslash G] = W^d \bigoplus \left(\oplus W_i^{d_i}\right)$ where $W \not\simeq W_i$, it follows from Schur's lemma that

$$\dim_{\mathbb{C}} \mathrm{Hom}_G(W, \mathbb{C}[H\backslash G]) = d \tag{103}$$

By the previous reasoning, $\mathcal{H}_{\mathbb{C}}(H,G)$ is commutative if and only if for any irreducible W the vector space on the left (102) has dimension at most 1. For any G-representation on a finite dimensional vector space V, we can define the contragredient representation on the dual V^* as

$$(g \cdot \lambda)(w) := \lambda(g^{-1}w), \quad \text{for } \lambda \in V^*, w \in V, g \in G.$$

One checks immediately that the natural isomorphism $V \simeq V^{**}$ respects the G action defined on this way. Therefore, associating to a finite dimensional G-representation its contragredient gives a permutation of finite dimensional G-representations. Also, it can be checked that V is irreducible if and only if V^* is irreducible.

For the punchline, observe that an element $\lambda \in \mathrm{Hom}_H(W_H, 1)$ is a functional such that $\lambda(hw) = \lambda(w)$ for every $h \in H$. Therefore, $\mathrm{Hom}_H(W_H, 1)$ is the space of fixed H-fixed vectors of the contragredient representation W^*. Since mapping a representation to its contragredient is a permutation of the finite dimensional representations of G that preserves irreducible ones, we deduce that $\mathcal{H}(H, G)$ is commutative if and only if $\dim_{\mathbb{C}} V^H \leq 1$ for every irreducible G-representation V, as desired. ⧉

5.2. **Hecke operators for integral weight.** We now restrict to the special situation where $G = \mathrm{GL}_2^+(\mathbb{Q})$ and $\Gamma = \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a Hecke congruence subgroup.

Let $k \in \mathbb{N}$ be even and let χ be a Dirichlet character modulo N. Recall that we can lift χ to a multiplier system on $\Gamma_0(N)$ via

$$\chi(\gamma) = \chi(d) \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Note that we can assume $\chi(-1) = (-1)^k$, so that the so obtained multiplier system is consistent.

We define

$$\Delta_N = \left\{ \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}) \colon N \mid c,\ (a, N) = 1 \text{ and } \det(\alpha) > 0 \right\}.$$

Note that we have $\Gamma_0(N) \subseteq \Delta_N \subseteq G$. Furthermore, for $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_N$ we define

$$\chi^*(\alpha) = \chi(a)^{-1}.$$

Note that $\chi^*|_{\Gamma_0(N)} = \chi$, thus we have extended our multiplier system to Δ_N.

If M is the module of holomorphic functions $f \colon \mathbb{H} \to \mathbb{C}$ of polynomial growth (in the sense of Lemma 2.3.2), then we can let Δ_N act on M by[41]

$$[f \cdot \alpha](z) = \chi^*(\alpha)^{-1} \frac{\det(\alpha)^{\frac{k}{2}}}{(cz+d)^k} f\left(\frac{az+b}{cz+d}\right) = \chi^*(\alpha)^{-1} \det(\alpha)^{\frac{k}{2}} [f|_k\alpha](z).$$

In particular we observe that

$$M^{\Gamma_0(N)} = M_k(\Gamma_0(N), \chi).$$

[41]Note that we slightly diverge from standard notation and use $[f|_k\alpha](z) = j_\alpha(z)^{-k} f(\alpha z)$ also for $\alpha \in \mathrm{GL}_2^+(\mathbb{R})$. Sometimes the slash operator is defined by including the factor $\det(\alpha)^{\frac{k}{2}}$.

Thus the abstract theory from the previous section allows us to define an action of the Hecke algebra $\mathcal{H}(\Gamma_0(N), \Delta_M)$ on $M_k(\Gamma_0(N), \chi)$. The action is given by

$$[f|\Gamma_0(N)\alpha\Gamma_0(N)](z) = \sum_i [f \cdot \alpha_i](z) = \det(\alpha)^{\frac{k}{2}} \sum_i \chi^*(\alpha)^{-1}[f|_k\alpha_i](z),$$

where $\Gamma_0(N)\alpha\Gamma_0(N) = \bigsqcup_i \Gamma_0(N)\alpha_i$.

Remark 5.2.1. If we define the submodule

$$M_0 = \{f \in M\colon\ \mathrm{Im}(z)^{\frac{k}{2}} f(z) \text{ is bounded}\},$$

then $M_0^{\Gamma_0(N)} = S_k(\Gamma_0(N), \chi)$. Since the action of Δ_N preserves M_0 we see that the action of the Hecke algebra $\mathcal{H}(\Gamma_0(N), \Delta_N)$ preserves the subspace of cusp forms.

Remark 5.2.2. Let $d_N = \mathrm{diag}(N, 1)$, then

$$\alpha^\iota = d_N^{-1}\alpha^t d_N$$

defines an involution on Δ_N and we have $\Gamma_0(N)^\iota = \Gamma_0(N)$. One further checks that also

$$\Gamma_0(N)\alpha^\iota\Gamma_0(N) = \Gamma_0(N)\alpha\Gamma_0(N)$$

for all $\alpha \in \Delta_N$. Thus $\mathcal{H}(\Gamma_0(N), \Delta_N)$ is commutative.

While each double co-set $\Gamma_0(N)\alpha\Gamma_0(N)$ gives rise to a Hecke operator we are interested in special combinations of them. We define

$$\Delta_N(n) = \{\alpha \in \Delta_N\colon\ \det(\alpha) = n\}.$$

Lemma 5.2.3. *We have*

$$\Delta_N(n) = \bigsqcup_{\substack{ad=n,\\ a|d,\\ (a,N)=1}} \Gamma_0(N) \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \Gamma_0(N) = \bigsqcup_{\substack{ad=n,\\ (a,N)=1,\\ b \bmod d}} \Gamma_0(N) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Proof. The first identity follows (essentially) from the smith normal form. To see the second we consider the right co-sets $\Gamma_0(N)\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ for $ad = n$, $(a, N) = 1$ and b mod d. It is easy to see that they are contained in $\Delta_N(n)$ and that they are disjoint. Now pick $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_N(n)$. We chose co-prime integers g, h so that $ga + hc = 0$. Note that necessarily $N \mid g$. Thus there is a matrix $\gamma = \begin{pmatrix} * & * \\ g & h \end{pmatrix} \in \Gamma_0(N)$. And we have

$$\gamma \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & * \\ 0 & d' \end{pmatrix}.$$

It is clear that $a'd' = n$ must hold. Note that $(a, N) = (a', N) = 1$. Finally we can further multiply by $\pm T^j$ to make the diagonal positive and to force the upper right entry to lie between 0 and $d - 1$. ∎

Thus we define the element

$$\eta_n = \sum_{\substack{ad=n,\\ a|d,\\ (a,N)=1}} \Gamma_0(N) \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \Gamma_0(N) \in \mathcal{H}(\Gamma_0(N), \Delta_N).$$

This element is used to define the operator $T_n\colon M_k(\Gamma_0(N),\chi) \to M_k(\Gamma_0(N),\chi)$ given by

$$T_n f = n^{\frac{k}{2}-1} \cdot [f|\eta_n].$$

Note that we have included a normalizing factor, which will turn out to be convenient.[42] The operator T_n is what is usually refereed to as nth Hecke Operator. Unravelling the definition gives

$$T_n f(z) = \frac{1}{n} \sum_{\substack{ad=n,\\ (a,N)=1}} \chi(a) a^k \sum_{b \bmod d} f\left(\frac{az+b}{d}\right).$$

Note that for $p = n$ with $(p,N) = 1$ this reduces to (98). Note that T_1 is the identity operator.

Remark 5.2.4. Recall the classical Eisenstein Series $E_k(z) = \frac{1}{2\zeta(k)} e_k(1,z)$. We can write the action of T_p (for all p) on $E_k(z)$ as follows:

$$T_p E_k(z) = \frac{1}{2\zeta(k)} \frac{1}{p} \left(e(\frac{1}{p}, z) + \sum_{b=0}^{p-1} e\left(1, \frac{z+b}{p}\right)\right). \tag{104}$$

Now we write $L_z = \mathbb{Z} + \mathbb{Z}z \subseteq \mathbb{C}$ for the lattice in $\mathbb{C}$ generated by 1 and z. Since (at least for $k \geq 4$) the function $e_k(1,z)$ depends only on the lattice and not on our choice of basis we can write $e_k(L_z) = e_k(1,z)$. Staring at (104) long enough makes us realize that the lattices

$$\mathbb{Z} \cdot \frac{1}{p} + \mathbb{Z} \cdot z,\ \mathbb{Z} + \mathbb{Z} \cdot \frac{z}{p}, \dots,\ \mathbb{Z} + \mathbb{Z} \cdot \frac{z+(p-1)}{p}$$

are precisely those lattices $L \supseteq L_z$ with $[L\colon L_z] = p$. Therefore, we can rewrite

$$T_p E_k(z) = \frac{1}{2\zeta(k)} \frac{1}{p} \sum_{\substack{L \supseteq L_z,\\ [L\colon L_z]=p}} e_k(L).$$

This is a general phenomena. Indeed, when viewing elements of $M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ as functions on lattices we can interpret all the Hecke Operators T_n as averages over *neighbouring* lattices.

We will study finer properties of these operators. First we compute how they act on the Fourier expansion of a form:

[42] Attention: Normalizations of Hecke-Operators differ in the literature!

Lemma 5.2.5. *Suppose $f \in M_k(\Gamma_0(N), \chi)$ is given by $f(z) = \sum_{m=0}^{\infty} a_f(m;\infty)e(mz)$. Then we have*

$$[T_n f](z) = \sum_{m=0}^{\infty} \sum_{\substack{a|(n,m),\\ (a,N)=1}} \chi(a)a^{k-1}a_f(\frac{mn}{a^2};\infty)e(mz).$$

Proof. Inserting the Fourier expansion of f into the definition of the nth Hecke operator yields

$$\begin{aligned}[T_n f](z) &= \frac{1}{n}\sum_{m=0}^{\infty} a_f(m;\infty) \sum_{\substack{ad=n,\\ (a,N)=1}} \chi(a)a^k \sum_{b \bmod d} e(m \cdot \frac{az+b}{d}) \\ &= \sum_{m=0}^{\infty} a_f(m;\infty) \sum_{\substack{ad=n,\\ (a,N)=1}} \chi(a)a^{k-1}e(\frac{nm}{d^2}z)\frac{1}{d}\sum_{b \bmod d} e(m \cdot \frac{b}{d}).\end{aligned}$$

The b-sum vanishes unless $m \equiv 0 \bmod d$. Thus we get

$$\begin{aligned}[T_n f](z) &= \sum_{m'=0}^{\infty} \sum_{\substack{ad=n,\\ (a,N)=1}} a_f(m'd;\infty)\chi(a)a^{k-1}e(\frac{nm'}{d}z) \\ &= \sum_{m'=0}^{\infty} \sum_{\substack{a|n,\\ (a,N)=1}} a_f(m'n/a;\infty)\chi(a)a^{k-1}e(am'z) \qquad (105)\end{aligned}$$

The result follows by simply rewriting the summation accordingly. ∎

Remark 5.2.6. Recall that the Eisenstein Series $E_k(z) \in M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ is given by

$$E_k(z) = 1 + \frac{i^k 2k}{B_k}\sum_{m=1}^{\infty} \sigma_{k-1}(m)e(mz).$$

Thus applying the nth Hecke Operator T_n yields

$$[T_n E_k](z) = \sigma_{k-1}(n) + \frac{i^k 2k}{B_k}\sum_{m=1}^{\infty}\sum_{a|(n,m)} a^{k-1}\sigma_{k-1}(mn/a^2)e(mz).$$

We compute

$$\sum_{a|(n,m)} a^{k-1}\sigma_{k-1}(mn/a^2) = \sum_{a|(n,m)}\sum_{d|\frac{mn}{a^2}} (ad)^{k-1} = \sigma_{k-1}(n)\sigma_{k-1}(m).$$

Thus we see that

$$[T_n E_k](z) = \sigma_{k-1}(n)E_k(z).$$

We have found that the Eisenstein series E_k is an eigenfunction of all Hecke operators with multiplicative eigenvalues given by divisor functions.

Exercise 3, Sheet 11: Let $f : \mathbb{H} \to \mathbb{C}$ be holomorphic and suppose that $f|_k\gamma = f$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and a fixed even integer $k \geq 2$. Show that, if f is an eigenfunction of all Hecke operators T_n with $n \in \mathbb{N}$, then $f \in M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. (Even though we have not assumed that f is holomorphic at infinity, the Hecke operators act on it in the usual way.)

Solution. Denote the annulus of radii r_0 and R_0 by

$$A(r_0, R_0) := \{z \in \mathbb{C} : r_0 < |z| < R_0\},$$

where we allow $r_0 = 0$ or $R_0 = \infty$. Recall that if h is an holomorphic function defined on $A(r_0, R_0)$, then it admits an expansion

$$h(z) = \sum_{n=0}^{\infty} a_n z^n + \sum_{n=1}^{\infty} b_n z^{-n}$$

where the first series converges absolutely for $|z| < R_0$ and the second converges absolutely for $|z| > r_0$. We will briefly explain why. Denote by C_r the circumference of radius r traversed once counter clockwise. Define

$$I_r(h)(z) := \frac{1}{2\pi i} \int_{C_r} \frac{h(w)}{w - z}\, dw \quad (|z| \neq r),$$

for some $r_0 < r < R_0$. Then, for $|z| < r$ we can expand $(1 - z/w)^{-1}$ as a geometric series and obtain

$$I_r(h)(z) = \frac{1}{2\pi i} \int_{C_r} \frac{1}{w} \frac{h(w)}{1 - \frac{z}{w}}\, dw = \sum_{n=0}^{\infty} \left(\frac{1}{2\pi i} \int_{C_r} \frac{h(w)}{w^{n+1}}\, dw \right) z^n$$

where the power series expansion is valid for $|z| < r$ since the coefficients are bounded by

$$\left| \frac{1}{2\pi i} \int_{C_r} \frac{h(w)}{w^{n+1}}\, dw \right| \leq \left(\sup_{z \in C_r} |h(z)| \right) r^{-n}$$

Similarly, for $|z| > r$ we can expand $(1 - w/z)^{-1}$ as a geometric series and obtain

$$I_r(h)(z) = -\frac{1}{2\pi i} \int_{C_r} \frac{1}{z} \frac{h(w)}{1 - \frac{w}{z}}\, dw = -\sum_{n=1}^{\infty} \left(\frac{1}{2\pi i} \int_{C_r} h(w) w^{n-1}\, dw \right) z^{-n}$$

where the power series is absolutely convergent for $|z| > r$ since the coefficients are bounded by

$$\left| \frac{1}{2\pi i} \int_{C_r} h(w) w^{n-1}\, dw \right| \leq \left(\sup_{z \in C_r} |h(z)| \right) r^n \tag{106}$$

Now, for $r_0 < r < R < R_0$ we have

$$h(z) = I_R(h)(z) - I_r(h)(z) \text{ on } r < |z| < R$$

by Cauchy's theorem, since for every point outside $A(r_0, R_0)$ the winding number with respect to the cycle $C_R - C_r$ is 0, while the winding number of every point $r < |z| < R$ is one. Therefore, we get the expansion into power series

$$h(z) = \sum_{n=0}^{\infty} a_n z^n + \sum_{n=1}^{\infty} b_n z^{-n}$$

where

$$a_n = \frac{1}{2\pi i} \int_{C_r} \frac{h(w)}{w^{n+1}}\, dw \quad \text{and} \quad b_n = \frac{1}{2\pi i} \int_{C_r} h(w) w^{n-1}\, dw$$

for arbitrary $r_0 < r < R_0$.

Coming back to our exercise, note that since $f : \mathbb{H} \to \mathbb{C}$ is holomorphic and 1-periodic, it induces a well-defined holomorphic map on $A(0,1) = \{q \in \mathbb{C} : 0 < |q| < 1\}$ by $h(q) = f(z)$, where $q = e(z)$. Expanding h into its power series we get

$$f(z) = \sum_{n=0}^{\infty} a_n q^n + \sum_{n=1} b_n q^{-n}$$

where for any $0 < r < 1$ there exists $A_r := \sup_{|q|=r} |h(q)| < \infty$ such that $|a_n| \leq A_r r^{-n}$ for all $n \geq 0$, and $|b_n| \leq A_r r^n$ for all $n \geq 1$. In particular, both series converge absolutely for $z \in \mathbb{H}$. Recall that the Hecke operators for $N = 1$ and trivial multiplier act as

$$[T_n f](z) = \frac{1}{n} \sum_{ad=n} a^k \sum_{b \bmod d} f\left(\frac{az+b}{d}\right)$$

from which it follows that if $f(z) = \sum_{m\in\mathbb{Z}} c_m e(mz)$, with an absolutely convergent series for $z \in \mathbb{H}$, then (we reprove Lemma 5.2.5 with a general Laurent series expansion)

$$\begin{aligned}
[T_n f](z) &= \frac{1}{n} \sum_{m\in\mathbb{Z}} c_m \sum_{ad=n} a^k \sum_{b \bmod d} e\left(m\frac{az+b}{d}\right) \\
&= \sum_{m\in\mathbb{Z}} c_m \sum_{ad=n} a^{k-1} e\left(\frac{mn}{d^2} z\right) \frac{1}{d} \sum_{b \bmod d} e\left(m\frac{b}{d}\right) \\
&= \sum_{m\in\mathbb{Z}} c_m \sum_{\substack{ad=n \\ d|m}} a^{k-1} e\left(\frac{mn}{d^2} z\right) \\
&= \sum_{r\in\mathbb{Z}} \sum_{\substack{m\in\mathbb{Z},\, ad=n \\ d|m,\, mn=d^2 r}} c_m a^{k-1} e(rz) = \sum_{r\in\mathbb{Z}} \sum_{a|(n,r)} c_{\frac{rn}{a^2}} a^{k-1} e(rz).
\end{aligned}$$

To justify the last step, note that $ad = n$ implies that $mn = d^2 r$ is equivalent to $\frac{m}{d} a = r$, so necessarily $a \mid (n,r)$, and for any such a we solve $m = \frac{rd}{a} = \frac{rn}{a^2}$. In particular we observe that writing $[T_n f](z) = \sum_{r\in\mathbb{Z}} d_r e(rz)$ then

$$d_0 = \sigma_{k-1}(n)c_0, \quad d_1 = c_n, \quad \text{and} \quad d_{-1} = c_{-n}.$$

Now suppose that f is an eigenfunction of all the Hecke operators T_n, with eigenvalue λ_n. Then it follows that

$$\lambda_n c_0 = \sigma_{k-1}(n)c_0, \quad \lambda_n c_1 = c_n, \quad \text{and} \quad \lambda_n c_{-1} = c_{-n}. \tag{107}$$

If $c_0 \neq 0$, we deduce that $\lambda_n = \sigma_{k-1}(n)$. If in addition $c_{-1} \neq 0$, then $c_{-n} = \sigma_{k-1}(n)c_{-1}$. Since $k \geq 2$, letting $n \to \infty$ we obtain a contradiction to the bound

$$|c_{-n}| = |b_n| \leq A_r r^n$$

for any $0 < r < 1$ and A_r depending on r. Therefore, if $c_0 \neq 0$ we have seen that f is holomorphic at infinity, therefore $f \in M_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. In fact, we deduce the stronger statement that $c_n = \sigma_{k-1}(n)c_1$, so that f is of the form $f = c + dE_k$, and since $k \geq 2$ it must be $c = 0$ and $k \geq 4$ (since $M_2(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}}) = 0$).

On the other hand, if $c_0 = 0$ we have two cases. If $c_{-1} = 0$ then we are finished, since using (107) we deduce that $c_{-n} = 0$ for all $n \geq 1$, arriving at the conclusion that $f \in S_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. If $c_{-1} \neq 0$, then from (107) we see that

$$c_n = \frac{c_1}{c_{-1}} c_{-n} \text{ for all } n \geq 1 \quad \text{implying that } |c_n| \leq B_r r^{|n|} \text{ for all } n \in \mathbb{Z}$$

where $0 < r < 1$ is arbitrary and the constant B_r depends on f and r. From this bound, the function

$$f(z) = \sum_{n\in\mathbb{Z}} c_n e(nz) \tag{108}$$

initially defined only for $z \in \mathbb{H}$, admits an holomorphic extension to the entire complex plane $\mathbb{C}$ (since the power series on the right hand side converges absolutely for any $z \in \mathbb{C}$).

To get a contradiction, we recall Lemma 2.3.2, which asserted that if f is holomorphic in $\mathbb{H}$ and satisfies $f|_k\alpha = f$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, then $f \in S_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$ if and only if the function $g(z) := |\mathrm{Im}(z)^{k/2} f(z)|$ is bounded on $\mathbb{H}$. Observing that $g(\alpha z) = g(z)$ for any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, we deduce that g is bounded on $\mathbb{H}$ if and only if it is bounded on a fundamental domain $\mathcal{D}$. We can choose $\mathcal{D}$ to have the cusp at a point of $\mathbb{R}$ (not at infinity),[43] and then $\mathcal{D}$ is a bounded subset with compact closure in $\mathbb{C}$. Since f extends continuously to $\mathbb{C}$, we see that g is bounded on $\mathcal{D}$ and we conclude that $f \in S_k(\mathrm{SL}_2(\mathbb{Z}), \vartheta_{\mathrm{tr}})$. Since we assumed that $c_{-1} \neq 0$, we have found the contradiction we were looking for. ◻

[43]For example, let $S \in \mathrm{SL}_2(\mathbb{Z})$ be such that $S(z) = -1/z$ and consider $\mathcal{D} := S(\mathcal{F})$, where $\mathcal{F}$ is the usual fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ with the cusp at ∞. Then $\mathcal{D}$ is a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ with the cusp at 0.

The next result gives us valuable relations between the different Hecke Operators:[44]

Proposition 5.2.7. *Let $n, m \in \mathbb{N}$. Then*

$$T_n T_m = \sum_{\substack{d|(m,n),\\ (d,N)=1}} \chi(d) d^{k-1} T_{\frac{mn}{d^2}}.$$

Proof. We directly compute

$$mn \cdot [T_n T_m f](z) = \sum_{\substack{a_1 d_1 = m,\\ a_2 d_2 = n,\\ (a_1 a_2, N)=1}} \chi(a_1 a_2)(a_1 a_2)^k \sum_{\substack{b_1 \bmod d_1,\\ b_2 \bmod d_2}} f\left(\frac{a_1 a_2 z + a_1 b_2 + b_1 d_2}{d_1 d_2}\right).$$

We write $\delta = (a_1, d_2)$ and note that necessarily $\delta \mid (n, m)$. Put $a_1' = a_1/\delta$ and $d_2' = d_2/\delta$. Then we get

$$mn \cdot [T_n T_m f](z) = \sum_{\substack{\delta|(n,m),\\ (\delta,N)=1}} \chi(\delta)\delta^k \sum_{\substack{a_1' d_1 = m/\delta,\\ a_2 d_2' = n/\delta,\\ (a_1' a_2, N)=1,\\ (a_1', d_2')=1}} \chi(a_1' a_2)(a_1' a_2)^k \cdot \sum_{\substack{b_1 \bmod d_1,\\ b_2 \bmod d_2'\delta}} f\left(\frac{a_1' a_2 z + a_1' b_2 + b_1 d_2'}{d_1 d_2'}\right).$$

Note that since f is one periodic we find

$$\sum_{\substack{b_1 \bmod d_1,\\ b_2 \bmod d_2'\delta}} f\left(\frac{a_1' a_2 z + a_1' b_2 + b_1 d_2'}{d_1 d_2'}\right) = \delta \sum_{b \bmod d_1 d_2'} f\left(\frac{a_1' a_2 z + b}{d_1 d_2'}\right).$$

Finally we can write $a = a_1' a_2$ and $d = d_1 d_2'$. Then $ad = nm/\delta^2$ and $(a, N) = 1$. Note that we have a bijection

$$\{(a_1', a_2, d_1, d_2') \colon a_1' d_1 = m/\delta,\ a_2 d_2' = n/\delta,\ (a_1' a_2, N) = 1 \text{ and } (a_1', d_2') = 1\} \stackrel{1:1}{\leftrightarrow} \{(a, d) \colon ad = nm/\delta^2 \text{ and } (a, N) = 1\}.$$

Indeed the inverse assignment is given by

$$a_1' = \frac{m/\delta}{(m/\delta, d)},\ d_1 = (m/\delta, d),\ d_2' = \frac{d}{(m/\delta, d)} \text{ and } a_2 = \frac{a}{a_1'} = \frac{n/\delta}{d_2'}.$$

[44] In particular we obtain a direct proof that the Hecke operators are commutative.

Thus we see that

$$mn \cdot [T_n T_m f](z) = \sum_{\substack{\delta|(n,m),\\ (\delta,N)=1}} \chi(\delta)\delta^{k+1} \sum_{\substack{ad=nm/\delta^2,\\ (a,N)=1}} \chi(a)a^k \cdot \sum_{b \bmod d} f\left(\frac{az+b}{d}\right)$$
$$= \sum_{\substack{\delta|(n,m),\\ (\delta,N)=1}} \chi(\delta)\delta^{k+1} \cdot \frac{mn}{\delta^2} T_{mn/\delta^2}.$$

This completes the proof. ∎

This has two direct implications, which we will frequently use in what follows:

- The Hecke operators are multiplicative: $T_m T_n = T_{mn}$ if $(m,n) = 1$;
- For a prime p and $l \in \mathbb{N}$ we have

$$T_{p^{l+1}} = T_p T_{p^l} - \chi(p)p^{k-1}T_{p^{l-1}}. \tag{109}$$

Theorem 5.2.8. *Let $(n,N) = 1$. The operator T_n acting on $S_k(\Gamma_0(N),\chi)$ is normal and satisfies*

$$\langle T_n f, g\rangle = \chi(n)\langle f, T_n g\rangle \text{ for } f,g \in S_k(\Gamma_0(N),\chi).$$

Proof. By using (109) (inductively) and the multiplicative nature of the Hecke operators we observe that it is sufficient to check the desired property for T_p with p prime.

By definition we have

$$\langle T_p f, g\rangle = p^{k-1} \sum_{\alpha \in \Gamma_0(N)\backslash\Delta_N(p)} \chi^*(\alpha)^{-1}\langle f|_k\alpha, g\rangle.$$

As we have seen above we can take $\alpha = \begin{pmatrix} a & b \\ 0 & d\end{pmatrix}$. Put

$$\alpha' = p \cdot \alpha^{-1}.$$

We claim that

$$\langle f|_k\alpha, g\rangle = \langle f, g|_k\alpha'\rangle \tag{110}$$

From here we can finish the proof as follows. For $\gamma_1, \gamma_2 \in \Gamma_0(N)$ we compute

$$\chi^*(\alpha)^{-1}\langle f, g|_k[\alpha']\rangle = \chi(p)\langle f, \chi^*(\alpha')^{-1}g|_k\alpha'\rangle$$
$$= \chi(p)\langle f, \chi^*(\gamma_1\alpha'\gamma_2^{-1})^{-1}g|_k[\gamma_1\alpha'\gamma_2^{-1}]\rangle.$$

We can now choose γ_1 and γ_2 such that $\gamma_1\alpha'\gamma_2^{-1} = \alpha$. (To *guess* the right matrices is an exercise.) Inserting this above gives the desired result.

However, we still have to show (110). This is essentially a change of variables. Let $\mathcal{F}$ be a fundamental domain for $\Gamma(pN) \subseteq \Gamma_0(N)$. Then, for α as above, $f|_k\alpha$

is $\Gamma(pN)$ invariant. Recall $\mathrm{Im}(\alpha z) = \frac{\det(\alpha)}{|j_\alpha(z)|^2}\mathrm{Im}(z)$. We compute

$$\begin{aligned}
\det(\alpha)^k \cdot \langle f|_k\alpha, g|_k\alpha\rangle &= \frac{1}{[\overline{\Gamma(pN)} \colon \overline{\Gamma_0(N)}]}\int_{\mathcal{F}} f(\alpha z)\overline{g(\alpha z)}\,\mathrm{Im}(\alpha z)^k d\mu(z) \\
&= \frac{1}{[\overline{\Gamma(pN)} \colon \overline{\Gamma_0(N)}]}\int_{\alpha\mathcal{F}} f(z)\overline{g(z)}\,\mathrm{Im}(z)^k d\mu(z) \\
&= \langle f, g\rangle.
\end{aligned}$$

We are done since

$$g = g|_k[\alpha' \cdot \frac{1}{p}\alpha] = p^k[g|_k\alpha']|_k\alpha,$$

so that

$$\langle f|_k\alpha, g\rangle = p^k\langle f|_k\alpha, [g|\alpha']|_k\alpha\rangle = \langle f, g|_k\alpha'\rangle.$$

We make two observations that follow directly:

- If $(n,N)=1$ and $T_nf = \lambda_f(n)f$ then $\lambda_f(n) = \chi(n)\overline{\lambda_f(n)}$; and
- If f_1 and f_2 are two eigenfunctions of T_n (for $(n,N)=1$) with different eigenvalues then $\langle f_1, f_2\rangle = 0$.

Corollary 5.2.9. *The space $S_k(\Gamma_0(N),\chi)$ has an orthogonal basis of simultaneous eigenfunctions of all Hecke operators T_n with $(n,N)=1$.*

Lemma 5.2.10. *Assume that $f(z) = \sum_{m=1}^\infty a_f(m;\infty)e(mz) \in S_k(\Gamma_0(N),\chi)$ is an eigenfunction of T_n with eigenvalue $\lambda_f(n)$. Then*

$$\lambda_f(n)a_f(1;\infty) = a_f(n;\infty).$$

Proof. Write $T_nf = \lambda_f(n)f$ and compare Fourier coefficients using Lemma 5.2.5.

So far we have seen that the theory of the Hecke operators T_n is very nice as soon as $(n,N)=1$. Our next goal is to study the remaining operators.

Exercise 1, Sheet 11: Let $\Delta \in S_{12}(\mathrm{SL}_2(\mathbb{Z}),\vartheta_{\mathrm{tr}})$ be the Ramanujan function. Show that $\Delta(z)+\Delta(6z) \in S_{12}(\Gamma_0(6),\vartheta_{\mathrm{tr}})$ is not an eigenfunction of all Hecke operators.

Solution. Recall the definition of the Hecke operator T_n for $\Gamma_0(N)$, weight k and multiplier χ. In our particular case $N=6$, $k=12$ and $\chi=\vartheta_{\mathrm{tr}}$ we have

$$T_nf(z) = \frac{1}{n}\sum_{\substack{ad=n,\\(a,6)=1}} a^{12}\sum_{b \bmod d} f\left(\frac{az+b}{d}\right).$$

In particular, when $n = 6$ the only option for a is $a = 1$, and this gives

$$T_6 f(z) = \frac{1}{6} \sum_{b \bmod 6} f\left(\frac{z+b}{6}\right).$$

The result is that, if f has an expansion at infinity $f(z) = \sum_{n=0}^{\infty} a_n e(nz)$ then

$$T_6 f(z) = \frac{1}{6} \sum_{n=0}^{\infty} a_n e\left(\frac{nz}{6}\right) \sum_{b \bmod 6} e\left(\frac{nb}{6}\right) = \sum_{n \equiv 0 \bmod 6}^{\infty} a_n e\left(\frac{nz}{6}\right) = \sum_{n=0}^{\infty} a_{6n} e(nz)$$

(which is the formula of Lemma 5.2.5, since there we can only take $a = 1$). Writing $\Delta(z) = \sum_{n=1}^{\infty} \tau(n) e(nz)$ we obtain $T_6 \Delta(z) = \sum_{n=1} \tau(6n) e(nz)$. On the other hand

$$\Delta(6z) = \sum_{k=1}^{\infty} \tau(k) e(6kz) = \sum_{n=1}^{\infty} \delta_{6|n} \tau(n/6) e(nz)$$

and therefore,

$$(T_6 \Delta(6\cdot))(z) = \sum_{n=1}^{\infty} \tau(n) e(nz) = \Delta(z).$$

If $\Delta(\cdot) + \Delta(6\cdot)$ was an eigenfunction for T_6, then for some $\lambda \in \mathbb{C}$ it would hold that

$$\lambda \left(\sum_{n=1}^{\infty} \tau(n) e(nz) + \sum_{n=1}^{\infty} \tau(n) e(6nz) \right) = T_6(\Delta(\cdot) + \Delta(6\cdot))(z) = \sum_{n=1}^{\infty} \tau(6n) e(nz) + \sum_{n=1}^{\infty} \tau(n) e(nz).$$

After equating coefficients, this is equivalent to

$$\tau(n) + \tau(6n) = \lambda \tau(n) + \lambda \delta_{6|n} \tau\left(\frac{n}{6}\right) \qquad \text{for } n \in \mathbb{Z}_{\geq 1}.$$

Putting $n = 1$, using $\tau(1) = 1$ we get $\tau(6) = \lambda - 1$, and putting $n = 2$ we get $\tau(12) = (\lambda - 1)\tau(2) = \tau(6)\tau(2)$. By looking at a table of values we can see that this identity does not hold ($\tau(2) = -24$, $\tau(6) = -6048$ and $\tau(12) = -370944$). ◻

Definition 5.2.1. We define the conductor of a Dirichlet character χ modulo N to be the smallest (positive integer) $q = \mathrm{cond}(\chi)$ such that $\chi(n + qm) = \chi(n)$ for all $n, m \in \mathbb{Z}$ with $(n, N) = (n + qm, N) = 1$. Of course this implies $q \mid N$. We call the character $\chi_0(n) = \delta_{(n,N)=1}$ the principal character modulo N. Further we call χ a primitive character modulo N if $\mathrm{cond}(\chi) = N$. (Note that for us the principle character χ_0 counts as a primitive character modulo 1. This is not standard!)

The idea behind this definition is the following. If $M \mid N$, then we have the canonical (surjective) map

$$p_{N \to M} \colon (\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/M\mathbb{Z})^\times$$

This can be used to lift a character χ of $(\mathbb{Z}/M\mathbb{Z})^\times$ to a character χ' on $(\mathbb{Z}/N\mathbb{Z})^\times$ by setting

$$\chi'(n) = \chi(p_{N \to M}(n)).$$

Recall that Dirichlet characters modulo N are nothing but characters of $(\mathbb{Z}/N\mathbb{Z})^\times$ that are extended to $\mathbb{Z}$ in the obvious way. One finds that χ is primitive if and only if χ is not obtained from a character of $(\mathbb{Z}/M\mathbb{Z})^\times$ when M is a proper divisor of N.

A similar (but slightly more complicated) phenomenon occurs for modular forms. A taste of what follows can be explicitly observed when taking a closer look at the Eisenstein space:

Remark 5.2.11. Recall that $M_k(\Gamma_0(N),\chi) = E_k(\Gamma_0(N),\chi) \oplus S_k(\Gamma_0(N),\chi)$. It is desirable to also find a convenient basis for the (non cuspidal) part of the space that is spanned by Eisenstein series. For $N = 1$ this is no problem, since we have seen by Remark 5.2.6 that E_k is an eigenfunction of all Hecke operators. In general one has to work a little harder.

Let us assume $k \geq 3$ to avoid convergence problems. Then a basis of $E_k(\Gamma_0(N),\chi)$ is given by the Eisenstein series $E_{\mathfrak{a}}$ associated to singular cusps $\mathfrak{a}$. This basis usually does not diagonalize the Hecke operators.

Instead we will consider the following Eisenstein series:

$$E_{\chi_1,\chi_2}(z) = \frac{1}{2} \sum_{\substack{(c,d)=1,\\ (c,N_1)=(d,N_2)=1}} \frac{\chi_1(c)\chi_2(d)}{(cN_2z+d)^k},$$

attached to two primitive Dirichlet characters χ_i modulo N_i (with $i = 1, 2$). One checks that $E_{\chi_1,\chi_2}(z) \in M_k(\Gamma_0(N_1N_2), \chi_1\chi_2^{-1})$. The Fourier expansion reads

$$E_{\chi_1,\chi_2}(z) = \delta_{N_1=1} + C_k(\chi_1,\chi_2) \cdot \sum_{m=1}^{\infty} \sigma_{\chi_1,\chi_2,k-1}(m)e(mz),$$

where

$$\begin{aligned} C_k(\chi_1,\chi_2) &= \frac{(-i2\pi)^k \tau(\chi_2)}{N_2^k \Gamma(k) L(k,\chi_1\chi_2)} \text{ and} \\ \sigma_{\chi_1,\chi_2,k-1}(m) &= \sum_{\substack{ab=m,\\ (a,N_1)=(b,N_2)=1}} \chi_1(a)\chi_2(b)^{-1}b^{k-1}. \end{aligned}$$

Note that the Fourier coefficient $\sigma_{\chi_1,\chi_2,k-1}(m)$ is a generalized divisor sum. Furthermore

$$\tau(\chi_2) = \frac{1}{\sqrt{N_2}} \sum_{\substack{x \bmod N_2,\\ (x,N_2)=1}} \chi_2(x) e\left(\frac{x}{N_2}\right)$$

is a (generalized) Gauß sum and

$$L(s,\chi_1\chi_2) = \sum_{\substack{n=1,\\ (n,N_2)=1}}^{\infty} [\chi_1\chi_2](n)n^{-s}$$

is a Dirichlet L-function. We have omitted the proofs for the properties summarized above, since they are routine modification of the arguments in Section 2.5.

Repeating the computation from Remark 5.2.6 shows that

$$T_n E_{\chi_1,\chi_2}(z) = \sigma_{\chi_1,\chi_2,k-1}(n) \cdot E_{\chi_1,\chi_2}(z)$$

for all n. We call $E_{\chi_1,\chi_2}(z) \in M_k(\Gamma_0(N_1N_2), \chi_1\chi_2^{-1})$ (holomorphic) newform Eisenstein series (of weight k). Keep in mind that we have only considered primitive characters χ_1 and χ_2 so far.

To generate the space $E_k(\Gamma_0(N),\chi)$ we first recall that a full set of non-equivalent cusps for $\Gamma_0(N)$ is given by $\frac{u}{v}$ with $v \mid N$, $(u,v)=1$ and u mod $(v, N/v)$. One can explicitly compute a scaling matrix and observe that $\frac{u}{v}$ is singular with respect to χ if and only if χ is $\frac{N}{(v,N/v)}$-periodic. In particular, if χ has conductor q, then there are

$$\sharp\{\text{singular cusps}\} = \sum_{\substack{v\mid N,\\ (v,N/v)\mid \frac{N}{q}}} \varphi((v,N/v)).$$

For $k \geq 3$ this is precisely the dimension of $E_k(\Gamma_0(N),\chi)$ because

$$E_k(\Gamma_0(N),\chi) = \langle E_{\mathfrak{a}}(z) \colon \mathfrak{a} \text{ singular cusp}\rangle.$$

We claim that one also has

$$\begin{aligned} E_k(\Gamma_0(N),\chi) = \langle E_{\chi_1,\chi_2}(Mz) \colon \chi_i &\text{ primitive character modulo } N_i \\ &\text{and } MN_1N_2 \mid N \text{ and } \chi = \chi_1\chi_2^{-1}\rangle. \end{aligned}$$

To prove this one could proceed as follows. First, it is easy to see that the Eisenstein series $E_{\chi_1,\chi_2}(Mz)$ appearing on the right hand side are linearly independent. Second, one checks that they are orthogonal to cusp-forms. Finally one can match up the dimension. Let us remark that one can actually compute an explicit change of basis between the two sets of Eisenstein series considered above.

Motivated by these observations we make the following definition. Let χ be a Dirichlet character modulo N with conductor q. For $q \mid N' \mid N$ and $M \mid \frac{N}{N'}$ we define

$$\iota_{N',M} \colon S_k(\Gamma_0(N'),\chi) \to S_k(\Gamma_0(N),\chi), f \mapsto f|_k a_M,$$

where $a_d = \operatorname{diag}(M,1)$. The images of these maps (with $N' \neq N$) make up the those modular forms (of level N, weight k and nebentypus χ) that come from smaller levels. These play the same role as non-primitive Dirichlet characters. We define

$$S_k^\flat(\Gamma_0(N),\chi) = \langle \iota_{N',M} f \colon q \mid N' \mid N,\ N' \neq N,\ M \mid \frac{N}{N'} \text{ and } f \in S_k(\Gamma_0(N'),\chi)\rangle.$$

Elements of this space are called oldforms. We denote the orthogonal complement by

$$S_k^\sharp(\Gamma_0(N),\chi) = [S_k^\flat(\Gamma_0(N),\chi)]^\perp.$$

Lemma 5.2.12. *The spaces $S_k^\sharp(\Gamma_0(N),\chi)$ and $S_k^\flat(\Gamma_0(N),\chi)$ are stable under the Hecke Operators T_n with $(n,N)=1$.*

Proof. This follows from the diagram

$$\begin{array}{ccc} S_k(\Gamma_0(N'),\chi)) & \xrightarrow{T_n} & S_k(\Gamma_0(N'),\chi)) \\ \big\downarrow{\scriptstyle \iota_{N',M}} & & \big\downarrow{\scriptstyle \iota_{N',M}} \\ S_k(\Gamma_0(N),\chi)) & \xrightarrow{T_n} & S_k(\Gamma_0(N),\chi)) \end{array}$$

which is easily seen to be commutative. ◻

Exercise 2, Sheet 11: Let $N>1$ be an integer and let $M \mid N$ be a divisor of N. Let $f \in S_k(\Gamma_0(N),\theta_{\mathrm{tr}})$. Show that the following two properties are equivalent:

i) f is orthogonal to $\langle i_{N/M,1}(g) : g \in S_k(\Gamma_0(N/M),\vartheta_{\mathrm{tr}})\rangle$;

ii) f satisfies

$$\frac{1}{[\Gamma_0(N/M):\Gamma_0(N)]}\sum_{\alpha\in\Gamma_0(N)\backslash\Gamma_0(N/M)} f|_k\alpha \equiv 0.$$

Solution. Recall the following fact from functional analysis.

Proposition 5.2.13. *Let H_1,H_2 be Hilbert spaces, $T : H_1 \to H_2$ a continuous linear map and let $T^* : H_2 \to H_1$ be its adjoint, which is automatically continuous, and is defined as the unique linear map that satisfies*

$$\langle Tv,w\rangle_{H_2} = \langle v,T^*w\rangle_{H_1} \text{ for all } v\in H_1, w\in H_2$$

Then the kernel of T^* is equal to the orthogonal complement of the image of T. In symbols, we have $T(H_1)^\perp = \ker(T^*)$.

Proof. Let $w \in H_2$. Then

$$w\in\ker(T^*) \text{ iff } \langle v,T^*w\rangle_{H_1}=0 \text{ for all } v\in H_1 \text{ iff } \langle Tv,w\rangle_{H_2}=0 \text{ for all } v\in H_1 \text{ iff } w\in T(H_1)^\perp.$$

◻

We now show that the maps $i_{N/M,1} : S_k(\Gamma_0(N/M),\vartheta_{\mathrm{tr}}) \to S_k(\Gamma_0(N),\vartheta_{\mathrm{tr}})$ and $p_{N,N/M} : S_k(\Gamma_0(N),\vartheta_{\mathrm{tr}}) \to S_k(\Gamma_0(N/M),\vartheta_{\mathrm{tr}})$ given by

$$p_{N,N/M}(f) = \frac{1}{[\Gamma_0(N/M):\Gamma_0(N)]}\sum_{\alpha\in\Gamma_0(N)\backslash\Gamma_0(N/M)} f|_k\alpha$$

are adjoint with respect to the following normalization of the Petersson inner product. For a congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, define the inner product on the space $S_k(\Gamma,\vartheta)$ by

$$\langle f,g\rangle_\Gamma := \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma]}\int_{\mathcal{F}_\Gamma} f(z)\overline{g(z)}y^k\frac{dx\,dy}{y^2}$$

where $\mathcal{F}_\Gamma$ is a fundamental domain for Γ. In our case, let $\mathcal{F}_{N/M}$ be a fundamental domain for $\Gamma_0(N/M)$ and note that a fundamental domain for $\mathcal{F}_N$ is given by

$$\mathcal{F}_N = \bigsqcup_{\alpha\in\Gamma_0(N)\backslash\Gamma_0(N/M)} \alpha\mathcal{F}_{N/M}$$

Then

$$\begin{aligned}
\langle i_{N/M,1}(g), f\rangle_{\Gamma_0(N)} &= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(N)]}\int_{\mathcal{F}_N} g(z)\overline{f(z)}y^k\frac{dx\,dy}{y^2}\\
&= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(N)]}\sum_{\alpha\in\Gamma_0(N)\backslash\Gamma_0(N/M)}\int_{\alpha\mathcal{F}_{N/M}} g(z)\overline{f(z)}y^k\frac{dx\,dy}{y^2}\\
&= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(N)]}\sum_{\alpha\in\Gamma_0(N)\backslash\Gamma_0(N/M)}\int_{\mathcal{F}_{N/M}} [g|_k\alpha](z)\overline{[f|_k\alpha](z)}y^k\frac{dx\,dy}{y^2}\\
&= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(N/M)]}\frac{1}{[\Gamma_0(N/M):\Gamma_0(N)]}\sum_{\alpha\in\Gamma_0(N)\backslash\Gamma_0(N/M)}\int_{\mathcal{F}_{N/M}} g(z)\overline{[f|_k\alpha](z)}y^k\frac{dx\,dy}{y^2}\\
&= \frac{1}{[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(N/M)]}\int_{\mathcal{F}_{N/M}} g(z)\,\overline{p_{N,N/M}(f)(z)}y^k\frac{dx\,dy}{y^2} = \langle g, p_{N,N/M}(f)\rangle_{\Gamma_0(N/M)}.
\end{aligned}$$

Therefore, $i_{N/M,1}$ and $p_{N,N/M}$ are adjoint and the exercise follows by the proposition above. ⌧

Example 5.2.14. It turns out that $S^\sharp_{12}(\Gamma_0(2),\vartheta_{\mathrm{tr}}) = \{0\}$. In particular, we find that

$$S_{12}(\Gamma_0(2),\vartheta_{\mathrm{tr}}) = \langle \iota_{1,1}(\Delta), \iota_{1,2}(\Delta)\rangle.$$

Note that these are eigenfunctions of all Hecke operators T_n with $2\nmid n$. Let us compute the action of

$$T_2 f(z) = \frac{1}{2}\left[f\left(\frac{z}{2}\right) + f\left(\frac{z+1}{2}\right)\right]$$

on these functions. It is easy to see that $T_2\iota_{1,2}(\Delta) = \iota_{1,1}(\Delta)$. To compute its action on $\iota_{1,1}(\Delta)$ we recall the Fourier expansions

$$\begin{aligned}
\iota_{1,1}(\Delta)(z) &= 1\cdot e(z) - 24\cdot e(2z) + 252\cdot e(3z) - 1472\cdot e(4z) + \ldots \text{ and}\\
\iota_{1,2}(\Delta)(z) &= 0\cdot e(z) + 1\cdot e(2z) + 0\cdot e(3z) - 24\cdot e(4z) + \ldots.
\end{aligned}$$

We compute

$$\begin{aligned}
T_2\iota_{1,1}(\Delta)(z) &= \frac{1}{2}[\Delta(\frac{z}{2}) + \Delta(\frac{z+1}{2})] = \sum_{m=0}^\infty \tau(2n)e(mz)\\
&= -24e(z) - 1472e(2z) - 6048e(3z) + 84480\cdot e(4z) + \ldots.
\end{aligned}$$

By comparing (the first two) Fourier coefficients we find that

$$T_2\iota_{1,1}(\Delta)(z) = -24\iota_{1,1}(\Delta)(z) - 2048\cdot\iota_{1,2}(\Delta)(z).$$

In summary, the action of T_2 on $S_{12}(\Gamma_0(2), \vartheta_{\mathrm{tr}})$ (with respect to the basis $\{\iota_{1,1}(\Delta), \iota_{1,2}(\Delta)\}$ is given by the matrix

$$\begin{pmatrix} -24 & 1 \\ -2048 & 0 \end{pmatrix}.$$

This turns out to be diagonalizable (over $\mathbb{C}$).

Our hope is that the space $S_k^\sharp(\Gamma_0(N), \chi)$ has a convenient basis. Furthermore, it is reasonable to expect that the spaces $S_k^\sharp(\Gamma_0(N'), \chi)$ can be used to study $S_k^\flat(\Gamma_0(N), \chi)$. The following theorem is the technical key input.

Theorem 5.2.15 (Atkin-Lehner 1970)**.** *Let* $f(z) = \sum_{m=1}^\infty a_f(m; \infty) e(mz) \in S_k(\Gamma_0(N), \chi)$ *such that* $a_f(m; \infty) = 0$ *whenever* $(m, N) = 1$*, then* $f \in S_k^\flat(\Gamma_0(N), \chi)$*.*

Proof. Long and technical, but essentially elementary. We sketch the steps, but leave out several technical details.

Let $p_1, \ldots, p_r$ be the prime divisors of N. We say that f is of length s, if $a_f(m; \infty) = 0$ unless $p_i \mid m$ for some $1 \leq i \leq s$. We will show the following statement, which allows one to complete the argument via induction. Suppose $f \in S_k(\Gamma_0(N), \chi)$ is of length $\leq s$, then there is $h \in S_k(\Gamma_0(N/p_s), \chi)$ such that $f - \iota_{N/p_s, p_s} h$ is of length $\leq s - 1$.

We define the two operators

$$V_p f(z) = f(pz) \text{ and } U_p f(z) = \sum_{m \equiv 0 \bmod p} a_f(m; \infty) e(\frac{m}{p} z).$$

(Note that in some sense $V_p = \iota_{N,p}$.) We observe that

$$[V_p U_p f](z) = \sum_{m \equiv 0 \bmod p} a_f(m; \infty) e(mz).$$

In particular the condition that f is of length $\leq s$ can be written as

$$0 = \prod_{i=1}^{s} (\mathrm{id} - V_p U_p) f.$$

We first look at the situation when χ is not defined modulo N/p_s. Then we claim that $V_p U_p f = 0$. Put $\tilde{f} = U_{p_s} f$ and observe that $\tilde{f}|_k T = \tilde{f}$. In particular we see that $V_{p_s} \tilde{f}(z + \frac{1}{p}) = V_{p_s} \tilde{f}(z)$. We abuse notation and write $V_{p_s} \tilde{f}(z + \frac{1}{p}) = V_{p_s} \tilde{f}|_k T^{\frac{1}{p}}$ where $T^{\frac{1}{p}} = \begin{pmatrix} 1 & 1/p \\ 0 & 1 \end{pmatrix}$. On the other hand

$$B_N = \begin{pmatrix} 1 & 1 \\ N & N+1 \end{pmatrix} \in \Gamma_0(N).$$

Thus $V_{p_s}\tilde{f}|_k B_N = V_{p_s}\tilde{f}$ since $\chi(B_N) = 1$. Set

$$A_N(u,v) = T^{\frac{u}{p}} B_N t^{\frac{v}{p}} = \begin{pmatrix} 1 + \frac{N}{p_s}u & 1 + \frac{N}{p_s}u + \frac{u+v+Nuv/p_s}{p_s} \\ N & 1 + \frac{N}{p_s}v + N \end{pmatrix},$$

so that

$$V_{p_s}\tilde{f} = V_{p_s}\tilde{f}|_k A_N(u,v) = \chi(A_N(u,v))V_p\tilde{f}.$$

Note that here we select $u, v \in \mathbb{Z}$ with $p_s \mid (u + v + Nuv/p_s)$. The point is that one can play around with u and v to cook up a combination with $\chi(A_N(u,v)) \neq 1$, which implies that f must vanish.[45] In conclusion, if we suppose that χ is not defined modulo N/p_s we find that

$$0 = \prod_{i=1}^{s}(\mathrm{id} - V_pU_p)f = \prod_{i=1}^{s-1}(\mathrm{id} - V_pU_p)f.$$

We conclude that f is itself of length $\leq s-1$ and we are done.

The case when $p_s^2 \mid N$ and χ is defined modulo N/p_s can be treated as follows. In this case we claim that

$$U_{p_s}f \in S_k(\Gamma_0(N/p_s), \chi). \tag{111}$$

With this at hand we can put $h = U_{p_s}f$ and observe that $V_{p_s}U_{p_s}f = \iota_{N/p_s}h$. Thus we have

$$0 = \prod_{i=1}^{s}(\mathrm{id} - V_pU_p)f = \prod_{i=1}^{s-1}(\mathrm{id} - V_pU_p)[f - \iota_{N/p_s,p_s}h].$$

In particular we see that $f - \iota_{N/p_s,p_s}h$ has length $\leq s-1$ as desired. To see (111) we (again) observe that

$$U_pf(z) = \frac{1}{p}\sum_{b=0}^{p-1} f\left(\frac{z+b}{p}\right).$$

Now put $\tilde{f}(z) = f(p_s^{-1}z)$. It is easy to check that $\tilde{f} \in S_k(\Gamma_0(N/p_s, p_s), \chi)$ where

$$\Gamma_0(N/p_s, p_s) = \left\{ \begin{pmatrix} * & b \\ * & * \end{pmatrix} \in \Gamma_0(N/p_s) \colon p_s \mid b \right\}.$$

Now $U_pf(z) = \frac{1}{p}\sum_{b=0}^{p-1}[\tilde{f}|_kT^b](z)$. But we can check that for $p_s \mid N/p_s$ one has

$$\Gamma_0(N/p_s) = \bigsqcup_{b=0}^{p-1} \Gamma_0(N/p_s, p_s)T^b.$$

Thus the claim is now obvious since we average over a system of representatives for $\Gamma_0(N/p_s, p_s)\backslash\Gamma_0(N/p_s)$.

[45] Finding these combinations of u and v is not to hard and we leave it as an exercise to do so. This crucially uses that χ is not defined modulo N/p_s.

Finally we suppose that $p_s \mid N$, $p_s^2 \nmid N$ and χ is defined modulo N/p_s. Without loss of generality we can assume that all primes $p_1, \dots, p_s$ have these properties. (Otherwise we simply re-order them and apply one of the earlier cases.) We set

$$f^{(i+1)} = \prod_{j=1}^{i} (\mathrm{id} - V_{p_j} U_{p_j}) f \text{ and } g_i = U_{p_i} f^{(i)}.$$

Note that $f = \sum_{i=1}^{s} V_{p_i} g_{p_i}$. One can check that

$$V_{p_i} g_i \in S_k(\Gamma_0(Np_1 \cdots p_i)) \subseteq S_k(\Gamma_0(N^2/p_s), \chi) \text{ for } i < s.$$

In particular,

$$V_{p_s} g_s = f - \sum_{i=1}^{s-1} V_{p_i} g_i \in S_k(\Gamma_0(N^2/p_s), \chi).$$

This suffices to conclude that $g_s \in S_k(\Gamma_0(N^2/p_s^2), \chi)$. As before we write

$$[U_{p_s} f](z) = \frac{1}{p_s} \sum_{b=0}^{p_s - 1} [\tilde{f}|_k T^b](z) \text{ with } \tilde{f}(z) = f(z/p_s).$$

Recall that $\tilde{f}(z) \in S_k(\Gamma_0(N/p_s, p_s), \chi)$. Since by assumption $p_s \nmid N/p_s$ we now have

$$\Gamma_0(N/p_s) = \Gamma_0(N/p_s, p_s) \underbrace{\begin{pmatrix} p_s x & 1 \\ \frac{N^2}{p_s^2} y & 1 \end{pmatrix}}_{=Q \in \mathrm{SL}_2(\mathbb{Z})} \sqcup \bigsqcup_{b=0}^{p_s - 1} \Gamma_0(N/p_s, p_s) T^b,$$

for suitable $x, y \in \mathbb{Z}$. We can thus write

$$[U_{p_s} f](z) = \underbrace{\frac{1}{p_s} \sum_{\alpha \in \Gamma_0(N/p_s, p_s) \backslash \Gamma_0(N/p_s)} [\tilde{f}|_k \alpha](z)}_{=h(z) \in S_k(\Gamma_0(N/p_s), \chi)} - \underbrace{\frac{1}{p_s} [\tilde{f}|_k Q](z)}_{=:[W_{p_s} f](z)}.$$

Since $g_s \in S_k(\Gamma_0(N^2/p_s^2), \chi)$ and $Q \in \Gamma_0(N^2/p_s^2)$ we have

$$W_p V_p g_s = \frac{1}{p_s} g_s|_k Q = \frac{1}{p_s} g_s.$$

We now compute

$$\begin{aligned} h = U_{p_s} f + W_{p_s} f &= \sum_{i=1}^{s} [U_{p_s} V_{p_i} g_i + W_{p_s} V_{p_i} g_i] \\ &= (1 + \frac{1}{p}) g_s + \sum_{i=1}^{s-1} [V_{p_i} U_{p_s} g_i + W_{p_s} V_{p_i} g_i]. \end{aligned}$$

Finally this allows us to write

$$f-(1-\frac{1}{p})^{-1}V_{p_s}h = f-V_p g_s-(1-\frac{1}{p_s})^{-1}\sum_{i=1}^{s-1}[V_{p_s}V_{p_i}U_{p_s}g_i+V_{p_s}W_{p_s}V_{p_i}g_i] \in S_k(\Gamma_0(N),\chi).$$

It turns out that the right hand side is of length $s-1$. (This is particularly easy to see for the case $s=1$.) ◻

Theorem 5.2.16 (Multiplicity One). *Let $0 \neq f(z) \in S_k^{\sharp}(\Gamma_0(N),\chi)$ be an eigenfunction of all Hecke-operators T_n with $(n,N)=1$. Then we have*

(1) $a_f(1;\infty) \neq 0$.
(2) *If $g \in S_k^{\sharp}(\Gamma_0(N),\chi)$ is another eigenfunction of all Hecke-operators T_n with $(n,N)=1$. Suppose that $\lambda_f(n)=\lambda_g(n)$ for all $(n,N)=1$, then $g \in \mathbb{C}f$. (Here $T_n f = \lambda_f(n) f$ and $T_n g = \lambda_g(n) g$.)*
(3) *f is automatically an eigenfunction of all Hecke eigenvalues. (Also of those with $(n,N)>1$!)*
(4) *We can normalize f so that $a_f(1,\infty)=1$, then we have $a_f(m,\infty)=\lambda_f(m)$ for all $m \in \mathbb{N}$. In particular, the Fourier coefficents of f at infinity are multiplicative.*

Proof. We start by observing that if $a_f(1,\infty)=0$, then by Lemma 5.2.10 we have $a_f(m,\infty)=0$ for all $(m,N)=1$. Applying the previous theorem yields $f \in S_k^{\flat}(\Gamma_0(N),\chi)$. This is a contradiction.

Thus from now on we can assume $a_f(1,\infty)=1$ so that $a_f(m,\infty)=\lambda_f(m)$ for $(m,N)=1$. Let g be as in (2). Without loss of generality we can assume that $a_g(1,\infty)=1$ as well. We observe then that the mth Fourier coefficient of $f-g$ vanish for $(m,N)=1$. Thus we have $f-g \in S_k^{\flat}(\Gamma_0(N),\chi)$. But this is another contradiction.

Let T_n be any Hecke operator with $n \in \mathbb{N}$. We put $g = T_n f \in S_k(\Gamma_0(N),\chi)$. Our goal is to show that g is a multiple of f (i.e. f is an eigenform of T_n.) Since the Hecke operators commute we have $T_m g = \lambda_f(m) g$ for all $(m,N)=1$. We write $g = g^{\sharp}+g^{\flat}$ for $g^{\sharp} \in S_k^{\sharp}(\Gamma_0(N),\chi)$ and $g^{\flat} \in S_k^{\flat}(\Gamma_0(N),\chi)$. We first observe that $T_m g^{\sharp} = \lambda_f(n) g^{\sharp}$, so that $g^{\sharp} \in \mathbb{C}f$. It remains to be seen that $g^{\flat}=0$. By definition of the old-space and an inductive argument we can write

$$g^{\flat}(z) = \sum_{\substack{q|N'|N,\\ N'\neq N}} \sum_{M|N/N'} \iota_{N',M}(h_{N',M}) \text{ for } h_{N',M} \in S_k^{\sharp}(\Gamma_0(N'),\chi).$$

The $h_{N',M}$ are eigenfunctions of all T_m with $(m,N)=1$. Note that they all have the same Hecke-eigenvalues, namely $\lambda_f(m)$ (for $(m,N)=1$). Suppose there is $h_{N',M} \neq 0$, then we find $\alpha \neq 0$ so that $h_{N',M}-\alpha f \in S_k^{\flat}(\Gamma_0(N),\chi)$. But this implies

$$f = -\alpha^{-1}(h_{N',M}-\alpha f)+\alpha^{-1}h \in S_k^{\flat}(N,\chi),$$

which is a contradiction. ◻

Definition 5.2.2. If $f \in S_k^\sharp(\Gamma_0(N),\chi)$ is an eigenfunction of all Hecke-operators and $a_f(1,\infty)=1$, then we call f a newform.

Remark 5.2.17. The newforms form an orthogonal basis of $S_k^\sharp(\Gamma_0(N),\chi)$. Note that the definition includes the so called *arithmetic normalization* $a_f(1,\infty) = 1$. Another natural normalization would be $\langle f,f\rangle = 1$. This is the analytic normalization. Passing between the two normalizations is possible using the so called Rankin-Selberg method and the scaling factor involved turns out to be a rather interesting number associated to f.

Let us get back to (what we claimed to be) Hecke's motivation. Given a Dirichlet character ξ modulo M and $f \in M_k(\Gamma_0(N),\chi)$ we associate the twisted L-function

$$L(s,f,\xi) = \sum_{n=1}^{\infty} \xi(n)a_f(n;\infty)\cdot n^{-\frac{k-1}{2}-s}.$$

If $f \in S_k(\Gamma_0(N),\chi)$, then this is absolutely convergent for $\mathrm{Re}(s) > 5/4$. Indeed, recall that by Theorem 4.2.2 we have[46]

$$|L(s,f,\xi)| \leq C_{f,\epsilon}\sum_{n=1}^{\infty} n^{\frac{1}{4}-\mathrm{Re}(s)+\epsilon}.$$

(With a bit more care or by using (91) which is known in the case under consideration this can be improved to show absolute convergence for $\mathrm{Re}(s) > 1$.)

Lemma 5.2.18. *Suppose f is an eigenfunction of all Hecke operators, then we have*

$$L(s,f,\xi) = a_f(1;\infty)\cdot\prod_p \left(1-\xi(p)\lambda_f(p)p^{-\frac{k-1}{2}-s}+\chi(p)\xi(p)^2p^{-2s}\right)^{-1}$$

in the region of absolute convergence.

Proof. First, we recall that by Lemma 5.2.10 we have $a_f(n;\infty) = \lambda_f(n)a_f(1;\infty)$. Since the Hecke-operators are multiplicative the fundamental theorem of arithmetic implies that

$$L(s,f,\xi) = a_f(1;\infty)\cdot\prod_p\left(\sum_{k=0}[\xi(p)p^{-s}]^k\lambda_f(p^k)\right)$$

Finally, the result follows by inductively using the recursion $T_{p^{k+1}} = T_pT_{p^k} - \chi(p)p^{k-1}T_{p^{k-1}}$ given in (109). ∎

In particular, if $f \in S_k(\Gamma_0(N),\chi)$ is a newform, then the associated (twisted) L-function will have a nice Euler product involving only the Hecke eigenvalues

[46]Note that the statement of Theorem 4.2.2 does not directly apply to the situation at hand, but the same argument gives the desired result.

$\lambda_f(p)$ and the values of the characters ξ and χ on primes. We will see now that more is true.

Remark 5.2.19. We write $L(s, f) = L(s, f, 1)$, where we wrote 1 for the principal charter modulo 1. We also define

$$[\xi \otimes f](z) = \sum_{n=1}^{\infty} \xi(n) a_f(n; \infty).$$

Thus we can write

$$L(s, f, \xi) = L(s, \xi \otimes f).$$

If $f \in S_k(\Gamma_0(N), \chi)$ is a newform and ξ is a primitive character modulo M with $(M, N) = 1$, then $\xi \otimes f$ is a scalar multiple of a newform in $S_k(\Gamma_0(M^2N), \chi\xi^2)$. This statement is slightly stronger than what will be needed below, so that we leave the proof as an exercise.

Proposition 5.2.20. *Let $f \in S_k(\Gamma_0(N), \chi)$ and let ξ be a primitive Dirichlet character modulo M with $(M, N) = 1$. Define*

$$\Lambda(s, f, \xi) = (2\pi)^{-\frac{k-1}{2} - s} \Gamma(\frac{k-1}{2} + s) L(s, f, \xi).$$

We have

$$\Lambda(s, f, \xi) = i^k \xi(N) \chi(M) \frac{\tau(\xi)^2}{M} (M^2N)^{\frac{1}{2} - s} \Lambda(1 - s, g, \xi^{-1}).$$

Here $g = N^{\frac{k}{2}} f|_k w_N$ with $w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$.

Proof. We first note that $f|_k w_N \in S_k(\Gamma_0(N), \chi^{-1})$. To see this one notes that w_N normalizes $\Gamma_0(N)$. A direct computation shows the correct transformation behavior:

$$f|_k w_N|_k \gamma = f|_k w_N \gamma w_N^{-1}|_k w_N = \chi(\gamma)^{-1} f|_k w_N.$$

For notational simplicity we write $g = f|_k w_N$.

We start from the identity

$$\xi(n) e(nz) = \frac{\xi(-1)\tau(\xi)}{M} \sum_{\substack{x \bmod M, \\ (x,M)=1}} \xi(x)^{-1} e(n \frac{z + x}{M}).$$

Thus

$$[\xi \otimes f](z) = \frac{\xi(-1)\tau(\xi)}{M} \sum_{\substack{x \bmod M, \\ (x,M)=1}} \xi(x)^{-1} [f|_k \alpha_{x,M}](z) \text{ with } \alpha_{x,M} = \begin{pmatrix} M & x \\ 0 & M \end{pmatrix}.$$

This allows us to compute

$$
\begin{aligned}
[\xi\otimes f]|_k w_{M^2N}(z) &= (NM)^{-k}\left[(\xi\otimes f)|_k\begin{pmatrix}0 & \frac{-1}{MN}\\ M & 0\end{pmatrix}\right](z)\\
&= \frac{\xi(-1)\tau(\xi)}{N^{\frac{k}{2}}M^{1+k}}\sum_{\substack{x \bmod M,\\ (x,M)=1}}\xi(x)^{-1}\cdot\left[g|_k\begin{pmatrix}0 & 1\\ -N & 0\end{pmatrix}\begin{pmatrix}M & x\\ 0 & M\end{pmatrix}\begin{pmatrix}0 & \frac{-1}{MN}\\ M & 0\end{pmatrix}\right](z)\\
&= \frac{\xi(-1)\tau(\xi)}{N^{\frac{k}{2}}M^{1+k}}\sum_{\substack{x \bmod M,\\ (x,M)=1}}\xi(x)^{-1}\cdot\left[g|_k\begin{pmatrix}M & -r\\ -Nx & s\end{pmatrix}\begin{pmatrix}M & r\\ 0 & M\end{pmatrix}\right](z),
\end{aligned}
$$

where $r=r(x)$ and $s=s(x)$ are integers with $Ms-rNx=1$. Note that $\xi(x)^{-1}=\xi(-N)\xi(r)$. Further we have

$$
g|_k\begin{pmatrix}M & -r\\ -Nx & s\end{pmatrix}=\chi(D)g.
$$

Thus we get

$$
\begin{aligned}
[\xi\otimes f]|_k w_{M^2N}(z) &= \chi(D)\frac{\xi(N)\tau(\xi)}{N^{\frac{k}{2}}M^{1+k}}\sum_{\substack{r \bmod M,\\ (r,M)=1}}\xi(r)\cdot\left[g|_k\begin{pmatrix}D & r\\ 0 & D\end{pmatrix}\right](z)\\
&= N^{-\frac{k}{2}}M^{-k}\chi(D)\xi(-N)\frac{\tau(\xi)}{\tau(\xi^{-1})}[\xi^{-1}\otimes g](z)\\
&= \chi(D)\xi(N)\frac{\tau(\xi)^2}{N^{\frac{k}{2}}M^{1+k}}[\xi^{-1}\otimes g](z).
\end{aligned}
$$

The triviality $[\xi\otimes f]=[(\xi\otimes f)|_k w_{M^2N}]|_k w_{M^2N}^{-1}$ yields

$$
[\xi\otimes f](iy)=i^k y^{-k}\chi(D)\xi(N)\frac{\tau(\xi)^2}{N^{\frac{k}{2}}M^{1+k}}[\xi^{-1}\otimes g]\left(\frac{i}{NM^2y}\right). \tag{112}
$$

We now compute

$$
\int_0^\infty[\xi\otimes f](iy)y^{\frac{k-1}{2}+s}\frac{dy}{y}=\sum_{n=1}^\infty\xi(n)a_f(n;\infty)\int_0^\infty e(nz)y^{\frac{k-1}{2}+s}\frac{dy}{y}=\Lambda(s,f,\xi).
$$

Note that this integral is convergent for all s, because f is a cusp form. Thus, it defines an analytic function. To see the functional equation we use (112) to get

$$
\begin{aligned}
\Lambda(s,f,\xi) &= i^k\chi(D)\xi(N)\frac{\tau(\xi)^2}{N^{\frac{k}{2}}M^{1+k}}\int_0^\infty[\xi^{-1}\otimes g]\left(\frac{i}{NM^2y}\right)y^{-\frac{k+1}{2}+s}\frac{dy}{y}\\
&= i^k\chi(D)\xi(N)(NM^2)^{\frac12-s}\frac{\tau(\xi)^2}{M}\int_0^\infty[\xi^{-1}\otimes g]\,(iy)\,y^{\frac{k+1}{2}-s}\frac{dy}{y}\\
&= i^k\chi(D)\xi(N)(NM^2)^{\frac12-s}\frac{\tau(\xi)^2}{M}\Lambda(s,g,\xi^{-1}).
\end{aligned}
$$

There is much more to the theory of (integral weight) Hecke Operators than what we can discuss here. Other important results are for example:

- (Strong Multiplicity One) Let $f \in S_k(\Gamma_0(N_1), \chi_1)$ and $g \in S_k(\Gamma_0(N_2), \chi_2)$ be newforms. (In particular f and g are eigenfunctions of all Hecke operators.) Suppose there is $M \in \mathbb{N}$ such that $\lambda_f(n) = \lambda_g(n)$ for all $(n, M) = 1$. Then $N_1 = N_2$, $\chi_1 = \chi_2$ and $f = g$.
- We have the decomposition
$$S_k(\Gamma_0(N), \chi) = \bigoplus_{q|N'|N} \bigoplus_{\substack{f \in S_k^\sharp(\Gamma_0(N'),\chi),\\ \text{newform}}} \langle \iota_{N',d} f \colon d \mid \frac{N}{N'} \rangle_{\mathbb{C}},$$
where χ is a Dirichlet character modulo N of conductor q.
- (Weil's Converse Theorem 1967) Let $\mathcal{R}$ be a set of integers with $1 \in \mathcal{R}$ so that for every $(a, c) = 1$ there is $r \in \mathcal{R}$ with $r \equiv a \bmod c$. Suppose that $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are polynomial bounded sequences such that
$$\begin{aligned}\Lambda(s, (a_n), \xi) &:= (2\pi)^{-\frac{k-1}{2}-s}\Gamma(\frac{k-1}{2} + s) \sum_{n=1}^{\infty} \frac{a_n \xi(n)}{n^{\frac{k-1}{2}+s}} \\ &= i^k \xi(N)\chi(r)\frac{\tau(\xi)^2}{r}(r^2N)^{\frac{1}{2}-s} \cdot \underbrace{(2\pi)^{s-\frac{k+1}{2}}\Gamma(\frac{k+1}{2} - s)\sum_{n=1}^{\infty} \frac{b_n\xi^{-1}(n)}{n^{\frac{n+1}{2}-s}}}_{:=\Lambda(1-s,(b_n),\xi^{-1})}\end{aligned}$$
for every primitive Dirichlet character ξ modulo r with $r \in \mathcal{R}$. Further assume that $\Lambda(s, (a_n), \xi)$ and $\Lambda(s, (b_n), \xi^{-1})$ are entire and bounded in vertical strips. Then
$$f(z) = \sum_{n=1}^{\infty} a_n e(nz) \in S_k(\Gamma_0(N), \chi) \text{ and } g(z) = \sum_{n=1}^{\infty} b_n e(nz) = N^{\frac{k}{2}} f|_k w_N.$$

5.3. **Hecke Operators for Half Integral weight.** We define G to be the set of pairs (γ, ϕ), where $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$ and $\phi \colon \mathbb{H} \to \mathbb{C}$ is a holomorphic function satisfying $\phi(z)^2 = \pm\frac{cz+d}{\sqrt{\det(\gamma)}}$. We turn G into a group by introducing the product
$$(\alpha, \phi)(\beta, \psi) = (\alpha\beta, z \mapsto \phi(\beta z)\psi(z)).$$
It is easy to see that G is really a group and one has the short exact sequence
$$1 \to \mu_4 \to G \to \mathrm{GL}_2^+(\mathbb{Q}) \to 1,$$
where μ_4 is the group of fourth roots of unity. For $k \in \mathbb{N}$ we define the action
$$[f\tilde{|}_{k/2}(g, \phi)](z) = \phi(z)^k f(gz)$$
of $(g, \phi) \in G$ on functions $f \colon \mathbb{H} \to \mathbb{C}$.

Throughout this section $k \in \mathbb{N}$ will be odd, so that $k/2$ is not an integer. Recall that the basic theta multiplier $\vartheta^\circ_{\mathrm{th}}$ for weight $\frac{1}{2}$ can be obtained by

$$\vartheta^\circ_{\mathrm{th}}(\gamma)\sqrt{cz+d} = \theta(\gamma z)/\theta(z),$$

where $\gamma \in \Gamma_0(4)$ and $\theta(z) = \sum_{m\in\mathbb{Z}} e(m^2 z)$ is the standard theta function. More explicitly we have

$$\vartheta^\circ_{\mathrm{th}}(\gamma) = \left(\frac{c}{d}\right)\bar{\epsilon}_d, \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4).$$

Remark 5.3.1. Note that for $A \in \mathcal{SP}_k$ with odd k we have $2 \mid \det(A)$, so that in particular $2 \mid N_A$. Furthermore we have seen in Theorem 3.0.13 that

$$\theta_{1,Q_A}(z) \in M_{\frac{k}{2}}(\Gamma_0(2N_A), \vartheta_{\mathrm{th}}).$$

Here the multiplier system ϑ_{th} depends on A and we have

$$\vartheta_{\mathrm{th}}(\gamma) = \left(\frac{\det(A)}{d}\right) \cdot \vartheta^\circ_{\mathrm{th}}(\gamma)^k.$$

We cover these spaces when we consider more generally $M_{\frac{k}{2}}(\Gamma_0(N), \chi\cdot(\vartheta^\circ_{\mathrm{th}})^k)$ where $4 \mid N$ and χ is a Dirichlet character modulo N.

Given a congruence subgroup $\Gamma = \Gamma_0(N) \subseteq \Gamma_0(4)$ we define its lift Γ^{th} to G by setting

$$\Gamma^{\mathrm{th}} = \{\tilde{\gamma} := (\gamma, z \mapsto \vartheta^\circ_{\mathrm{th}}(\gamma)\cdot\sqrt{cz+d}) \colon \gamma \in \Gamma\}.$$

The transformation behaviour of $f \in M_{\frac{k}{2}}(\Gamma_0(N), \chi\cdot(\vartheta^\circ_{\mathrm{th}})^k)$ can be rephrased as

$$[f\widetilde{|}_{k/2}\tilde{\gamma}](z) = \chi(d)f(z) \text{ for all } \gamma \in \Gamma_0(N).$$

One can now get to work and use this framework to implement an action of the Hecke Algebra $\mathcal{H}(\Gamma_0(N)^{\mathrm{th}}, \widetilde{\Delta}_N)$ for a suitable semigroup $\widetilde{\Delta}_N$. We will be more concrete and consider only the necessary double co-sets in what follows.

Lemma 5.3.2. *Take $\xi = (\alpha, \phi) \in G$ and put $\Lambda = \alpha^{-1}\Gamma\alpha \cap \Gamma$. (Recall that Λ has finite index in Γ.) There is $\gamma_1 \in \Gamma$ so that $\gamma = \alpha^{-1}\gamma_1\alpha \in \Lambda$. Then we have*

1. *$\tilde{\gamma}$ and $\xi^{-1}\tilde{\gamma}_1\xi$ differ by an element $(1,t) \in G$ with $t = t(\gamma) \in \mu_4$.*
2. *The map $\gamma \mapsto t(\gamma)$ is a homomorphism from Λ to μ_4, that does not depend on ϕ.*
3. *For $(n, N) = 1$ and $\alpha = diag(1, n)$ we have*

$$t(\gamma) = \left(\frac{n}{d}\right) \textit{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Lambda.$$

Proof. See the exercise below. ∎

Exercise 2, Sheet 10: We define G to be the set of pairs (γ, ϕ), where $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$ and $\phi : \mathbb{H} \to \mathbb{C}$ is a holomorphic function satisfying $\phi(z)^2 = \pm \frac{cz+d}{\sqrt{\det(\gamma)}}$. We turn G into a group by introducing the product

$$(\alpha, \phi)(\beta, \psi) = (\alpha\beta, z \mapsto \phi(\beta z)\psi(z)) \tag{113}$$

a) Check that G is a group and show that we have a short exact sequence

$$1 \longrightarrow \mu_4 \longrightarrow G \longrightarrow \mathrm{GL}_2^+(\mathbb{Q}) \longrightarrow 1$$

Given a congruence subgroup $\Gamma = \Gamma_0(N) \subset \Gamma_0(4)$ we define its lift Γ^{th} to G by setting

$$\Gamma^{\mathrm{th}} := \{\widetilde{\gamma} := (\gamma, z \mapsto \vartheta^\circ_{\mathrm{th}}(\gamma)\sqrt{cz+d}) : \gamma \in \Gamma\}.$$

Take $\xi = (\alpha, \phi) \in G$ and put $\Lambda := \alpha^{-1}\Gamma\alpha \cap \Gamma$ (recall that Λ has finite index in Γ). For any $\gamma \in \Lambda$ there is $\gamma_1 \in \Gamma$ so that $\gamma = \alpha^{-1}\gamma_1\alpha$.

b) Show that $\widetilde{\gamma}$ and $\xi^{-1}\widetilde{\gamma_1}\xi$ differ by an element $(1, t) \in G$ with $t = t(\gamma) \in \mu_4$.
c) Show that the map $\gamma \mapsto t(\gamma)$ is a homomorphism from Γ to μ_4, that does not depend on ϕ.
d) For $(n, N) = 1$ and $\alpha = \mathrm{diag}(1, n)$ we have

$$t(\gamma) = \left(\frac{n}{d}\right) \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Solution. Clearly (I_2, const_1) is a unit for the operation. Given $(\alpha, \phi) \in G$, its inverse is given by $(\alpha^{-1}, \phi(\alpha^{-1}\cdot)^{-1})$. This element is in G since

$$\phi(\alpha^{-1}z)^2 = \pm\frac{j_\alpha(\alpha^{-1}z)}{\sqrt{\det(\alpha)}} = \pm\left(\frac{j_{\alpha^{-1}(z)}}{\sqrt{\det(\alpha^{-1})}}\right)^{-1}$$

where we used the cocycle identity $j_{\alpha\beta}(z) = j_\alpha(\beta z)j_\beta(z)$ for $\beta = \alpha^{-1}$. To check associativity, we compute

$$((\alpha, \phi)(\beta, \psi))\,(\gamma, \zeta) = (\alpha\beta, \phi(\beta\cdot)\psi(\cdot))(\gamma, \zeta) = (\alpha\beta\gamma, \phi(\beta\gamma\cdot)\psi(\gamma\cdot)\zeta(\cdot))$$

and similarly

$$(\alpha, \phi)\,((\beta, \psi)(\gamma, \zeta)) = (\alpha, \phi)(\beta\gamma, \psi(\gamma\cdot)\zeta(\cdot)) = (\alpha\beta\gamma, \phi(\beta\gamma\cdot)\psi(\gamma\cdot)\zeta(\cdot)).$$

To obtain the exact sequence, note that $(\alpha, \phi) \mapsto \alpha$ is clearly a group homomorphism of G into $\mathrm{GL}_2^+(\mathbb{Q})$. To see surjectivity, let $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$ arbitrary and note that $\mathbb{H}$ is simply connected, so that any non vanishing holomorphic function has a square root. In particular, this holds for $z \mapsto \frac{j_\gamma(z)}{\sqrt{\det(\gamma)}}$, and we can find ϕ holomorphic on $\mathbb{H}$ such that $\phi(z)^2 = \frac{j_\gamma(z)}{\sqrt{\det(\gamma)}}$, showing that $(\gamma, \phi) \in G$. That the kernel of the map is isomorphic to μ_4 is clear, since the kernel consists of all functions ϕ such that $\phi^2(z) = \pm 1$, equivalently $\phi^4(z) = 1$, and since $\mathbb{H}$ is connected, it must be that ϕ equals everywhere a fixed fourth root of unity.

After Γ^{th} has been introduced, first note that $\gamma \mapsto \widetilde{\gamma}$ is a group homomorphism from Γ to Γ^{th}. Indeed, one checks immediately that

$$\begin{aligned}\widetilde{\gamma_1}\widetilde{\gamma_2} &= (\gamma_1\gamma_2, z \mapsto \vartheta^\circ_{\text{th}}(\gamma_1)\vartheta^\circ_{\text{th}}(\gamma_2) j_{\gamma_1}(\gamma_2 z)^{1/2} j_{\gamma_2}(z)^{1/2}) \\ &= (\gamma_1\gamma_2, z \mapsto \vartheta^\circ_{\text{th}}(\gamma_1\gamma_2) j_{\gamma_1\gamma_2}(z)^{1/2}).\end{aligned}$$

The last equality follows from the fact that $\vartheta^\circ_{\text{th}}$ is a multiplier system of weight $1/2$ for $\Gamma_0(4)$. To obtain part b), note that the image of $\widetilde{\gamma}$ and $\xi^{-1}\widetilde{\gamma_1}\xi$ to $\mathrm{GL}_2^+(\mathbb{Q})$ agree. By the exact sequence above, it must be that $\widetilde{\gamma} = t\xi^{-1}\widetilde{\gamma_1}\xi$ for some $t \in \mu_4$. It is very important to observe that $\mu_4 \subset Z(G)$, the centre of G. Indeed, for any constant $c \in \{\pm 1, \pm i\}$ we have

$$(I_2, c)(\alpha, \phi) = (\alpha, c\phi) = (\alpha, \phi)(I_2, c).$$

In particular, this shows that it doesn't matter whether we write $\widetilde{\gamma} = t\xi^{-1}\widetilde{\gamma_1}\xi$ or $\widetilde{\gamma} = \xi^{-1}\widetilde{\gamma_1}\xi t$.

If ϕ is replaced by ϕ' such that both $\xi = (\alpha, \phi)$ and $\xi' = (\alpha, \phi')$ are in G, the exact sequence above implies that $\xi' = t_\xi \xi$ for some $t_\xi \in \mu_4$. Since μ_4 is central in G, we deduce that

$$(\xi')^{-1}\widetilde{\gamma_1}\xi' = \xi^{-1}t_\xi^{-1}\widetilde{\gamma_1}t_\xi\xi = \xi^{-1}\widetilde{\gamma_1}\xi.$$

Therefore, $t(\gamma)$ does not depend on ϕ. Finally, to show that $\gamma \mapsto t(\gamma)$ it is a homomorphism from Λ to μ_4, let $\gamma, \delta \in \Lambda$, with γ_1, δ_1 defined as above. Note that $(\gamma\delta)_1 = \gamma_1\delta_1$, since conjugation is an homomorphism. By definition,

$$\widetilde{\gamma} = t(\gamma)\xi^{-1}\widetilde{\gamma_1}\xi \quad \text{ and } \widetilde{\delta} = t(\delta)\xi^{-1}\widetilde{\delta_1}\xi.$$

We have $\widetilde{\gamma\delta} = \widetilde{\gamma}\widetilde{\delta}$, and also $\gamma_1\delta_1 = (\gamma\delta)_1$ and thus also $\widetilde{\gamma_1}\widetilde{\delta_1} = \widetilde{\gamma_1\delta_1} = \widetilde{(\gamma\delta)_1}$, and since μ_4 is central in G, we arrive at

$$\widetilde{\gamma\delta} = t(\gamma)t(\delta)\xi^{-1}\widetilde{(\gamma\delta)_1}\xi$$

which proves part c). Finally, for part d), since $j_\alpha(z) = n$ and $\sqrt{\det(\alpha)} = \sqrt{n}$, we can choose $\xi = (\alpha, n^{1/4})$. We calculate at once that $\Lambda := \alpha^{-1}\Gamma_0(N)\alpha \cap \Gamma_0(N) = \Gamma(N, n)$, which is defined as

$$\Gamma(N, n) := \left\{ \begin{pmatrix} a & nb \\ Nc & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \text{ and } ad - nNbc = 1 \right\}.$$

For $\gamma \in \Lambda$, we have

$$\gamma = \begin{pmatrix} a & nb \\ Nc & d \end{pmatrix} \text{ and then } \gamma_1 = \alpha\gamma\alpha^{-1} = \begin{pmatrix} a & b \\ Nnc & d \end{pmatrix}$$

We obtain

$$\xi^{-1}\widetilde{\gamma_1}\xi = (\alpha^{-1}\gamma_1, z \mapsto n^{-1/4}\vartheta^\circ_{\text{th}}(\gamma_1) j_{\gamma_1}(z)^{1/2})(\alpha, n^{1/4}) = (\alpha^{-1}\gamma_1\alpha, z \mapsto \vartheta^\circ_{\text{th}}(\gamma_1) j_{\gamma_1}(\alpha z)^{1/2}).$$

On the other hand
$$\widetilde{\gamma} = (\gamma, z \mapsto \vartheta^\circ_{\mathrm{th}}(\gamma) j_\gamma(z)^{1/2}).$$
Since $\alpha z = z/n$, it follows that $j_{\gamma_1}(\alpha z) = Ncz/n + d = Ncz + d = j_\gamma(z)$. Therefore, $t(\gamma) = \vartheta^\circ_{\mathrm{th}}(\gamma)\vartheta^\circ_{\mathrm{th}}(\gamma_1)^{-1}$. Since $\vartheta^\circ_{\mathrm{th}}(\gamma) = \left(\frac{Nc}{d}\right)\overline{\epsilon}_d$ and $\vartheta^\circ_{\mathrm{th}}(\gamma_1) = \left(\frac{Nnc}{d}\right)\overline{\epsilon}_d$, we deduce that
$$t(\gamma) = \left(\frac{n}{d}\right)$$
as desired. ◻

For $f \in M_{k/2}(\Gamma_0(N), \chi \cdot (\vartheta^\circ_{\mathrm{th}})^k)$ and $(n, N) = 1$ we put
$$\xi_n = \left(\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}, n^{\frac{1}{4}}\right) \in G.$$
The action of the double co-set generated by ξ_n acts on f by
$$\widetilde{T}_n f(z) = n^{\frac{k}{4}-1}[f|\Gamma_0(N)^{\mathrm{th}}\xi_n\Gamma_0(N)^{\mathrm{th}}](z) = n^{\frac{k}{4}-1}\sum_i \chi(\alpha_i)^{-1}[f\tilde{|}_{\frac{k}{2}}\tilde{\alpha}_i](z),$$
where
$$\Gamma_0(N)^{\mathrm{th}}\xi_n\Gamma_0(N)^{\mathrm{th}} = \bigsqcup_i \Gamma_0(N)^{\mathrm{th}}\tilde{\alpha}_i.$$

Theorem 5.3.3. *For $(n, N) = 1$ and n **not** a perfect square, we have $\widetilde{T}_n = 0$.*

Proof. Put $\alpha = \mathrm{diag}(1, n)$, $\Lambda = \alpha^{-1}\Gamma_0(N)\alpha \cap \Gamma_0(N)$ and let $t\colon \Lambda \to \mu_4$ be the map from lemma 5.3.2. Further let $K = \ker(t)$ and $\widetilde{\Lambda} = \xi_n^{-1}\Gamma_0(N)^{\mathrm{th}}\xi_n \cap \Gamma_0(N)^{\mathrm{th}}$. We claim that $K^{\mathrm{th}} = \widetilde{\Lambda}$:

- $\supseteq$: Take $\tilde{\gamma} = \xi_n^{-1}\tilde{\gamma}_1\xi_n \in \widetilde{\Lambda}$. Then $\gamma = \alpha^{-1}\gamma_1\alpha \in \Lambda$ and $\tilde{\gamma}(1, t(\gamma)) = \xi_n^{-1}\tilde{\gamma}_1\xi_n$ by definition of $t(\gamma)$. This implies $t(\gamma) = 1$ as desired.
- $\subseteq$: For $\gamma \in K \subseteq \Lambda$ we clearly have $\tilde{\gamma} = \xi_n^{-1}\tilde{\gamma}_1\xi_n \in \widetilde{\Lambda}$.

From here we observe that $K = \Lambda$ if and only if t is trivial if and only if n is a perfect square. Thus, if n is not a perfect square, then $\widetilde{\Lambda} = K^{\mathrm{th}}$ has index two in Λ^{th}. Thus we can write
$$\Lambda^{\mathrm{th}} = \widetilde{\Lambda} \cup \widetilde{\Lambda}\tilde{\tau} \text{ for } \tilde{\tau} = \xi_n^{-1}\tilde{\tau}_1\xi_n \cdot (1, -1), \text{ and } \tau_1 \in \Gamma_0(N).$$
Furthermore, if we choose representatives γ_j for $\Lambda\backslash\Gamma_0(N)$, then we have
$$\Gamma_0(N)^{\mathrm{th}} = \bigsqcup_j \widetilde{\Lambda}\tilde{\gamma}_j \sqcup \bigsqcup_j \widetilde{\Lambda}\tilde{\tau}\tilde{\gamma}_j$$
so that
$$\Gamma_0(N)^{\mathrm{th}}\xi_n\Gamma_0(N)^{\mathrm{th}} = \bigsqcup_j \Gamma_0(N)^{\mathrm{th}}\xi_n\tilde{\gamma}_j \sqcup \bigsqcup_j \Gamma_0(N)^{\mathrm{th}}\xi_n\tilde{\tau}\tilde{\gamma}_j.$$
Since k is odd we have $f\tilde{|}_{k/2}(1, -1) = -f$. We conclude the proof by observing that
$$f\tilde{|}_{k/2}\xi_n\tilde{\tau}\tilde{\gamma}_j = -f\tilde{|}_{k/2}\xi_n\tilde{\gamma}_j.$$

Analogously to the integral case it can be seen that the operators $\widetilde{T}_{p^2}$ for primes $(p, N) = 1$ commute and generate the algebra

$$\langle \widetilde{T}_{p^2} \colon (p, N) = 1, \text{ prime}\rangle_{\mathbb{C}} = \langle \widetilde{T}_{n^2} \colon (n, N) = 1, \, n \in \mathbb{N}\rangle_{\mathbb{C}}.$$

As in the integral case we can express the action of $\widetilde{T}_{p^2}$ on a modular form in terms of Fourier coefficients:

Proposition 5.3.4. *Let $f \in M_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta_{th}^{\circ})^k)$. Then we have*

$$a_{\widetilde{T}_{p^2} f}(n; \infty) = a_f(p^2 n; \infty) + \chi(p) \left(\frac{(-1)^{\frac{k-1}{2}} n}{p}\right) p^{\frac{k-3}{2}} a_f(n; \infty) + \delta_{p^2|n} \chi(p^2) p^{k-2} a_f(\frac{n}{p^2}; \infty),$$

for $(p, N) = 1$.

Proof. The argument is more involved than in the integral weight case and we omit the proof.

Corollary 5.3.5. *Let $f \in M_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta_{th}^{\circ})^k)$ be an eigenfunction of $\widetilde{T}_{p^2}$ with eigenvalue $\lambda_f(p^2)$. Suppose $p \nmid N$ and $p^2 \nmid m$. Then we have*

$$\sum_{n=0}^{\infty} a_f(mp^{2n}; \infty) X^n = a_f(m; \infty) \cdot \frac{1 - \chi(p) \left(\frac{(-1)^{\frac{k-1}{2}} m}{p}\right) p^{\frac{k-3}{2}} X}{1 - \lambda_f(p^2) X + \chi(p^2) p^{k-2} X^2}. \tag{114}$$

Proof. Using the result above we can compare Fourier Coefficients of $\widetilde{T}_{p^2} f = \lambda_f(p^2) f$ to deduce

$$\lambda_f(p^2) a_f(m; \infty) = a_f(mp^2; \infty) + p^{\frac{k-3}{2}} \chi(p) \left(\frac{(-1)^{\frac{k-1}{2}} m}{p}\right) a_f(m; \infty) \text{ and}$$

$$\lambda_f(p^2) a_f(mp^{2n}; \infty) = a_f(mp^{2(n+1)}; \infty) + p^{\frac{k-3}{2}} \chi(p) \left(\frac{(-1)^{\frac{k-1}{2}} m}{p}\right) a_f(mp^{2n}; \infty) + p^{k-2} \chi(p^2) a_f(mp^{2(n-1)}; \infty).$$

Now the claimed result can be seen easily by multiplying both sides of (114) with $1 - \lambda_f(p^2) X + \chi(p^2) p^{k-2} X^2$ and comparing coefficients.

Remark 5.3.6. It is a remarkable theorem due to G. Shimura (1973) that for $f \in S_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta_{\mathrm{th}}^{\circ})^k)$ such that $\widetilde{T}_{p^2} f = \lambda_f(p^2) f$ for all primes p there is $\mathcal{S} f \in M_{\frac{k-1}{2}}(\Gamma_0(N/2), \chi^2)$ such that $T_p \mathcal{S} f = \lambda_f(p^2) \mathcal{S} f$ for all primes p. Even more, If $k \geq 5$, then $\mathcal{S} f$ is a cusp form. Note that one can relax the statement to apply to eigenforms of almost all Hecke Operators.

As usual Hecke operators that *interfere* with the level behave slightly different. It turns out that, if $p \mid N$, then

$$a_{\widetilde{T}_{p^2} f}(n; \infty) = a_f(p^2 n).$$

Furthermore, if $4p \mid N$, then we can define an operator

$$\widetilde{T}_p \colon M_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta_{\mathrm{th}}^\circ)^k) \to M_{\frac{k}{2}}(\Gamma_0(N), \chi_p \chi \cdot (\vartheta_{\mathrm{th}}^\circ)^k)$$

by

$$\widetilde{T}_p f(z) = p^{-1} \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right).$$

One checks that $a_{\widetilde{T}_p f}(n; \infty) = a_f(pn; \infty)$. We also define the shift operator

$$V_p f(z) = f(pz).$$

This operator maps $M_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta_{\mathrm{th}}^\circ)^k)$ to $M_{\frac{k}{2}}(\Gamma_0(Np), \chi\chi_p \cdot (\vartheta_{\mathrm{th}}^\circ)^k)$, where χ_p is the unique quadratic character of conductor p.

It is again an interesting question to see if one can find a basis of eigenfunctions for all T_{p^2} with $p \nmid N$. For the subspace of cusp forms one can run the same argument as in the integral weight case using the Petersson inner product. On the other hand (at least for $\frac{k}{2} > 2$) the complement can be understood using Eisenstein series.

However for weight $\frac{1}{2}$ there is a particularly nice argument, which we will now sketch.

Lemma 5.3.7. *There is a basis of $M_{\frac{1}{2}}(\Gamma_0(N), \chi \cdot \vartheta_{th}^\circ)$ consisting of eigenforms for all the T_{p^2} with $p \nmid N$.*

Proof. For weight $\frac{1}{2}$ it turns out that the Petersson inner product

$$\langle f, g \rangle = \int_{\Gamma_0(N)\backslash\mathbb{H}} f(z)\overline{g(z)}\, \mathrm{Im}(z)^{-\frac{3}{2}} dz$$

is defined for $f, g \in M_{\frac{1}{2}}(\Gamma_0(N), \chi \cdot \vartheta_{\mathrm{th}}^\circ)$.[47] Since the Hecke operators $\widetilde{T}_{p^2}$ for $(p, N) = 1$ still satisfy

$$\langle \widetilde{T}_{p^2} f, g \rangle = \chi(p^2) \langle f, \widetilde{T}_{p^2} g \rangle,$$

we can diagonalize the full space at once (without considering Eisenstein series separately). ◻

Lemma 5.3.8. *Let $f \in M_{\frac{1}{2}}(\Gamma_0(N), \chi \cdot \vartheta_{th}^\circ)$ be non-zero and let p be a prime not dividing N. Suppose that $\widetilde{T}_{p^2} f = \lambda_f(p^2) f$. For $m \in \mathbb{N}$ with $p^2 \nmid m$ we have*

(1) $a_f(mp^{2n}; \infty) = a_f(m; \infty)\chi(p)^n \left(\frac{m}{p}\right)^n$ *for every $n \geq 0$.*

[47] This was observed by Deligne and is a numerical coincidence.

(2) *We have* $\lambda_f(p^2) = \chi(p)\left(\frac{m}{p}\right)(1+p^{-1})$.

Proof. We will use the following two facts:

(1) There is a basis for $M_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta_{\text{th}}^{\circ})^k)$ of forms with Fourier coefficients in some number field.
(2) If $f \in M_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta_{\text{th}}^{\circ})^k)$ and the Fourier coefficients $a_f(n;\infty)$ are algebraic numbers, then they have bounded denominators.

By the first point we can assume that the Fourier Coefficients of f are algebraic. Put $\alpha = \chi(p)\left(\frac{m}{p}\right)p^{-1}$, $\beta+\gamma = \lambda_f(p^2)$ and $\beta\gamma = \chi(p^2)p^{-1}$. Then, by (114) we get

$$A(X) = \sum_{n=0}^{\infty} a_f(mp^{2n};\infty)X^n = a_f(m;\infty)\frac{1-\alpha X}{(1-\beta X)(1-\gamma X)}.$$

For $p^2 \nmid m$. If $a_f(m;\infty) = 0$, then $a_f(mp^{2n};\infty) = 0$ for all n. Since $f \neq 0$ we can assume that $a_f(m;\infty) \neq 0$. By the first fact above we can view $A(T)$ as a power series with coefficients in some finite (sufficiently large) extension K_p of $\mathbb{Q}_p$. By the second fact the coefficients have bounded denominators, so that $A(T)$ converges absolutely for X in the unit disc U_p of K_p. In particular $A(T)$, which we have seen is a rational function in X can not have a pole in U_p. But, since $\beta\gamma = \chi(p^2)p^{-1} \in U_p$, one of the numbers β^{-1} or γ^{-1} must lie in U_p. Lets say $\gamma^{-1} \in U_p$, then we must have $\alpha = \gamma$ such that

$$A(X) = a_f(m;\infty)(1-\beta X)^{-1} = a_f(m;\infty) \cdot \sum_{n=0}^{\infty} \beta^n X^n.$$

By comparing coefficients we find that $a_f(mp^{2n};\infty) = \beta^n a_h(m;\infty)$. It is easy to see that $\beta = \chi(p)\left(\frac{m}{p}\right)$. We conclude that

$$a_f(mp^{2n};\infty) = \chi(p)^n \left(\frac{m}{p}\right)^n a_f(m;\infty). \tag{115}$$

We deduce that $\lambda_f(p^2) = \beta+\gamma = \alpha+\beta = \chi(p)\left(\frac{m}{p}\right)(1+p^{-1})$. It is also easy to see now that if $a_f(m;\infty) \neq 0$, then $p \nmid m$ so that $\lambda_f(p^2) \neq 0$. ◻

The theory of newforms turns out to be difficult and not as satisfying as in the integral weight case. Nonetheless there are some interesting aspects to it.

Definition 5.3.1. Let $f \in M_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta_{\text{th}}^{\circ})^k)$ be an eigenfunction of almost all operators $\widetilde{T}_{p^2}$. We say that f is an oldform if there exists a prime $p \mid \frac{N}{4}$ such that (exactly) one of the following holds:

- χ is defined modulo N/p and $f \in M_{\frac{k}{2}}(\Gamma_0(N/p), \chi \cdot (\vartheta_{\text{th}}^{\circ})^k)$;
- $\chi \cdot \chi_p$ is definable modulo N/p and $f = V_p g$ with $g \in M_{\frac{k}{2}}(\Gamma_0(N/p), \chi\chi_p \cdot (\vartheta_{\text{th}}^{\circ})^k)$.

The space spanned by all oldforms will be denoted by $M^\flat_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta^\circ_{\mathrm{th}})^k)$. If $f \notin M^\flat_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta^\circ_{\mathrm{th}})^k)$ is an eigenfunction of almost all Hecke Operators $\widetilde{T}_{p^2}$, then f is said to be a newform.[48]

It is not difficult (but technical) to prove the following statements:

- If $h \in M^\flat_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta^\circ_{\mathrm{th}})^k)$ is non-zero, then there is a divisor $N' \mid N$, a character χ' modulo N' and a newform $g \in M_{\frac{k}{2}}(\Gamma_0(N'), \chi' \cdot (\vartheta^\circ_{\mathrm{th}})^k)$ such that h and g have the same eigenvalues for all but finitely many $\widetilde{T}_{p^2}$.
- Let $f \in M_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta^\circ_{\mathrm{th}})^k)$ be non-zero so that $a_f(n;\infty) = 0$ unless $p \mid n$. Then $p \mid \frac{N}{4}$, $\chi\chi_p$ is defined modulo N/p and $f = V_p g$ for some $g \in M_{\frac{k}{2}}(\Gamma_0(N/p), \chi\chi_p \cdot (\vartheta^\circ_{\mathrm{th}})^k)$.
- Let $f \in M_{\frac{k}{2}}(\Gamma_0(N), \chi \cdot (\vartheta^\circ_{\mathrm{th}})^k)$ such that $a_f(n;\infty) = 0$ for all n with $(n,m) = 1$. Then we can write f as
$$f = \sum_{\substack{p \mid m, \\ 4p \mid N}} V_p g_p$$
with $g_p \in M_{\frac{k}{2}}(\Gamma_0(N/p), \chi\chi_p \cdot (\vartheta^\circ_{\mathrm{th}})^k)$. (This is comparable to Theorem 5.2.15.)

In general the theory has its complications. However in the next section we will focus on the case of weight $\frac{1}{2}$ and see that there some interesting results can be proven.

6. Finale: The Serre-Stark Theorem

The Serre-Stark theorem gives an explicit basis for the space $M_{\frac{1}{2}}(\Gamma_0(4N), \chi \cdot \vartheta^\circ_{\mathrm{th}})$. Among other things this allows one to explicitly compute these spaces of modular forms.

Given $t \in \mathbb{Z}$ we attach a character χ_t as follows. First, if t is a perfect square, then $\chi_t = 1$ is the trivial character. Otherwise put
$$\chi_t(m) = \left(\frac{D}{m}\right),$$
where D is the discriminant of $\mathbb{Q}(\sqrt{t})$ (over $\mathbb{Q}$). In particular χ_t is quadratic and has conductor D.

Using Proposition 3.0.7 one can show that
$$\theta(z;\xi,t) := \sum_{n \in \mathbb{Z}} \xi(n) e(tn^2 z) \in M_{\frac{1}{2}}(\Gamma_0(4q^2 t), \chi_t \xi \cdot \vartheta^\circ_{\mathrm{th}}),$$

[48]Recall that in the integral weight case a newform was assumed to be normalized so that the first Fourier Coefficient is 1. This is not assumed here.

where ξ is an even primitive character modulo $q = q(\xi)$. The details are left as an **Exercise**.

We define the set

$$\Omega(N, \chi) = \{(\xi, t)\colon 4q(\xi)^2 t \mid N \text{ and } \chi(n) = \xi(n)\chi_t(n) \text{ for all } (n, N) = 1\}.$$

We now have the following result.

Theorem 6.0.1 (Serre-Stark 1976)**.** *The theta series $\theta(z; \xi, t)$ with $(\xi, t) \in \Omega(N, \chi)$ form a basis of $M_{\frac{1}{2}}(\Gamma_0(N), \chi \cdot \vartheta^{\circ}_{th})$.*

Remark 6.0.2. With a bit more work one can find a subset $\Omega_c(N, \chi) \subseteq \Omega(N, \chi)$ such that the theta series $\theta(z; \xi, t)$ with $(\xi, t) \in \Omega_c(N, \chi)$ form a basis for $S_{\frac{1}{2}}(\Gamma_0(N), \chi)$. Even though this has man interesting implications unfortunately we have no time to discuss this any further.

Before we can prove the theorem we to understand the structure of newforms for weight $\frac{1}{2}$. We start with a simple observation concerning the action of the Hecke Operators:

Proposition 6.0.3. *Let $0 \neq f \in M_{\frac{1}{2}}(\Gamma_0(N), \chi \cdot \vartheta^{\circ}_{th})$ and let $N \mid D$. Suppose that f is an eigenfunction of all Hecke Operators $\widetilde{T}_{p^2}$ with $p \nmid D$. Then there is a unique square-free integer $t \geq 1$ such that $a_f(n; \infty) = 0$ if n/t is not a square. Furthermore we have*

- *$t \mid D$;*
- *$\lambda_f(p^2) = \chi(p) \left(\frac{t}{p}\right) (1 + p^{-1})$ for $p \nmid D$; and*
- *$a_f(nu^2; \infty) = a_f(n; \infty)\chi(u) \left(\frac{t}{u}\right)$ if $(u, D) = 1$ and $u \geq 0$.*

Proof. Suppose $a_f(m; \infty) \neq 0$ and $a_f(m'\infty) \neq 0$. The by (115) we get

$$\chi(p) \left(\frac{m}{p}\right) (1 + p^{-1}) = \lambda_f(p^2) = \chi(p) \left(\frac{m'}{p}\right) (1 + p^{-1}),$$

for all primes $p \nmid Dmm'$. Thus $\left(\frac{m}{p}\right) = \left(\frac{m'}{p}\right)$ for all these primes. It is clear that this implies that m/m' is a square. The first part of the statement (i.e. the existence of t) follows directly. The remaining properties are also easily derived from the properties of c_p mentioned below (115). ◻

A direct consequence of this is the following.

Corollary 6.0.4. *If $a_f(1; \infty) \neq 0$, then $t = 1$ and $\lambda_f(p^2) = \chi(p)(1 + p^{-1})$ for $p \nmid D$.*

Now let us consider a newform $f \in M_{\frac{1}{2}}(\Gamma_0(N); \chi\vartheta^{\circ}_{\mathrm{th}})$. Let t denote the unique square-free integer $t \geq 1$ such that $a_f(n; \infty) = 0$ unless n/t is a square.

Lemma 6.0.5. *We have $a_f(1; \infty) \neq 0$ and $t = 1$.*

Proof. Suppose $a_f(1;\infty)=0$, then an argument from earlier shows that $a_f(n;\infty)=0$ for all $(n,D)=1$. But this implies that f is an oldform, which is a contradiction. It is clear that if $a_f(1;\infty)\neq 0$ we must have $t=1$. ∎

We are now in the situation to obtain a result that is familiar from the theory of integral weight:

Lemma 6.0.6. *Let $g\in M_{\frac{1}{2}}(\Gamma_0(N),\chi\vartheta_{th}^{\circ})$ be an eigenfunction of all Hecke Operators $\widetilde{T}_{p^2}$ with $(p,D)=1$. If $\lambda_f(p^2)=\lambda_g(p^2)$ for all $p\nmid D$, then $g\in\mathbb{C}f$.*

Proof. The proof is left as an Exercise. ∎

Lemma 6.0.7. *The newform f is an eigenform of $\widetilde{T}_{p^2}$ for every prime p. Further, we have*

$$D_f(s):=\sum_{n=1}^{\infty}a_f(n;\infty)n^{-s}=\prod_{p\mid N}(1-\lambda_f(p^2)p^{-2s})^{-1}\cdot\prod_{p\nmid N}\left(1-\chi(p)p^{-2s}\right)^{-1}.$$

If $4p\mid N$, then $\lambda_f(p^2)=0$.

Proof. That f is an eigenform of all $\widetilde{T}_{p^2}$ is clear by applying the previous Lemma to $g=\widetilde{T}_{p^2}f$.

Next, we note that according to Proposition 6.0.3 we can write

$$\sum_{n=1}^{\infty}a_f(n;\infty)n^{-s}=t^{-s}\left(\sum_{n\mid D^{\infty}}a_f(tn^2;\infty)n^{-2s}\right)\cdot\prod_{p\nmid D}\left(1-\chi(p)\left(\frac{t}{p}\right)p^{-2s}\right)^{-1}.$$

Using that $t=1$ as well as (115) gives the desired Euler Product.

If $4p\mid N$ we observe that

$$\widetilde{T}_pf(z)=\sum_{n=0}^{\infty}a_f(np;\infty)e(nz)=\sum_{n=0}^{\infty}a_f(n^2p^2)e(n^2p)=\lambda_f(p^2)V_pf(z)\in M_{\frac{1}{2}}(\Gamma_0(N),\chi_p\chi\vartheta_{\mathrm{th}}^{\circ}).$$

If $\lambda_f(p^2)\neq 0$ one deduces $f\in M_{\frac{1}{2}}(\Gamma_0(N/p),\chi\vartheta_{\mathrm{th}}^{\circ})$. This is a contradiction. ∎

We are now ready to prove the following key result:

Proposition 6.0.8. *If $f\in M_{\frac{1}{2}}(\Gamma_0(N),\chi\vartheta_{th}^{\circ})$ is a newform and q is the conductor of χ, then $N=4q^2$ and $f(z)=\frac{a_f(1;\infty)}{2}\theta(z;\chi,1)$.*

Proof. Without loss of generality we assume that $a_f(1;\infty)=1$. Note that the Dirichlet series $D_f(s)$ converges for $\mathrm{Re}(s)$ sufficiently large. Similarly we define

$$D_{\overline{f}}(s)=\sum_{n=1}^{\infty}\overline{a_f(n)}n^{-s}.$$

Mimicking the proof of Proposition 5.2.20 we obtain[49]

$$(2\pi)^{-s}\Gamma(s)D_f(s) = \eta \cdot \left(\frac{2\pi}{N}\right)^{-(\frac{1}{2}-s)} \Gamma(\frac{1}{2}-s)D_{\overline{f}}(\frac{1}{2}-s).$$

Note that we are using that

$$\eta \cdot \overline{f(-\overline{z})} = [f\tilde{|}_{\frac{1}{2}}(w_N, N^{\frac{1}{4}}(-iz)^{\frac{1}{2}})](z).$$

We also obtain a meromorphic continuation. However, since f is not assumed to be a cusp-form we may have a simple pole at $\frac{1}{2}$. consider

$$L(2s,\chi) = \sum_{n=1}^{\infty} \chi(n)n^{-2s}.$$

It is well known that this Dirichlet L-functions satisfies the functional equation

$$(2\pi)^{-s}\Gamma(s)L(2s,\chi) = \eta' \left(\frac{2\pi}{4q^2}\right)^{-(\frac{1}{2}-s)} \Gamma(\frac{1}{2}-s)L(1-2s,\chi^{-1}).$$

Taking the quotient we obtain

$$\prod_{p|M}\left(\frac{1-\lambda_f(p^2)p^{-2s}}{1-\chi(p)p^{-2s}}\right) = \frac{L(2s,\chi)}{D_f(s)} = \frac{\eta'}{\eta}\left(\frac{4q^2}{N}\right)^{\frac{1}{2}-s} \prod_{p|M}\left(\frac{1-\overline{\lambda_f(p^2)}p^{2s-1}}{1-\chi^{-1}(p)p^{2s-1}}\right). \tag{116}$$

Here M is the product of primes where $\chi(p) \neq \lambda_f(p^2)$.

If $\chi(p) \neq 0$ for $p \mid M$, then the left hand side of (116) has infinitely many poles on the lune $\mathrm{Re}(s) = 0$. But the right hand side can have at most finitely many. Thus we have $\chi(p) = 0$ for $p \mid M$ (i.e. $p \mid q$). Since $\lambda_f(p) \neq \chi(p) = 0$ we can write

$$\prod_{p|M}(1-\lambda_f(p^2)p^{-2s}) = \frac{\eta'}{\eta}\left(\frac{4q^2}{N}\right)^{\frac{1}{2}-s} \prod_{p|M}\left(-\frac{\overline{\lambda_f(p^2)}}{p}p^{2s}(1-\frac{p}{\overline{\lambda_f(p^2)}}p^{-2s})\right).$$

Looking at the zeros on vertical lines one deduces that $|\lambda_f(p^2)|^2 = p$. We get

$$\frac{\eta'}{\eta}\left(\frac{4q^2}{NM^2}\right)^{\frac{1}{2}-s} \prod_{p|M}\left(-\overline{\lambda_f(p^2)}\right) = 1.$$

In particular $4q^2 = M^2N$. Recall that $\lambda_f(p^2) = 0$ for $4p \mid N$. Thus the only possibility is $M = 1$ or $M = 2$. Note that $M = 2$ can only occur if $8 \nmid N$ and $4 \mid q$. But this is a contradiction to $8 \nmid N$ since $4q^2 = M^2N = 4N$. Thus $M = 1$ so that $N = 4q^2$.

The point of this argument was that we now obtain

$$D_f(s) = L(2s,\chi).$$

[49] Note that here the coefficients are normalized differently, so that the center of the functional equation is slightly shifted.

By comparing coefficients we find that $f - \frac{1}{2}\theta(z;\chi,1)$ is a constant. However it is still a modular form of weight $\frac{1}{2}$. We conclude that $f - \frac{1}{2}\theta(z;\chi,1) = 0$ and the proof is complete. ∎

Proof of Theorem 6.0.1. We first show linear independence. Suppose we have a linear combination

$$\lambda_1\theta(z;\xi_1,t_1) + \ldots + \lambda_k\theta(z;\xi_m,t_m) = 0$$

with $(\xi_i,t_i) \in \Omega(N,\chi)$. Note that t_i determines ξ_i and each $t \in \mathbb{Z}$ occurs as the second entry of at most one $(\xi,t) \in \Omega(N,\chi)$. Without loss of generality we can assume that $t_1 < \ldots < t_m$ and $\lambda_i \neq 0$ for $i = 1,\ldots,m$. Looking at the t_1th-Fourier coefficient gives $2\lambda_1 = 0$. (This is because $a_{\theta(\cdot,\xi_1,t_1)}(t_1;\infty) = 2$.)

To see that the theta series $\theta(z,\xi,t)$ with $(\xi,t) \in \Omega(N,\chi)$ generate the full space is slightly harder, but we have done most of the work. By Lemma 5.3.7 it suffices to show that every eigenfunction f of all $\widetilde{T}_{p^2}$ with $(p,N) = 1$ linear combinations of $\theta(z,\xi,t)$. If f is a newform we are done by Proposition 6.0.8. Thus we can assume that f is an oldform. Here we have to consider two cases

- If χ is defined modulo N/p and f belongs to $M_{\frac{1}{2}}(\Gamma_0(N/p),\chi\cdot\vartheta_{\mathrm{th}}^{\circ})$. In this case we conclude by induction.
- Otherwise $\chi\cdot\chi_p$ is defined modulo N/p and
$$f = V_p g \text{ for some } g \in M_{\frac{1}{2}}(\Gamma_0(N/p),\chi\chi_p\cdot\vartheta_{\mathrm{th}}^{\circ}).$$
By induction we can write g as a linear combination of $\theta(z;\xi,t)$ with $(\xi,t) \in \Omega(N/p,\chi\chi_p)$. But this implies that f is a linear combination of $\theta(z;\xi,tp)$.

This completes the proof. ∎