An Introduction to Classical Modular Forms

Michael H. Mertens

August 16, 2018

Contents

Introduction

The present manuscript is a more or less verbatim transcript of a series of three one-hour lectures on classical (elliptic) modular forms that I delivered at the Summer Research Institute on q-series at Nankai University between 24 July and 15 August, 2018.

Modular forms play a role in so many important branches of number theory, but also mathematics in general (e.g. (algebraic) geometry, topology, Lie theory, just to name a few) and also mathematical physics, that it seems more and more valuable to know at least some basic facts about them. Due to the limited amount of time, it is not possible to do all of the important aspects of the theory itself, let alone its numerous applications, full justice, so these notes can give but a glimpse of what is going on with theses functions.

The sections of these notes roughly represent the individual lectures and are organized as follows: In the first two lectures/sections, I give a brief overview of some basic facts and definitions of modular forms, focussing on modular forms for the full modular group $\mathrm{SL}_2(\mathbb{Z})$ in the first lecture and on the more general setting of modular forms for (congruence) subgroups, including some examples such as Eisenstein series, the Δ-function, theta series and eta quotients. I also briefly touch on the less classical theory of Jacobi forms and even more briefly on singular moduli in the second lecture. The third lecture/section will cover some particular applications of the theory of modular forms to partitions, namely a sketch of the proof of Rademacher's series representation of the partition numbers, a proof of the famous Ramanujan congruences, and finally a short outline on a general framework for further congruences of the partition function.

I will give a (also not in the least exhaustive) list of some textbooks and (shorter) introductory notes on modular forms that the readers of these notes might want to consider to get a deeper understanding about the details that cannot be conveyed properly here. Some of the sections in these notes are actually taken rather directly from some of these sources, in which case I will give the respective reference in the body of the text. For original references to the results presented here, I refer to the cited textbook and expository sources.

As a last point I would like to point out that these notes have not been proof-read and hence might contain several typos, which I hope they don't to too great an extent.

Tianjin, July 2018, Michael H. Mertens

1 Basics

1.1 The upper half-plane

Throughout, we denote by $\mathfrak{H}$ the *complex upper half-plane*,

$$\mathfrak{H} = \{\tau = u + iv \in \mathbb{C} \,:\, \mathrm{Im}(\tau) = v > 0\}.$$

This is a model for the hyperbolic plane.

Its group of holomorphic isometries (with respect to the hyperbolic metric) or biholomorphic automorphisms is well-known to be isomorphic to $\mathrm{PSL}_2(\mathbb{R})$. We are actually not going to worry about the projective group here and consider $\mathrm{SL}_2(\mathbb{R})$ instead. This group acts on $\mathfrak{H}$ via *Möbius transformations*,

$$\left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau\right) \mapsto \gamma.\tau := \frac{a\tau + b}{c\tau + d}.$$

For this note for instance that

$$\mathrm{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2},$$

hence the action is well-defined. That we actually have a group action whose core is generated by $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ is an easy direct verification.

It is now a natural question to ask whether there exist holomorphic, say, functions $f : \mathfrak{H} \to \mathbb{C}$ which are invariant under the action of discrete subgroups of $\mathrm{SL}_2(\mathbb{R})$, the most straightforward example of which is probably $\mathrm{SL}_2(\mathbb{Z})$. Unfortunately, it turns out that the answer to this question is *no*, except for constant functions, but it is yes if we relax the invariance requirement a bit.

Before we get to this, it is worthwhile to look for a fundamental domain of the action of $\mathrm{SL}_2(\mathbb{Z})$. It can be seen in an abstract way that such a fundamental domain must exist through Baire's category principle, but it can be verified in a much more elementary way, that an exact fundamental domain of the action of $\mathrm{SL}_2(\mathbb{Z})$, i.e. a connected domain[1] $\mathcal{F} \subseteq \mathfrak{H}$ such that for any $\tau \in \mathfrak{H}$ there exists a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma.\tau \in \mathcal{F}$ and for any two distinct points $\tau \neq \tau' \in \mathfrak{H}$ there is no $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma\tau = \tau'$, is given by

$$\mathcal{F} := \left\{\tau \in \mathfrak{H} \,:\, -\frac{1}{2} < \mathrm{Re}(\tau) \leq \frac{1}{2}, |\tau| \geq 1, \text{ and } |\tau| > 1 \text{ for } \mathrm{Re}(\tau) < 0\right\},$$

which is the famous modular triangle. An important fact on its own and also important in proving that $\mathcal{F}$ is indeed a fundamental domain is the fact that $\mathrm{SL}_2(\mathbb{Z})$ is generated by two elements,

$$\mathrm{SL}_2(\mathbb{Z}) = \left\langle T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

[1] Actually, the fundamental domain is not open, but its interior is a domain

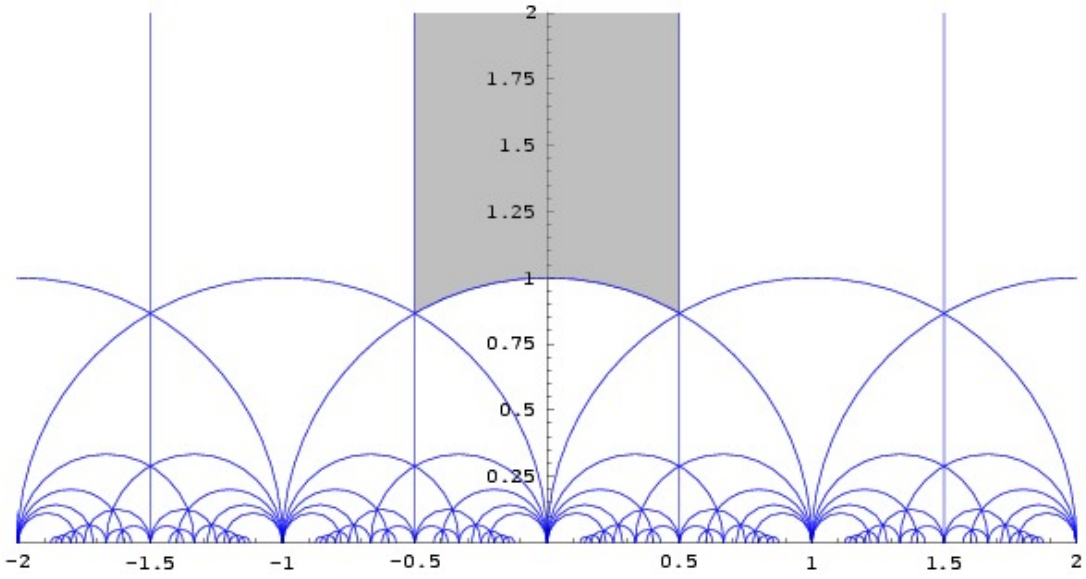

Figure 1: Standard fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$ (Source: wikipedia.org)

The matrices T and S are often referred to as *translation* and *(modular) inversion* respectively, which is why in some places in the literature the letter J instead of S is used.

There are two special points in $\mathcal{F}$, as will be important later, namely the points i and $\rho = \frac{1+i\sqrt{3}}{2}$, which are the only points in $\mathcal{F}$ which have a non-trivial stabilizer in $\mathrm{SL}_2(\mathbb{Z})$: i is fixed by S, which has order 4 and ρ is fixed by $U = TS = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ which has order 6. We call such points *elliptic fixed points*. Note that every other point in $\mathcal{F}$ is only fixed (trivially) by $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

1.2 Basic definitions and first results on modular forms

Returning to the question whether there are functions (essentially) invariant under $\mathrm{SL}_2(\mathbb{Z})$, we define the notion of modular forms.

Definition 1.1. *A function $f : \mathfrak{H} \to \mathbb{C}$ is called a* modular form *of weight $k \in \mathbb{Z}$ for $\mathrm{SL}_2(\mathbb{Z})$ if*

(i) f is holomorphic on $\mathfrak{H}$,

(ii) f is invariant under the weight k Petersson slash operator*, that is we have*

$$(f|_k\gamma)(\tau) := (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right) = f(\tau)$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathfrak{H}$,

(iii) f *is* holomorphic at ∞, *i.e.* $f(iv)$ *is bounded as* $v \to \infty$.

If we even have that $f(iv) \to 0$ *as* $v \to \infty$, *we call* f *a* cusp form.

In the following remarks we record a couple of elementary observations on modular forms.

Remark 1.2. *Modular forms resp. cusp forms of weight* k *form a vector space over* $\mathbb{C}$ *which we denote by* M_k *resp.* S_k. *It is clear that products of modular forms are again modular forms and products of modular forms and cusp forms are again cusp forms, i.e. we have*

$$M_k \cdot M_\ell \subseteq M_{k+\ell} \quad \textit{and} \quad S_k \cdot M_\ell \subseteq S_{k+\ell}.$$

Remark 1.3. *Since* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the two matrices* T *and* S *which map* $\tau \in \mathfrak{H}$ *to* $\tau + 1$ *and* $-1/\tau$ *resp., a function* $f : \mathfrak{H} \to \mathbb{C}$ *satisfies the transformation law in* (ii) *of Definition 1.1 if and only if we have*

$$f(\tau + 1) = f(\tau) \quad \textit{and} \quad f(-1/\tau) = \tau^k f(\tau)$$

for all $\tau \in \mathfrak{H}$. *In particular the invariance* $f(\tau+1) = f(\tau)$ *implies through a standard fact of complex analysis that a modular form* $f \in M_k$ *has a* Fourier expansion *of the form*

$$f(\tau) = \sum_{n \in \mathbb{Z}} \alpha_f(n) e^{2\pi i n \tau}.$$

The growth condition in (iii) *of Definition 1.1 actually yields that actually* $\alpha_f(n) = 0$ *for* $n < 0$ *for* $f \in M_k$ *and and that we additionally have* $\alpha_f(0) = 0$ *if and only if* f *is a cusp form.*

Remark 1.4. *Since* $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ *we find for* $f \in M_k$ *that*

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

hence there are no non-zero modular forms of odd weight.

The following requires a little more work.

Lemma 1.5. *There are no non-zero modular forms of negative weight.*

Proof. Let $k < 0$ and $f \in M_k$. It is not hard to see that the non-holomorphic function $\tilde{f}(\tau) := v^{k/2}|f(\tau)|$ satisfies $\tilde{f}(\gamma.\tau) = \tilde{f}(\tau)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. If $k < 0$, $\tilde{f}$ is bounded as $v \to \infty$ because f is, so in particular it is bounded for all τ with $\mathrm{Im}(\tau) > \varepsilon > 0$. Thus we find for the Fourier coefficients of f that

$$|\alpha_f(m)| = \left| e^{2\pi m v} \int_0^1 f(u+iv) e^{-2\pi i m u} du \right| \leq v^{-k/2} e^{2\pi m v} \int_0^1 \tilde{f}(u+iv) \leq C v^{-k/2} e^{2\pi m v}$$

for some constant C which doesn't depend on v. Since the left-hand side of this inequality doesn't depend on v, we can take the limit $v \to 0$ which yields $\alpha_f(m) = 0$ for all m, hence $f \equiv 0$, so the claim follows. □

One is now inclined to ask whether there actually are any non-trivial examples of modular forms at all. In fact one can construct very explicit and important examples, which are actually motivated by the theory of elliptic functions, which we cannot touch on here.

Example 1.6. *We define the* Eisenstein series *of weight k by*

$$G_k(\tau) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} (m\tau+n)^{-k}.$$

One can show that this series is absolutely and locally uniformly convergent on $\mathfrak{H}$ as soon as $k \geq 3$. Assuming this from now on, we can verify that these functions are indeed modular. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then we have

$$\begin{aligned} G_k\left(\frac{a\tau+b}{c\tau+d}\right) &= \sum_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} \left(m\cdot\frac{a\tau+b}{c\tau+d}+n\right)^{-k} \\ &= (c\tau+d)^k \sum_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} ((ma+nc)\tau+(mb+nd))^{-k}. \end{aligned}$$

Since clearly with (m,n) also $(m,n)\cdot\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = (ma+nc, mb+nd)$ runs through all of $\mathbb{Z}^2\setminus\{0\}$, this yields, as claimed,

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

It remains to verify that Eisenstein series don't always vanish identically (which by Remark 1.4 they do if k is odd). For this we can compute their Fourier expansion.

Theorem 1.7. *For even $k \geq 4$ we have that*

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

where $\zeta(s)$ denotes the Riemann zeta function, $\sigma_k(n) := \sum_{d|n} d^k$ denotes the usual divisor power sum and we use the standard abbreviation $q := e^{2\pi i\tau}$.

The normalized *Eisenstein series are given by*

$$E_k(\tau) := \frac{1}{2\zeta(k)}G_k(\tau) = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n,$$

where B_k denotes the kth Bernoulli number *(which is always rational and non-zero if k is even).*

Example 1.8. *The first few normalized Eisenstein series are given explicitly by*

$$E_4(\tau) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n,$$
$$E_6(\tau) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n,$$
$$E_8(\tau) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n,$$
$$E_{10}(\tau) = 1 - 264 \sum_{n=1}^{\infty} \sigma_9(n) q^n,$$
$$E_{12}(\tau) = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n.$$

We now want to turn a little more towards the structure of modular forms. For this, we need the following very important theorem known as the *valence formula* for $\mathrm{SL}_2(\mathbb{Z})$. We are not going to give a proof, but we mention that it actually can be thought of as an instance of the Riemann-Roch theorem.

Theorem 1.9. *Let $f : \mathfrak{H} \to \mathbb{C}$, $f \not\equiv 0$, be a meromorphic function satisfying $f|_k\gamma \equiv f$ for some $k \in \mathbb{Z}$ (note that in this setup, k might very well be negative) and suppose that f has a Fourier expansion $f(\tau) = \sum_{n=n_0}^{\infty} \alpha_f(n) q^n$ for some $n_0 \in \mathbb{Z}$ with $\alpha_f(n_0) \neq 0$. Further define $\mathrm{ord}_\infty(f) := n_0$. Then we have that*

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\,\mathrm{ord}_i(f) + \frac{1}{3}\,\mathrm{ord}_\rho(f) + \sum_{w \in \mathcal{F} \setminus \{i,\rho\}} \mathrm{ord}_w(f) = \frac{k}{12}.$$

It should be remarked that in fact only finitely many terms in the sum over points in the fundamental domain can be non-zero due to the identity theorem (a non-zero meromorphic modular form can only have finitely many zeros or poles in the fundamental domain). Furthermore, the strange looking factors $\frac{1}{2}$ and $\frac{1}{3}$ in front of $\mathrm{ord}_i(f)$ and $\mathrm{ord}_\rho(f)$ originate from the fact that i and ρ are elliptic fixed points whose stabilizers have orders $2 \cdot 2$ and $2 \cdot 3$.

As a not completely immediate, but not too complicated corollary to the valence formula, one finds the dimension formula for the spaces M_k.

Theorem 1.10. *We have*

$$\dim_{\mathbb{C}} M_k = \begin{cases} \lfloor k/12 \rfloor & \text{if } k \equiv 2 \pmod{12}, \\ \lfloor k/12 \rfloor + 1 & \text{if } k \not\equiv 2 \pmod{12}. \end{cases}.$$

In particular, one finds that $M_2 = \{0\}$, $M_4 = \mathbb{C}E_4$, $M_6 = \mathbb{C}E_6$, $M_8 = \mathbb{C}E_8$.

Remark 1.11. *The finite-dimensionality of M_k is the source of numerous sometimes surprising identities. For instance it follows from Remark 1.2 that $E_4^2 \in M_8 = \mathbb{C}E_8$, so, since E_4^2 and E_8 have the same leading Fourier coefficient, we must have $E_4^2 = E_8$. Comparing the coefficients, one finds the so-called* Hurwitz identity *for divisor sums,*

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{r=1}^{n-1} \sigma_3(r)\sigma(n-r).$$

It is interesting to note that this identity can be formulated entirely in terms of elementary number theory without appealing to modular forms or other advanced mathematics, but an elementary proof is, to the author's knowledge, at least very complicated.

The following important result which also can be derived essentially from the valence formula in Theorem 1.9 is that it is possible to generate all modular forms very easily.

Theorem 1.12. *The space*

$$M_* := \bigoplus_{k=0}^{\infty} M_k$$

is an infinite-dimensional $\mathbb{C}$-algebra. More precisely, we have that

$$M_* = \mathbb{C}[E_4, E_6]$$

is the free polynomial algebra generated by E_4 and E_6 (which are easily seen to be algebraically independent).

Remark 1.13. *In view of the results in Section 2 where modular forms for other groups than $\mathrm{SL}_2(\mathbb{Z})$ are considered it is important to point out that it is* **not** *always the case that the algebra of modular forms is isomorphic to a free polynomial algebra. In fact this is almost never true except for finitely many exceptions. It is always true however that the algebra of modular forms is a finitely generated $\mathbb{C}$-algebra, but there usually are non-trivial relations among the generators.*

We conclude this subsection by discussing one further example of modular forms, in fact the first non-trivial example of a cusp form.

Example 1.14. *Consider the so-called Δ-function defined by*

$$\Delta(\tau) := \frac{E_4^3 - E_6^2}{1728} =: \sum_{n=1}^{\infty} \tau(n) q^n = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 + O(q^6) \in S_{12}$$

This is a cusp form of weight 12. *The coefficients* $\tau(n)$ *are referred to as the Ramanujan* τ*-function. We clearly have* $\mathrm{ord}_\infty(\Delta) = 1$*, so the valence formula applied to* Δ *yields*

$$1 + \frac{1}{2}\,\mathrm{ord}_i(\Delta) + \frac{1}{3}\,\mathrm{ord}(\Delta) + \sum_{w \in \mathcal{F}\setminus\{i,\rho\}} \mathrm{ord}_w(\Delta) = 1.$$

Since Δ *is holomorphic on* $\mathfrak{H}$ *by definition, we must have* $\mathrm{ord}_\tau(\Delta) \geq 0$ *for all* $\tau \in \mathfrak{H}$*, hence it must be that* $\Delta(\tau) \neq 0$ *for all* $\tau \in \mathfrak{H}$*. Through a standard fact in complex analysis, this implies that* Δ *must admit an representation as an infinite product. Indeed, one can show either through the theory of elliptic functions or using properties of the Dedekind eta function (see Section 2.2.2) that*

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

1.3 Operators

In the previous section, we saw various examples of modular forms. We can construct new modular forms from these in a fairly general manner. First we extend the definition of the slash operator to the larger group $\mathrm{GL}_2^+(\mathbb{Q})$ of 2×2-matrices with rational entries and positive determinant by setting

$$(f|k\gamma)(\tau) := (\det \gamma)^{k/2} (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right).$$

Then for $f \in M_k$ the function $f|_k\gamma$ for any $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$ is again a modular form of weight k, although usually not for the full modular group $\mathrm{SL}_2(\mathbb{Z})$, but for the conjugated group $\gamma^{-1}\,\mathrm{SL}_2(\mathbb{Z})\gamma \leq \mathrm{SL}_2(\mathbb{Q})$. Since one usually considers modular forms for subgroups of $\mathrm{SL}_2(\mathbb{Z})$, one can also view $f_k\gamma$ as a modular form for the subgroup $\Gamma = (\gamma^{-1}\,\mathrm{SL}_2(\mathbb{Z})\gamma) \cap \mathrm{SL}_2(\mathbb{Z})$, which always has finite index in $\mathrm{SL}_2(\mathbb{Z})$.

Some standard operators on modular forms can be expressed in terms of this generalized slash operators.

Definition 1.15. *For* $f \in M_k$ *and* $m, N, r \in \mathbb{N}$ *and* χ *a Dirichlet character mod* N *we*

define the operators

$$f|V_m := m^{-k/2} f|_k \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$$

$$f|U_m := m^{k/2-1} \sum_{j=0}^{m-1} f|_k \begin{pmatrix} 1 & j \\ 0 & m \end{pmatrix}$$

$$f|S_{N,r} := \frac{1}{N} \sum_{j=0}^{N-1} e^{-2\pi i r j/N} f|_k \begin{pmatrix} 1 & j/N \\ 0 & 1 \end{pmatrix}$$

$$f \otimes \chi := \sum_{r=0}^{N} \chi(r)(f|S_{N,r}).$$

For all these operators it is usually very convenient to consider their action on the Fourier expansion of a modular form.

Lemma 1.16. *Let $f \in M_k$ be a modular form with Fourier expansion $f(\tau) = \sum_{n=0}^{\infty} \alpha_f(n) q^n$. Then we have in the notation of Definition 1.15*

$$(f|V_m)(\tau) = f(m\tau) = \sum_{n=0}^{\infty} \alpha_f(n) q^{mn},$$

$$(f|U_m)(\tau) = \sum_{n=0}^{\infty} \alpha_f(mn) q^n,$$

$$(f|S_{N,r})(\tau) = \sum_{n \equiv r \ (N)} \alpha_f(n) q^n,$$

$$(f \otimes \chi)(\tau) = \sum_{n=0}^{\infty} \alpha_f(n)\chi(n) q^n.$$

Probably the most important operators on modular forms are *Hecke operators*. In order to define these, we consider the set

$$\mathcal{M}_m := \{M \in \mathbb{Z}^{2\times 2} \ : \ \det M = m\}$$

for $m \in \mathbb{N}$. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{M}_m$ by left and right multiplication on $\mathcal{M}_m$,

$$\mathrm{SL}_2(\mathbb{Z}) \cdot \mathcal{M}_m = \mathcal{M}_m = \mathcal{M}_m \cdot \mathrm{SL}_2(\mathbb{Z}).$$

As one can show without too much difficulty, the set

$$\mathrm{SL}_2(\mathbb{Z}) : \mathcal{M} := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathcal{M}_m \ : \ ad = m, \ d > 0, \ b \in \{0, ..., d-1\} \right\}$$

is a full set of representatives of $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{M}_m$, which is easily seen to have cardinality

$$\#(\mathrm{SL}_2(\mathbb{Z}) : \mathcal{M}_m) = \sigma_1(m),$$

so in particular, it is finite. With this we can define the following.

Definition 1.17. *For $m \in \mathbb{N}$ and $f \in M_k$ we define the mth* Hecke operator *acting on f by*

$$f|T_m^{(k)} := m^{k/2-1} \sum_{M \in \mathrm{SL}_2(\mathbb{Z}):\mathcal{M}} f|_k M.$$

Note that since the weight k is usually clear from context, we often write T_m instead of $T_m^{(k)}$. We now record the action of Hecke operators on Fourier expansions.

Lemma 1.18. *Let $f \in M_k$ with Fourier expansion $f(\tau) = \sum_{n=0}^{\infty} \alpha_f(n) q^n$ and let $g = f|T_m$. Then g has a Fourier expansion with coefficients*

$$\alpha_g(n) = \sum_{d|\gcd(m,n)} d^{k-1} \alpha_f(mn/d^2) \text{ mit } n \geq \begin{cases} 0 & \text{if } \alpha_f(0) \neq 0 \\ 1 & \text{if } \alpha_f(0) = 0. \end{cases}.$$

From this we can deduce one of the most important properties of Hecke operators.

Theorem 1.19. *For $f \in M_k$ and $m \in \mathbb{N}$ we have $f|T_m \in M_k$. If $f \in S_k$, then so is $f|S_k$.*

Proof. We first verify the transformation property. Since $f|_k\gamma = f$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the definition of T_m is independent of the choice of representatives and since for $M \in \mathcal{M}_m$ we also have $M\gamma \in \mathcal{M}_m$, we have that

$$\begin{aligned} f|T_m|\gamma &= \sum_{M \in \mathrm{SL}_2(\mathbb{Z}):\mathcal{M}_m} (f|_k M)|_k \gamma = \sum_{M \in \mathrm{SL}_2(\mathbb{Z}):\mathcal{M}_m} f|_k (M\gamma) \\ &= \sum_{M \in (\mathrm{SL}_2(\mathbb{Z}):\mathcal{M}_m)\gamma} f|_k M = f|T_m \end{aligned}$$

since $(\mathrm{SL}_2(\mathbb{Z}) : \mathcal{M}_m)\gamma$ is simply another set of representatives of $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{M}_m$. The claim on cusp forms follows immediately from Lemma 1.18. □

We recored some important facts about the Hecke operators themselves in the following theorem, which we are not going to prove.

Theorem 1.20. *Let $m, n \in \mathbb{N}$ be coprime, p a prime, $r \in \mathbb{N}$, and $f \in M_k$. Then the following are true.*

(i) $(f|T_m)|T_n = (f|T_{mn})$, so the Hecke operators are multiplicative in their indices and in particular, they commute.

(ii) $(f|T_{p^r})|T_p = f|T_{p^{r+1}} + p^{k-1}f|T_{p^{r-1}}$.

Since the Hecke operators are endomorphisms of the vector space M_k and they all commute, it makes sense to ask for simultaneous eigenforms under all of them. These are usually referred to as *Hecke eigenforms* and play a very important role in the theory, which we cannot really go into here. We just record the following fact.

Theorem 1.21. *Let $f \in M_k$ be not a constant with Fourier expansion $f(\tau) = \sum_{n=0}^{\infty} \alpha_f(n)q^n$. Then the following are equivalent.*

(i) *f is a simultaneous eigenform for all T_m, $m \in \mathbb{N}$.*

(ii) *f is a simultaneous eigenform for all T_p, where p is prime.*

(iii) *$\alpha_f(1) \neq 0$ and for any coprime $m, n \in \mathbb{N}$ we have $\alpha_f(m)\alpha_f(n) = \alpha_f(1)\alpha_f(mn)$, so the Fourier coefficients of Hecke eigenforms are (essentially) multiplicative functions.*

Remark 1.22. *The multiplicativity of the Fourier coefficients of Hecke eigenform is an extremely important property, for example when one talks about their L-functions (naively speaking, one replaces q^n in the Fourier expansion of a modular form by n^{-s} for some $s \in \mathbb{C}$ with $\mathrm{Re}(s)$ sufficiently large). This multiplicativity then translates to the fact that these L-functions have so-called Euler products. A toy example of this is the Riemann zeta function which for $\mathrm{Re}(s) > 1$ can be written as*

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

L-functions of modular forms have played a central role in the past century of number theory, for example in the proof of Fermat's Last Theorem or the Birch and Swinnerton-Dyer Conjecture.

We note one important corollary of Theorem 1.21, which had been conjectured by Ramanujan after he had computed about 30 values of the Ramanujan τ-function (i.e. Fourier coefficients of the cusp form Δ) and first proven by Mordell, some 15 years before Hecke set up his general theory of operators.

Corollary 1.23. *The Ramanujan τ-function is multiplicative.*

Proof. The space S_{12} is one dimensional, hence, since Hecke operators map cusp forms to cusp forms, Δ must be a simultaneous Hecke eigenform, so by Theorem 1.21 its Fourier coefficients are multiplicative. □

2 More advanced theory

2.1 More general settings for modular forms

As we have already seen above, one can produce modular forms for subgroups of $\mathrm{SL}_2(\mathbb{Z})$ from those for the full modular group by slashing with matrices in $\mathrm{GL}_2^+(\mathbb{Q})$. We now give a general definition of such forms.

Definition 2.1. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a finite-index subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Then a function $f : \mathfrak{H} \to \mathbb{C}$ is called a* modular form *of weight $k \in \mathbb{Z}$ for Γ if*

(i) f is holomorphic on $\mathfrak{H}$,

(ii) $f|_k\gamma \equiv f$ for all $\gamma \in \Gamma$,

(iii) f is holomorphic at the cusps*, which means that for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we have $(f|_k\gamma)(iv)$ is bounded as $v \to \infty$.*

If f satisfies instead of (iii) the stronger condition that $(f|_k\gamma)(iv) \to 0$ as $v \to \infty$, we call f a cusp form for Γ. We denote the spaces of weight k modular forms resp. cusp forms by $M_k(\Gamma)$ resp. $S_k(\Gamma)$.

Remark 2.2. *It should be remarked that since Γ has finite index in $\mathrm{SL}_2(\mathbb{Z})$, one just needs to check condition (iii) in Definition 2.1 for a finite set of representatives of $\mathrm{SL}_2(\mathbb{Z})/\Gamma$. Note however that this is not always trivial to do in practice. Also, one cannot see in general if f is a cusp form just by looking at its Fourier expansion.*

It often happens in applications that one wants to relax Definition 2.1 even further by requiring instead of (ii) the weaker condition that

$$f|_k\gamma = \varepsilon(\gamma)f$$

for a certain type of function $\varepsilon : \Gamma \to \mathbb{C}$ called a *multiplier system*. We won't define this term in full generality, one should essentially think of a one-dimensional representation of Γ which (for convenience) should satisfy that there is some $N \in \mathbb{N}$ with $\varepsilon(\gamma)^N = 1$ for all $\gamma \in \Gamma$. The corresponding spaces are denoted by $M_k(\Gamma, \varepsilon)$ resp. $S_k(\Gamma, \varepsilon)$.

Remark 2.3. *Note that if $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \notin \Gamma$, there might very well be modular forms of odd weight for Γ (but none for negtive weight). If $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \Gamma$, then $M_k(\Gamma, \varepsilon)$ can only be non-trivial if $\varepsilon(\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)) = (-1)^k$.*

There are the following very important subgroups of $\mathrm{SL}_2(\mathbb{Z})$. For this let $N \in \mathbb{N}$ be

some positive integer.

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

The group $\Gamma(N)$ is called the *principal congruence subgroup* of level N. We also give the indeces of these groups here.

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right),$$

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] = N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right),$$

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right).$$

Sometimes one also wants to consider modular forms of half-integral weight. Essentially because the complex square-root function is inherently multivalued, this cannot be achieved by simply allowing half-integer powers in the automorphy factors. Instead one is essentially required to consider a different group under which these functions are invariant, the *metaplectic group*. One can however circumvent this using the following definition.

Definition 2.4. *A function $f : \mathfrak{H} \to \mathbb{C}$ is called a modular form of weight $k \in \frac{1}{2} + \mathbb{Z}$ for $\Gamma_0(4N)$ if*

(i) f is holomorphic on $\mathfrak{H}$,

(ii) we have

$$(f|_k\gamma)(\tau) := \left(\frac{c}{d}\right) \left(\frac{-4}{d}\right)^k (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right) = f(\tau)$$

for all $\gamma \in \Gamma_0(4N)$ and all $\tau \in \mathfrak{H}$, where here $\left(\frac{a}{b}\right)$ denotes the Jacobi symbol and we choose the principal branch of the square-root, which is positive for positive real arguments,

(iii) f is holomorphic at the cusps.

Note that by choosing an appropriate multiplier system it is possible to have different kinds of half-integer weight modular forms, as we see for instance in the context of the Dedekind eta function in Section 2.2.2.

Even though we have now relaxed the notion of modular form quite considerably, we still have the following result.

Theorem 2.5. *For any subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index, multiplier system ε and weight $k \in \frac{1}{2}\mathbb{Z}$, the space $M_k(\Gamma, \varepsilon)$ is finite-dimensional, more precisely we have*

$$\dim_{\mathbb{C}} M_k(\Gamma, \varepsilon) \leq C(k+1)(\mathrm{vol}(\Gamma \setminus \mathfrak{H}) + 1),$$

for some constant $C > 0$, where $\mathrm{vol}(\Gamma\setminus\mathfrak{H})$ denotes the (hyperbolic) volume of a fundamental domain of Γ.

One of the important appeals of the theory of modular forms is that it is a source of sometimes surprising identities, which arise by comparing two modular forms. A first example of this is the Hurwitz identity in Remark 1.11. To do this in general, the following result often referred to as the *Sturm bound*, although it is essentially already due to Hecke, is invaluable.

Theorem 2.6. *Let $f, g \in M_k(\Gamma)$ for some $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index with Fourier expansions $f(\tau) = \sum_{n=0}^{\infty} \alpha_f(n) q^n$ and $g(\tau) = \sum_{n=0}^{\infty} \alpha_g(n)$. Then we have $f(\tau) = g(\tau)$ for all $\tau \in \mathfrak{H}$ if and only if*

$$\alpha_f(n) = \alpha_g(n) \text{ for all } n \leq \left(\left\lfloor \frac{k}{12} \right\rfloor + 1 \right) [\mathrm{SL}_2(\mathbb{Z}) : \Gamma].$$

So comparing two modular forms boils down to checking finitely many of their Fourier coefficients, even though in many applications, the indeces of the groups involved are so large that one has to do more or less clever tricks before it is feasible to actually do this in practice.

2.2 Further examples

In this section, we will discuss some further examples of sources of modular forms.

2.2.1 Theta series

In this section let $Q \in \mathbb{Z}_{>0}^{m\times m}$ be a positive definite integer matrix whose diagonal entries are even (one should think of the term *even quadratic form* here). Then we define the *Theta series* of Q by

$$\Theta_Q(\tau) := \sum_{\ell \in \mathbb{Z}^m} q^{\ell^{tr} Q \ell / 2} = \sum_{n=0} r_Q(n) q^n,$$

where we set

$$r_Q(n) := \#\{\ell \in \mathbb{Z}^m \ : \ \ell^{tr} Q \ell = 2n\}.$$

These numbers $r_Q(n)$ have played an important role in number theory for centuries, dating back at least to Fermat, possibly even Diophantus, who asked (and partly answered) the

question which numbers can be represented for instance as the sum of 2 or 4 squares. In those cases, Q would just be twice the 2×2 or 4×4 identity matrix, so they asked when $r_Q(n) \neq 0$. It is even more interesting to ask for an (elementary) formula for $r_Q(n)$. This can often be provided through the theory of modular forms by means of the following important theorem due to Schoeneberg.

Theorem 2.7. *The function Θ_Q is a modular form of weight $m/2$ for some $\Gamma_0(N)$ and some multiplier system which can be determined explicitly. In particular, if $\det Q = 1$, we have $\Theta_Q \in M_{m/2}(\mathrm{SL}_2(\mathbb{Z}))$.*

The basic idea of the proof is essentially *Poisson summation* which in its simplest form states that for a function $f : \mathbb{R} \to \mathbb{R}$ with sufficiently rapid decay at $\pm\infty$ one has

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{m \in \mathbb{Z}} \widehat{f}(m),$$

where $\widehat{f}$ denotes the *Fourier transform* of f. As it turns out, the Fourier transform of $\exp(-\ell^{tr} Q \ell \pi v)$ is closely related to $\exp(-\ell^{tr} Q \ell \pi / v)$, from where Schoeneberg's theorem can be inferred.

Example 2.8. *It can be inferred from Theorem 2.7 that if $\det Q = 1$, then we must have $8 \mid m$, so the lowest dimension where the second part of that theorem applies is $m = 8$. Indeed, there is an 8×8 matrix with this property,*

$$\mathbb{E}_8 = \begin{pmatrix} 4 & -2 & 0 & 0 & 0 & 0 & 0 & 1 \\ -2 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

So by Schoenebergs theorem, we know that $\Theta_{\mathbb{E}_8} \in M_4(\mathrm{SL}_2(\mathbb{Z}))$, which implies immediately, because this space is one-dimensional, that $\Theta_{\mathbb{E}_8} = E_4$, so by comparing coefficients we find

$$r_{\mathbb{E}_8}(n) = 240\sigma_3(n)$$

for all n.

2.2.2 The Dedekind eta function

One extremely important modular form that can be used to build a surprisingly large proportion of modular forms in general is the *Dedekind eta function*. It is defined by

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

Recall that we already saw that

$$\Delta(\tau) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \eta(\tau)^{24}.$$

So one may think of the eta function as the 24th root of Δ, which somewhat suggests that it should be a modular form of weight $12/24 = 1/2$ in some sense. Figuring this out in detail however is not so easy. One has the obvious transformation behaviour

$$\eta(\tau+1) = e^{\pi i/12}\eta(\tau)$$

under translation. It is a bit less obvious to see that

$$\eta(-1/\tau) = \sqrt{\tau/i}\eta(\tau),$$

where, as always we choose the principal branch of the square-root. So there is a reasonably transformation behaviour under both generators of $\mathrm{SL}_2(\mathbb{Z})$ which confirms that η is a modular form of weight $1/2$ with some multiplier system. It is however not at all easy to figure out the general transformation behaviour of η under a general matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. This was first done by Dedekind who proved the following result.

Theorem 2.9. *For $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $c > 0$ we have that*

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right) = \exp\left(\pi i\left(\frac{a+d}{12c} + s(-d,c) - \frac{1}{4}\right)\right)\sqrt{\frac{c\tau+d}{i}}\eta(\tau),$$

where for coprime integers h, k, $k > 0$, we denote by

$$s(h,k) = \sum_{r=1}^{k-1}\left(\frac{r}{k} - \frac{1}{2}\right)\left(\frac{rh}{k} - \left\lfloor\frac{rh}{k}\right\rfloor - \frac{1}{2}\right)$$

the Dedekind sum*.*

Even though this multiplier system seems rather complicated, it is relatively well controllable. For example we can use this (in principle) to show the following version of Euler's famous Pentagonal Number Theorem.

Corollary 2.10. *We have*

$$\eta(24\tau) = \frac{1}{2}\sum_{n\in\mathbb{Z}}\chi_{12}(n)q^{n^2} \in S_{1/2}(576,\chi_{12}),$$

where $\chi_{12}(n) = \left(\frac{12}{n}\right)$.

One important feature of the eta function is that it can be used to build new modular forms in pretty easy way.

Definition 2.11. *For $N \in \mathbb{N}$ and integers $r_d \in \mathbb{Z}$, $d \mid N$, we call the expression*

$$\prod_{d|N} \eta(d\tau)^{r_d}$$

an eta quotient *of level N.*

By investigating the arithmetic properties of Dedekind sums, one can give explicit criteria when an eta quotient of level N defines e.g. a modular form in $M_k(\Gamma_0(N))$. In many cases (but not all), the algebra of modular forms for $\Gamma_0(N)$, $M_*(\Gamma_0(N)) = \bigoplus_{k=0}^{\infty} M_k(\Gamma_0(N))$, is even generated by such eta quotients.

2.2.3 Poincaré series

An important general way to construct modular forms in $M_k(\Gamma, \varepsilon)$ in an almost completely general setting is through so-called *Poincaré series*, which we briefly want to mention in this section. The idea here is to average some function over the group Γ. More precisely, let $\varphi : \mathfrak{H} \to \mathbb{C}$ be a holomorphic function invariant under the group $\Gamma_\infty = \mathrm{Stab}_\Gamma(\infty)$. In the case of $\Gamma = \Gamma_0(N)$ for instance, one has $\Gamma_\infty = \langle \pm T \rangle$, so that here, φ should be one-periodic. With this, we formally define the series

$$\mathbb{P}(\tau) := \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \varepsilon(\gamma)(\varphi|_k \gamma)(\tau).$$

It is easy to see that $\mathbb{P}$ is holomorphic on $\mathfrak{H}$ and transforms like a modular form in $M_k(\Gamma, \varepsilon)$, provided that it converges absolutely and locally uniformly. If φ has moderate growth approaching 0, this is the case as soon as the weight k is sufficiently large.

In many cases, one can give explicit formulas for their Fourier coefficients, often in terms of infinite sums of so-called *Kloosterman sums* and Bessel functions, but we refrain from giving these expressions here.

2.3 Jacobi forms

Jacobi forms are in a sense an amalgam of elliptic functions (i.e. doubly-periodic functions) and modular forms. They have deep connections to many important types of modular forms. Even though there are examples dating back to Jacobi (hence the name), their systematic study originated from certain *Siegel modular forms*, which are a certain kind of multivariable modular forms.

Definition 2.12. *A function $\phi : \mathbb{C} \times \mathfrak{H} \to \mathbb{C}$ is called a* Jacobi form *of weight k and index m if*

(i) ϕ *is holomorphic on* $\mathbb{C} \times \mathfrak{H}$,

(ii) we have

$$\phi(z + \lambda\tau + \mu, \tau) = e^{-2\pi i m(\lambda^2\tau + 2\lambda z)}\phi(z, \tau)$$

for all $\lambda, \mu \in \mathbb{Z}$, $z \in \mathbb{C}$, $\tau \in \mathfrak{H}$ *(*elliptic transformation law*),*

(iii) we have

$$\phi\left(\frac{z}{c\tau + d}, \frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k e^{2\pi i m \frac{cz^2}{c\tau + d}}\phi(z, \tau)$$

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, $z \in \mathbb{C}$, $\tau \in \mathfrak{H}$ *(*modular transformation law*),*

(iv) ϕ *has a Fourier epansion*

$$\phi(z, \tau) = \sum_{n,r \in \mathbb{Z}} c(n, r) q^n \zeta^r,$$

where $\zeta = e^{2\pi i z}$ *with* $c(n, r) = 0$ *whenever* $n < r^2/4m$.

The space of Jacobi forms of weight k *and index* m *is denoted by* $J_{k,m}$.

The prototypical examples of Jacobi forms are the *Jacobi theta functions*

$$\theta_{m,\ell}(z, \tau) = \sum_{\substack{r \in \mathbb{Z} \\ r \equiv \ell \ (2m)}} q^{r^2/4m} \zeta^r,$$

which are Jacobi forms of weight $1/2$ and index m for some subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Here, we introduce the three most direct ways in which a Jacobi form can capture modular forms. The first such way is through evaluation at so-called *torsion points*.

Theorem 2.13. *Let* $\phi \in J_{k,m}$ *and* $\alpha, \beta \in \mathbb{Q}$. *Then* $\phi(\alpha\tau + \beta, \tau)$ *is a modular form of weight* k *for some explicitly known congruence subgroup depending on* α, β *and* m.

Next to the Fourier expansion, a Jacobi form has at least two other important expansion. The first one is discussed in the following theorem.

Theorem 2.14. *Let* $\phi \in J_{k,m}$ *be a Jacobi form. Then we can write*

$$\phi(z, \tau) = \sum_{\ell \pmod{2m}} h_\ell(\tau)\theta_{m,\ell}(z, \tau),$$

which we call the theta expansion *of* ϕ. *The functions* h_ℓ *are then modular forms of weight* $k - 1/2$ *for some specific subgroup of* $\mathrm{SL}_2(\mathbb{Z})$.

Remark 2.15. *If one considers the vector* $\vec{h}(\tau) = (h_0(\tau), ..., h_{2m-1}(\tau))$*, one finds that this vector transforms indeed like a modular form for the full modular group* $\mathrm{SL}_2(\mathbb{Z})$ *for a certain representation, called the* Weil representation*, meaning that there is a map* $\rho : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{GL}_{2m}(\mathbb{C})$*, such that*

$$\vec{h}\left(\frac{a\tau+b}{c\tau+d}\right) = \rho\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)\left(\frac{c\tau+d}{i}\right)^{k-1/2}\vec{h}(\tau).$$

The third important expansion of a Jacobi form that yields modular forms is its Taylor expansion in $z = 0$.

Theorem 2.16. *Define the space of* weak *Jacobi forms* $\widetilde{J}_{k,m}$ *by relaxing condition* (iv) *in Definition 2.12 to* $c(n, r) = 0$ *whenever* $n < 0$*. Then the Taylor coefficients of* $\phi \in \widetilde{J}_{k,m}$ *in* $z = 0$ *are essentially modular forms of even weight for* $\mathrm{SL}_2(\mathbb{Z})$*. More precisely, there is an explicit isomorphism*

$$\widetilde{J}_{k,m} \to \begin{cases} M_k \oplus M_{k+2} \oplus ... \oplus M_{k+2m} & k \text{ even,} \\ M_{k+1} \oplus M_{k+3} \oplus ... \oplus M_{k+2m-3} & k \text{ odd.} \end{cases}$$

For even weight, the isomorphism is given by

$$\phi(z, \tau) \mapsto \left(\sum_{\ell\,(2m)} [h_\ell(\tau), \theta(0, \tau)]_\nu\right)_{\nu=0}^{m},$$

where $[\bullet, \bullet]_\nu$ *denotes the* ν*th* Rankin-Cohen bracket*, a bilinear differential operator on modular forms that acts essentially like a product. A similar formula holds also in the case of odd weight.*

2.4 Singular moduli

This sections follows closely the exposition on the subject in Section 6 of [1-2-3].

The subject of singular moduli is certainly one of the most important in the arithmetic theory of modular forms. Let us motivate it by the following observation that

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999250072...$$

is surprisingly close to an integer. Here we would like to briefly outline an explanation for this phenomenon.

For this we look at *Klein's modular invariant*

$$j(\tau) := \frac{E_4(\tau)^3}{\Delta(\tau)} = q^{-1} + 744 + 196\,884q + 21\,493\,760q^2 + O(q^3).$$

This clearly transforms like a modular form of weight 0, so we have indeed

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

but it has a pole at infinity and is therefore not a modular form in our sense, but rather a *modular function*, i.e. a meromorphic function transforming like a modular form of weight 0. In a sense, j can be viewed as the most important modular function of them all.

Theorem 2.17. *(i) Every modular function for* $\mathrm{SL}_2(\mathbb{Z})$ *is a rational function in* j*.*

(ii) Every modular function for $\mathrm{SL}_2(\mathbb{Z})$ *which is holomorphic in* $\mathfrak{H}$ *(but may have a pole at* ∞*) is a polynomial in* j*.*

(iii) Every modular function for any finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ *is an algebraic function in* j*.*

One can compute several special values of j, e.g.

$$j(\rho)=0,\quad j(i)=1728,\quad j(i\sqrt{2})=8000,\quad j\left(\frac{1+i\sqrt{7}}{2}\right)=-3375,$$

$$j\left(\frac{1+i\sqrt{15}}{2}\right)=-\frac{191025+85995\sqrt{5}}{2},\ldots$$

It is a rather striking phenomenon, when a transcendental function evaluated at algebraic arguments again gives algebraic values. In this case, the reason lies in the following theorem.

Theorem 2.18. *For every* $m\in\mathbb{N}$ *there is a polynomial* $\Psi_m(X,Y)\in\mathbb{Z}[X,Y]$ *of degree* $\sigma_1(m)$ *in both variables such that*

$$\Psi_m(j(M.\tau),j(\tau))\equiv 0$$

for all $M\in\mathcal{M}_m$ *with* $\mathcal{M}_m$ *as in Section 1.3.*

Sketch of proof. Consider

$$\prod_{M\in\mathrm{SL}_2(\mathbb{Z}):\mathcal{M}_m}(X-j(M.\tau))=:\Psi_m(X,j(\tau)).$$

Then this is well defined because $j(\gamma.\tau)=j(\tau)$ for all $\gamma\in\mathrm{SL}_2(\mathbb{Z})$ and we have

$$\Psi_m(X,j(\gamma.\tau))=\Psi_m(X,j(\tau))$$

because $\mathcal{M}_m\cdot\gamma=\mathcal{M}_m$ (recall that we used a similar argument in the context of Hecke operators). This means that the coefficient of X^r in $\Psi_m(X,j(\tau))$ is a modular function in τ for $\mathrm{SL}_2(\mathbb{Z})$ which has no poles in $\mathfrak{H}$ (because none of the $j(M.\tau)$ do), so each coefficient is a polynomial in $j(\tau)$, which yields the definition of a polynomial $\Psi_m(X,Y)\in\mathbb{C}[X,Y]$. For the sake of brevity, we omit the proof that $\Psi_m(X,Y)$ has indeed integral coefficients and the same degree in both variables. □

This yields the following theorem.

Theorem 2.19. *Let $\mathfrak{z} \in \mathfrak{H}$ be a* CM point*, i.e. there are $A, B, C \in \mathbb{Z}$ sucht that $A\mathfrak{z}^2 + B\mathfrak{z} + C = 0$. Then $j(\mathfrak{z})$ is an algebraic integer.*

Sketch of proof. The matrix $M = \left(\begin{smallmatrix} B & C \\ -A & 0 \end{smallmatrix}\right)$ satisfies $M.\mathfrak{z} = \mathfrak{z}$ as one immediately checks. Since $\det M = AC$, we have

$$\Psi_{AC}(j(M.\mathfrak{z}), j(\mathfrak{z})) = \Psi_{AC}(j(\mathfrak{z}), j(\mathfrak{z})) = 0.$$

□

Remark 2.20. *One should say about the above proof sketch that it is not necessarily clear that $\Psi_m(X, X)$ is not just the zero polynomial (in fact this can happen). But since one can redefine $\Psi_m(X, Y)$ by dividing out all factors $(X - Y)$ without changing the important properties in Theorem 2.18, this can be reconciled.*

Remark 2.21. *One can in fact show, e.g. by using (iii) of Theorem 2.17, that $f(\mathfrak{z})$ is an algebraic number (not necessarily integral) for every modular function for any finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with algebraic Fourier coefficients.*

The values $j(\mathfrak{z})$ for CM points $\mathfrak{z}$ play an important role in class field theory, as we shall explain now. Let $Q(X, Y) = AX^2 + BXY + CY^2 =: [A, B, C] \in \mathbb{Z}[X, Y]$ be a binary quadratic form of discriminant $D = B^2 - 4AC < 0$ and $A > 0$ and define $\mathfrak{z}_Q \in \mathfrak{H}$ by $Q(\mathfrak{z}_Q, 1) = 0$. Also define $\mathcal{Q}_D = \{[A, B, C] : B^2 - 4AC = D\}$ as the set of quadratic forms of discriminant D.

Theorem 2.22. *Let $D < 0$ be a* fundamental discriminant*, i.e. the discriminant of a quadratic field, and set*

$$H_D(X) = \prod_{Q \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathcal{Q}_D} (X - j(\mathfrak{z}_Q)).$$

The $H_D(X) \in \mathbb{Z}[X]$ and $\deg H_D(X) = h(D)$, the class number *of D. The splitting field of $H_D(X)$ is the so-called* Hilbert class field *of $\mathbb{Q}(\sqrt{D})$, i.e. a Galois extension of $\mathbb{Q}(\sqrt{D})$ whose Galois group is isomorphic to the ideal class group of $\mathbb{Q}(\sqrt{D})$.*

3 Applications to partitions

In this section, we explore some applications of the theory of modular forms to *partitions*. It is well-known that the generating function of the *partition function*

$$p(n) := \#\{(\lambda_1, ..., \lambda_\ell) \,:\, \lambda_1 \geq ... \geq \lambda_\ell > 0, \lambda_1 + ... + \lambda_\ell = n\}$$

has a very simple description as an infinite product,

$$P(q) = \sum_{n=0}^{\infty} p(n) q^n = \prod_{n=1}^{\infty} (1-q^n)^{-1} = \frac{q^{1/24}}{\eta(\tau)}.$$

Hence, $P(q)$ is essentially a weakly holomorphic modular form (i.e. it has poles at cusps) of weight $-1/2$ with some multiplier system, namely the inverse of that of the Dedekind eta function. We want to exploit this fact to say something about the numbers $p(n)$.

3.1 Asymptotics

This part of the exposition is essentially a short summary of Chapter 5 of [Apo].

By Cauchy's Theorem, we have that

$$p(n) = \frac{1}{2\pi i} \int_C \frac{P(q)}{q^{n+1}} dq,$$

where C is a simple, closed contour inside the unit disk looping around $q = 0$ exactly once.

From the product expansion we can see that $P(q)$ has a singularity whenever q approaches a root of unity. The idea now is to choose a special contour C and let it approach the unit circle form inside in a certain way to be able to replace $P(q)$ in Cauchy's Theorem above by a more elementary function plus some (small) error. For this we divide C into parts $C_{h,k}$ for coprime h, k with $k \leq N$ for some previously chosen $N \in \mathbb{N}$, which are close to the roots of unity $e^{2\pi i h/k}$ of order up to N,

$$p(n) = \frac{1}{2\pi i} \int_C \frac{P(q)}{q^{n+1}} dq = \sum_{k=1}^{N} \sum_{h\ (k)^*} \int_{C_{h,k}} \frac{P(q)}{q^{n+1}} dq = \sum_{k=1}^{N} \sum_{h\ (k)^*} \int_{C_{h,k}} \frac{\psi_{h,k}(q)}{q^{n+1}} dq + \text{“Error”},$$

where here and from now on, $\sum_{a\ (b)^*}$ means a sum over all $a = 0, ..., b-1$ coprime to b.

In order to do this, we require the following lemma which is a convenient reformulation of Dedekind's Theorem 2.9.

Lemma 3.1. *Let* $q = \exp\left(\frac{2\pi i h}{k} - \frac{2\pi z}{k^2}\right)$, $q' = \exp\left(\frac{2\pi i H}{k} - \frac{2\pi}{z}\right)$ *with* $\mathrm{Re}(z) > 0$, $\gcd(h,k) = 1$ *and* $hH \equiv -1 \pmod{k}$. *Further define* $\omega(h,k) = e^{\pi i s(h,k)}$ *and*

$$\Psi_k(z) = z^{1/2} \exp\left(\frac{\pi}{12z} - \frac{\pi z}{12k^2}\right).$$

Then we have

$$P(q) = \omega(h,k) \frac{\Psi_k(z)}{k^{1/2}} P(q').$$

Next, following Rademacher, we choose a special path of integration. Suppose C is a circular contour inside the unit disk (in the q-plane). Then this essentially corresponds to a line-integral from i to $i+1$ in the τ-plane. Now we replace this line integral by an integral along the arcs of so-called *Ford circles* (see Figure 2). Denote this path by $\mathcal{P}(N)$.

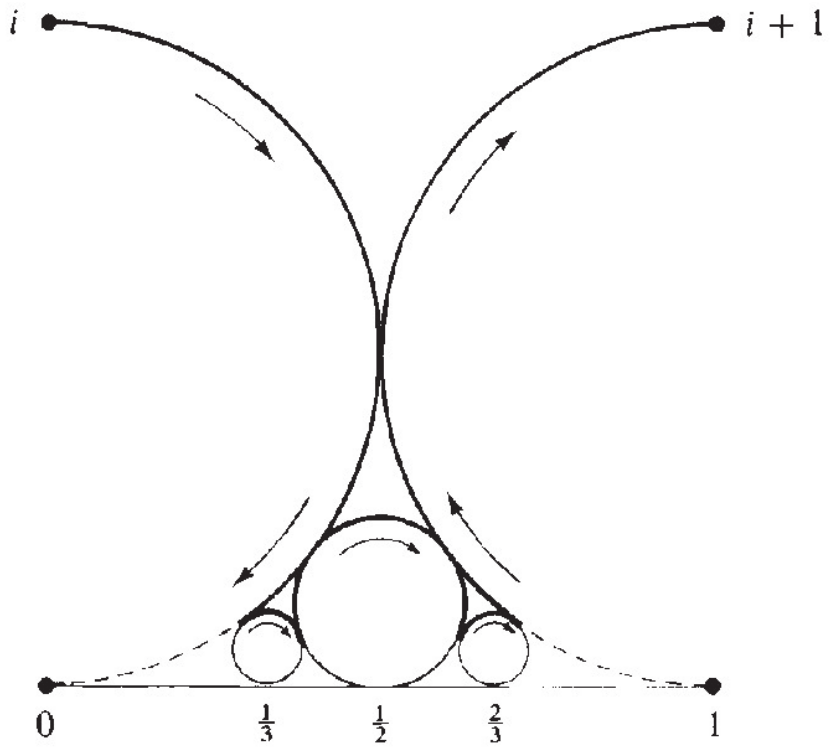

Figure 2: Rademacher path $\mathcal{P}(3)$ (graphic from [Apo, Figure 5.5]).

By making an appropriate change of variables we can write

$$\begin{aligned} p(n) &= \frac{1}{2\pi i}\sum_{C}\frac{P(q)}{q^{n+1}}dq \\ &= \int_{i}^{i+1} P(e^{2\pi i\tau})e^{-2\pi in\tau}d\tau \\ &= \int_{\mathcal{P}(N)} P(e^{2\pi i\tau})e^{-2\pi in\tau}d\tau \\ &= \sum_{k=1}^{N}\sum_{h\ (k)^*} ik^{-2}e^{-2\pi inh/k}\int_{z_1(h,k)}^{z_2(h,k)} e^{2\pi nz/k^2}P\left(\exp\left(\frac{2\pi ih}{k}-\frac{2\pi z}{k^2}\right)\right)dz, \end{aligned}$$

where $z_1(h,k)$ and $z_2(h,k)$ are the images of points where the Ford circles in the path $\mathcal{P}(N)$ touch under the change of variables $\tau = \frac{h}{k} + \frac{iz}{k^2}$ which occurred in the last step and the contour becomes the arc of a circle around $1/2$ of radius $1/2$ joining these points. Using Lemma 3.1, one can then write

$$p(n) = \sum_{h,k} ik^{-5/2}\omega(h,k)e^{-2\pi inh/k}(I_1(h,k) + I_2(h,k)),$$

where $\sum_{h,k}$ for the double sum over h and k and we define

$$I_1(h,k) = \int_{z_1(h,k)}^{z_2(h,k)} \Psi_k(z)e^{2\pi hz/k^2}dz$$

and

$$I_2(h,k) = \int_{z_1(h,k)}^{z_2(h,k)} \Psi_k(z)\left[P\left(\exp\left(\frac{2\pi iH}{k} - \frac{2\pi}{z}\right)\right) - 1\right]e^{2\pi nz/k^2}dz.$$

One can show now that $|I_2(h,k)| \leq Ck^{3/2}N^{-3/2}$ for some constant $C > 0$, whence

$$\left|\sum_{h,k} ik^{-5/2}\omega(h,k)e^{-2\pi inh/k}I_2(h,k)\right| \leq CN^{-1/2}.$$

Therefore we find that

$$p(n) = \sum_{h,k} ik^{-5/2}\omega(h,k)e^{-2\pi inh/k}I_1(h,k) + O(N^{-1/2}).$$

Now letting $N \to \infty$ and evaluating the integral $I_1(h,k)$ explicitly one arrives at the following important theorem due to Rademacher.

Theorem 3.2. *For $n \in \mathbb{N}$, we have the following formula for $p(n)$,*

$$p(n) = \frac{1}{\pi\sqrt{2}}\sum_{k=1}^{\infty} A_k(n)k^{1/2}\frac{d}{dn}\left(\frac{\sinh\left(\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n - \frac{1}{24}\right)}\right)}{\sqrt{n - \frac{1}{24}}}\right)$$

with

$$A_k(n) = \sum_{h\ (k)^*} e^{\pi is(h,k) - 2\pi inh/k}.$$

Essentially by specializing to the term $k = 1$ in the above series for $p(n)$, one recovers an older result due to Hardy and Ramanujan.

Theorem 3.3. *As $n \to \infty$, we have the asymptotic equality*

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}.$$

Remark 3.4. *Hardy and Ramanujan in fact had a full asymptotic expansion for $p(n)$, using essentially the argument outlined here, but their expansion does not give a convergent series. Some 20 years after their work was published, Rademacher realized that the proof by Hardy-Ramanujan could be modified slightly to yield the convergent series expression in Theorem 3.2.*

It should also be pointed out that there are many much easier ways to obtain just the main term of the asymptotic expansion given in Section 3.1, one very important one being to use a so-called Tauberian theorem due to Ingham.

3.2 Congruences

This section is essentially a short summary of parts of Chapter 5 of [Ono].

Many people know the famous *Ramanujan congruences*,

$$\begin{aligned} p(5n+4) &\equiv 0 \pmod 5, \\ p(7n+5) &\equiv 0 \pmod 7, \\ p(11n+6) &\equiv 0 \pmod{11}. \end{aligned}$$

Over the last 100 years, many proofs of these congruences, both using formal or q-series, but also modular forms techniques, have been published, also generalizations for congruences modulo powers of 5, 7, and 11 have been found (some of which have been conjectured by Ramanujan). In this last section, we want to construct further congruences of the form

$$p(An+B) \equiv 0 \pmod M.$$

In fact, for any M coprime to 6, there are infinitely many non-nested arithmetic sequences $An+B$, such that such a congruence holds. Here are some examples modulo larger primes,

$$\begin{aligned} p(17 \cdot 41^4 + 1122838) &\equiv 0 \pmod{17}, \\ p(19 \cdot 101^4 + 815655) &\equiv 0 \pmod{19}, \\ p(23 \cdot 5^4 + 3474) &\equiv 0 \pmod{23}, \\ &\vdots \end{aligned}$$

In this last section, we would like to explain the outline the proof of the following theorem due to Ahlgren and Ono underlying these and in fact all (known) congruences for $p(n)$.

For this we define for a prime $\ell \geq 5$ the set

$$\mathcal{S}_\ell := \left\{ \beta \in \{0, ..., \ell - 1\} \ : \ \left(\frac{\beta - \delta_\ell}{\ell} \right) \in \{0, \varepsilon_\ell\} \right\}$$

where $\delta_\ell := \frac{\ell^2-1}{24}$ and $\varepsilon_\ell := \left(\frac{-6}{\ell}\right)$.

Theorem 3.5. *Let $\ell \geq 5$ prime, $m \in \mathbb{N}$, $\beta \in \mathcal{S}_\ell$, then a positive proportion of primes $Q \equiv -1 \pmod{24\ell}$ satisfy*

$$p\left(\frac{Q^3 n + 1}{24} \right) \equiv 0 \pmod{\ell^m}$$

for all $n \equiv 1 - 24\beta \pmod{24\ell}$ and $\gcd(Q, n) = 1$.

The proof of this result hinges on the following one.

Proposition 3.6. *Given a prime $\ell \geq 5$, $m \in \mathbb{N}$, $\beta \in \mathcal{S}_\ell$, there exists $\lambda_{\ell,m} \in \mathbb{Z}$ and $F_{\ell,m,\beta} \in S_{\lambda_{\ell,m}+1/2}(576\ell^5) \cap \mathbb{Z}[[q]]$ such that*

$$F_{\ell,m,\beta} \equiv \sum_{n=0}^{\infty} p(\ell n + \beta) q^{24\ell n + 24\ell\beta - 1} \pmod{\ell^m}.$$

Sketch of proof. The function

$$E_{\ell,t}(\tau) := \frac{\eta(\tau)^{\ell^t}}{\eta(\ell^t \tau)}$$

is a modular form of weight $(\ell^t - 1)/2$ for the group $\Gamma_0(\ell^t)$ with multiplier system $\chi_{\ell,t} = \left(\frac{(-1)^{(\ell^t-1)/2} \ell^t}{\cdot} \right)$, which follows from Dedekind's Theorem 2.9. It is almost a cusp form in the sense that it vanishes at all cusps except ∞, i.e. $(E_{\ell,t}|\gamma)(iv) \to 0$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z}) \setminus \Gamma_0(\ell^t)$ and we have $E_{\ell,t}^{\ell^{m-1}} \equiv 1 \pmod{\ell^m}$.

Next we define

$$f_\ell(\tau) := \frac{\eta(\ell\tau)^\ell}{\eta(\tau)} =: \sum_{n=0}^{\infty} a_\ell(n) q^n,$$

which defines a modular form in $M_{(\ell-1)/2}(\Gamma_0(\ell), \left(\frac{\cdot}{\ell}\right))$. We can also write this as

$$f_\ell(\tau) = \sum_{n=0}^{\infty} p(n) q^{n+\delta_\ell} \prod_{n=1}^{\infty} (1 - q^{\ell n})^\ell.$$

We require the following twisted version of f_ℓ,

$$\tilde{f}_\ell(\tau) := \sum_{n=1}^{\infty} \left(1 - \varepsilon_\ell \left(\frac{n}{\ell} \right) \right) a_\ell(n) q^n,$$

which through standard theory of modular operators as outlined in Section 1.3 defines a modular form in $M_{(\ell-1)/2}(\Gamma_0(\ell^3), \left(\frac{\cdot}{\ell}\right))$. Since $\tilde{f}_\ell$ vanishes at the cusp ∞ and the function $E_{\ell,t}$ defined above vanishes at all other cusps, the function

$$f_{\ell,m'}(\tau) := E_{\ell,t}^{\ell^{m'}}(\tau)\tilde{f}_\ell(\tau)$$

is in fact a cusp form on $\Gamma_0(\ell^3)$ with multiplier system $\chi_{\ell,t}\left(\frac{\cdot}{\ell}\right)$ with $k = m'(\ell^t - 1)/2 + (\ell - 1)/2$, provided that m' is sufficiently large. We also have

$$f_{\ell,m'} \equiv \tilde{f}_\ell \pmod{\ell^m}$$

since $E_{\ell,t} \equiv 1 \pmod{\ell^m}$ and $\mathrm{ord}_\infty(f_{\ell,m'}) \geq \delta_\ell + 1$ because $\mathrm{ord}_\infty(f_\ell) \geq \delta_\ell$ and by construction, the leading term in $f_\ell(\tau)$ disappears in $\tilde{F}_\ell(\tau)$. Thus the function

$$F_{\ell,m'}(\tau) := \frac{f_{\ell,m'}(\tau)}{\eta(\ell\tau)^\ell}$$

vanishes at infinity and hence is a cusp form if m' is sufficiently large. By noting that

$$\tilde{F}_{\ell,m'}(\tau) \equiv \sum_{n \equiv 0\ (\ell)} p(n - \delta_\ell)q^{n-\ell^2/24} + 2 \sum_{\left(\frac{n}{\ell}\right) = -\varepsilon_\ell} p(n - \delta_\ell)q^{n-\ell^2/24} \pmod{\ell^m}.$$

Again through application of standard operators, we find that $\tilde{F}_{\ell,m'}(24\tau) \in S_{k'}(\Gamma_0(576\ell^3))$ for m' sufficiently large for suitable k'. The result now follows by applying an appropriate sieve operator. □

To complete the proof of Theorem 3.5, we need the following general lemma on Hecke operators for half-integer weight modular forms. For prime index p coprime to $4N$, one can define the Hecke operator T_{p^2} acting on $S_{\lambda+1/2}(\Gamma_0(4N))$ in terms of the operators defined in Section 1.3 by

$$f|T_{p^2} := f|U_{p^2} + \left(\frac{(-1)^\lambda}{p}\right) p^{\lambda-1} f \otimes \left(\frac{\cdot}{p}\right) + p^{2\lambda-1} f|V_{p^2}.$$

Lemma 3.7. *Let $N \in \mathbb{N}$, $\lambda \in \mathbb{N}$ and let $f \in S_{\lambda+1/2}(\Gamma_0(4N))$ with integer Fourier coefficients. Then for any $M \in \mathbb{N}$, a positive proportion of primes $p \equiv -1 \pmod{4MN}$ satisfies*

$$f|T_{p^2} \equiv 0 \pmod{0} \pmod{M}.$$

If we now apply the above lemma to the cusp form $F_{\ell,m,\beta}$ from Proposition 3.6, we find that for a positive proportion of primes $Q \equiv -1 \pmod{24\ell}$ satisfies

$$F_{\ell,m,\beta}|T_{Q^2} \equiv 0 \pmod{\ell^m}.$$

But

$$F_{\ell,m,\beta}(\tau) \equiv \sum_{n=0}^{\infty} a_{\ell,m,\beta}(n) q^n \equiv \sum_{n \equiv 24\beta - 1 \ (24\ell)} p((n+1)/24) q^n \pmod{\ell^m}.$$

By looking at the Qnth coefficient of $F|T_{Q^2}$, one finds that

$$0 \equiv a_{\ell,m,\beta}(Q^3 n) \equiv p\left(\frac{Q^3 n + 1}{24}\right) \pmod{\ell^m},$$

which is the claim from Theorem 3.5.

References

[Apo] T. M. Apostol, *Modular Forms and Dirichlet Series in Number Theory*, Springer-Verlag, 1990.

[CS] H. Cohen and F. Strömberg, *A Classical Introduction to Modular Forms*, Graduate Studies in Mathematics **179**, 2017.

[EZ] M. Eichler and D. Zagier, *The theory of Jacobi forms*, Birkhäuser-Verlag, 1985.

[Kil] L. J. P. Kilford, *Modular Forms: A Classical and Computational Introduction*, Imperial College Press, 2008.

[Ono] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS **102**, 2004.

[Ste] W. Stein, *Modular Forms: A Computational Approach*, available at `https://wstein.org/books/modform/stein-modform.pdf`

[Zag] D. Zagier, Modular Forms, in *From Number Theory to Physics*, Springer-Verlag, Springer-Verlag, 1992, available at `http://people.mpim-bonn.mpg.de/zagier/`

[1-2-3] D. Zagier, Elliptic Modular Forms and Their Applications, in *The 1-2-3 of Modular Forms*, Springer-Verlag, 2008.