Modular Forms

Notes for Advanced Number Theory (Master in Advanced Mathematics, UAB/UB)

Marc Masdeu

2025-01-01

Contents

Preface

These are notes used by the author on part of a course on *Advanced Number Theory* taught at UB/UAB during Spring 2024. They evolved from a course on Modular Forms taught at the University of Warwick during autumn of 2015, and are based on a variety of sources, mainly:

1. The books Diamond and Shurman [3] and Serre [4] listed in the bibliography.
2. Notes from a course taught by Peter Bruin in the spring term of 2014, which in turn are based on
3. Notes from a course taught by David Loeffler in the autumn term of 2011;
4. Notes from a course taught by Scott Ahlgren (UIUC) in 2006.

Typeset with Quarto. To learn more about it, see https://quarto.org/docs/books.

1 Modular forms of level one

1.1 Two examples

Modular forms have been for a while a central object in number theory. They have connections to many research areas: arithmetic, combinatorics, analysis, geometry, representation theory,...Since they appear essentially everywhere you look at, it is quite reasonable to wish to understand them.

Here is a not too serious reason: have you ever tried to calculate $e^{\pi\sqrt{163}}$? It turns out that it is

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999250072597\ldots$$

which seems *too close* to an integer to be a coincidence. That is, until you learn about modular forms: it turns out that this number is related to a value of a modular funtion (the j-function), which is known to be an integer.

In this introduction I give two more examples that hopefully convince the reader of the importance of modular forms in number theory. You can find many more examples in [1, Chapter 1].

1.1.1 Partitions and Ramanujan's τ-function

For each $n \geq 0$, define the *partition function* $p(n)$ as

$$p(n) = \#\{\text{ways of representing } n \text{ as a sum of natural numbers }\}.$$

As a convention, $p(0) = 1$. Also, note that:

$$\begin{aligned}
&p(1) = 1\\
&p(2) = 2 = \#\{1+1, 2\}\\
&p(3) = 3 = \#\{1+1+1, 1+2, 3\}\\
&p(4) = 5 = \#\{1+1+1+1, 1+1+2, 1+3, 2+2, 4\}\\
&p(5) = 7 = \#\{1+1+1+1+1, 1+1+1+2, 1+1+3, 1+4, 1+2+2, 2+3, 5\}\\
&\quad\ldots
\end{aligned}$$

In order to package all these numbers we may consider the following formal powers series:

$$P(q) = \sum_{n=0}^{\infty} p(n)q^n,$$

where we think of q as a formal variable.

Lemma 1.1. *There is an infinite product decomposition*

$$P(q) = \prod_{m=1}^{\infty} \frac{1}{1-q^m}.$$

Proof. We need to look at the right-hand side. Each of the factors can be written as $\sum_{k=0}^{\infty} q^{km}$, so the right-hand side looks like

$$\prod_{m=1}^{\infty} \sum_{k=0}^{\infty} q^{km}.$$

Now we collect the terms contributing to q^n, for a fixed n. These come from taking 1 from all but finitely many of the infinite sums, and then collecting $q^{k_1 m_1}$, $q^{k_2 m_2}$, ..., $q^{k_r m_r}$ from r other factors. This is subject to the condition

$$k_1 m_1 + k_2 m_2 + \cdots + k_r m_r = n,$$

and note that the m_i are all different because they are taken from different factors. There are exactly $p(n)$ such choices, as we wanted to show. □

In view of the previous lemma, a convenient way to study the partition function is through another very popular function, defined by the following infinite product:

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

Note that we have:

$$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24} = \frac{q \prod (1-q^n)^{25}}{\prod 1-q^n} = \left(\prod_{n=1}^{\infty} (1-q^n)^{25} \right) \sum_{n=0}^{\infty} p(n) q^{n+1}.$$

We define the *Ramanujan's tau* function as the Fourier coefficients of Δ. That is,

$$\Delta(q) = \sum_{n=1}^{\infty} \tau(n) q^n.$$

Later in this course you will be able to prove the following striking result.

Theorem 1.1. *For each $n \geq 1$, we have:*

$$\tau(n) \equiv \sum_{d|n} d^{11} \pmod{691}.$$

Moreover, the partition function satisfies the following congruences:

$$p(5n+4) \equiv 0 \pmod{5}, \quad \forall n,$$

$$p(7n+5) \equiv 0 \pmod{7}, \quad \forall n,$$

$$p(11n+6) \equiv 0 \pmod{11}, \quad \forall n.$$

1.1.2 A modular form of level 11 that knows about congruences

Consider another modular form:

$$f(z) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 + \cdots = \sum_{n=1}^{\infty} a(n)q^n.$$

Theorem 1.2.

1. *$a(nm) = a(n)a(m)$ whenever $(n,m) = 1$.*
2. *$|a(p)| \leq 2\sqrt{p}$ for all prime p.*

Consider the equation:

$$E\colon Y^2 + Y = X^3 - X^2 - 10X - 20,$$

and let $N(p)$ be the number of solutions in $\mathbb{F}_p$. Heuristically we should think that $N(p) \simeq p$.

Theorem 1.3. $|p - N(p)| \leq 2\sqrt{p}$.

The theory of modular forms allows to prove that the E and f "correspond" to each other:

Theorem 1.4. *For all primes p, we have $a(p) = p - N(p)$.*

This allows us to easily calculate (from f) what is $N(p)$ for all p. We say in this case that E "is modular". In [3] you can learn how to attach an elliptic curve to a modular form (this is called the "Eichler–Shimura" construction). It is **much** harder to reverse this process, and this is what A.Wiles did in order to prove Fermat's Last Theorem.

1.2 The upper half-plane

This section introduces the seemingly innocuous upper half-plane $\mathbb{H}$.

Definition 1.1. The *upper half-plane* $\mathbb{H}$ is the set of complex numbers with positive imaginary part:

$$\mathbb{H} = \{z = x + iy \mid \Im(z) > 0\}.$$

The upper half-plane appears in the classification of Riemann surfaces: there are only three of them which are simply connected which are the complex plane, the complex sphere, and $\mathbb{H}$.

The *general linear group* $\mathrm{GL}_2(\mathbb{R})$ consists of all 2×2 invertible matrices with entries in $\mathbb{R}$. It contains the subgroup $\mathrm{GL}_2^+(\mathbb{R})$ of matrices with positive determinant. The $\mathrm{SL}_2(\mathbb{R}) \subset \mathrm{GL}_2^+(\mathbb{R})$ consists of those matrices with determinant 1. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ and $z \in \mathbb{H}$, define γz as:

$$\gamma z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}. \tag{1.1}$$

Lemma 1.2. *Let* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$. *Then:*

$$\Im(\gamma\tau) = \frac{\det(\gamma)}{|c\tau + d|^2}\Im(\tau), \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Proof. One just needs to compute

$$\begin{aligned} \Im(\gamma\tau) = \Im(\frac{a\tau + b}{c\tau + d}) &= \Im\left(\frac{(a\tau + b)(c\bar{\tau} + d)}{|c\tau + d|^2}\right) \\ &= \frac{\Im(ac|\tau|^2 + ad\tau + bc\bar{\tau} + bd)}{|c\tau + d|^2} = \frac{ad\Im(\tau) - bc\Im(\tau)}{|c\tau + d|^2}. \end{aligned}$$

□

Corollary 1.1. $\mathrm{GL}_2^+(\mathbb{R})$ *acts on the left on* $\mathbb{H}$.

Note that the determinant gives a decomposition

$$\mathrm{GL}_2^+(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R}) \times \mathbb{R},$$

and since the scalar matrices (those of the form $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$) act trivially on $\mathbb{H}$, from now on we will restrict our attention to $\mathrm{SL}_2(\mathbb{R})$. In fact, since the scalar matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ belongs to $\mathrm{SL}_2(\mathbb{R})$, the above action on $\mathbb{H}$ factors through $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$, which is called the .

From this action we can deduce a right action on functions on $\mathbb{H}$, by precomposing:

$$(f \cdot \gamma)(z) = f(\gamma z).$$

However, we will need slightly more general actions on functions, but before we introduce a piece of notation that will later prove useful.

Definition 1.2. The j-function is the function

$$j\colon \mathrm{GL}_2^+(\mathbb{R}) \times \mathbb{H} \longrightarrow \mathbb{C}$$

given by:

$$j(\gamma, z) = cz + d, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

The following lemma gives a very interesting property of the automorphy factor.

Lemma 1.3. *For every γ_1, γ_2 in $\mathrm{GL}_2^+(\mathbb{R})$ and for every $z \in \mathbb{H}$ we have:*

$$j(\gamma_1\gamma_2, z) = j(\gamma_1, \gamma_2 z) j(\gamma_2, z).$$

Finally, we define an action of $\mathrm{GL}_2^+(\mathbb{R})$ on functions $f\colon \mathbb{H} \longrightarrow \mathbb{C}$, for each $k \in \mathbb{Z}$.

Definition 1.3. The slash operator is defined as

$$(f|_k\gamma)(z) = (\det\gamma)^{k-1} j(\gamma, z)^{-k} f(\gamma z).$$

The cocycle property and the multiplicativity of the determinant implies that if f is a function, then:

$$f|_k(\gamma_1\gamma_2) = (f|_k\gamma_1)|_k\gamma_2, \quad \forall \gamma_1, \gamma_2 \in \mathrm{GL}_2^+(\mathbb{R}).$$

That is, for each k the weight-k slash operator defines an action of $\mathrm{GL}_2^+(\mathbb{R})$ on functions on the upper-half plane.

1.2.1 Group-theoretic description of $\mathbb{H}$

Recall that $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{H}$. If $\tau = x + iy \in \mathbb{H}$, then define

$$s_\tau = \begin{pmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2} \end{pmatrix}.$$

Note that $s_\tau i = \tau$, and therefore $\mathrm{SL}_2(\mathbb{R})$ acts transitively on $\mathbb{H}$.

Lemma 1.4. *The stabilizer in $\mathrm{SL}_2(\mathbb{R})$ of i is the compact subgroup of $\mathrm{SL}_2(\mathbb{R})$:*

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \mid \theta \in [0, 2\pi] \right\}$$

Proof. Let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ stabilize i. That means that:

$$\frac{ai+b}{ci+d} = i,$$

or equivalently that

$$ai + b = -c + di.$$

Since the entries of g are real, this means that $a = d$ and $b = -c$. Therefore $g = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$. Since moreover $\det(g) = a^2 + b^2 = 1$, we deduce that $g \in \mathrm{SO}_2(\mathbb{R})$. □

The lemma gives a bijection:

$$\mathbb{H} \longrightarrow \mathrm{SL}_2(\mathbb{R})/\,\mathrm{SO}_2(\mathbb{R}), \quad \tau \mapsto s_\tau\,\mathrm{SO}_2(\mathbb{R}),$$

whose inverse maps $g\,\mathrm{SO}_2(\mathbb{R}) \mapsto g \cdot i$.

1.2.2 The quotient $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ as a topological space

We end this section by showing that the quotient $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is a Hausdorff space.

Lemma 1.5. *Let U_1 and U_2 be two open sets in $\mathbb{H}$. Then the set*

$$S = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma U_1 \cap U_2 \neq \emptyset\}$$

is finite.

Proof. First observe that the matrices $s_{\gamma\tau}$ and γs_τ both send i to $\gamma\tau$. By the identification $\mathbb{H} = \mathrm{SL}_2(\mathbb{R})/\,\mathrm{SO}_2(\mathbb{R})$ we deduce that $\gamma s_\tau\,\mathrm{SO}_2(\mathbb{R}) = s_{\gamma\tau}\,\mathrm{SO}_2(\mathbb{R})$. Given two points τ_1 and τ_2 of $\mathbb{H}$, we have $\gamma\tau_1 = \tau_2$ if and only if $s_{\gamma\tau_1}\,\mathrm{SO}_2(\mathbb{R}) = s_{\tau_2}\,\mathrm{SO}_2(\mathbb{R})$. We have just seen that the left hand side equals $\gamma s_{\tau_1}\,\mathrm{SO}_2(\mathbb{R})$. We deduce that $\gamma\tau_1 = \tau_2$ if and only if γ belongs to the conjugate: $s_{\tau_2}\,\mathrm{SO}_2(\mathbb{R})s_{\tau_1}^{-1}$. Therefore the set S is a subset of the set

$$\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma\overline{U}_1 \cap \overline{U}_2 \neq \emptyset\}$$

which in turn can be written as

$$\mathrm{SL}_2(\mathbb{Z}) \cap s_{\overline{U}_2}\,\mathrm{SO}_2(\mathbb{R})s_{\overline{U}_1}^{-1}.$$

Since $\mathrm{SL}_2(\mathbb{Z})$ is discrete and the other term is compact, the intersection, and hence S, is finite. □

Proposition 1.1. *The action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ is proper discontinuous. That is, given any τ_1, τ_2 in $\mathbb{H}$, there are neighborhoods U_1 and U_2 such that for each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ either*

1. $\gamma\tau_1 = \tau_2$, *or*
2. $\gamma U_1 \cap U_2 = \emptyset$.

Proof. Let U_1 and U_2 be any two neighborhoods of τ_1 and τ_2, and let $\gamma \in S$. If $\gamma\tau_1 = \tau_2$ then we do not need to do anything. Otherwise, if $\gamma U_1 \cap U_2 \neq \emptyset$ then we may replace U_2 with V_2 and U_1 with $\gamma^{-1}V_1$ if $V_1 \cap V_2 = \emptyset$, $\tau_2 \in V_2$ and $\gamma\tau_1 \in V_1$:

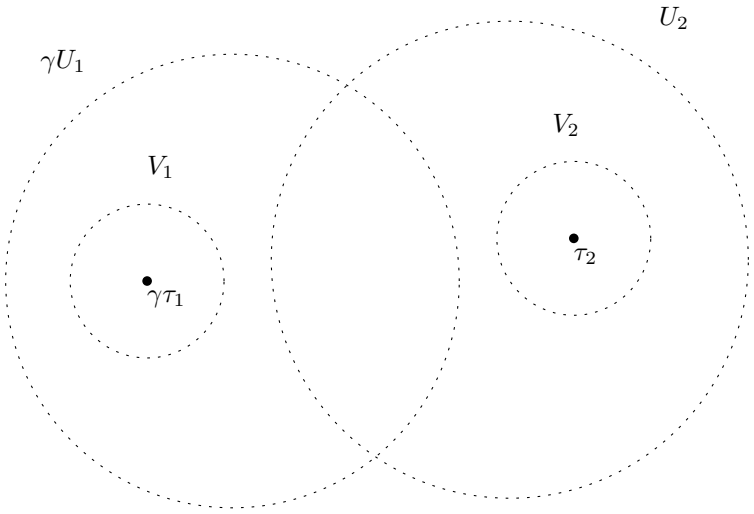

Figure 1.1: Shrinking the neighborhoods

Since the set of γ such that these intersections are nonempty is finite, this process terminates after a finite number of steps and will leave us with the right neighborhoods. □

Corollary 1.2. *The quotient* $Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ *is Hausdorff.*

Proof. Pick $\pi(\tau_1) \neq \pi(\tau_2)$ in $Y(1)$, and let U_1 and U_2 be neighborhoods as in the Proposition. For every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we have $\gamma\tau_1 \neq \tau_2$ by the choice of τ_1 and τ_2. Therefore for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we have $\gamma U_1 \cap U_2 = \emptyset$. Therefore $\pi(U_1) \cap \pi(U_2) = \emptyset$. It remains to show that $\pi(U_i)$ is an open set. Indeed, if $U \subseteq \mathbb{H}$ is an open set, then

$$\pi^{-1}(\pi(U)) = \cup_{\gamma\in\mathrm{SL}_2(\mathbb{Z})}\gamma U$$

is a union of open sets. Therefore it is open. We have showed that $\pi(U)$ is open (because of the quotient topology). Therefore each of the $\pi(U_i)$ is open, as we wanted to show. □

1.3 Basic definitions of modular forms

Let $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{SL}_2(\mathbb{R})$ be the subgroup of matrices with entries in $\mathbb{Z}$ (and determinant 1), which of course still acts on functions as we have seen.

Definition 1.4. A holomorphic function $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ is called *weakly modular* of weight $k \in \mathbb{Z}$ for $\mathrm{SL}_2(\mathbb{Z})$ if $f|_k\gamma = f$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Explicitly:

$$f(\gamma \cdot z) = j(\gamma, z)^k f(z), \quad \forall \gamma \in \mathrm{SL}_2(\mathbb{Z}). \tag{1.2}$$

Note that since $-I \in \mathrm{SL}_2(\mathbb{Z})$, then there are no non-zero weakly-modular functions of odd weight:

$$f(z) = (-1)^k f(z) \implies f = 0.$$

We will need an extra analytic property to define modular forms for $\mathrm{SL}_2(\mathbb{Z})$. For now, note that:

$$\frac{d(\gamma \cdot z)}{dz} = j(\gamma, z)^{-2},$$

so we can rewrite the weakly-modular property by asking that the differential $f(z)(dz)^{k/2}$ is invariant under $\mathrm{SL}_2(\mathbb{Z})$. It also shows that if Equation 1.2 holds for γ_1 and γ_2, then it also holds for $\gamma_1\gamma_2$.

We will see later (see Corollary 1.3) that $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Together with the previous observation, this implies that for f to be weakly-modular it is enough to check Equation 1.2 for T and S:

$$f(z+1) = f(z), \quad f(-1/z) = z^k f(z).$$

The transformation property (rather, the fact that $f(z+1) = f(z)$) implies that f has a Fourier expansion. Another way to think about it is that there is a holomorphic map:

$$\exp\colon \mathbb{H} \longrightarrow \{0 < |q| < 1\}, \quad z \mapsto q = e^{2\pi i z}.$$

If f is holomorphic and 1-periodic, then we can define $g(q) = f(z)$. That is, we may define:

$$g(q) = f\left(\frac{\log q}{2\pi i}\right),$$

where we may choose any branch of the logarithm because of the periodicity of f. The function g is holomorphic on D', and thus it has a Laurent expansion

$$g(q) = \sum_{n=-\infty}^{\infty} a(n) q^n.$$

Therefore f has an expansion

$$f(z) = \sum_{n=-\infty}^{\infty} a(n) e^{2\pi i n z}.$$

Definition 1.5. We say that f is *meromorphic at infinity* (respectively *holomorphic at infinity*) if $f(z) = \sum_{n \geq n_0} a(n) q^n$ (respectively if in addition $n_0 = 0$).

Note that checking that f is holomorphic at infinity is the same as checking that $f(z)$ is bounded as z approaches $i\infty$. If f is holomorphic at infinity, then the value of f at infinity is defined to be $f(\infty) = a(0)$.

Definition 1.6. We say that f is *cuspidal* if $n_0 = 1$. Equivalently, if $f(\infty) = 0$.

Definition 1.7. Let $k \in \mathbb{Z}$ and let $f\colon \mathbb{H} \longrightarrow \mathbb{C}$. We say that f is a *modular form* of weight k for $\mathrm{SL}_2(\mathbb{Z})$ if:

1. f is holomorphic,
2. $f(\gamma z) = (cz + d)^k f(z)$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, and
3. f is holomorphic at infinity.

A *cusp form* is a modular form which vanishes at infinity.

The space of modular forms of weight k is written $M_k = M_k(\mathrm{SL}_2(\mathbb{Z}))$, and it contains the space of cusp forms of weight k, which in turn is written $S_k = S_k(\mathrm{SL}_2(\mathbb{Z}))$.

Remark 1.1. If we replace "holomorphic" with "meromorphic" above, we obtain what can be called an *automorphic form*. Other authors call them modular functions, but this name is used in different contexts and we will avoid it.

Note that both M_k and S_k are $\mathbb{C}$-vector spaces. Also, multiplication of functions gives $M = \bigoplus_{k \in \mathbb{Z}} M_k$ the structure of a *graded ring*. That is, $M_r M_s \subseteq M_{r+s}$. Finally, for all odd k one has $M_k = \{0\}$.

1.4 Eisenstein series

For $k \geq 3$, define

$$G_k(z) = \sum_{(m,n) \in \mathbb{Z}^2}{}' (mz + n)^{-k}.$$

Proposition 1.2. *For all $k \geq 3$, the function $G_k(z)$ is a weight-k modular form, with $G_k(\infty) = 2\zeta(k)$, where ζ is Riemann's zeta function.*

In order to prove the above result, we will need to auxiliary lemmas.

Lemma 1.6. *If $k \geq 2$, the series*

$$\sum_{(c,d)\neq(0,0)} \max(c,d)^{-k}$$

converges absolutely.

Proof. Consider the partial sum of the series in the box $\{|c| \leq N, |d| \leq N\}$. We can explicitly compute this sum, which equals

$$\sum_{n=1}^{N} (2n+1)n^{-k}.$$

Evaluating this sum we obtain the exact value $\zeta(k) + 2\zeta(k-1)$. □

Lemma 1.7. *Given positive real numbers $A > 0$ i $B > 0$, consider the compact set*

$$\Omega = \{z \in \mathbb{H} : |\Re(z)| \leq A, \Im(z) \geq B\}.$$

There exists a constant $C = C_{A,B}$ such that

$$|z+\delta| > L \max(1, |\delta|), \quad \forall \delta \in \mathbb{R}.$$

Proof. If $|\delta| < 1$, then $|z+\delta| \geq B = B\max(1,|\delta|)$. If $1 \leq |\delta| \leq 10A$, then if $\Im(z) > A$ we have

$$|z+\delta| > A \geq \frac{|\delta|}{10},$$

and if $B \leq \Im z \leq A$ then the function

$$\left|\frac{z+\delta}{\delta}\right|$$

has an absolute minimum m in the compact set $1 \leq |\delta| \leq 10A$ i $B \leq \Im z \leq A$.

Finally, if $|\delta| > 10A$, then

$$|z+\delta| \geq |\delta| - |z| > |\delta| - A > \frac{9}{10}|\delta|.$$

□

of the proposition. First, we need to show the convergence of the series for all z. In order to simplify notation, we will restrict the sum to the pairs in the first quadrant. Restricting further the double sum to pairs in the box $\{0 \leq c, d \leq N\}$, we have on one hand

$$\sum_{d=1}^{N} d^{-k} + \sum_{c=1}^{N}\sum_{d=1}^{N} (cz+d)^{-k}.$$

The first summand is bounded by $\zeta(k)$ and so we will ignore it. By restricting z to the compact $\Omega_{A,B}$ as above, the second summand can be rewritten as

$$\begin{aligned}\sum_{c=1}^{N}\sum_{d=1}^{N} c^{-k}|z+d/c|^{-k} &\leq \sum_{c=1}^{N}\sum_{d=1}^{N} c^{-k}L^k \max(1, d^{-k}/c^{-k}) \\ &= L^k \sum_{c=1}^{N}\sum_{d=1}^{N} \max(c,d)^{-k}.\end{aligned}$$

By the first lemma, this series converges absolutely. We have already seen that it also converges absolutely in compact sets that cover all of $\mathbb{H}$, and thus we deduce that it converges to a holomorphic function on $\mathbb{H}$.

In order to compute $G_k(\infty)$, we take the limit as $\Im(z) \longrightarrow \infty$, which can be done while keeping $z \in D$. In this case, thanks to the uniforme convergent of the series, we can take the term-wise limit. All terms with $c \neq 0$ tend to zero, so we get

$$\lim G_k(z) = \sum_{n\neq 0} n^{-k} = 2\zeta(k).$$

□

Proposition 1.3. *For each $k \geq 3$ the holomorphic function G_k is weakly modular.*

Proof. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be a matrix in $\mathrm{SL}_2(\mathbb{Z})$. We compute

$$\begin{aligned}G_k(\gamma z) &= {\sum_{(m,n)}}' \left(m\frac{az+b}{cz+d} + n\right)^{-k} \\ &= {\sum_{(m,n)}}' (cz+d)^k \left(m(az+b)+n(cz+d)\right)^{-k} \\ &= (cz+d)^k {\sum_{(m,n)}}' \left((am+cn)z + (bm+dn)\right)^{-k}.\end{aligned}$$

Note that the pair $(am+cn, bm+dn)$ is the result of multiplying the row vector (m,n) by the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Since $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is invertible, the pair $(am+cn, bm+dn)$ runs through all values of $\mathbb{Z}^2$ as (m,n) does. Therefore, by reordering the sum (which we can do thanks to absolute convergence) we get:

$$G_k(\gamma z) = (cz+d)^k {\sum_{(m',n')}}' \left(m'z+n'\right)^{-k} = (cz+d)^k G_k(z),$$

as wanted. □

We have already seen that G_k is holomorphic at infinity, and in fact we know its value there. The next task will be to compute its Fourier series. We start by introducing the Bernoulli numbers, which appear in the Fourier series for G_k.

Definition 1.8. The *Bernoulli numbers* are defined [1] by:

$$\frac{x}{e^x-1}=\sum_{k=0}^{\infty}B_k\frac{x^k}{k!}=1-\frac{1}{2}x+\frac{1}{6}\frac{x^2}{2}-\frac{1}{30}\frac{x^4}{24}+\cdots. \tag{1.3}$$

Recall the definition of Riemann's zeta function

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\quad \Re(s)>1.$$

It has a simple pole of residue 1 at $s=1$, and extends to a meromorphic function on $\mathbb{C}$, holomorphic on $\mathbb{C}\setminus\{1\}$. The Bernoulli numbers appear also naturally in the formulas:

$$\zeta(k)=\sum_{n=1}^{\infty}\frac{1}{n^k}=-\frac{(2\pi i)^k}{2}\frac{B_k}{k!},\quad \forall k\geq 2,\quad \zeta(1-n)=-\frac{B_n}{n},\quad \forall n\geq 1. \tag{1.4}$$

An odd prime p is called if p does not divide the numerator of B_2, B_4,...B_{p-3}. This is equivalent to p not dividing the class number of $\mathbb{Q}(\sqrt[p]{1})$. Under this assumption, Fermat's Last Theorem was proved by Kummer around 1850, and probably by Fermat himself. Although Siegel conjectured that about 60% of primes are regular, it is not know even whether there are infinitely many of them.

We will derive the Fourier expansion of G_k from that of the cotangent:

Lemma 1.8. *The following identity of holomorphic functions holds.*

$$\frac{1}{z}+\sum_{d=1}^{\infty}\left(\frac{1}{z-d}+\frac{1}{z+d}\right)=\pi\cot(\pi z)=\pi i-2\pi i\sum_{m=0}^{\infty}q^m,\quad q=e^{2\pi iz}.$$

Proof. Consider Euler's product formula for the sine function:

$$\sin(\pi z)=\pi z\prod_{n=1}^{\infty}\left(1-\frac{z^2}{n^2}\right).$$

Taking the logarithmic derivative of this equation yields

$$\pi\cot(\pi z)=\frac{1}{z}+\sum_{d=1}^{\infty}\frac{2z}{z^2-n^2}=\frac{1}{z}+\sum_{d=1}^{\infty}\left(\frac{1}{z-d}+\frac{1}{z+d}\right).$$

On the other hand, we can use the expression of sin and cos in terms of the exponential function to write:

$$\begin{aligned}\pi\cot(\pi z)=\pi\frac{\cos(\pi z)}{\sin(\pi z)}&=\pi\frac{\frac{e^{i\pi z}+e^{-i\pi z}}{2}}{\frac{e^{i\pi z}-e^{-i\pi z}}{2i}}=\pi i\frac{e^{i\pi z}+e^{-i\pi z}}{e^{i\pi z}-e^{-i\pi z}}\\&=\pi i\left(1-2\frac{e^{-i\pi z}}{e^{-i\pi z}-e^{i\pi z}}\right)=\pi i\left(1-2\frac{1}{1-e^{2\pi iz}}\right).\end{aligned}$$

[1] These are called "first Bernoulli numbers", and differ by a sign from those defined originally by Bernoulli.

Finally, write $q = e^{2\pi i z}$ and the formula follows from the identity

$$\frac{1}{1-q} = \sum_{m=0}^{\infty} q^m, \quad |q| < 1.$$

□

Lemma 1.9. *For each $k \geq 2$ we have*

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

Proof. From Lemma 1.8 we have

$$\frac{1}{z} + \sum_{d=1}^{\infty} \left(\frac{1}{z-d} + \frac{1}{z+d} \right) = \pi i - 2\pi i \sum_{d=0}^{\infty} q^d, \quad q = e^{2\pi i z}.$$

Differentiating both sides with respect to z gives

$$\frac{-1}{z^2} + \sum_{d=1}^{\infty} \left(\frac{-1}{(z-d)^2} + \frac{-1}{(z+d)^2} \right) = -(2\pi i)^2 \sum_{d=1}^{\infty} d q^d.$$

Since each of the terms in the infinite sum of the left hand side converges absolutely, we can reorder the series and obtain the identity

$$\sum_{d\in\mathbb{Z}} \frac{1}{(z+d)^2} = (2\pi i)^2 \sum_{d=1}^{\infty} d q^d.$$

This is proves the formula for $k = 2$. The identity for general k follows by induction, by differentiating the identity for $k-1$. □

We have finally all the ingredients to prove the sought expansion. As a piece of notation for the next result, for $m \geq 0$ the is:

$$\sigma_m(n) = \sum_{d|n} d^m.$$

Theorem 1.5. *Let $k \geq 4$ be even. Then*

$$G_k(z) = 2\zeta(k) E_k(z), \text{ where } E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \in \mathbb{Q}[\![q]\!].$$

Proof. Consider now $k \geq 4$ and calculate

$$G_k(z) = \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(mz+n)^k} = \sum_{n\neq 0} \frac{1}{n^k} + \sum_{m\neq 0}\sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^k}$$
$$= 2\zeta(k) + 2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^k}.$$

Here we have used the definition of Riemann's zeta function at k and the fact that k is even. Using now the formula of Lemma 1.9 where z gets substituted by mz, we can replace the second term, and obtain the formula

$$G_k(z) = 2\zeta(k) + 2\sum_{m=1}^{\infty}\left(\frac{(-2\pi i)^k}{(k-1)!}\sum_{d=1}^{\infty} d^{k-1}q^{dm}\right) = 2\zeta(k) + \frac{2\cdot(-2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\sum_{d=1}^{\infty} d^{k-1}q^{md}.$$

Finally, group the terms in the inner sum that contribute to q^n. These consist of all pairs of positive integers (m,d) such that $md = n$. That is, for each n we must consider all divisors d' of n, and we can rewrite:

$$\sum_{m=1}^{\infty}\sum_{d=1}^{\infty} d^{k-1}q^{md} = \sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n.$$

This gives the desired expansion, by using Equation 1.4. □

Example 1.1. Define the

$$E_4 = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \in M_4$$

and

$$E_6 = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n \in M_6.$$

Since both E_4^3 and E_6^2 are both in M_{12}, its difference is also there. Computing we see that

$$E_4^3 - E_6^2 = (1 + 720q + \cdots) - (1 - 1008q + \cdots) = 1728q + \cdots \in S_{12},$$

and thus we may define

$$\Delta(z) = \frac{E_4^3 - E_6^2}{1728} = q - 24q^2 + 252q^3 + \cdots,$$

which is a cusp form of weight 12.

1.5 Fundamental domains

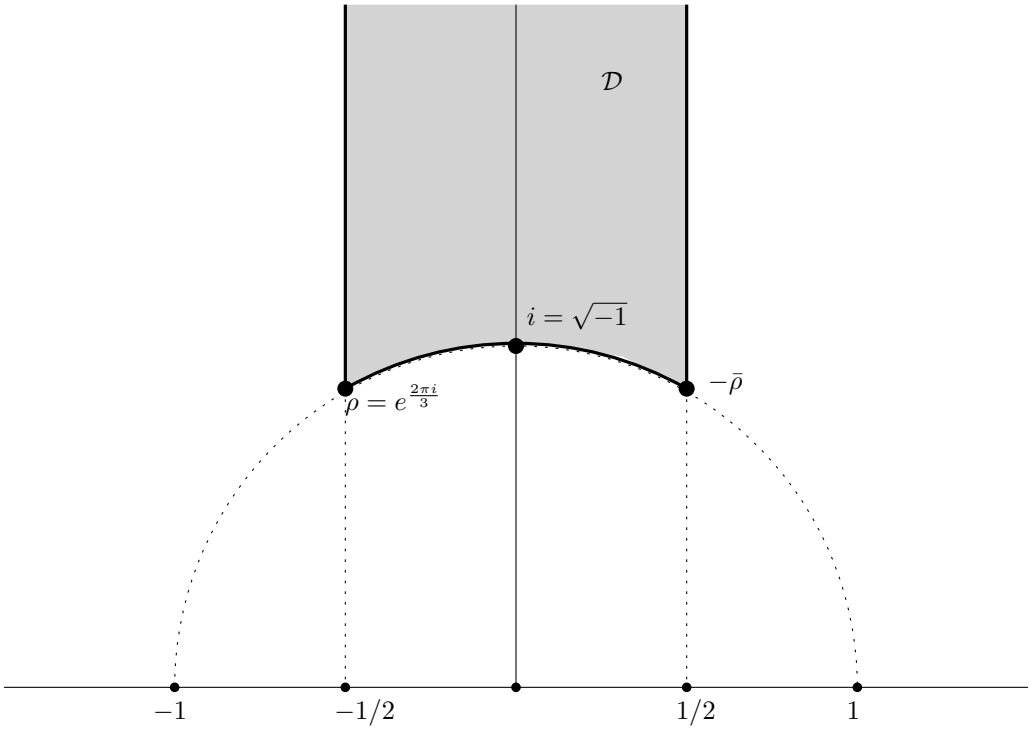

Figure 1.2: Fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

Definition 1.9. Let Γ be a group acting on $\mathbb{H}$. A for Γ is closed subset $\mathcal{D} \subset \mathbb{H}$ such that

1. The set $\mathcal{D}$ is the closure of its interior.
2. Every point in $\mathbb{H}$ is Γ-equivalent to a point of $\mathcal{D}$.
3. If $z, z' \in \mathcal{D}$ are two distinct points which are Γ-equivalent then they lie on the boundary of $\mathcal{D}$.

Theorem 1.6. *The subset $\mathcal{D}$ of $\mathbb{H}$ as above is a (connected) fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$. Moreover the stabilizer H_z of a point $z \in \mathcal{D}$ in $\mathrm{SL}_2(\mathbb{Z})$ is*

$$H_z = \begin{cases} C_6 = \langle ST \rangle = \langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \rangle & z = \rho, \\ C_6' = \langle TS \rangle = \langle \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) \rangle & z = \rho + 1, \\ C_4 = \langle S \rangle = \langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \rangle & z = i, \\ C_2 = \langle -I \rangle = \langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \rangle & \textit{else.} \end{cases}$$

Proof. Let $z \in \mathbb{H}$. We have seen that, if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then

$$\mathfrak{I}(\gamma z) = \frac{\mathfrak{I}(z)}{|cz+d|^2}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

There are finitely many pairs $(c,d) \in \mathbb{Z}^2$ such that $|cz+d| < 1$. In particular, one can choose a matrix $\gamma \in \langle S, T\rangle \subseteq \mathrm{SL}_2(\mathbb{Z})$ such that

$$\mathfrak{I}(\gamma z) \geq \mathfrak{I}(\gamma' z), \quad \forall \gamma' \in \langle S, T\rangle \subseteq \mathrm{SL}_2(\mathbb{Z}).$$

By premultiplying γ by an appropriate power of T (which does not change the imaginary part), we may and do assume that $|\mathfrak{R}(\gamma z)| \leq \frac{1}{2}$. We will now show that $|\gamma z| \geq 1$:

$$\mathfrak{I}(\gamma z) \geq \mathfrak{I}(S\gamma z) = \mathfrak{I}(-1/\gamma z) = \frac{\mathfrak{I}(\gamma z)}{|\gamma z|^2}.$$

This implies $|\gamma z| \geq 1$, and hence $\gamma z \in \mathcal{D}$, thus proving (1).

In order to show (2), suppose that $z' = \gamma z$ and both z and z' lie in $\mathcal{D}$. Without loss of generality, we may assume that $\mathfrak{I}(\gamma z) \geq \mathfrak{I}(z)$, or equivalently that

$$|cz+d|^2 = |cx+d|^2 + |cy|^2 \leq 1. \quad \text{(we write } z = x+iy\text{)}.$$

Since $y > 1/2$, this implies that $|c| \leq 1$. The case $c = 0$ gives that $|d| \leq 1$ and since $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ this means that $\gamma = \pm \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$, a translation matrix. Therefore $z' = z \pm 1$.

Let us suppose that $c = 1$ (the case $c = -1$ is completely analogous). Then the condition $|z+d|^2 \leq 1$ is only satisfied when $|z| = 1$ ($d = 0$), when $z = \rho$ ($d = 1$), or when $z = \rho + 1$ ($d = -1$), giving (2).

To study the stabilizers of points $z \in \mathcal{D}$, we can use the calculations that we have used to show (2). If $\gamma z = z$, then necessarily $c = \pm 1$, and by changing γ to $-\gamma$ we may assume $c = 1$. The quadratic equation given by $\gamma z = z$ gives that $|a+d| < 2$, so $|a+d| \leq 1$. At the same time, the fact that $z \in \mathcal{D}$ gives $|a-d| \leq 1$. Together, these two inequalities give $|a| \leq 1$. We obtain the following possibilities:

γ	z	$z' = \gamma z$	fixed points
$\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	all	z	all
$\pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$	$\mathfrak{R}(z) = -\frac{1}{2}$	$z+1$	none
$\pm \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$	$\mathfrak{R}(z) = \frac{1}{2}$	$z-1$	none
$\pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$	$\lvert z\rvert = 1$	$-1/z$	i
$\pm \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right), \pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$	ρ	ρ	ρ
$\pm \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right), \pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$	$\rho + 1$	$\rho + 1$	$\rho + 1$

By studying this table we conclude the classification of stabilizers. □

Corollary 1.3. *The group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the matrices* T *and* S.

Proof. Let z_0 be a point in the interior of $\mathcal{D}$. Given $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the theorem provides a matrix $\delta \in \langle T, S\rangle$ such that $\delta\gamma^{-1}z_0 \in \mathcal{D}$. Therefore $\delta\gamma^{-1}z_0 = z_0$ and hence $\delta\gamma^{-1} = \pm I$. Since $S^2 = -I$, we are done by possibly multiplying δ by S^2. □

1.6 Valence formula

Let f be a meromorphic function on some open subset of $\mathbb{H}$. Write $v_p(f)$ for the order (or valuation) of f at $p \in \mathbb{H} \cup \{\infty\}$. This is the unique integer n such that $(z-p)^{-n}f(z)$ is holomorphic and non-vanishing at p. If n is positive we say that f has a zero of order n, and if n is negative we say that f has a pole of order $-n$. If f is weakly modular and meromorphic at infinity, then also define $v_\infty(f) = n_0$ if

$$f(q) = \sum_{n \geq n_0} a_n q^n, \quad a_{n_0} \neq 0.$$

Next, suppose that f has a Laurent expansion of the form

$$f(z) = \sum_{n \geq n_0} c_n (z-p)^n.$$

The of f at p is $\mathrm{res}_p(f) = c_{-1} \in \mathbb{C}$. One can calculate the order of f at p by using residues, using the following lemma.

Lemma 1.10. *If* f *is a meromorphic function around a point* p*, then*

$$\mathrm{res}_p(f'/f) = v_p(f).$$

Proof. If $v_p(f) = n$, write $f(z) = (z-p)^n g(z)$ with $g(z)$ holomorphic and non-vanishing at p. Then calculate the residue of f'/f by hand. □

We recall without proof two basic results of complex analysis.

Theorem 1.7. *Let* g *be a holomorphic function on an open subset* $U \subseteq \mathbb{C}$ *and let* C *be a contour in* U*. For each* $p \in U$*,*

$$\int_C \frac{g(z)}{z-p} dz = 2\pi i g(p).$$

Corollary 1.4. *Let* $C(p, r, \alpha)$ *be an arc of a circle, of radius* r *and angle* α *around a point* p*. If* g *is holomorphic at* p*, then*

$$\lim_{r \longrightarrow 0} \int_{C(p,r,\alpha)} \frac{g(z)}{z-p} dz = \alpha i g(p).$$

The following result relates the contour integral of the logarithmic derivative of f to the orders of f at the interior points.

Theorem 1.8. *Let f be a meromorphic function on an open subset $U \subseteq \mathbb{C}$ and let C be a contour in U not passing through any zeros or poles of f. Then:*

$$\int_C \frac{f'(z)}{f(z)} dz = 2\pi i \sum_{z \in \mathrm{int}(C)} v_z(f).$$

Corollary 1.5. *Let $C(p, r, \alpha)$ be an arc of a circle, of radius r and angle α around a point p. If f is meromorphic at p, then*

$$\lim_{r \longrightarrow 0} \int_{C(p,r,\alpha)} \frac{f'(z)}{f(z)} dz = \alpha i v_p(f).$$

We will study weakly modular meromorphic functions $f \colon \mathbb{H} \longrightarrow \mathbb{C}$. In this case, the order of vanishing makes sense in $\mathrm{SL}_2(\mathbb{Z})$-orbits: suppose that f has weight k. Then an easy computation shows that, for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$,

$$\lim_{z \longrightarrow \gamma p} (z - \gamma p)^{-n} f(z) = j(\gamma, p)^{k+2n} \lim_{z \longrightarrow p} (z - p)^{-n} f(z).$$

But note now that $j(\gamma, p)$ is nonzero because $p \notin \mathbb{Q} \cup \{\infty\}$. We conclude that $v_p(f) = v_{\gamma p}(f)$.

Theorem 1.9. *Let f be a non-zero weakly modular meromorphic form of weight k on $\mathrm{SL}_2(\mathbb{Z})$. Then:*

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\tau \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}'} v_\tau(f) = \frac{k}{12}.$$

Here the sum runs through the orbits in $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ other than those of i and ρ.

Before proving this theorem we will see how helpful it is in studying the spaces of modular forms.

Theorem 1.10.

1. *$M_k = \{0\}$ if $k < 0$ or $k = 2$.*
2. *$S_k = \{0\}$ if $k < 12$.*
3. *$M_0 = \mathbb{C}$.*
4. *$S_{12} = \mathbb{C}\Delta$.*

Proof. Proof.

1. Since the left-hand side of the valence formula is non-negative, the right hand side must be non-negative too, hence $k \geq 0$. If $k = 2$, then we get $1/6$ on the right-hand side. However, the left-hand side is a sum of non-negative multiples of 1, $1/2$ and $1/3$, thus a contradiction.

2. If $0 \neq f \in S_k$, then $v_\infty(f) \geq 1$. Therefore the valence formula gives $k \geq 12$.

3. Let $f \in M_0$. Since the constant function $g = f(\infty)$ also belongs to M_0, the difference $f - g$ belongs to $S_0 = \{0\}$. Therefore $f = g$ is constant, and $M_0 = \mathbb{C}$ is the space of constant functions on $\mathbb{H}$.

4. If $f \in S_{12}$, then $v_\infty(f) \geq 1$. Therefore by the valence formula $v_\infty(f) = 1$ and f has no other zeros or poles. Define

$$g(z) = f(z) - \frac{f(i)}{\Delta(i)}\Delta(z).$$

   Then $g(z) \in S_{12}$ and $g(i) = 0$. If g is non-zero, then the valence formula applied to g would give a contradiction because $v_\infty(g) \geq 1$ and $v_i(g) \geq 1$. Therefore $g = 0$ and f is a multiple of Δ.

□

Corollary 1.6.

1. *For all k, we have $S_{k+12} = \Delta M_k$.*

2. *For $k \geq 4$ we have*

$$M_k = (\mathbb{C}E_k) \oplus S_k$$

3. *If k is odd or negative then $M_k = \{0\}$. For each even $k \geq 2$, we have:*

$$\dim(M_k) = \begin{cases} \lfloor \frac{k}{12} \rfloor & k \equiv 2 \pmod{12}, \\ 1 + \lfloor \frac{k}{12} \rfloor & k \not\equiv 2 \pmod{12}. \end{cases}$$

Proof. For $k < 0$ the first statement is trivial, and we just proved it also for $k = 0$. Given $f \in S_{k+12}$, the function $g = f/\Delta$ is holomorphic on $\mathbb{H}$ because Δ is non-vanishing, and it belongs to M_k because $v_\infty(g) = v_\infty(f) - v_\infty(\Delta) = v_\infty(f) - 1 \geq 0$.

Consider the linear map

$$\varphi \colon M_k \longrightarrow \mathbb{C}, \quad f \mapsto f(\infty).$$

Then $S_k = \ker \varphi$. Also φ is surjective because $\varphi(E_k) = 1$. Therefore $M_k = \mathbb{C}E_k \oplus S_k$.

Note that this gives a recursive way to obtain M_k:

$$M_k = \mathbb{C}E_k \oplus S_k = \mathbb{C}E_k \oplus (\Delta M_{k-12}).$$

For k odd we know that $M_k = \{0\}$ by the weak-modularity condition. For $k < 0$ we also know $M_k = \{0\}$ by the previous part. We prove the remaining formula by induction on k. Note that we already know it for $k = 0$ and $k = 2$. For $k = 4, 6, 8, 10$ then since $\dim(M_k) = 1 + \dim(S_k) = 1 + \dim(M_{k-12}) = 1$ we get $\dim(M_k) = 1$. If k is even and $k \geq 12$, then:

$$\dim(M_k) = 1 + \dim(M_{k-12}).$$

□

Corollary 1.7. *The space M_k has for basis the following set:*

$$M_k = \langle E_4^a E_6^b \mid a \geq 0, b \geq 0, 4a + 6b = k \rangle.$$

Proof. We start by showing that the given monomials $E_4^a E_6^b$ generate M_k. For $k = 2, 4, 6$ this is clear because we know $M_2 = \{0\}$, and $M_4 = \mathbb{C}E_4$ and $M_6 = \mathbb{C}E_6$. For $k \geq 8$ we induct on k. Choose some pair (a, b) such that $4a + 6b = k$ (convince yourself that this is always possible). If $f \in M_k$, then since $E_4^a E_6^b(\infty) = 1$, the function $g(z) = f(z) - f(\infty)E_4^a E_6^b$ is a cusp form in S_k. Therefore $g = \Delta h$, for some $h \in M_{k-12}$. By induction hypothesis, h is a linear combination of monomials $E_4^x E_6^y$ for appropriate pairs (x, y). Using the expression $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$ we deduce the result for f.

Now we show that the given monomials are linearly independent. We can use induction on k in steps of 12 once more, to show that the number of such monomials agrees with $\dim M_k$. This can be checked by hand for $k \leq 14$. Suppose that $k \geq 14$. Note that each monomial $E_4^a E_6^b$ of weight $k - 12$ gives a monomial $E_4^a E_6^{b+2}$ of weight k. All such monomials are obtained in this way, except for those of the form E_4^a or $E_4^a E_6$. When $k \equiv 0 \pmod 4$ then $E_4^{k/4}$ is of weight k, and when $k \equiv 2 \pmod 4$ then $E_4^{(k-6)/2} E_6$ is of weight k, thus in any case there is exactly one more monomial of weight k than there are of weight $k - 12$. This completes the proof. □

Example 1.2. This allows to write down all spaces of modular and cusp forms for $\mathrm{SL}_2(\mathbb{Z})$. For example,

$$M_{18} = \mathbb{C}E_{18} \oplus S_{18} = \mathbb{C}E_{18} \oplus \Delta M_6 = \mathbb{C}E_{18} \oplus \mathbb{C}\Delta E_6.$$
$$M_{30} = \mathbb{C}E_{30} \oplus \mathbb{C}\Delta E_{18} \oplus \mathbb{C}\Delta^2 E_6.$$

Another basis for the same space (which is better because it is expressed in terms of E_4, E_6 and Δ):

$$M_{30} = \mathbb{C}E_6^5 \oplus \Delta E_6^3 \oplus \Delta^2 E_6.$$

Note that these forms are linearly independent (why?). Since $\dim M_{30} = 3$, they form a basis.

Suppose that $f(z)$ is a non-zero weakly-modular form of weight 0. Then $f(\gamma z) = f(z)$. By the valence formula, f has the same number of zeros as poles. This number is called the *valence* of f, and hence the name for the theorem.

Another very powerful application of the valence formula is the following:

Theorem 1.11. *Let f be a modular form of weight k. Suppose that f has a q-expansion of the form $\sum_{n\geq 0} a_n q^n$. If $a_j = 0$ for all $0 \leq j \leq k/12$, then $f = 0$.*

Proof. The hypothesis means that $v_\infty(f) > k/12$. This is incompatible with the valence formula, and thus f must be zero. □

Corollary 1.8. *Let f and g be two modular forms of the same weight k, and suppose that their q-expansions coincide for the first $\lfloor k/12 \rfloor$ coefficients. Then $f = g$.*

1.6.1 The modular invariant j

Define the function

$$j(z) = \frac{E_4^3}{\Delta} = \frac{1 + \cdots}{q + \cdots} = q^{-1} + 744 + 196884q + \cdots.$$

Proposition 1.4.

1. *j is a meromorphic weakly-modular form of weight 0.*
2. *j is holomorphic on $\mathbb{H}$ and has a simple pole at infinity.*
3. *It induces a bijection $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \longrightarrow \mathbb{C}$.*

Proof. The fact that j it is meromorphic weakly-modular of weight 0 follows from it being a quotient of two modular forms of weight 12.

Since E_4 is non-vanishing at infinity and Δ has a simple zero then $j = E_4^3/\Delta$ has a simple pole at infinity (we can also see it from its q-expansion, which starts with q^{-1}). The valence formula shows that $v_\rho(E_4) = 1$, and therefore $j(z)$ has a triple zero at ρ. It is holomorphic on $\mathbb{H}$ because Δ is non-vanishing on $\mathbb{H}$.

Fix $c \in \mathbb{C}$. The function $j(z) - c = q^{-1} + 744 - c + \cdots$ is another meromorphic weakly-modular function of weight 0 and has a simple pole at ∞. The valence formula gives in this case that $j(z) - c$ has exactly one zero on $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. This gives the last claim. □

1.6.2 Proof of the valence formula

The proof presented here avoids algebraic geometry, at the cost of some complex analysis. Let f be a modular function, and consider the following contour:

The proof consists in integrating $f'(z)/f(z)$ around the indicated contour C in two different ways.

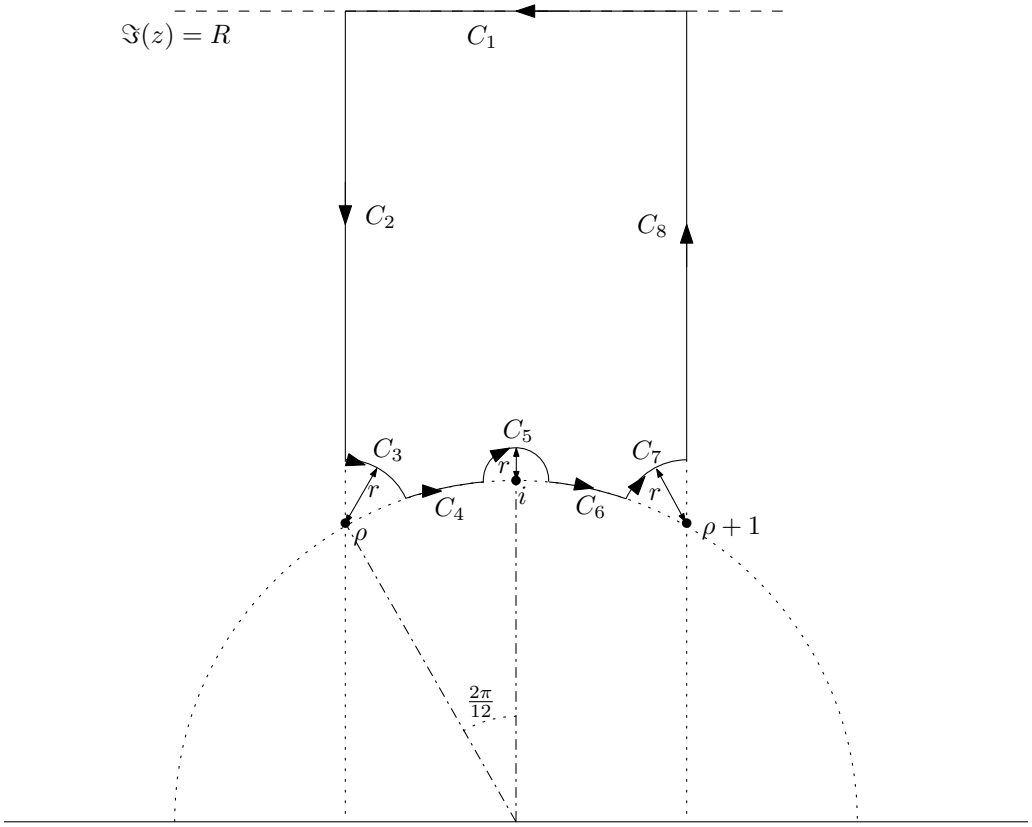

Figure 1.3: Contour to integrate

1.6.2.0.1 Integral residue formula:

This is the first way in which we calculate the contour integral. For R large enough so that the contour contains all zeros and poles of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}'$ with large imaginary part, we have:

$$\int_C \frac{f'(z)}{f(z)}dz = 2\pi i \sum_{p\in\mathrm{int}(C)} \mathrm{res}_p\left(\frac{f'}{f}\right) = 2\pi i \sum_{p\in\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}'} v_p(f).$$

The rest of the proof consists in computing the integral as the sum of the path integrals along C_1,..., C_8.

1.6.2.0.2 Integral along C_1:

Perform the change of variables $q(z) = e^{2\pi iz}$. Note that:

$$dq = 2\pi iq dz, \quad dz = \frac{1}{2\pi i}\frac{dq}{q}.$$

Moreover, the path $q(C_1)$ is a clockwise circle of radius $e^{-2\pi R}$ centered around 0. Finally,

$$\frac{d}{dz}f(q) = \frac{d}{dz}f(e^{2\pi iz}) = 2\pi iqf'(q).$$

Putting these together, we obtain:

$$\int_{C_1} \frac{f'(z)}{f(z)}dz = \int_{q(C_1)} \frac{f'(q)}{f(q)}dq.$$

Since f is meromorphic around infinity, this last quantity equals $-v_\infty(f)$.

1.6.2.0.3 Integral along C_2 and C_8:

Note that since f is modular it satisfies $f(z+1) = f(z)$. Therefore also $f'(z+1) = f'(z)$, and we get, by changing $w = z+1$:

$$\int_{C_8} \frac{f'(w)}{f(w)}dw = -\int_{C_2} \frac{f'(z+1)}{f(z+1)}dz = -\int_{C_2} \frac{f'(z)}{f(z)}dz.$$

Therefore the contributions of C_2 and C_8 cancel out.

1.6.2.0.4 Integral along C_4 and C_6:

In the same way that for C_2 and C_8 we considered the change $z \mapsto z+1$, here we consider the change $z \mapsto s(z) = -z^{-1}$. This change of variables transforms C_4 to $-C_6$. Weak-modularity of f implies also that $f(z) = z^{-k} f(s(z))$. Differentiating both sides yields:

$$f'(z) = -kz^{-k-1} f(s(z)) + z^{-k} f'(s(z)) s'(z).$$

This gives

$$\frac{f'(z)}{f(z)} = \frac{-k}{z} + \frac{f'(s(z))s'(z)}{f(s(z))}.$$

Therefore we may compute

$$\int_{C_4} \frac{f'(z)}{f(z)} dz = \int_{C_4} \frac{-k}{z} dz + \int_{C_4} \frac{f'(s(z))s'(z)}{f(s(z))} dz = 2\pi i \frac{k}{12} + \int_{-C_6} \frac{f'(s)}{f(s)} ds,$$

and hence

$$\int_{C_4+C_6} \frac{f'(z)}{f(z)} dz \longrightarrow_{r \longrightarrow 0} 2\pi i \frac{k}{12}.$$

1.6.2.0.5 Integral along C_5:

Using the argument principle we obtain

$$\int_{C_5} \frac{f'(z)}{f(z)} dz \overset{[}{r} \longrightarrow 0] \longrightarrow -\frac{1}{2} 2\pi i v_i(f).$$

1.6.2.0.6 Integrals along C_3 and C_7:

Applying again the argument principle we obtain

$$\int_{C_3} \frac{f'(z)}{f(z)} dz \overset{[}{r} \longrightarrow 0] \longrightarrow -\frac{1}{6} 2\pi i v_\rho(f), \text{ and } \quad \int_{C_5} \frac{f'(z)}{f(z)} dz \overset{[}{r} \longrightarrow 0] \longrightarrow -\frac{1}{6} 2\pi i v_{\rho+1}(f) = -\frac{1}{6} 2\pi i v_\rho(f).$$

Therefore

$$\int_{C_3+C_5} \frac{f'(z)}{f(z)} dz \overset{[}{r} \longrightarrow 0] \longrightarrow -\frac{1}{3} 2\pi i v_\rho(f).$$

1.6.2.0.7 Conclusion:

Putting together all the above calculations yields the sought formula.

1.7 A product formula for $\Delta(z)$

Consider the weight-2 Eisenstein series

$$G_2(z) = \sum_c \sum_d{}' \frac{1}{(cz+d)^2},$$

which does not converge absolutely. It is *not* a weight-2 modular form (there are no such other than 0), but we still have the formula:

$$G_2(z) = 2\zeta(2)E_2(z), \quad E_2(z) = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n.$$

The function $E_2(z)$ is holomorphic on $\mathbb{H}$, and $E_2(z+1) = E_2(z)$. However, we are about to see that

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

Sometimes these functions are called .

Theorem 1.12. *The function G_2 satisfies $G_2(z+1) = G_2(z)$ and it has the q-expansion*

$$G_2(z) = 2\zeta(2) - 8\pi^2\sum_{n=1}^{\infty}\sigma_1(n)q^n, \quad q = e^{2\pi i z}.$$

Moreover, G_2 satisfies the transformation property:

$$G_2(\gamma z) = (cz+d)^2 G_2(z) - 2\pi i c(cz+d), \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{1.5}$$

In particular, the non-holomorphic function $G_2^*(z) = G_2(z) - \pi/\Im(z)$ is weight-2-invariant for $\mathrm{SL}_2(\mathbb{Z})$.

Proof. To show that $G_2(z+1) = G_2(z)$, we must show that

$$\sum_{n\neq 0}\frac{1}{(m(z+1)+n)^2} = \sum_{n\neq 0}\frac{1}{(mz+n)^2}.$$

This follows from the fact that the sum converges absolutely and $n \mapsto n+m$ is a bijection of $\mathbb{Z}$ (for each fixed $m \in \mathbb{Z}$).

Next, we compute the q-expansion of G_2. First, note that

$$G_2(z) = 2\zeta(2) + 2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^2}.$$

Using now Lemma 1.9 with z substituted by mz, we obtain

$$G_2(z) = 2\zeta(2) - 8\pi^2 \sum_{m=1}^{\infty} \sum_{d=1}^{\infty} dq^{md}.$$

Grouping terms contributing to a given power of q gives the formula.

Next, by expanding $G_2(\gamma_1\gamma_2 z)$, using the cocycle property of $j(\gamma, z)$ and calculating the lower left entry of the product of two matrices, we see that if Equation 1.5 is satisfied for matrices γ_1 and γ_2 then it is also satisfied for $\gamma_1\gamma_2$ and γ_1^{-1}. Therefore to prove Equation Equation 1.5 it will be enough to prove it for the matrix $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

We next show that

$$G_2(-1/z) = z^2 \left(2\zeta(2) + \sum_{n\in\mathbb{Z}} \sum_{m\neq 0} \frac{1}{(mz+n)^2} \right).$$

This only differs from $z^2 G_2(z)$ in the order of summation! This is done by substituting $-1/z$ in the definition to get:

$$G_2(-1/z) = \sum_{n\neq 0} \frac{1}{n^2} + \sum_{m\neq 0} \sum_{n\in\mathbb{Z}} \frac{z^2}{(mz-n)^2} = \sum_{n\neq 0} \frac{1}{n^2} + \sum_{m\neq 0} \sum_{n\in\mathbb{Z}} \frac{z^2}{(m-nz)^2}$$

This can be rewritten as

$$2\zeta(2) + z^2 \left(\sum_{n\in\mathbb{Z}} \sum_{m\neq 0} \frac{1}{(mz+n)^2} \right) = 2\zeta(2) + z^2 \left(\sum_{n\neq 0} \sum_{m\neq 0} \frac{1}{(mz+n)^2} + 2\zeta(2) \right).$$

The outer term $2\zeta(2)$ can be put into the sum corresponding to the term $n = 0$, getting the desired formula. The partial fraction decomposition

$$\frac{1}{(mz+n)(mz+n+1)} = \frac{1}{mz+n} - \frac{1}{mz+n+1}$$

allows us to show (via a telescoping sum) that

$$\sum_{m\neq 0} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)(mz+n+1)} = 0$$

Subtracting this series from the definition of $G_2(z)$ (which can be done term by term, this only needs conditional convergence) we get the new formula involving an absolutely convergent sum:

$$G_2(z) = 2\zeta(2) + \sum_{\substack{m\neq 0 \\ n\in\mathbb{Z}}} \frac{1}{(mz+n)^2(mz+n+1)}.$$

Then we compute

$$z^{-2}G_2(-1/z) - G_2(z) = \sum_{n\in\mathbb{Z}}\sum_{m\neq 0}\frac{1}{(mz+n)^2} - \sum_{m\neq 0,n\in\mathbb{Z}}\frac{1}{(mz+n)^2(mz+n+1)}.$$

Subtracting term by term and using that

$$\frac{1}{(mz+n)^2} - \frac{1}{(mz+n)^2(mz+n+1)} = \frac{1}{(mz+n)(mz+n+1)}$$

gives an alternative formula for $G_2(z)$:

$$G_2(z) = z^{-2}G_2(-1/z) - \sum_{n\in\mathbb{Z}}\sum_{m\neq 0}\frac{1}{(mz+n)(mz+n+1)}.$$

Finally, consider the sum

$$\lim_{N\longrightarrow\infty}\sum_{n=-N}^{N-1}\sum_{m\neq 0}\left(\frac{1}{mz+n} - \frac{1}{mz+n+1}\right).$$

For each fixed N we can reverse the sum and calculate, since the inner sum telescopes:

$$\begin{aligned}\sum_{m\neq 0}\sum_{n=-N}^{N-1}\left(\frac{1}{mz+n} - \frac{1}{mz+n+1}\right) &= \sum_{m\neq 0}\left(\frac{1}{mz-N} - \frac{1}{mz+N}\right)\\ &= \frac{-1}{z}\sum_{m\neq 0}\left(\frac{1}{N/z+m} + \frac{1}{N/z-m}\right)\\ &= \frac{-2\pi}{z}\cot(\pi N/z).\end{aligned}$$

Taking the sum as $N\longrightarrow\infty$ and using that

$$\pi\cot(\pi N/z) = \pi i - 2\pi i\sum_{m=0}^{\infty}e^{2\pi i m N/z}$$

we get the formula:

$$\lim_{N\longrightarrow\infty}\sum_{n=-N}^{N-1}\sum_{m\neq 0}\left(\frac{1}{mz+n} - \frac{1}{mz+n+1}\right) = -\frac{2\pi i}{z}.$$

This finishes the proof. □

1.7.1 The Dedekind-eta function

Define $\eta(z)$ as through the following product

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

The function $\eta(z)$ is holomorphic and non-vanishing on $\mathbb{H}$ (to check it, it is enough to check that $\sum q^n$ converges absolutely and uniformly on compact subsets of $\mathbb{H}$).

Theorem 1.13. *The η function satisfies the following transformation property:*

$$\eta(-1/z) = \sqrt{z/i}\eta(z).$$

Proof. Note that:

$$\begin{aligned}\frac{d}{dz}\log\eta(z) &= \frac{2\pi i}{24} + \sum_{n=1}^{\infty} \frac{-2\pi i n q^n}{1-q^n} = \frac{2\pi i}{24}\left(1 - 24\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}\right) \\ &= \frac{\pi i}{12}\left(1 - 24\sum_{n=1}^{\infty} n\sum_{m=1}^{\infty} q^{nm}\right) = \frac{\pi i}{12}E_2(z).\end{aligned}$$

Using quasi-modularity of E_2, we deduce:

$$\mathrm{dlog}\left(\eta(-1/z)\right) = \mathrm{dlog}\left(\sqrt{z/i}\eta(z)\right).$$

Therefore $\eta(-1/z) = C\sqrt{z/i}\eta(z)$ and setting $z = i$ one gets $C = 1$, as we wanted. □

Theorem 1.14.

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

Proof. Note that:

$$\eta^{24}(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24},$$

so $\eta^{24}(z+1) = \eta^{24}(z)$. Moreover,

$$\eta^{24}(-1/z) = z^{12}\eta^{24}(z).$$

Since $\eta^{24}(z) = q + \cdots$ and $\eta^{24}(z) \in S_{12} = \mathbb{C}\Delta$, we deduce that $\eta^{24} = \Delta$. □

1.8 Growth of Fourier coefficients

In this final section we study the different behavior of the Fourier coefficients of a modular form f, depending on whether f is cuspidal or not. Intuitively, if f is cuspidal, the vanishing at infinity should force the coefficients to grow slower.

We start by studying Eisenstein series.

Proposition 1.5. *The Fourier coefficients $a_n(E_k)$ of the Eisenstein series E_k grow as n^{k-1}. Precisely, there exist constant $A, B > 0$ such that*

$$An^{k-1} \leq |a_n(E_k)| \leq Bn^{k-1}.$$

Proof. We will use that the Fourier coefficients of E_k have a simple formula:

$$E_k = 1 + C_k \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

and hence $|a_n(E_k)| = |C_k| \sigma_{k-1}(n)$. Therefore

$$|a_n(E_k)| = |C_k| \sum_{d|n} d^{k-1} \geq |C_k| n^{k-1},$$

and we may take $A = |C_k|$. On the other hand,

$$\frac{|a_n(E_k)|}{n^{k-1}} = |C_k| \sum_{d|n} \left(\frac{d}{n}\right)^{k-1} = |C_k| \sum_{d|n} \frac{1}{d^{k-1}}.$$

This last term can be coarsely estimated:

$$|C_k| \sum_{d|n} \frac{1}{d^{k-1}} \geq |C_k| \sum_{d=1}^{\infty} \frac{1}{d^{k-1}} = |C_k| \zeta(k-1).$$

Hence we may take $B = |C_k| \zeta(k-1)$. □

The following result shows that the coefficients of cusp forms grow much slower.

Theorem 1.15. *If $\sum_{n=1}^{\infty} a_n q^n$ is the q-expansion of a cusp form of weight k, then $a_n = O(n^{k/2})$. Precisely, there is a constant $M > 0$ such that*

$$|a_n| \leq M n^{k/2}.$$

Proof. Note that as $q \longrightarrow \infty$ we have $|f(z)| = O(q) = O(e^{-2\pi i})$, where $y = \Im(z)$. Consider the function

$$\phi(z) = |f(z)|y^{k/2}.$$

It is a continuous function $\mathbb{H} \longrightarrow \mathbb{R}_{\geq 0}$, and it is invariant under $\mathrm{SL}_2(\mathbb{Z})$. Since ϕ approaches 0 as y approaches infinity, we deduce that ϕ is bounded: $|f(z)| \leq M' y^{-k/2}$ for all $z \in \mathbb{H}$. Since $f(z)q^{-n-1} = \cdots + a_n q^{-1} + a_{n+1} + a_{n+2}q + \cdots$ the residue theorem implies that

$$a_n = \frac{1}{2\pi i} \int_{C_y} f(z) q^{-n-1} dq,$$

where C_y is the counter-clockwise circle described by $e^{2\pi i(x+iy)}$ when y is fixed and x moves from 0 to 1. This gives:

$$a_n = \int_0^1 f(x+iy) q^{-n} dx,$$

Using the bound for $|f|$ we obtain:

$$|a_n| \leq \int_0^1 M' y^{-k/2} |e^{-2\pi i n(x+iy)} dx = M' y^{-k/2} e^{2\pi y n}.$$

This expression is valid for all $y > 0$. In particular, for $y = 1/n$ we get $|a_n| \leq M' e^{2\pi} n^{k/2}$. Setting $M = M' e^{2\pi}$ finishes the proof. □

Corollary 1.9. *If f is not a cusp form, then the coefficients a_n grow as n^{k-1}.*

Proof. If f is a modular form of weight k, write $f = \lambda E_k + h$, where h is a cusp form. The hypothesis of f not being a cups form translates in $\lambda \neq 0$. Therefore

$$a_n(f) = \lambda a_n(E_k) + a_n(h).$$

Since n^{k-1} grows much faster than $n^{k/2}$ and $\lambda \neq 0$, we deduce that $a_n(f)$ grows as n^{k-1}. □

2 Modular forms for congruence subgroups

2.1 Congruence subgroups

Let $N \geq 1$ be an integer. In this section we will consider subgroups of $\mathrm{SL}_2(\mathbb{Z})$ that are especially nice to work with. There are other subgroups that are interesting but beyond the scope of this course.

Definition 2.1. The of level N is

$$\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}\}.$$

Note that $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$, so we are strictly generalizing Chapter 1. Note also that $\Gamma(N)$ can be defined as the kernel of the group homomorphism induced by the reduction map $\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}$:

$$\pi_N \colon \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Therefore, $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$, of finite index.

Proposition 2.1. *The map π_N is surjective.*

Proof. Exercise. □

There are too few principal congruence subgroups (only one for each $N \geq 1$), so it is desirable to consider more general subgroups.

Definition 2.2. A subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a if there is some $N \geq 1$ such that

$$\Gamma(N) \subseteq \Gamma \subseteq \mathrm{SL}_2(\mathbb{Z}).$$

The of a congruence subgroup Γ is the minimum N such that $\Gamma(N) \subseteq \Gamma$.

One can think of many different ways to construct congruence subgroups. There are two families that arise so frequently that have special notation for them:

Example 2.1. For each $N \geq 1$, define

$$\Gamma_1(N) = \{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod N\},$$

and also

$$\Gamma_0(N) = \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod N\}.$$

Lemma 2.1. *For each $N \geq 1$ there are inclusions $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$, and*

$$[\Gamma_1(N) \colon \Gamma(N)] = N, \quad [\Gamma_0(N) \colon \Gamma_1(N)] = N \prod_{p|N} \left(1 - \frac{1}{p}\right), \quad [\mathrm{SL}_2(\mathbb{Z}) \colon \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

Proof. Exercise. □

The inclusions are strict except for $N = 1$ (where all groups coincide) and for $\Gamma_0(2) = \Gamma_1(2)$.

Definition 2.3. A function $f \colon \mathbb{H} \longrightarrow \mathbb{C}$ is of weight k with respect to Γ if it is meromorphic on $\mathbb{H}$ and it satisfies

$$f|_k \gamma = f, \quad \forall \gamma \in \Gamma.$$

2.2 Cusps

Of course we will need to understand fundamental domains for the action of congruence subgroups on $\mathbb{H}$. Here is for example a fundamental domain for $\Gamma_0(2)$:

In this case, the fundamental domain contains two points in its closure which do not belong to $\mathbb{H}$: the cusp ∞ as before, but also 0. The following result gives a construction of a fundamental domain for any congruence subgroup, using translates of the fundamental domain $\mathcal{D}$ of $\mathrm{SL}_2(\mathbb{Z})$ seen in Chapter 1.

Proposition 2.2. *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. If there is a decomposition*

$$\Gamma \backslash \mathrm{SL}_2(\mathbb{Z}) = \bigcup_{h \in R} \Gamma h, \quad R \text{ finite},$$

then the set $\mathcal{D}_\Gamma = \cup_{h \in R} h\mathcal{D}$ is a (possibly non-connected) fundamental domain for Γ.

Proof. If $z \in \mathbb{H}$, then there exists $g \in \mathrm{SL}_2(\mathbb{Z})$ and $z_0 \in \mathcal{D}$ such that $z = gz_0$. The coset decomposition implies that there is some $\gamma \in R$ and some $h \in \Gamma$ such that $g = h\gamma$. Therefore

$$z = h\gamma z_0.$$

Since $z_0' = \gamma z_0 \in \gamma \mathcal{D} \subset \mathcal{D}_\Gamma$ we have written $z = hz_0'$ with $h \in \Gamma$.

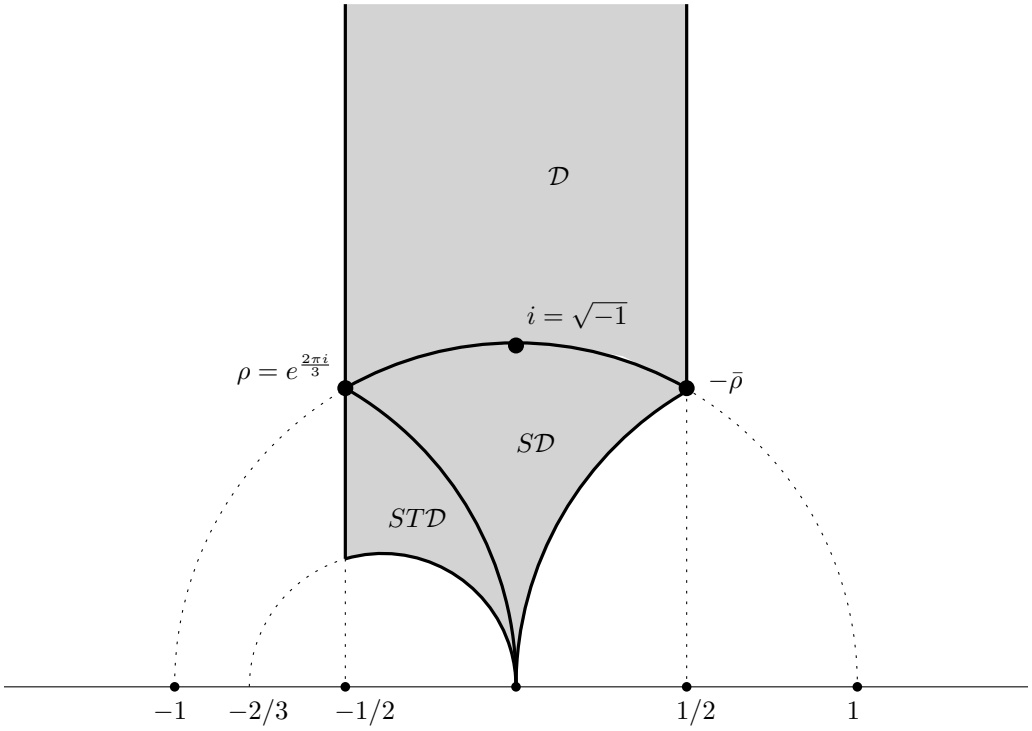

Figure 2.1: A fundamental domain for $\Gamma_0(2)$

It remains to be shown that if $z \in \overset{\circ}{\mathcal{D}}_\Gamma$ and $\gamma z \in \overset{\circ}{\mathcal{D}}_\Gamma$ for some $\gamma \in \Gamma$, then $\gamma = 1$. For that, let $\varepsilon > 0$ be small enough so that the ball $B_\varepsilon(z)$ of radius ε around z is fully contained in $\overset{\circ}{\mathcal{D}}_\Gamma$. The ball $B_\varepsilon(z)$ intersects some translates of $\mathcal{D}$, say:

$$B_\varepsilon(z) \cap h\mathcal{D} \neq \emptyset \iff h \in R' \subseteq R.$$

Consider the translated ball $\gamma B_\varepsilon(z) = B_\varepsilon(\gamma z)$. Since γz is also in the interior of $\mathcal{D}_\Gamma$, we deduce that $\gamma B_\varepsilon(z)$ must intersect the interior of some translate of $\mathcal{D}$, say $h\ \overset{\circ}{\mathcal{D}}$, for some $h \in R$. Therefore:

$$\gamma B_\varepsilon(z) \cap h\ \overset{\circ}{\mathcal{D}} \neq \emptyset \implies B_\varepsilon(z) \cap \gamma^{-1} h\ \overset{\circ}{\mathcal{D}} \neq \emptyset.$$

Since we listed all the translates whose interior intersected with $B_\varepsilon(z)$, we must have that $\gamma^{-1}h = h_0$. But now $\Gamma h = \Gamma\gamma^{-1}h = \Gamma h_0$, and since both h and h_0 belong to R, we must have $h = h_0$. Therefore $\gamma^{-1} = 1$, or $\gamma = 1$ as we wanted. □

In order to further study the cusps, we consider the $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. Note that $\mathrm{SL}_2(\mathbb{Z})$ (in fact $\mathrm{GL}_2(\mathbb{Q})$) acts on $\mathbb{P}^1(\mathbb{Q})$ by fractional linear transformations:

$$\gamma x = \frac{ax+b}{cx+d}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), x \in \mathbb{P}^1(\mathbb{Q}).$$

Here we understand that $\gamma\infty = \frac{a}{c}$, and $\gamma x = \infty$ if $cx = -d$.

Proposition 2.3. *The action of* $\mathrm{SL}_2(\mathbb{Z})$ *on* $\mathbb{P}^1(\mathbb{Q})$ *is transitive, and it induces a bijection*

$$\mathrm{SL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})_\infty \cong \mathbb{P}^1(\mathbsmall{\mathbb{Q}}), \quad \mathrm{SL}_2(\mathbb{Z})_\infty = \langle \pm T \rangle.$$

Proof. We will see that the orbit of ∞ is all of $\mathbb{P}^1(\mathbb{Q})$, where we note that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\infty = \frac{a}{c}$. Given $\frac{a}{c} \in \mathbb{P}^1(\mathbb{Q})$ in reduced terms (that is, such that $(a,c) = 1$), then Bézout's identity asserts the existence of integers b and d such that $ad - bc = 1$. Then the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ belongs to $\mathrm{SL}_2(\mathbb{Z})$ and takes ∞ to $\frac{a}{c}$.

The stabilizer of ∞, written $\mathrm{SL}_2(\mathbb{Z})_\infty$, is:

$$\mathrm{SL}_2(\mathbb{Z})_\infty = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix}\infty = \infty \right\} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \frac{a}{c} = \infty \right\} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right\} = \langle \pm T \rangle.$$

□

Definition 2.4. The set of of a congruence subgroup Γ is the set $\mathrm{Cusps}(\Gamma)$ of Γ-orbits of $\mathbb{P}^1(\mathbb{Q})$. Equivalently,

$$\mathrm{Cusps}(\Gamma) = \Gamma\backslash\mathrm{SL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})_\infty.$$

If $P = [\frac{a}{c}]$ is a cusp of Γ, set Γ_P for the of P in Γ, the elements of Γ fixing P.

Lemma 2.2. *If $\gamma_P(\infty) = P$, then*

$$\Gamma_P = \Gamma \cap \gamma_P \mathrm{SL}_2(\mathbb{Z})_\infty \gamma_P^{-1}.$$

Proof. Let $\gamma \in \Gamma$. Then observe that

$$\begin{aligned} \gamma \in \Gamma_P &\iff \gamma P = P \iff \gamma\gamma_P\infty = \gamma_P\infty \\ &\iff \gamma_P^{-1}\gamma\gamma_P\infty = \infty \\ &\iff \gamma_P^{-1}\gamma\gamma_P \in \mathrm{SL}_2(\mathbb{Z})_\infty \\ &\iff \gamma \in \gamma_P \mathrm{SL}_2(\mathbb{Z})_\infty \gamma_P^{-1}. \end{aligned}$$

This concludes the proof. □

Lemma 2.3. *The subgroup $H_P = \gamma_P^{-1}\Gamma\gamma_P \cap \mathrm{SL}_2(\mathbb{Z})_\infty \subseteq \mathrm{SL}_2(\mathbb{Z})_\infty$ does not depend on the choice of the representative for P, and has finite index in $\mathrm{SL}_2(\mathbb{Z})_\infty$.*

Proof. Just note that if $\frac{a'}{c'}$ is another representative for P, then γ_P gets modified into $\gamma\gamma_P$ for some $\gamma \in \Gamma$. Then $(\gamma\gamma_P)^{-1}\Gamma(\gamma\gamma_P) = \gamma_P^{-1}\Gamma\gamma_P$. □

Lemma 2.4. *Let H be a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})_\infty$, and let h be the index of $\{\pm 1\}H$ in $\mathrm{SL}_2(\mathbb{Z})_\infty$. Then H is one of he following:*

$$H = \begin{cases} \langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \rangle \\ \langle \left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right) \rangle \\ \{\pm 1\} \times \langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \rangle \end{cases}$$

Proof. Exercise. □

Definition 2.5. The integer $h_\Gamma(P) = h$ in the above lemma is called P for Γ. A cusp is an if $\gamma_P^{-1}\Gamma_P\gamma_P$ is of the form $\langle \left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right) \rangle$, and it is otherwise.

Example 2.2. In this example we show that if p is any prime, then $\mathrm{Cusps}(\Gamma_0(p)) = \{\infty, 0\}$.

Write an element $\gamma \in \Gamma_0(p)$ as $\left(\begin{smallmatrix} a & b \\ pc & d \end{smallmatrix}\right)$, with $a, b, c, d \in \mathbb{Z}$ satisfying $ad - pbc = 1$. The orbit of ∞ is:

$$\Gamma_0(p) \cdot \infty = \left\{ \begin{pmatrix} a & b \\ pc & d \end{pmatrix} \infty \right\} = \left\{ \frac{a}{pc} \ : \ a, c \in \mathbb{Z}, \gcd(a, pc) = 1 \right\} = \left\{ \frac{r}{s} \ : \ p \mid s, \gcd(r, s) = 1 \right\}.$$

We thus see the orbit of the cusp ∞ consists of infinity together with all the rationals which when expressed in reduced terms have a denominator which is divisible by p. One element which is not in this orbit is $0 = \frac{0}{1}$. Let us study then the orbit of 0.

$$\Gamma_0(p) \cdot 0 = \{ \begin{pmatrix} a & b \\ pc & d \end{pmatrix} 0 \} = \{ \frac{b}{d} \ : \ b, d \in \mathbb{Z}, \gcd(b, d) = 1, p \nmid d \}.$$

As we have seen in the example above, each cusp may have a different width. However, if Γ is a normal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, the subgroup H_P does not depend on the cusp P and hence all cusps have the same width and regularity.

Although one can have more cusps than the index of Γ, the last result of this section says that this is basically right, once one counts in a proper way. To prove it, we will need a group-theoretic result.

Lemma 2.5. *Let G be a group acting transitively on a set X and let H be a finite index subgroup of G. Then for any $x \in X$ the stabilizer of x in H has finite index in the stabilizer of x in G, and the following formula holds:*

$$\sum_{x \in H\backslash X} [G_x \colon H_x] = [G \colon H].$$

Proof. Let $x \in X$, and consider the inclusion map $G_x \longrightarrow G$. By taking the quotient by H we get $G_x \longrightarrow H\backslash G$. Suppose g_1, g_2 are mapped to the same element Hg in $H\backslash G$. This means that $Hg_1 = Hg_2$, or that $g_2 g_1^{-1}$ belongs to H. Since $g_2 g_1^{-1}$ stabilizes x as well, we deduce that $H_x g_1 = H_x g_2$. Therefore there is an injection of $H_x\backslash G_x \hookrightarrow H\backslash G$. Since by assumption the latter set is finite, so is the first. Note also that the image of the map is precisely $H\backslash HG_x$, and thus we also obtain $[G_x \colon H_x] = [HG_x \colon H]$.

To prove the second assertion, fix an element $x_0 \in X$, and consider the map

$$H\backslash G \longrightarrow H\backslash X, \quad Hg \mapsto Hgx_0$$

which is surjective because G acts transitively on X. The fibre T_{Hx} of an orbit Hx consists of the set of classes Hg such that $Hgx_0 = Hx$. Let $g_x \in G$ be such that $g_x x_0 = x$. Write $Hg = Hg' g_x$ and then we have:

$$T_{Hx} \cong \{Hg' \in H\backslash G \colon Hg' g_x x_0 = Hx\} = \{Hg' \in H\backslash G \colon Hg'x = Hx\} = H\backslash(HG_x) \cong H_x\backslash G_x.$$

This allows us to find a formula for $[G \colon H]$:

$$= \#(H\backslash G) = \sum_{x \in R} \#T_{Hx} = \sum_{x \in R} [G_x \colon H_x].$$

□

Theorem 2.1. *Let Γ be a congruence subgroup. Then we have*

$$\sum_{P \in \mathrm{Cusps}(\Gamma)} h_\Gamma(P) = [\mathrm{SL}_2(\mathbb{Z}) \colon \{\pm 1\}\Gamma].$$

Proof. Consider the group $G = \mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$, which acts transitively on the set $X = \mathbb{P}^1(\mathbb{Q})$. Let H be the image of Γ in G. Note that $H\backslash X = \mathrm{Cusps}(\Gamma)$. Also, G_∞ is the image in G of $\mathrm{SL}_2(\mathbb{Z})_\infty$. For each $x \in X$, let $\gamma \in G$ be such that $\gamma\infty = x$. Then

$$G_x = \gamma G_\infty \gamma^{-1}, \text{ and } \quad H_x = \gamma \left(\gamma^{-1} H \gamma\right)_\infty \gamma^{-1}.$$

Therefore

$$[G_x \colon H_x] = [\bar{\mathrm{SL}}_2(\mathbb{Z}) \colon \bar{\Gamma}_P] = h_\Gamma(P),$$

where by $\overline{(\cdot)}$ we write the image of the group inside G. Then applying Lemma 2.5 to this setting gives

$$\sum_{P \in \mathrm{Cusps}(\Gamma)} h_\Gamma(P) = [G \colon H] = [\mathrm{SL}_2(\mathbb{Z}) \colon \{\pm 1\}\Gamma].$$

□

2.3 Fourier expansion at infinity

Let Γ be a congruence subgroup of level N. Note that the matrix $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)$ belongs to $\Gamma(N)$, and thus there is a minimum $h > 0$ with the property that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$.

Definition 2.6. The of Γ is the minimum $h > 0$ such that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$.

The fan width of a congruence subgroup of level N is a divisor of N.

Write

$$q_h = q_h(z) = e^{\frac{2\pi i z}{h}},$$

and note that $z \mapsto q_h(z)$ is periodic with period h. Define g by $g = f \circ q_h^{-1}$. That is, $g(q_h) = f(z)$. Although q_h is not invertible, the above definition makes sense, and g has a Laurent expansion.

Definition 2.7. The q-expansion of f at infinity is the Laurent expansion:

$$f(z) = g(q_h) = \sum_{n=-\infty}^{\infty} a(n) q_h^n.$$

2.4 Expansions at cusps

Let s be a cusp, $s \neq \infty$. Write $s = \alpha\infty$ for some $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, and consider the equation:

$$f(\alpha z) = j(\alpha, z)^k (f|_k \alpha)(z).$$

Since $j(\alpha, z) \neq 0, \infty$ when z is near ∞, the behavior of $f(z)$ near s is related to the behavior of $(f|_k\alpha)(z)$ near ∞. Assume that f is weakly modular for the congruence subgroup Γ. Since

$$(f|_k\alpha)|_k(\alpha^{-1}\gamma\alpha) = (f|_k\gamma)|_k\alpha = f|_k\alpha,$$

the new function $f|_k\alpha$ is invariant under the group $\Gamma' = \alpha^{-1}\Gamma\alpha$. Since $\Gamma(N)$ is normal inside $\mathrm{SL}_2(\mathbb{Z})$, we deduce that Γ' is also a congruence subgroup of level N. Hence $f|_k\alpha$ has a Fourier expansion at infinity as in Section 2.3 in powers of q_N.

Definition 2.8. The s is the expansion:

$$f|_k\alpha = \sum_{n=-\infty}^{\infty} b(n)q_N^n.$$

2.5 Definition of modular forms

The expansions at different cusps allow us to define modular forms for arbitrary congruence subgroups.

Definition 2.9. A function $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ is a of weight k for a congruence subgroup Γ if:

1. f is holomorphic on $\mathbb{H}$,
2. $f|_k\gamma = f$ for all $\gamma \in \Gamma$, and
3. $f|_k\alpha$ is holomorphic at infinity for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

A function is a of weight k for a congruence subgroup Γ if instead of 3 is satisfies:

1. $f|_k\alpha$ vanishes at infinity for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

The of weight k for a congruence subgroup Γ is written $M_k(\Gamma)$; the of weight k for a congruence subgroup Γ is written $S_k(\Gamma)$.

Proposition 2.4. *Suppose that $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ satisfies 1 and 2 above. Suppose that f is holomorphic at infinity. That is,*

$$f(z) = \sum_{n=0}^{\infty} a(n)q_N^n.$$

Furthermore, suppose that there exists constants $C > 0$ and $r > 0$ such that:

$$|a(n)| < Cn^r, \quad \forall n > 0.$$

Then f satisfies 3, and thus $f \in M_k(\Gamma)$.

Proof. Exercise. □

In fact, the converse is also true: if the Fourier coefficients of f grow as Cn^r as above, then condition 3 in Definition 2.9 is satisfied. The proof of this fact uses Eisenstein series for congruence subgroups, and thus will be postponed until we introduce those.

Example 2.3. Let f be a weakly-modular form of weight k for the full modular subgroup. Consider the function $g(z) = f(Nz)$. If $\gamma \in \Gamma_0(N)$ is of the form $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then since $N \mid c$ the matrix

$$\gamma' = \begin{pmatrix} a & bN \\ c/N & d \end{pmatrix}$$

is in $\mathrm{SL}_2(\mathbb{Z})$. Therefore we may compute:

$$\begin{aligned} g(\gamma z) = f(N(\gamma z)) &= f(\frac{Naz + bN}{cz + d}) \\ &= f(\frac{a(Nz) + bN}{c/N(Nz) + d}) = f(\gamma'(Nz)) \\ &= (c/N(Nz) + d)^k f(Nz) = j(\gamma, z)^k g(z). \end{aligned}$$

Therefore the function g is weakly-modular of weight k for the congruence subgroup $\Gamma_0(N)$. In fact, this operation defines injections

$$M_k(\mathrm{SL}_2(\mathbb{Z})) \longrightarrow M_k(\Gamma_0(N))$$

which will play an important role later in the course, in the Atkin-Lehner-Li theory of old/new forms.

We end this section by realizing that the definition of modular forms can be checked by finitely many computations. Suppose that $\sigma = \alpha\infty$ and $\tau = \beta\infty$ are two cusps (here α and β are in $\mathrm{SL}_2(\mathbb{Z})$). Suppose that $\sigma = \gamma\tau$ with $\gamma \in \Gamma$.

Proposition 2.5. *If*

$$f|_k\alpha = \sum_{n=-\infty}^{\infty} a(n) q_h^n,$$

then

$$f|_k\beta = \sum_{n=-\infty}^{\infty} b(n) q_h^n, \quad b(n) = (\pm 1)^k e^{\frac{2\pi i n j}{h}} a(n), j \in \mathbb{Z}.$$

Proof. By assumption $\alpha\infty = \gamma\beta\infty$, so $\alpha^{-1}\gamma\beta\infty = \infty$, and therefore since the only matrices that fix infinity are of the form $\pm\left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right)$ we have:

$$\alpha^{-1}\gamma\beta = \pm \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}, \quad j \in \mathbb{Z}.$$

This means that

$$\beta = \pm\gamma^{-1}\alpha \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix},$$

and therefore:

$$\begin{aligned} f|_k\beta &= f|_k \pm I|_k\gamma^{-1}|_k\alpha|_k \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} = (\pm 1)^k \sum a(n) e^{\frac{2\pi i n z}{h}}|_k \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \\ &= (\pm 1)^k \sum a(n) e^{\frac{2\pi i n (z+j)}{h}}. \end{aligned}$$

□

Corollary 2.1. *For each $n \in \mathbb{Z}$, we have $a(n) = 0$ if and only if $b(n) = 0$. In particular, it is enough to check 3 or 3′ for one representative from each of the equivalence classes of cusps.*

2.6 Valence formula for congruence subgroups

Let Γ be a congruence subgroup of level N. In order to state the next result we need to define the order of a weakly-modular function at a cusps $P \in \mathrm{Cusps}(\Gamma)$.

Definition 2.10. Let f be a weakly-modular form of weight k for Γ, and let P be a cusp of Γ of width $h_\Gamma(P)$. Since $f(z+N) = f(z)$, we can write f as a Laurent series in $q_N = e^{\frac{2\pi i z}{N}}$, say

$$f(q_N) = \sum_{n \geq n_0} a_n q_N^n, \quad a_{n_0} \neq 0.$$

The of f at P is $v_P(f) = \frac{h_\Gamma(P)}{N} n_0$.

Here is a generalization of Theorem 1.9 to arbitrary congruence subgroups.

Theorem 2.2. *Let Γ be a congruence subgroup, and let k be an integer. Let f be a non-zero meromorphic function on $\mathbb{H} \cup \{\infty\}$, which is weakly-modular of weight k for Γ. Then we have*

$$\sum_{z \in \Gamma\backslash\mathbb{H}} \frac{v_z(f)}{\#\overline{\Gamma}_z} + \sum_{P \in \mathrm{Cusps}(\Gamma)} v_P(f) = \frac{k}{12}[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}].$$

Proof. Write $d_\Gamma = [\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}]$, let R be a set of coset representatives for $\overline{\Gamma}\backslash \mathrm{PSL}_2(\mathbb{Z})$, and define $F = \prod_{\gamma \in R} f|_k\gamma$. Note that F is weakly-modular of weight kd_Γ for $\mathrm{SL}_2(\mathbb{Z})$, and it is meromorphic at ∞. By Theorem 1.9 we have

$$v_\infty(F) + \frac{1}{2}v_i(F) + \frac{1}{3}v_\rho(F) + \sum_{w \in W} v_w(F) = \frac{k}{12} d_\Gamma.$$

Another way to write the above is:

$$v_\infty(F) + \sum_{z \in \mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}} \frac{v_z(F)}{\#\,\mathrm{PSL}_2(\mathbb{Z})_z} = \frac{k}{12} d_\Gamma.$$

We may now compute:

$$v_z(F) = \sum_{\gamma \in \overline{\Gamma}\backslash\,\mathrm{PSL}_2(\mathbb{Z})} v_z(f|_k\gamma) = \sum_{\gamma \in \overline{\Gamma}\backslash\,\mathrm{PSL}_2(\mathbb{Z})} v_{\gamma z}(f) = \sum_{w \in \overline{\Gamma}\backslash\,\mathrm{PSL}_2(\mathbb{Z})z} [\mathrm{PSL}_2(\mathbb{Z})_w \colon \overline{\Gamma}_w] v_w(f).$$

The last equality follows by grouping all elements γ such that $\gamma z = w$, for each possible w. Now, since $\mathrm{PSL}_2(\mathbb{Z})_w$ is finite and independent of $w \in \overline{\Gamma}\backslash\,\mathrm{PSL}_2(\mathbb{Z})z$, we get $[\mathrm{PSL}_2(\mathbb{Z})_w \colon \overline{\Gamma}_w] = \frac{\#\,\mathrm{PSL}_2(\mathbb{Z})_z}{\#\overline{\Gamma}_w}$. Dividing by $\#\,\mathrm{PSL}_2(\mathbb{Z})_z$ we obtain

$$\frac{v_z(F)}{\#\,\mathrm{PSL}_2(\mathbb{Z})_z} = \sum_{w \in \overline{\Gamma}\backslash\,\mathrm{PSL}_2(\mathbb{Z})z} \frac{v_w(f)}{\#\overline{\Gamma}_w}.$$

By summing over a set of representatives for $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}$ we finally obtain

$$\sum_{z \in \mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}} \frac{v_z(F)}{\#\,\mathrm{PSL}_2(\mathbb{Z})_z} = \sum_{z \in \mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}} \sum_{w \in \overline{\Gamma}\backslash\,\mathrm{PSL}_2(\mathbb{Z})z} \frac{v_w(f)}{\#\overline{\Gamma}_w} = \sum_{w \in \overline{\Gamma}\backslash\mathbb{H}} \frac{v_w(f)}{\#\overline{\Gamma}_w}.$$

In order to conclude the proof it remains to be shown that $v_\infty(F) = \sum_{P \in \mathrm{Cusps}(\Gamma)} v_P(f)$. We first prove it assuming that $\overline{\Gamma}$ is normal in $\mathrm{PSL}_2(\mathbb{Z})$. In this case, we have

$$\begin{aligned}
d_\Gamma v_\infty(F) &= \sum_{P \in \mathrm{Cusps}(\Gamma)} h_\Gamma(P) v_\infty(F) \\
&= \sum_{P \in \mathrm{Cusps}(\Gamma)} v_P(F) \\
&= \sum_{P \in \mathrm{Cusps}(\Gamma)} \sum_{\gamma \in R} v_{\gamma P}(f) \\
&= \sum_{P \in \mathrm{Cusps}(\Gamma)} \sum_{P' \in \mathrm{Cusps}(\Gamma)} \#\{\gamma \in R \mid \gamma P = P'\} v_{P'}(f) \\
&= \sum_{P' \in \mathrm{Cusps}(\Gamma)} \sum_{P \in \mathrm{Cusps}(\Gamma)} \#\{\gamma \in R \mid \gamma P = P'\} v_{P'}(f) \\
&= d_\Gamma \sum_{P' \in \mathrm{Cusps}(\Gamma)} v_{P'}(f).
\end{aligned}$$

Note that any congruence subgroup Γ contains a subgroup (for instance $\Gamma(N)$) which is normal in $\mathrm{SL}_2(\mathbb{Z})$, and such that it is of finite index. Therefore it is enough to show that, if $\Gamma' \subset \Gamma$ have finite index and g is weakly modular of weight k for Γ, then

$$\sum_{P' \in \mathrm{Cusps}(\Gamma')} v_{P'}(f) = \frac{d_{\Gamma'}}{d_\Gamma} \sum_{P' \in \mathrm{Cusps}(\Gamma')} v_{P'}(f).$$

Let $P \in \mathrm{Cusps}(\Gamma)$ and $P' \in \mathrm{Cusps}(\Gamma')$ be such that $[P] = [P']$ inside $\mathrm{Cusps}(\Gamma)$. Pick $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma\infty = [P]$ in $\mathrm{Cusps}(\Gamma)$. Write also $n_0 = v_P^\Gamma(g)$, and $m = \frac{h_{\Gamma'}}{h_\Gamma}$. Then:

$$(g|_k\sigma)(z) = \sum_{n \geq n_0} a_n(g) e^{\frac{2\pi i n z}{h_\Gamma}} = \sum_{n \geq n_0} a_n(g) e^{\frac{2\pi i n m z}{h_{\Gamma'}}} = \sum_{n \geq m n_0} a_n(g) e^{\frac{2\pi i n z}{h_{\Gamma'}}}.$$

Hence we have $v_{P'}(g) = m v_P(g)$, as we wanted. This concludes the proof of the valence formula. □

As for level 1, the valence formula gives a criterion for equality of modular forms:

Corollary 2.2. *Let f and g be two modular forms in $M_k(\Gamma)$, whose q-expansions (at one cusp of Γ) coincide up to the term $\frac{k}{12}[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}]$. Then f and g are equal.*

There are dimension formulas for congruence subgroups (see [3, Chapter 3]) but we will not see them in this course.

3 Moduli interpretation

In this chapter we reinterpret modular forms as functions on certain very interesting geometric objects.

3.1 Lattices and tori

Definition 3.1. A is a free $\mathbb{Z}$-module Λ of rank 2 inside $\mathbb{C}$ which contains an $\mathbb{R}$-basis for $\mathbb{C}$. Concretely, $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, where ω_1 and ω_2 are $\mathbb{R}$-linearly independent complex numbers. We will always assume that $\omega_1/\omega_2 \in \mathbb{H}$, which can always be accomplished by possible swapping them.

As you know, in general there are many choices for a basis of a given submodule.

Proposition 3.1. *Suppose that $\Lambda = \langle \omega_1, \omega_2 \rangle$ and $\Lambda' = \langle \omega_1', \omega_2' \rangle$. Then $\Lambda = \Lambda'$ if and only if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that*

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \gamma \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}.$$

Proof. Exercise. □

Lattices become interesting when we quotient $\mathbb{C}$ out by them.

Definition 3.2. A is the set $\mathbb{C}/\Lambda = \{z + \Lambda \mid z \in \mathbb{C}\}$. It has the structure of an abelian group, and analytically it is a torus (a genus one Riemann surface).

Proposition 3.2. *Suppose that $\varphi \colon \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ is a holomorphic map. Then there exist complex numbers m and b such that:*

1. *$m\Lambda \subseteq \Lambda'$, and*
2. *$\varphi(z + \Lambda) = mz + b + \Lambda'$.*

Moreover, φ is invertible if and only if $m\Lambda = \Lambda'$.

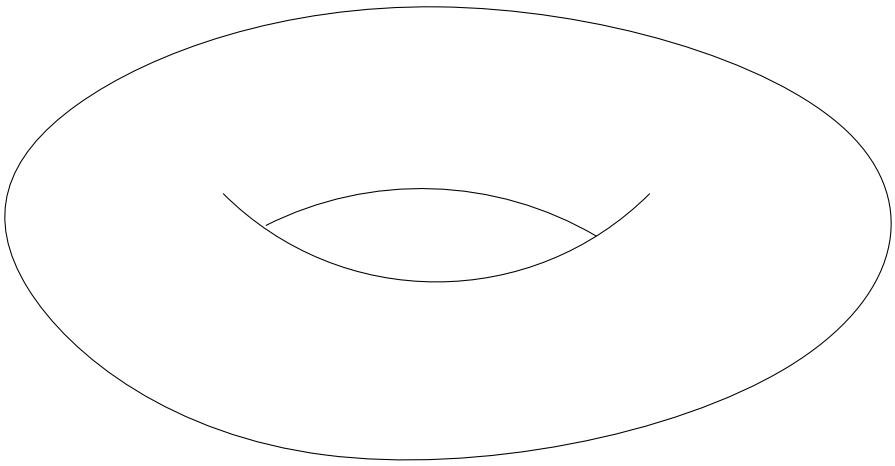

Figure 3.1: A torus

Proof. The complex plane $\mathbb{C}$ is the universal covering space of $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$. Therefore, φ can be lifted to a map $\tilde{\varphi}\colon \mathbb{C} \longrightarrow \mathbb{C}$. Suppose now that $\lambda \in \Lambda$, and define

$$f_\lambda(z) = \tilde{\varphi}(z+\lambda) - \tilde{\varphi}(z).$$

Then f_λ is continuous and has image in Λ'. Since Λ' is discrete, necessarily f_λ is constant. Consider the derivative. For each $\lambda \in \Lambda$, we have

$$\tilde{\varphi}'(z+\lambda) = \tilde{\varphi}'(z).$$

Therefore $\tilde{\varphi}'(z)$ is holomorphic and doubly-periodic, hence bounded. By Liouville's theorem, $\tilde{\varphi}'$ is constant. We deduce that $\tilde{\varphi}(z) = mz + b$, as wanted. □

Corollary 3.1. *Let $\varphi\colon \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ be a holomorphic map. Then φ is a group homomorphism if and only if $\varphi(0) = 0$, if and only if $b \in \Lambda'$.*

If φ as above is a holomorphic group isomorphism, then necessarily $m\Lambda = \Lambda'$ and also $\varphi(z+\Lambda) = mz + \Lambda'$.

Here are two examples of possible maps like the ones above.

Example 3.1. The map , usually written $[N]$, is a homomorphism

$$\mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda$$

which maps the class $z + \Lambda$ to $Nz + \Lambda$. The kernel of $[N]$ is the group of N-torsion points, isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

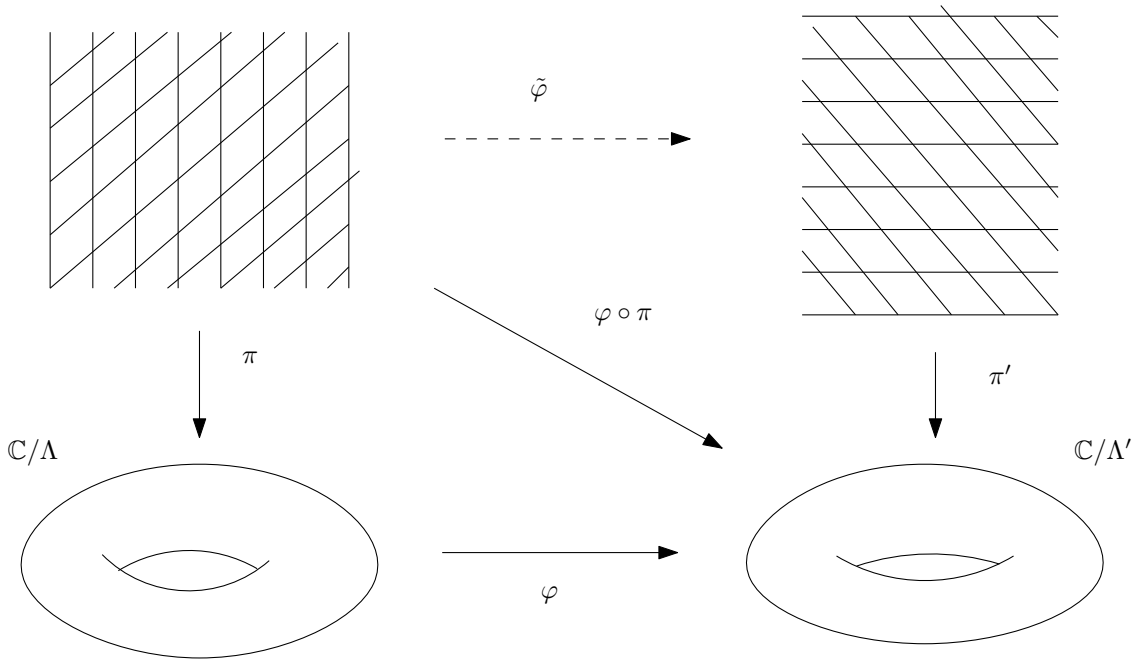

Figure 3.2: Lifting to the universal covering space

Example 3.2. Consider $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Define $\tau = \omega_1/\omega_2 \in \mathbb{H}$, and set $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$. Then $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda_\tau$.

The previous example can be brought a little bit further as follows.

Lemma 3.1. *The complex tori $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_{\tau'}$ are isomorphic if and only if $\tau = \gamma\tau'$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.*

Proof. Suppose that

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

Let $m = c\tau' + d$. Then $m\Lambda_\tau = \mathbb{Z}(a\tau' + b) \oplus \mathbb{Z}(c\tau' + d)$. By Proposition Proposition 3.1, this lattice is the same as $\mathbb{Z}\tau' \oplus \mathbb{Z} = \Lambda_{\tau'}$. The other direction is obtained by reading the equalities in reverse. □

We have just seen that there is a "natural bijection" between isomorphism classes of tori and elements $\tau \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. This innocent statement is **really** important.

Example 3.3. Let Λ be a lattice. Define, for $k > 2$ even,

$$G_k(\Lambda) = {\sum_{\omega\in\Lambda}}' \omega^{-k}.$$

Note that $G_k(\Lambda_\tau) = G_k(\tau)$ is the usual Eisenstein series defined in the previous chapter. The transformation law reads in this case:

$$G_k(m\Lambda) = m^{-k} G_k(\Lambda).$$

3.2 Tori and elliptic curves

The next goal is to relate $\mathbb{C}/\Lambda$ to elliptic curves. This will allow to think of modular forms as functions either on lattices or on elliptic curves.

3.2.1 Meromorphic functions on $\mathbb{C}/\Lambda$

Let $\mathbb{C}(\Lambda)$ be the field of meromorphic functions on $\mathbb{C}/\Lambda$. That is, meromorphic functions $f\colon \mathbb{C} \longrightarrow \mathbb{C}$ satisfying $f(z+\lambda) = f(z)$ for all $\lambda \in \Lambda$.

Proposition 3.3. *Let $f \in \mathbb{C}(\Lambda)$. Then:*

1. $\sum_{z \in \mathbb{C}/\Lambda} \operatorname{res}_z f = 0$.
2. $\sum_{z \in \mathbb{C}/\Lambda} \operatorname{ord}_z f = 0$.
3. $\sum_{z \in \mathbb{C}/\Lambda} z \operatorname{ord}_z f \in \Lambda$.

Proof. Consider a fundamental parallelepiped D which misses all zeroes and poles. This can be done because zeroes and poles form a discrete set. Now one can compute the quantities

$$\frac{1}{2\pi i}\int_{\partial D} f(z)dz, \quad \frac{1}{2\pi i}\int_{\partial D} \frac{f'(z)}{f(z)}dz \quad \text{, and } \frac{1}{2\pi i}\int_{\partial D} \frac{zf'(z)}{f(z)}dz.$$

□

Definition 3.3. The f is the number $\operatorname{ord}(f)$ of zeroes (which equals the number of poles) of f, when counted with multiplicities.

Note that the first statement in the above proposition implies that $\operatorname{ord}(f) \geq 2$.

3.2.2 The Weierstrass $\wp$-function

Consider the following function:

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{w\in\Lambda}{}' \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

It is immediate to see that $\wp_\Lambda$ is an even function, which converges absolutely and uniformly on compact sets away from Λ.

Lemma 3.2. *The function $\wp_\Lambda$ is Λ-periodic.*

Proof. Note that the derivative of $\wp_\Lambda$ is

$$\wp'_\lambda(z) = -2\sum_{w\in\Lambda} \frac{1}{(z-w)^3},$$

which is clearly Λ-periodic. Set $f(z) = \wp_\Lambda(z+w_1) - \wp_\Lambda(z)$, where $w_1 \in \Lambda$. Then $f'(z) = 0$, so f is constant, say $f(z) = c$. To determine c, set $z = -\frac{w}{2}$ and note that since $\wp_\Lambda$ is even, we get

$$c = \wp_\Lambda(w_1/2) - \wp_\Lambda(-w_1/2) = 0.$$

Therefore $f(z) = 0$, and thus $\wp_\Lambda$ is Λ-periodic. □

The lemma gives that $\wp_\lambda(z)$ belongs to $\mathbb{C}(\Lambda)$. In fact, $\mathbb{C}(\Lambda)$ is generated by $\wp_\Lambda$ and $\wp'_\Lambda$, but we are not going to prove this here.

Proposition 3.4. *The Laurent expansion of $\wp_\Lambda(z)$ at $z = 0$ is*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n\geq 2,\ even} (n+1)G_{n+2}(\Lambda)z^n,$$

and it has radius of convergence equal to the lattice point closest to the origin.

Proof. See [3, Proposition 1.4.1]. □

These expansions allow us to find algebraic relations between $\wp_\Lambda$ and $\wp'_\Lambda$. Since

$$\wp_\Lambda = \frac{1}{z^2} + 3G_4(\Lambda)z^2 + O(z^4)$$

and

$$\wp'_\Lambda = \frac{-2}{z^3} + 6G_4(\Lambda)z + O(z^3),$$

we deduce:

$$(\wp'_\Lambda)^2 = \frac{4}{z^6} + O(z^{-2}) = 4(\wp_\Lambda)^3 + O(z^{-2}).$$

We can work with a couple more terms of the expansions, to get:

$$(\wp'_\Lambda)^2 = 4(\wp_\Lambda)^3 - 60G_4(\Lambda)\wp_\Lambda - 140G_6(\Lambda) + F(z), \quad F(z) = O(z^2).$$

Finally, note that $F(z)$ is Λ-periodic so by Liouville's theorem it must be constant 0.

Proposition 3.5. *Let $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$. Then:*

1. *The point $(\wp_\Lambda(z), \wp'_\Lambda(z))$ lies on the elliptic curve*

$$E_\Lambda \colon Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda).$$

2. *E_Λ can be written as $Y^2 = 4(X - e_1)(X - e_2)(X - e_3)$, where*

$$e_i = \wp_\Lambda(w_i/2), \quad w_3 = w_1 + w_2.$$

Moreover, this equation is nonsingular (that is, the e_i are all distinct).

Proof. It only remains to prove the second statement. Since $\wp'_\Lambda$ is odd and periodic, we get:

$$\wp'_\Lambda(w_i/2) = \wp'_\Lambda(-w_i/2) = -\wp'_\Lambda(w_i/2),$$

so $\wp'_\Lambda(w_i/2)$ is 0. Since $\wp_\Lambda$ takes the value e_i twice and $\wp_\Lambda$ has degree 2, it does not take the value e_i at any other points outside the 2-torsion. □

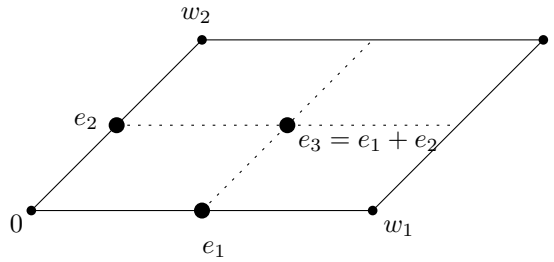

Figure 3.3: The 2-torsion points of E_Λ

To summarize, what we have found is that there is a holomorphic map:

$$\mathbb{C}/\Lambda \longrightarrow E_\Lambda, \quad z + \Lambda \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z)),$$

and this map is indeed a bijection: if $x \in \mathbb{C}$ is any complex number, then $\wp_\Lambda$ takes the value x twice, since $\wp_\Lambda(\pm z + \Lambda) = x$. Therefore we get two y-values unless $y = 0$ (which happens only when $z = w_i/2$). In this case, $\wp_\Lambda(z) = e_i$, and $\wp_\Lambda(z)$ takes the value e_i "twice" at z.

The following result is crucial:

Theorem 3.1. *If $E\colon Y^2 = 4X^3 - g_2X - g_3$ is any elliptic curve, then there exists some lattice Λ such that $g_2(\Lambda) = g_2$ and $g_4(\Lambda) = g_4$.*

Proof. It uses that $j(z)$ is surjective. See [3, Proposition 1.4.3] □

1. For $\tau \in \mathbb{H}$, consider the elliptic curve $E_\tau = E_{\Lambda_\tau}$.

$$E_\tau\colon Y^2 = 4X^3 - g_2(\tau)X - g_3(\tau).$$

   One can compute that the discriminant of the cubic polynomial on X that is the right-hand side is

$$\tilde{\Delta}(\tau) = \frac{1}{16}(g_2(\tau)^3 - 27g_3(\tau)^2),$$

   which equals $\frac{(2\pi)^{12}}{16}\Delta(\tau)$, where $\Delta(\tau)$ is the modular form already studied in

   1.

2. The map $\mathbb{C}/\Lambda \longrightarrow E_\Lambda$ is a group homomorphism. Or if we prefer, we may define the group structure on E_Λ via transport of structure.

3.2.3 Moduli space interpretation

Consider the set S of isomorphism classes of elliptic curves. Every elliptic curve is isomorphic to $\mathbb{C}/\Lambda$ for some lattice Λ, and in fact it is isomorphic to $\mathbb{C}/\Lambda_\tau$ for some $\tau \in \mathbb{H}$. Moreover,

$$\mathbb{C}/\Lambda_\tau \cong \mathbb{C}/\Lambda_{\tau'} \iff \mathrm{SL}_2(\mathbb{Z})\tau = \mathrm{SL}_2(\mathbb{Z})\tau'.$$

Therefore there is a natural bijection

$$S \longleftrightarrow \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}, \quad [\mathbb{C}/\Lambda_\tau] \mapsto \mathrm{SL}_2(\mathbb{Z})\tau.$$

The quotient $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is called the for isomorphism classes of elliptic curves.

Let now $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ be a modular form of weight k. Define the following function F on the set of complex tori:

$$F(\mathbb{C}/\Lambda_\tau) = f(\tau).$$

This is well defined, because if $\Lambda_\tau = \Lambda_{\tau'}$ then $\tau = \tau' + b$ for some $b \in \mathbb{Z}$, and $f(\tau + b) = f(\tau)$. Moreover, suppose that $m\Lambda_\tau = \Lambda_{\tau'}$. Then

$$\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau', \quad m = c\tau' + d.$$

Then we may compute:

$$F(\mathbb{C}/m\Lambda_\tau) = F(\mathbb{C}/\Lambda_{\tau'}) = f(\tau') = (c\tau' + d)^{-k} f(\tau) = F(\mathbb{C}/\Lambda_\tau)m^{-k}.$$

From this we deduce that

$$F(\mathbb{C}/m\Lambda) = m^{-k}F(\mathbb{C}/\Lambda).$$

We could thus define modular forms as functions on complex tori satisfying the above relations. This prototype can be pushed to work for other congruence subgroups, although isomorphism classes of elliptic curves will have to be replaced by objects carrying more data.

3.3 Moduli interpretation for $\Gamma_0(N)$ and $\Gamma_1(N)$

We will write $E[N]$ for the N-torsion in $E = \mathbb{C}/\Lambda$, which is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

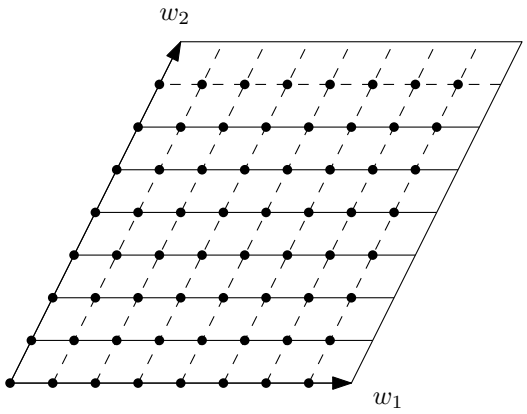

Figure 3.4: The 8-torsion of a complex torus $\mathbb{C}/(\mathbb{Z}w_1 + \mathbb{Z}w_2)$.

In order to give a moduli interpretation for modular forms on $\Gamma_0(N)$, we need to add more structure to the elliptic curves (or complex tori) that we consider.

Definition 3.4. An for $\Gamma_0(N)$ is a pair (E, C), where E is an elliptic curve and C is a cyclic subgroup of order N in $E[N]$. Two enhanced elliptic curves (E, C) and (E', C') are equivalent if there exists an isomorphism $\varphi\colon E \xrightarrow{\simeq} E'$ such that $\varphi(C) = C'$.

We write $S_0(N)$ for the set of equivalence classes of enhanced elliptic curves.

Theorem 3.2. *With the above notation,*

1. *Each class in $S_0(N)$ has a representative of the form $(\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle)$, for some $\tau \in \mathbb{H}$.*
2. *Two pairs $(\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle)$ and $(\mathbb{C}/\Lambda_{\tau'}, \langle \frac{1}{N} + \Lambda_{\tau'} \rangle)$ are equivalent if and only if $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Therefore the map $\tau \mapsto (\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle)$ induces a bijection of $Y_0(N) = \Gamma_0(N)\backslash\mathbb{H} \cong S_0(N)$.*

Proof. Consider an enhanced elliptic curve $(\mathbb{C}/\Lambda, C)$. We have already seen that there is an isomorphism $\varphi\colon \mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda_{\tau'}$ for some $\tau' \in \mathbb{H}$. Since C is cyclic of order N, the same is true for $\varphi(C)$. Therefore $(\mathbb{C}/\Lambda, C)$ is equivalent to $(\mathbb{C}/\Lambda_{\tau'}, \langle \frac{c\tau'+d}{N} + \Lambda_{\tau'}\rangle)$ for some integers c and d coprime to each other and to N. Since reduction modulo N gives a surjection $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N/ZZ)$, one can find a matrix

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

such that $c' \equiv c \pmod N$ and $d' \equiv d \pmod N$. Set now $\tau = \gamma\tau'$ and $m = c'\tau' + d'$, so $m\Lambda_\tau = \Lambda_{\tau'}$ and, as we wanted to show,

$$m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{c'\tau' + d'}{N} + \Lambda_{\tau'} = \frac{c\tau' + d}{N} + \Lambda_{\tau'},.$$

As for the second part, for an isomorphism between $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_{\tau'}$ to exist there needs to exist $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$(c\tau' + d)\Lambda_\tau = \Lambda_{\tau'}.$$

Moreover, for the corresponding isomorphism to respect the cyclic subgroups one needs to have

$$\langle (c\tau' + d)(\frac{1}{N} + \Lambda_\tau)\rangle = \langle \frac{1}{N} + \Lambda_{\tau'}\rangle.$$

That is, γ satisfies

$$\langle \frac{c\tau' + d}{N} + \Lambda_{\tau'}\rangle = \langle \frac{1}{N} + \Lambda_{\tau'}\rangle,$$

which is equivalent to $N \mid c$ (and then d is necessarily coprime to N). This last condition is precisely saying that γ must belong to $\Gamma_0(N)$. □

In this context, one may define a weight-k homogeneous function F for $\Gamma_0(N)$ as a function on enhanced elliptic curves for $\Gamma_0(N)$ such that

$$F((\mathbb{C}/m\Lambda, mC) = m^{-k}F(\mathbb{C}/\Lambda, C), \quad \forall m \in \mathbb{C}.$$

Given such an F, one can define $f(\tau) = F(\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau\rangle)$ and check that $f(\tau)$ is weakly modular of weight k for $\Gamma_0(N)$.

We have a similar construction for $\Gamma_1(N)$.

Definition 3.5. An for $\Gamma_1(N)$ is a pair (E, P), where E is an elliptic curve and P is a point of exact order N in $E[N]$. Two enhanced elliptic curves (E, P) and (E', P') are equivalent if there exists an isomorphism $\varphi\colon E \xrightarrow{\simeq} E'$ such that $\varphi(P) = P'$.

We write $S_1(N)$ for the set of equivalence classes of enhanced elliptic curves for $\Gamma_1(N)$.

Theorem 3.3. *With the above notation,*

1. *Each class in $S_1(N)$ has a representative of the form $(\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau)$, for some $\tau \in \mathbb{H}$.*
2. *Two pairs $(\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau)$ and $(\mathbb{C}/\Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'})$ are equivalent if and only if $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. Therefore the map $\tau \mapsto (\mathbb{C}/\Lambda_\tau, \frac{1}{N} + \Lambda_\tau)$ induces a bijection of $Y_1(N) = \Gamma_1(N)\backslash\mathbb{H} \cong S_1(N)$.*

Proof. Let (E, Q) be any point in $S_1(N)$. Since E is isomorphic to $\mathbb{C}/\Lambda_{\tau'}$ for some $\tau' \in \mathbb{H}$, we may take $E = \mathbb{C}/\Lambda_{\tau'}$, and hence $Q = (c\tau' + d)/N + \Lambda_{\tau'}$ for some $c, d \in \mathbb{Z}$. The fact that the order of Q is exactly N means that $\gcd(c, d, N) = 1$, and therefore there exists $a, b, k \in \mathbb{Z}$ such that

$$ad - bc - kN = 1.$$

Note that this means that the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant 1 (mod N). Using that $\mathrm{SL}_2(\mathbb{Z})$ surjects into $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and the fact that c and d only matter modulo N, we find a matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with lower low (c, d). Let $\tau = \gamma\tau'$, and let $m = c\tau' + d$. Then we obtain $m\tau = a\tau' + b$, which implies that $m\Lambda_\tau = \Lambda_{\tau'}$. Moreover,

$$m\,(1/N + \Lambda_\tau) = \frac{c\tau' + d}{N} + \Lambda_{\tau'} = Q.$$

Therefore the class $[E, Q]$ is the same as $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau]$.

Finally, given two points $\tau, \tau' \in \mathbb{H}$ such that $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$, we may write $\tau = \gamma\tau'$ for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$. Letting $m = c\tau' + d$, then:

$$m\Lambda_\tau = \Lambda_{\tau'}, \quad m\,(1/N + \Lambda_\tau) = \frac{c\tau' + d}{N} + \Lambda_{\tau'}.$$

Since $(c, d) \equiv (0, 1)$ (mod N), the last term is just $1/N + \Lambda_{\tau'}$, as we wanted to show. □

Moreover, note that there is a natural map $S_1(N) \longrightarrow S_0(N)$, which sends the class of (E, P) to that of $(E, \langle P \rangle)$.

There is a moduli space description of $\Gamma(N)\backslash\mathbb{H}$ which classifies pairs of an elliptic curve E with a *basis* for $E[N]$, but its precise description requires the Weil pairing, which we have not seen in this course.

4 Hecke Theory

4.1 Double coset operators

Let Γ_1 and Γ_2 be two congruence subgroups, and let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$.

Definition 4.1. The $\Gamma_1\alpha\Gamma_2$ is the set

$$\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 \mid \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}.$$

Multiplication gives a left action of Γ_1 on $\Gamma_1\alpha\Gamma_2$ and another right action of Γ_2. Consider a decomposition of this double coset into (disjoint) orbits:

$$\Gamma_1\alpha\Gamma_2 = \cup\Gamma_1\beta_j.$$

Lemma 4.1.

1. *If Γ is a congruence subgroup and $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, then $\alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z})$ is also congruence subgroup.*
2. *Any two congruence subgroups Γ_1, Γ_2 are . That is,*

$$[\Gamma_1 \colon \Gamma_1 \cap \Gamma_2] < \infty \quad \textit{and} \quad [\Gamma_2 \colon \Gamma_1 \cap \Gamma_2] < \infty.$$

Proof. Let N be a positive integer such that $\Gamma(N) \subseteq \Gamma$, $N\alpha \in M_2(\mathbb{Z})$ and $N\alpha^{-1} \in M_2(\mathbb{Z})$. Set $M = N^3$. Then one can check that $\alpha\Gamma(M)\alpha^{-1} \subseteq \Gamma(N)$, which implies that $\Gamma(M) \subseteq \alpha^{-1}\Gamma\alpha$. Since $\Gamma(M)$ is also contained in $\mathrm{SL}_2(\mathbb{Z})$, we are done with the first statement.

For the second assertion, just note that there is some M such that $\Gamma(M) \subseteq \Gamma_1 \cap \Gamma_2$. Therefore the indices to compute are bounded above by $[\mathrm{SL}_2(\mathbb{Z}) \colon \Gamma(M)]$, which is finite. □

Proposition 4.1. *Let Γ_1 and Γ_2 be two congruence subgroups, and let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. Set Γ_3 to be the congruence subgroup:*

$$\Gamma_3 = (\alpha^{-1}\Gamma_1\alpha) \cap \Gamma_2.$$

The map $\gamma_2 \mapsto \Gamma_1\alpha\gamma_2$ induces a bijection

$$\Gamma_3\backslash\Gamma_2 \cong \Gamma_1\backslash\Gamma_1\alpha\Gamma_2.$$

Proof. Consider the map

$$\Gamma_2 \longrightarrow \Gamma_1\backslash(\Gamma_1\alpha\Gamma_2), \quad \gamma_2 \mapsto \Gamma_1\alpha\gamma_2.$$

It is clearly surjective. Moreover, two elements γ_2 and γ_2' get mapped to the same orbit if and only if:

$$\Gamma_1\alpha\gamma_2 = \Gamma_1\alpha\gamma_2' \iff \gamma_2'\gamma_2^{-1} \in \alpha^{-1}\Gamma_1\alpha,$$

and the latter happens if and only if γ_2 and γ_2' are in the same coset for $(\alpha^{-1}\Gamma_1\alpha)\cap\Gamma_2 = \Gamma_3$. □

Corollary 4.1. *Let $\Gamma_2 = \cup\Gamma_3\gamma_j$ be a coset decomposition of $\Gamma_3\backslash\Gamma_2$. Then*

$$\Gamma_1\alpha\Gamma_2 = \cup\Gamma_1\alpha\gamma_j$$

is an orbit decomposition. In particular, the number of orbits of $\Gamma_1\alpha\Gamma_2$ under the action of Γ_1 is finite.

Let $f \in M_k(\Gamma_1)$ be a modular form of weight k for a congruence subgroup Γ_1. Let $\Gamma_1\alpha\Gamma_2$ be a double coset, where Γ_2 is a congruence subgroup and $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. The on f is defined as:

$$f|_k(\Gamma_1\alpha\Gamma_2) = \sum f|_k\beta_j,$$

if $\Gamma_1\alpha\Gamma_2 = \cup\Gamma_1\beta_j$ is any orbit decomposition.

The action is well defined, independent of the choice of the β_j. This is so because f is k-invariant under Γ_1.

The next goal is to show that the double coset operator maps $M_k(\Gamma_1)$ to $M_k(\Gamma_2)$ and preserves cusps forms. We will need a technical lemma to treat the cusp conditions.

Lemma 4.2. *Suppose that for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the function $f|_k\gamma$ has an expansion of the form*

$$\sum_{n\geq n_0} a(n)q_N^n,$$

with n_0 and $a(n)$ depending on γ. Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. Then for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the function $f|_k(\alpha\gamma)$ has the expansion

$$\sum_{n\geq an_0} b(n)q_{Nd}^n,$$

where a and d are positive integers depending only on α.

Proof. First, note that, for $a > 0$,

$$f|_k\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a^{2(k-1)}a^{-k}f = a^{k-2}f.$$

So without loss of generality we may assume that $\alpha \in M_2(\mathbb{Z})$. Let $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$ be such that $\gamma_0^{-1}\alpha = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ (upper-triangular), with a and d being positive integers. Then:

$$f|_k\alpha = (f|_k\gamma_0)|_k \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \left(\sum_{n\geq n_0} a(n)e^{\frac{2\pi i n z}{N}}\right)|_k \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$
$$= (\cdots)\sum_{n\geq n_0} a(n)e^{\frac{2\pi i n(az+b)}{dN}} = (\cdots)q_{Nd}^{an_0} + \cdots$$

This concludes the proof. □

Proposition 4.2. *Let Γ_1 and Γ_2 be two congruence subgroups, and let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. The rule $f \mapsto f|_k\Gamma_1\alpha\Gamma_2$ induces a map $M_k(\Gamma_1) \longrightarrow M_k(\Gamma_2)$.*

Proof. Write $\Gamma_3 = (\alpha^{-1}\Gamma_1\alpha) \cap \Gamma_2$, and consider a coset decomposition $\Gamma_2 = \cup\Gamma_3\gamma_j$. One can take as set of representatives $\beta_j = \alpha\gamma_j$. If $\gamma_2 \in \Gamma_2$, then $\{\gamma_j\gamma_2\}_j$ is a complete set of representatives for $\Gamma_3\backslash\Gamma_2$, and hence $\{\alpha\gamma_j\gamma_2\}_j$ is a complete set of representatives for $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$. This implies that $f|_k\Gamma_1\alpha\Gamma_2$ is k-invariant for Γ_2.

If f is holomorphic on $\mathbb{H}$, then $f|_k\beta_j$ is holomorphic on $\mathbb{H}$ for any $\beta_j \in \mathrm{GL}_2^+(\mathbb{Q})$, so it only remains to check the cusp conditions. But Lemma 4.2 precisely ensures that these are preserved. □

4.1.1 First examples

Consider the case $\Gamma_2 \subseteq \Gamma_1$ and $\alpha = 1$. Then $\Gamma_1\alpha\Gamma_2 = \Gamma_1$, and $\Gamma_1 = \Gamma_1 1$ is an orbit decomposition. Therefore $f|_k\Gamma_1\alpha\Gamma_2 = f|_k 1 = f$. This just says that $M_k(\Gamma_1)$ is a subspace of $M_k(\Gamma_2)$.

As a more interesting example, given $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ consider the conjugate $\Gamma' = \alpha^{-1}\Gamma\alpha$. Then $\Gamma\alpha\Gamma' = \Gamma\alpha$ is an orbit decomposition. This implies that acting by α induces a map

$$M_k(\Gamma) \longrightarrow M_k(\alpha^{-1}\Gamma\alpha).$$

Since the inverse of this map is given by the action of α^{-1}, we conclude that $M_k(\Gamma)$ and $M_k(\alpha^{-1}\Gamma\alpha)$ are naturally isomorphic.

Finally, consider the case $\Gamma_1 \subseteq \Gamma_2$ and $\alpha = 1$. Then $\Gamma_1\alpha\Gamma_2 = \cup\Gamma_1\beta_j$, where β_j is a set of coset representatives for $\Gamma_1\backslash\Gamma_2$. The map

$$f \mapsto \sum_j f|_k\beta_j$$

is to be seen as a *trace operator* from $M_k(\Gamma_1) \longrightarrow M_k(\Gamma_2)$. In particular, it maps $f \in M_k(\Gamma_2)$ to $[\Gamma_2 : \Gamma_1]f$ and thus it is surjective.

4.2 Hecke operators for $\Gamma_1(N)$

Fix now $\Gamma = \Gamma_1(N)$. We will describe the Hecke operators for the group Γ.

4.2.1 The T_p operators

Let p be a prime. The at p is defined as:

$$T_p f = f|_k \Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N).$$

By Proposition 4.2, the operator T_p acts on $M_k(\Gamma_1(N))$.

In order to describe the action of T_p more precisely, we need to understand the double coset $\Gamma_1(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma_1(N)$. Note first that if $\gamma \in \Gamma_1(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma_1(N)$ then:

1. $\det \gamma = p$, and
2. $\gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & p \end{smallmatrix}\right) \pmod N$.

In fact, the converse is true:

Lemma 4.3. *We have that*

$$\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) = \left\{ \gamma \in M_2(\mathbb{Z}) \mid \det \gamma = p, \gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & p \end{smallmatrix}\right) \pmod N \right\}.$$

Proof. To prove the remaining inclusion, let $\gamma \in M_2(\mathbb{Z})$ have determinant p, and satisfy $\gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & p \end{smallmatrix}\right) \pmod N$. Consider $L = \mathbb{Z}^2$ and

$$L_0 = L_0(N) = \{ \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in L \colon y \equiv 0 \pmod N \}.$$

Note that $\gamma L_0 \subseteq L_0$. Since $\det \gamma = p > 0$, we have:

$$[L \colon \gamma L_0] = [L \colon L_0][L_0 \colon \gamma L_0] = Np.$$

Choose a basis of L adapted to γL_0. That is, a basis u, v such that $\det(u|v) = 1$ and such that

$$\gamma L_0 = mu\mathbb{Z} \oplus nv\mathbb{Z}, \text{ with } 0 < m \mid n, mn = Np.$$

We will show:

1. $\gamma L_0 = u\mathbb{Z} \oplus Npv\mathbb{Z}$.
2. $L_0 = u\mathbb{Z} \oplus Nv\mathbb{Z}$.
3. $\gamma L = u\mathbb{Z} + pv\mathbb{Z}$.

In fact, since $\gamma\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) \in \gamma L_0$, we have that $\left(\begin{smallmatrix}a\\b\end{smallmatrix}\right) \equiv \left(\begin{smallmatrix}0\\0\end{smallmatrix}\right) \pmod{m}$. Since $\gcd(a, N) = 1$, this implies that $\gcd(m, N) = 1$. Now, if $p \mid m$, then $p \mid n$, and so $p^2 \mid mn = Np$. Therefore $p \mid N$, which is a contradiction with $\gcd(m, N) = 1$. Therefore $p \nmid m$ and hence $m = 1$ and $n = Np$.

The two other facts follow because $L_0 \subset L$ is a subgroup of index N, and $\gamma L \subset L$ is of index p in L. This proves the above three statements.

Next, set $\gamma_1 = (u|v)$, which belongs to $\Gamma_0(N)$ because u belongs to L_0. Set also $\gamma_2 = (\gamma_1 \left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right))^{-1}\gamma$, so that $\gamma = \gamma_1 \left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right) \gamma_2$. Note that γ_2 belongs to $\mathrm{SL}_2(\mathbb{Q})$. It remains to show that γ_1 and γ_2 belong to $\Gamma_1(N)$. This will follow if we can prove:

1. $\gamma_2 \in \Gamma_0(N)$.
2. $\Gamma_0(N) \left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right) \Gamma_0(N) = \Gamma_1(N) \left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right) \Gamma_0(N)$.
3. If $\gamma = \gamma_1 \left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right) \gamma_2$ with $\gamma_1 \in \Gamma_1(N)$ and $\gamma_2 \in \Gamma_0(N)$, then γ_2 belongs to $\Gamma_1(N)$.

Each of these statements can be easily proved, and we ommit these proofs. □

Proposition 4.3. *Let $f \in M_k(\Gamma_1(N))$. Then $T_p f$ is given by:*

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} & p \mid N, \\ \sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} + f|_k \begin{pmatrix} mp & n \\ Np & p \end{pmatrix} & p \nmid N. \end{cases}$$

Here the matrix $\left(\begin{smallmatrix}mp&n\\Np&p\end{smallmatrix}\right)$ is chosen such that $\gamma_\infty = \left(\begin{smallmatrix}mp&n\\N&1\end{smallmatrix}\right)$ belongs to $\Gamma_1(N)$.

Proof. We just need to trace the definition of the double coset operator. That is, we need to find an explicit coset decomposition of $\Gamma_3 \backslash \Gamma_1(N)$, where

$$\Gamma_3 = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}^{-1} \Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \cap \Gamma_1(N).$$

Define $\Gamma^0(p)$ to be the group of matrices which are lower triangular modulo p. It is easy to see that

$$\Gamma_3 = \Gamma_1(N) \cap \Gamma^0(p).$$

Consider the matrices $\gamma_j = \left(\begin{smallmatrix}1&j\\0&1\end{smallmatrix}\right)$, with j ranging from 0 to $p-1$ inclusive. These are all distinct modulo $\Gamma_1(N) \cap \Gamma^0(p)$ (check it). Given any matrix $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right) \in \Gamma_1(N)$, note that

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

Therefore if $p \nmid a$ we can make the right-hand side to belong to $\Gamma^0(p)$ for some j. This means that if p divides N then p will not divide a (because of the determinant condition), and thus

the set $\{\gamma_j\}$ is a complete set of representatives. If $p \nmid N$, we need to consider matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $p \mid a$. Choose some $\gamma_\infty = \left(\begin{smallmatrix} mp & n \\ N & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$. Then:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma_\infty^{-1} = \begin{pmatrix} * & -na + bmp \\ 0 & * \end{pmatrix}.$$

Since p divides $-na + bmp$, the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is in the coset of γ_∞ modulo $\Gamma^0(p)$. Hence $\{\gamma_j\} \cup \{\gamma_\infty\}$ forms a complete set of representatives. In order to get the orbit representatives for the double coset, we just need to multiply the γ_j by the fixed element $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. □

4.2.2 The diamond $\langle d \rangle$ operators

We define another (finite) set of operators on $M_k(\Gamma_1(N))$, called the diamond operators. First we need some preliminaries on characters.

Definition 4.2. A modulo N is a group homomorphism

$$\chi \colon (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times.$$

It can be extended to a map $\chi \colon \mathbb{Z} \longrightarrow \mathbb{C}$ by the recipe

$$\chi(d) = \begin{cases} \chi(d \bmod N) & (d, N) = 1 \\ 0 & (d, N) \neq 1. \end{cases}$$

The resulting function is totally multiplicative: it satisfies

$$\chi(d_1 d_2) = \chi(d_1)\chi(d_2) \quad \forall d_1, d_2 \in \mathbb{Z}.$$

Consider the map $\Gamma_0(N) \longrightarrow \mathbb{Z}/N\mathbb{Z}^\times$ sending a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to $d \bmod N$. Its kernel is precisely $\Gamma_1(N)$, and therefore we obtain an isomorphism

$$\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/NZ)^\times, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Gamma_1(N) \mapsto d \bmod N.$$

Definition 4.3. Given $d \in \mathbb{Z}$ coprime to N, the $\langle d \rangle$ is the operator on $M_k(\Gamma_1(N))$ defined as

$$\langle d \rangle f = f|_k \begin{pmatrix} a & b \\ c & d' \end{pmatrix},$$

where a, b, c, d' are chosen so that $\left(\begin{smallmatrix} a & b \\ c & d' \end{smallmatrix}\right)$ belongs to $\Gamma_0(N)$ and $d' \equiv d \pmod N$.

Note that the above is well defined, and only depends on the class of d modulo N. This is precisely because $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/NZ)^\times$. The operator $\langle d \rangle$ is a linear invertible map, and thus it makes sense to look at its eigenspaces.

Definition 4.4. The *space of modular forms with character* χ is

$$M_k(\Gamma_0(N), \chi) = \{f \in M_k(\Gamma_1(N)) \mid f|_k \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \chi(d)f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)\}.$$

The χ is defined similarly and written $S_k(\Gamma_0(N), \chi)$.

Note that $M_k(\Gamma_0(N), \chi)$ can also be defined as

$$M_k(\Gamma_0(N), \chi) = \{f \in M_k(\Gamma_1(N)) \mid \langle d \rangle f = \chi(d)f, \quad d \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$

Theorem 4.1. *There is a decomposition of* $\mathbb{C}$*-vector spaces*

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi \bmod N} M_k(\Gamma_0(N), \chi),$$

where the sum runs over the $\phi(N) = \#(\mathbb{Z}/N\mathbb{Z})^\times$ *Dirichlet characters modulo* N*.*

Proof. Picking a basis of $M_k(\Gamma_1(N))$, we get a representation

$$\rho \colon (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathrm{GL}_n(\mathbb{C}), \quad \rho(d) = \langle d \rangle,$$

where n is the dimension of $M_k(\Gamma_1(N))$. Since $(\mathbb{Z}/N\mathbb{Z})^\times$ is abelian, the representation ρ decomposes as a sum of irreducible representations, which are necessarily one-dimensional. This means that we can pick a basis for $M_k(\Gamma_1(N))$ such that

$$\rho(d) = \mathrm{diag}(\chi_1(d), \dots, \chi_n(d)).$$

This means that $\langle d \rangle$ acts as $\chi_i(d)$ on the ith component. One just needs to collect then the repeated χ to form $M_k(\Gamma_0(N), \chi)$. □

4.2.3 Hecke operators on q-expansions

In order to study the action of Hecke operators on q-expansion, we introduce two simple operators: if $f = \sum a_n q^n$, define:

$$U_p f = \sum a_{np} q^n = \sum a_n q^{n/p}.$$

The second equality is an abuse of notation: we define $q^{n/p} = 0$ if $p \nmid n$. We define also:

$$V_p f = f(pz) = \sum a_n q^{np} = \sum a_{n/p} q^n.$$

Lemma 4.4. *If* $f = \sum a_n q^n$*, then*

1. $$U_p f = \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) = \sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}.$$

2.

$$V_p f = p^{1-k} f|_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

Proof. Note that if $\zeta_p = e^{\frac{2\pi i}{p}}$ is a primitive pth root of unity, then

$$\sum_{j=0}^{p-1} \zeta_p^{nj} = \begin{cases} p & p \mid n \\ 0 & p \nmid n. \end{cases}$$

Now compute:

$$\sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} = p^{k-1} p^{-k} \sum_j f\left(\frac{z+j}{p}\right).$$

Since f is 1-periodic, this is the same as:

$$\frac{1}{p} \sum_j \sum_n a_n e^{2\pi i \frac{z+j}{p}} = \sum_n a_n e^{\frac{2\pi i n z}{p}} \frac{1}{p} \sum_j \zeta_p^{nj}.$$

This proves the first statement. The second statement is clear. □

Putting together what we have seen so far, we get a description of T_p in terms of U_p, V_p and the diamond operators.

Theorem 4.2. *We have:*

$$T_p f = \begin{cases} U_p f & p \mid N, \\ U_p f + p^{k-1} V_p \langle p \rangle f & p \nmid N. \end{cases}$$

Corollary 4.2. *If $f \in M_k(\Gamma_0(N), \chi)$ then for all p we have:*

$$T_p f = U_p f + \chi(p) p^{k-1} V_p f.$$

In particular, if $f \in M_k(\Gamma_0(N))$ then:

$$T_p f = \begin{cases} U_p f & p \mid N, \\ U_p f + p^{k-1} V_p f & p \nmid N. \end{cases}$$

Moreover, the relation between U_p and T_P allows us to think of U_p as an operator on modular forms, which possibly raises the level.

Corollary 4.3.

1. *If $p \mid N$ then U_p maps $M_k(\Gamma_1(N))$ to itself.*

2. If $p \nmid N$ then U_p maps $M_k(\Gamma_1(N))$ to $M_k(\Gamma_1(Np))$.

Example 4.1. Consider the Eisenstein series

$$E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \in M_k(\Gamma_1(1)).$$

Proposition 4.4. *We have:*

$$T_p E_k = \sigma_{k-1}(p) E_k = (1 + p^{k-1}) E_k.$$

That is, E_k is an eigenform for all T_p, with eigenvalue $\sigma_{k-1}(p)$.

Proof. In general we have seen that, since $E_k \in M_k(\Gamma_0(1)))$,

$$a_n(T_p f) = a_n(U_p f) + p^{k-1} a_n(V_p f) = a_{np}(f) + p^{k-1} a_{n/p}(f).$$

So

$$a_0(T_p E_k) = a_0(E_k) + p^{k-1} a_0(E_k) = \sigma_{k-1}(p) a_0(E_k).$$

For $n \geq 1$, we get

$$a_n(T_p E_k) = \frac{-2k}{B_k} \left(\sigma_{k-1}(np) + p^{k-1} \sigma_{k-1}(n/p) \right),$$

where we understand that $\sigma_{k-1}(n/p) = 0$ if $p \nmid n$. We claim that:

$$\sigma_{k-1}(pn) + p^{k-1} \sigma_{k-1}(n/p) = \sigma_{k-1}(p) \sigma_{k-1}(n), \quad \forall n \geq 1.$$

When $p \nmid n$, this is just the multiplicativity of σ_{k-1}. If $p \mid n$, write $n = p^e m$ with $p \nmid m$. Then we need to show that for all $e \geq 1$

$$\sigma_{k-1}(p^{e+1} m) + p^{k-1} \sigma_{k-1}(p^{e-1} m) = \sigma_{k-1}(p) \sigma_{k-1}(p^e m).$$

This follows easily by dividing both sides by $\sigma_{k-1}(m)$, which is a common factor of both sides of the equation again by multiplicativity of σ_{k-1}. □

If $f = 1 + \sum_{n \geq 1} a_n q^n$ is a modular form for $\mathrm{SL}_2(\mathbb{Z})$ of weight k and it is an eigenform for T_p, then the eigenvalue must be $\sigma_{k-1}(p)$, by the first calculation of the above proof. The real content of the proposition is thus that E_k is actually an eigenform.

4.3 The Hecke algebra

Definition 4.5. Let $N \geq 1$ and $k \in \mathbb{Z}$. The acting on $M_k(\Gamma_1(N))$ is the $\mathbb{C}$-subalgebra of $\mathrm{End}_{\mathbb{C}} M_k(\Gamma_1(N))$ generated by

$$\Big\langle T_p \colon p \text{ prime; and } \langle d \rangle \colon d \in (\mathbb{Z}/N\mathbb{Z})^\times \Big\rangle.$$

The Hecke algebra is denoted by $\mathbb{T}(M_k(\Gamma_1(N)))$. Similarly we define $\mathbb{T}(S_k(\Gamma_1(N)))$ as a subalgebra of $\mathrm{End}_{\mathbb{C}} S_k(\Gamma_1(N))$.

Theorem 4.3. *For every $N \geq 1$ the Hecke algebra $\mathbb{T}(M_k(\Gamma_1(N)))$ is commutative.*

Proof. We must show that for all primes p, q and all elements e and d of $(\mathbb{Z}/N\mathbb{Z})^\times$ we have:

1. $\langle d \rangle T_p = T_p \langle d \rangle$,
2. $\langle d \rangle \langle e \rangle = \langle e \rangle \langle d \rangle$, and
3. $T_p T_q = T_q T_p$.

First we show (2) and (3) assuming (1). Note that (1) means that T_p preserves the spaces $M_k(\Gamma_0(N), \chi)$ and so it's enough to check (2) and (3) for forms $f \in M_k(\Gamma_0(N), \chi)$. This makes (2) obvious. As for (3), we can use the q-expansions: if $f = \sum a_n q^n$, then

$$a_n(T_p f) = a_{pn}(f) + \chi(p) p^{k-1} a_{n/p}(f).$$

Then:

$$\begin{aligned} a_n(T_p T_q f) &= a_{pn}(T_q f) + \chi(p) p^{k-1} a_{n/p}(T_q f) \\ &= a_{pqn}(f) + \chi(q) q^{k-1} a_{pn/q}(f) + \chi(p) p^{k-1} (a_{nq/p}(f) + \chi(q) q^{k-1} a_{n/(pq)}(f)). \end{aligned}$$

This formula is symmetric in p and q so we are done.

Finally, to prove (1) we must write $\langle d \rangle$ as a double coset. Let $\gamma \equiv \left(\begin{smallmatrix} * & * \\ 0 & d \end{smallmatrix}\right) \pmod{N}$. Write $\Gamma = \Gamma_1(N)$. Then, since Γ is normal in $\Gamma_0(N)$, we have

$$\Gamma \gamma \Gamma = \Gamma \gamma,$$

and thus $\langle d \rangle f = f|_k \gamma$. We want to show that $\langle d \rangle^{-1} T_p \langle d \rangle = T_p$. Write $\Gamma \alpha \Gamma = \bigcup_j \Gamma \beta_j$ for the orbit decomposition of the double coset corresponding to T_p. We thus need to show that

$$\Gamma \alpha \Gamma = \bigcup_j \Gamma(\gamma \beta_j \gamma^{-1}).$$

We note that

$$\bigcup_j \Gamma(\gamma\beta_j\gamma^{-1}) = \gamma\left(\bigcup_j \Gamma\beta_j\right)\gamma^{-1} = \gamma(\Gamma\alpha\Gamma)\gamma^{-1} = \Gamma(\gamma\alpha\gamma^{-1})\Gamma,$$

and one just checks then that

$$\Gamma\alpha\Gamma = \Gamma(\gamma\alpha\gamma^{-1})\Gamma.$$

□

Next, we define operators T_n and $\langle n\rangle$ for all $n \geq 1$. First, define $\langle p\rangle = 0$ whenever $p \mid N$. One can implicitly define T_n by the following formula:

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_p \frac{1}{1 - T_p p^{-s} + \langle p\rangle p^{k-1-2s}}.$$

This in turn is equivalent to the following conditions:

1. $T_{nm} = T_n T_m$ if $(n, m) = 1$,
2. $T_1 = \mathrm{id}$, and
3. for all primes p and for all $r \geq 2$,

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}}.$$

From the definition we can see that each T_n is an explicit polynomial on the T_p, and therefore all T_n commute with each other.

Theorem 4.4. *Suppose $f \in M_k(\Gamma_1(N))$ has an expansion of the form $\sum a_m(f)q^m$. Then $T_n(f) = \sum a_m(T_n f)q^m$, where*

$$a_m(T_n f) = \sum_{d|(m,n)} d^{k-1} a_{\frac{mn}{d^2}}(\langle d\rangle f).$$

In particular, if $f \in M_k(\Gamma_0(N), \chi)$ then

$$a_m(T_n f) = \sum_{d|(m,n)} \chi(d) d^{k-1} a_{\frac{mn}{d^2}}(f).$$

Proof. A long computation. □

We end this section with the notion of Hecke eigenforms.

Definition 4.6. A (or just eigenform) is a non-zero modular form $f \in M_k(\Gamma_1(N))$ which is an eigenvector for all the Hecke algebra $\mathbb{T}(M_k(\Gamma_1(N))$. A (or normalized eigenform) is an eigenform satisfying $a_1(f) = 1$.

Let $f \in M_k(\Gamma_1(N))$ be an eigenform, say $T_n f = \lambda_n f$ for all n. Then we obtain

$$a_n(f) = a_1(T_n f) = \lambda_n a_1(f), \quad n \geq 1.$$

So if $a_1(f) = 0$ then all $a_n(f) = 0$ and thus $f = 0$. Therefore a non-constant non-zero eigenform must have $a_1(f) \neq 0$ and it may be scaled to a normalized eigenform. In particular, we have the following.

Theorem 4.5. *Let $f \in M_k(\Gamma_1(N))$ be a normalized eigenform. Then the eigenvalues of the Hecke operators on f are precisely the coefficients of the q-expansion of f at the cusp ∞:*

$$T_n f = a_n(f) f, \quad n \geq 1. \tag{4.1}$$

Proof. Write λ_n for the eigenvalue of the Hecke operator T_n. By Equation 4.1 we have $a_n(f) = a_1(T_n f) = \lambda_n a_1(f)$. Since f is normalized, $a_1(f) = 1$ and hence $a_n(f) = \lambda_n$. □

In fact, the Fourier coefficients of a modular form readily tell whether it is a normalized eigenform:

Proposition 4.5. *Let $f \in M_k(\Gamma_0(N), \chi)$ be a modular form with q-expansion $\sum_{n=0}^{\infty} a_n(f) q^n$. Then f is a normalized eigenform if and only if:*

1. $a_1(f) = 1$,
2. $a_{mn}(f) = a_m(f) a_n(f)$ *whenever* $(m, n) = 1$, *and*
3. $a_{p^r}(f) = a_p(f) a_{p^{r-1}}(f) - p^{k-1} \chi(p) a_{p^{r-2}}(f), \quad r \geq 2.$

Proof. The implication $\implies$ follows directly from the previous proposition and the definition of the Hecke operators T_n. For the converse, if $f \in M_k(\Gamma_0(N), \chi)$ satisfies (1), (2) and (3) then f is already normalized, so to be an eigenform we must show that it satisfies

$$a_m(T_p f) = a_p(f) a_m(f), \quad \forall p \text{ prime}, \forall m \geq 1.$$

If $p \nmid n$ then it follows from the formula that we have for T_m on q-expansions that $a_m(T_p f) = a_{pm}(f)$, which by (2) is $a_p(f) a_m(f)$. If $p \mid m$ then writing $m = p^r m'$ with $r \geq 1$ and $p \nmid m'$ we have by the same formula

$$a_m(T_p f) = a_{p^{r+1} m'}(f) + \chi(p) p^{k-1} a_{p^{r-1} m'}(f).$$

Using now conditions (2) and (3) this can be rewritten as $a_p(f) a_m(f)$, as wanted. □

4.4 Petersson inner product

4.4.1 Surface integrals

Let $V \subseteq \mathbb{C}$. A 2-form on V is an expression of the form $\omega = f(z, \bar{z})dz \wedge d\bar{z}$. Note that

$$dz \wedge d\bar{z} = (dx + idy) \wedge (dx - idy) = -2idx \wedge dy.$$

The integral of ω on V is:

$$\int_V \omega = \int_V f(z, \bar{z}dz \wedge d\bar{z} = \int \int -2if(x + iy, x - iy)dxdy.$$

Consider now, for $\alpha \in \mathrm{GL}_2^+(\mathbb{R})$, the change $z \mapsto \alpha z$. Then:

$$\Im(\alpha z) = \frac{\det \alpha}{|cz + d|^2}\Im(z),$$

and also

$$d(\alpha z) = \frac{\det \alpha}{(cz + d)^2}dz, \quad \overline{d(\alpha z)} = \frac{\det \alpha}{\overline{(cz + d)^2}}d\bar{z}.$$

This gives that:

$$d(\alpha z) \wedge d\overline{\alpha z} = \frac{(\det \alpha)^2}{|cz + d|^4}dz \wedge d\bar{z}.$$

Therefore the 2-form $\frac{dz \wedge d\bar{z}}{\Im(z)^2}$ is invariant under changes of the form $z \mapsto \alpha z$. We will work instead with a certain multiple of this 2-form. Define

$$d\mu(z) = \frac{dx \wedge dy}{y^2} = \frac{-1}{2i}\frac{dz \wedge d\bar{z}}{\Im(z)^2}.$$

We can define the of $\mathrm{SL}_2(\mathbb{Z})$ as

$$\mathrm{covol}(\mathrm{SL}_2(\mathbb{Z})) = \int_{D^*} d\mu(z).$$

where D^* is a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$.

Lemma 4.5.

$$\mathrm{covol}(\mathrm{SL}_2(\mathbb{Z})) = \frac{\pi}{3}.$$

Proof. Exercise. □

Corollary 4.4. *If φ is a bounded function on D^*, then $\int_{D^*} \varphi(z)d\mu(z)$ is a well-defined complex number.*

4.4.2 Integral over $X(\Gamma)$

Let $\mathcal{D}$ be a fundamental domain for a congruence subgroup Γ. Such a fundamental domain is the union (almost disjoint) of translates of D^*:

$$\mathcal{D} = \cup_j \alpha_j D^*,$$

where $\{\alpha_j\}$ is a set of coset representatives for $(\pm 1 \cdot \Gamma)\backslash \mathrm{SL}_2(\mathbb{Z})$. If φ is Γ-invariant, then we may define the integral of φ on $X(\Gamma) = \Gamma\backslash\mathbb{H}$ as:

$$\int_{X(\Gamma)} \varphi(\tau) d\mu(\tau) = \sum_j \int_{\alpha_j D^*} \varphi(\tau) d\mu(\tau) = \sum_j \int_{D^*} \varphi(\alpha_j \tau) d\mu(\alpha_j \tau) = \sum_j \int_{D^*} \varphi(\alpha_j \tau) d\mu(\tau).$$

The last term in the above equality shows that the definition is independent of the choice of coset representatives. We may calculate the covolume of Γ as:

Lemma 4.6. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. Then*

$$\mathrm{covol}(\Gamma) = \int_{X(\Gamma)} d\mu(\tau) = [\mathrm{PSL}_2(\mathbb{Z}) \colon \overline{\Gamma}]\mathrm{covol}(\mathrm{SL}_2(\mathbb{Z})) = \frac{\pi}{3}[\mathrm{PSL}_2(\mathbb{Z}) \colon \overline{\Gamma}].$$

Let f and g be two cusp forms for Γ of weight k, and set $\varphi(\tau) = f(\tau)\overline{g(\tau)}\mathfrak{I}(\tau)^k$.

Lemma 4.7. *The function φ is Γ-invariant and, for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, the translate $\varphi(\alpha\tau)$ is bounded on D^*.*

Proof. If γ belongs to Γ, then we may compute:

$$\varphi(\gamma\tau) = f|_k \gamma j(\gamma,\tau)^{-k} \overline{g|_k \gamma j(\gamma,\tau)^{-k}} j(\gamma,\tau)^{2k} \mathfrak{I}(z)^k = \varphi(\tau).$$

If α belongs to $\mathrm{SL}_2(\mathbb{Z})$, then:

$$\varphi(\alpha\tau) = f|_k \alpha \overline{g|_k \alpha} \mathfrak{I}(\tau)^k = O(q_h)\overline{O(q_h)} y^k = O(|q_h|^2 y^k).$$

This approaches 0 as y approaches infinity, because $q_h = e^{\frac{2\pi i(x+iy)}{z}}$. This gives boundedness. □

The previous lemma allows us to define an inner product on the spaces of cusp forms:

Definition 4.7. The of f and g is:

$$\langle f, g \rangle_\Gamma = \frac{1}{\mathrm{covol}(\Gamma)} \int_{X(\Gamma)} f(\tau)\overline{g(\tau)}\mathfrak{I}(\tau)^k d\mu(\tau).$$

For the above to converge it is enough that one of the forms f and g is in S_k. Therefore the product of a modular form with a cusp form is well defined.

The reason to divide by $\mathrm{covol}(\Gamma)$ is that, in this way, if $\Gamma \subseteq \Gamma'$ then

$$\langle f, g\rangle_\Gamma = \langle f, g\rangle_{\Gamma'}.$$

Proposition 4.6. *The Petersson inner product is a positive-definite hermitian product on the $\mathbb{C}$-vector space $S_k(\Gamma)$. That is:*

1. $\langle a_1 f_1 + a_2 f_2, g\rangle_\Gamma = a_1\langle f_1, g\rangle_\Gamma + a_2\langle f_2, g\rangle_\Gamma$.
2. $\langle g, f\rangle_\Gamma = \overline{\langle f, g\rangle_\Gamma}$.
3. $\langle f, f\rangle \geq 0$, *with equality if and only if* $f = 0$.

Although the Petersson inner product does not extend to all of $M_k(\Gamma)$, it still allows us to define an "orthogonal complement to $S_k(\Gamma)$:

Definition 4.8. The of $M_k(\Gamma)$ is the space

$$\mathcal{E}_k(\Gamma) = \{f \in M_k(\Gamma) \mid \langle f, g\rangle_\Gamma = 0 \quad \forall g \in S_k(\Gamma)\}.$$

4.4.3 Adjoint operators

If $\langle\cdot,\cdot\rangle$ is an hermitian product on a $\mathbb{C}$-vector space V and $T\colon V \longrightarrow V$ is a linear operator, the of T is defined as the operator T^* which satisfies:

$$\langle Tf, g\rangle = \langle f, T^* g\rangle.$$

The goal of this subsection is to calculate the adjoint operators to the Hecke operators. We will need the following technical result.

Lemma 4.8. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$.*

1. *If $\varphi\colon \mathbb{H} \longrightarrow \mathbb{C}$ is continuous, bounded and Γ-invariant then:*

$$\int_{\alpha^{-1}\Gamma\alpha\backslash\mathbb{H}} \varphi(\alpha\tau)d\mu(\tau) = \int_{\Gamma\backslash\mathbb{H}} \varphi(\tau)d\mu(\tau).$$

2. *If $\alpha^{-1}\Gamma\alpha$ is contained in $\mathrm{SL}_2(\mathbb{Z})$ then Γ and $\alpha^{-1}\Gamma\alpha$ have equal covolumes and indices in $\mathrm{SL}_2(\mathbb{Z})$.*

3. *Let* $n = [\Gamma : \alpha^{-1}\Gamma\alpha \cap \Gamma] = [\Gamma : \alpha\Gamma\alpha^{-1} \cap \Gamma]$. *There are matrices* $\beta_1, \dots, \beta_n \in \mathrm{GL}_2^+(\mathbb{Q})$ *inducing disjoint unions*

$$\Gamma\alpha\Gamma = \bigcup \Gamma\beta_j = \bigcup \beta_j\Gamma.$$

Proof. The first two statements are easy and follow from the change of variables formula and Lemma 4.6. The equality of indices in (3) follows by applying (2) to $\alpha\Gamma\alpha^{-1} \cap \Gamma$ instead of Γ and using multiplicativity of indices. Therefore there exist $\gamma_1, \dots \gamma_n$ and $\tilde{\gamma}_1, \dots, \tilde{\gamma}_n$ in Γ such that

$$\Gamma = \bigcup (\alpha^{-1}\Gamma\alpha \cap \Gamma)\gamma_j = \bigcup (\alpha\Gamma\alpha^{-1} \cap \Gamma)\tilde{\gamma}_j^{-1}.$$

By how coset representatives are linked to orbit representatives in a double coset, we get:

$$\Gamma\alpha\Gamma = \bigcup \Gamma\alpha\gamma_j, \quad \Gamma\alpha^{-1}\Gamma = \bigcup \Gamma\alpha^{-1}\tilde{\gamma}_j^{-1}.$$

By taking inverses in the second decomposition we get

$$\Gamma\alpha\Gamma = \bigcup \tilde{\gamma}_j\alpha\Gamma.$$

Suppose that $\Gamma\alpha\gamma_j \cap \tilde{\gamma}_j\alpha\Gamma = \emptyset$. Then

$$\Gamma\alpha\gamma_j \subset \bigcup_{i \neq j} \tilde{\gamma}_i\alpha\Gamma.$$

Multiply from the right by Γ to get $\Gamma\alpha\Gamma \subset \bigcup_{i\neq j} \tilde{\gamma}_i\alpha\Gamma$, a contradiction with the decomposition of $\Gamma\alpha\Gamma$ into n orbits for Γ. Therefore we deduce that $\Gamma\alpha\gamma_j$ intersects $\tilde{\gamma}_j\alpha\Gamma$, for each j. Let β_j be any element in this intersection. This gives

$$\Gamma\alpha\Gamma = \bigcup \Gamma\beta_j = \bigcup \beta_j\Gamma.$$

□

This allows us to compute adjoints of double coset operators.

Proposition 4.7. *Let* $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ *be a congruence subgroup and let* $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. *Let* $\alpha^* = \det(\alpha)\alpha^{-1}$ *be the classical adjoint to* α. *Then*

1. *If* $\alpha^{-1}\Gamma\alpha \subseteq \mathrm{SL}_2(\mathbb{Z})$, *and* $f \in S_k(\Gamma)$ *and* $g \in S_k(\alpha^{-1}\Gamma\alpha)$,

$$\langle f|_k\alpha, g\rangle_{\alpha^{-1}\Gamma\alpha} = \langle f, g|_k\alpha^*\rangle_\Gamma.$$

2. *For all* $f, g \in S_k(\Gamma)$,

$$\langle f|_k[\Gamma\alpha\Gamma], g\rangle = \langle f, g|_k[\Gamma\alpha^*\Gamma]\rangle.$$

Proof. We prove only (1). The second statement follows easily. We will use the equalities that we have already seen:

$$j(\alpha, \alpha^* z) = j(\alpha\alpha^*, z) j(\alpha^*, z)^{-1} = \det \alpha \, j(\alpha^*, z)^{-1}, \quad \mathfrak{I}(\alpha^* z) = \frac{\det \alpha^*}{|j(\alpha^*, z)|^2} \mathfrak{I}(z).$$

Let $M = \mathrm{covol}(\Gamma) = \mathrm{covol}(\alpha^{-1}\Gamma\alpha)$. Then we compute:

$$\begin{aligned}
M\langle f|_k \alpha, g\rangle_{\alpha^{-1}\Gamma\alpha} &= \int_{\alpha^{-1}\Gamma\alpha\backslash\mathbb{H}} (\det\alpha)^{k-1} j(\alpha, z)^{-k} f(\alpha z)\overline{g(z)}\mathfrak{I}(z)^k d\mu(z) \\
&= \int_{\Gamma\backslash\mathbb{H}} (\det\alpha)^{k-1} j(\alpha, \alpha^* z)^{-k} f(z)\overline{g(\alpha^* z)}\mathfrak{I}(\alpha^* z)^k d\mu(z) \\
&= \int_{\Gamma\backslash\mathbb{H}} (\det\alpha)^{k-1} (\det\alpha)^{-k} f(z) j(\alpha^*, z)^k \overline{g(\alpha^* z)} \frac{(\det\alpha^*)^k}{|j(\alpha^*, z)|^{2k}} \mathfrak{I}(z)^k d\mu(z) \\
&= \int_{\Gamma\backslash\mathbb{H}} f(z) (\det\alpha)^{k-1} \overline{j(\alpha^*, z)}^{-k} \overline{g(\alpha^* z)} \mathfrak{I}(z)^k d\mu(z) \\
&= \int_{\Gamma\backslash\mathbb{H}} f(z)\overline{g|_k \alpha^*(z)}\mathfrak{I}(z)^k d\mu(z) = M\langle f, g|_k \alpha^*\rangle_\Gamma.
\end{aligned}$$

□

Definition 4.9. A linear operator T is if it commutes with its adjoint:

$$TT^* = T^* T.$$

Theorem 4.6. *Consider the $\mathbb{C}$-vector space $S_k(\Gamma_1(N))$. If $p \nmid N$ then:*

$$\langle p\rangle^* = \langle p\rangle^{-1} = \langle p^{-1}\rangle, \text{ and } T_p^* = \langle p\rangle^{-1} T_p.$$

Proof. Write $\langle p\rangle = [\Gamma\alpha\Gamma]$, where $\alpha \in \Gamma_0(N)$ is such that modulo N is congruent to $\left(\begin{smallmatrix} a & b \\ 0 & p \end{smallmatrix}\right)$. By Proposition 4.7, we have that $\langle p\rangle^*$ consists on acting with $\alpha^* = \det\alpha\alpha^{-1}$. Since $\det\alpha = 1$, then $\alpha^* = \alpha^{-1}$ and thus $\langle p\rangle^* = \langle p^{-1}\rangle = \langle p\rangle^{-1}$.

As for the second part, we set $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ and we need to compute $\Gamma\alpha^*\Gamma$. Note that

$$\alpha^* = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ N & mp \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} p & n \\ N & m \end{pmatrix}, \quad mp - nN = 1.$$

In the right-hand side, the first matrix is in $\Gamma_1(N)$ and the last is in $\Gamma_0(N)$. Since $\Gamma_0(N)$ is normal in $\Gamma_1(N)$, we get

$$\Gamma_1(N) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N) = \Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) \begin{pmatrix} p & n \\ N & m \end{pmatrix}.$$

Since $m \equiv p^{-1} \pmod{N}$, the matrix $\begin{pmatrix} p & n \\ N & m \end{pmatrix}$ acts as $\langle p^{-1} \rangle$. Therefore:

$$T_p^* f = \sum_j f|_k \beta_j \begin{pmatrix} p & n \\ N & m \end{pmatrix} = (T_p f)|_k \begin{pmatrix} p & n \\ N & m \end{pmatrix} = \langle p^{-1} \rangle T_p f.$$

□

Corollary 4.5. *If n is coprime to N, the Hecke operators T_n and $\langle n \rangle$ are normal.*

Theorem 4.7. *Let T be a normal operator on a finite dimensional $\mathbb{C}$-vector space. Then T has an orthogonal basis of eigenvectors.*

Applying this theorem multiple times we deduce that if a $\mathbb{C}$-vector space has a family of normal, pairwise commuting operators then it has a basis of simultaneous eigenvectors. Particularizing to our situation, we get the following result.

Corollary 4.6. *The space $S_k(\Gamma_1(N))$ has an orthogonal basis of simultaneous eigenforms for all the T_n and $\langle n \rangle$ with $(n, N) = 1$.*

Proof. Apply the spectral theorem for the first of the T_n, to get an orthogonal basis of eigenforms. To each of the subspaces one can apply the second of the T_n to refine the basis, thanks to the fact that the Hecke operators commute with each other and hence preserve eigenspaces. The process terminates after a finite number of steps because $S_k(\Gamma_1(N))$ is finite-dimensional. □

Consider $S_k(\mathrm{SL}_2(\mathbb{Z})) = S_k(\Gamma_1(1))$. It has a basis of eigenforms for *all* the Hecke operators T_n (and $\langle n \rangle$). We may normalize the eigenforms f so that $a_1(f) = 1$. Then we will obtain:

$$T_n f = a_n(f) f, \quad \forall n.$$

Therefore each system of eigenvalues $\{a_n(f)\}_{n \geq 1}$ corresponds to a *unique* eigenform f. We say that $S_k(\mathrm{SL}_2(\mathbb{Z}))$ satisfies . In other words, $S_k(\mathrm{SL}_2(\mathbb{Z}))$ decomposes into a direct sum of one-dimensional eigenspaces. In the next section we investigate when this fails to be true, and what can be done to remedy it.

4.5 Atkin-Lehner-Li theory

Let us consider $S_k(\Gamma_1(N))$ for an arbitrary N. We have already seen that there is a basis of simultaneous eigenforms for the T_n and $\langle n \rangle$ operators, as long as n is coprime to N. We want to investigate if the components of this basis are also eigenforms for the remaining Hecke operators and if multiplicity one is satisfied.

Recall the operator $V_d \colon M_k(\Gamma_1(M)) \longrightarrow M_k(\Gamma_1(Md))$ which was introduced before for d a prime:

$$(V_d f)(\tau) = f(d\tau) = d^{1-k} f|_k \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}.$$

If $(t, d) = 1$ then it is easy to check that $V_d U_t = U_t V_d$, and hence $V_d T_n = T_n V_d$ whenever $(n, d) = 1$.

4.5.1 Examples

Both $\Delta(z)$ and $\Delta(2z)$ are cusp forms in $S_{12}(\Gamma_1(2))$. Write

$$\Delta = \sum_{n \geq 1} \tau(n) q^n,$$

so that $T_p \Delta = \tau(p)\Delta$ for all p. Here, by T_2 we mean the Hecke operator as acting on $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$. By what we have seen above, we have:

$$T_p(\Delta(2z)) = \tau(p)\Delta(2z), \quad p \neq 2.$$

Therefore $\Delta(z)$ and $\Delta(2z)$ have, when considered in $S_{12}(\Gamma_1(2))$, the same "system of eigenvalues" $\{\tau(n)\}_{(n,2)=1}$. Therefore $S_{12}(\Gamma_1(2))$ does not satisfy multiplicity one.

However, the Hecke operator $T_2 = U_2$ as acting on $S_{12}(\Gamma_1(2))$ satisfies:

$$U_2(\Delta(2z)) = \Delta(z), \text{ and } U_2(\Delta(z)) = T_2\Delta - 2^{11} V_2(\Delta) = -24\Delta(z) - 2^{11}\Delta(2z).$$

Therefore U_2 acts on $S_{12}(\Gamma_1(2))$ with matrix

$$[U_2] = \begin{pmatrix} -24 & 1 \\ -2^{11} & 0 \end{pmatrix},$$

which is diagonalizable. The eigenvectors

$$f_\pm = \Delta(z) + (12 \pm 4\sqrt{-119})\Delta(2z)$$

can be completed to give a basis of eigenforms for all the T_n.

The following example shows that sometimes one may not get a basis of eigenforms for all T_p. Let $f \in S_2(\Gamma_1(N))$ be an eigenform for $\{T_q\}_{q\nmid N} \cup \{U_q\}_{q|N}$, and let $p \nmid N$. Let S be the following 4-dimensional $\mathbb{C}$-vector subspace of $S_2(\Gamma_1(Np^3))$:

$$S = \mathrm{span}_{\mathbb{C}}\{f(\tau), f(p\tau), f(p^2\tau), f(p^3\tau)\}.$$

Since T_q commutes with V_p, the subspace S is stable under $\{T_q\}_{q\nmid Np^3}$. Moreover, S is also stable under $\{T_q = U_q\}_{q|N}$. The following result shows that S does not satisfy multiplicity one.

Proposition 4.8.

1. *S is stable under $\{T_q\}_{q\nmid Np^3} \cup \{T_q = U_q\}_{q|N} \cup \{T_p = U_p\}$.*
2. *The matrix of U_p is not diagonalizable.*

Proof. Exercise. □

4.5.2 New and old forms

Suppose that $M \mid N$ are two positive integers. There are many ways to embed $S_k(\Gamma_1(M))$ into $S_k(\Gamma_1(N))$. For example, for any d such that $dM \mid N$, we can map f to $V_d f$.

Definition 4.10. The , denoted by $S_k(\Gamma_1(N))^{\mathrm{old}}$ is:

$$S_k(\Gamma_1(N))^{\mathrm{old}} = \mathrm{span}_{\mathbb{C}}\left\{V_d(S_k(\Gamma_1(M))) \,:\, dM \mid N, M \neq N\right\}.$$

The , denoted by $S_k(\Gamma_1(N))^{\mathrm{new}}$ is the orthogonal complement (with respect to the Petersson inner product) of $S_k(\Gamma_1(N))^{\mathrm{old}}$ in $S_k(\Gamma_1(N))$.

Theorem 4.8. *The spaces $S_k(\Gamma_1(N))^{old}$ and $S_k(\Gamma_1(N))^{new}$ are stable under* all *Hecke operators.*

Proof. Let ℓ be a prime dividing N. We may define

$$S_k(\Gamma_1(N))^{\ell-\mathrm{old}} = \iota S_k(\Gamma_1(N/\ell)) + V_\ell S_k(\Gamma_1(N/\ell)),$$

where ι is embedding induced by $f \mapsto f$. In this way,

$$S_k(\Gamma_1(N))^{\mathrm{old}} = \sum_{\ell|N} S_k(\Gamma_1(N))^{\ell-\mathrm{old}},$$

where the sum runs over prime divisors ℓ of N. What we will prove is that each of the spaces $S_k(\Gamma_1(N))^{\ell-\mathrm{old}}$ is stable under the diamond operators, the Hecke operators T_p, and their

adjoints. Note also that if $V \subset S_k(\Gamma_1(N))$ is a subspace which stable under an operator T, then the orthogonal complement to V is stable under the adjoint T^*.

Let $f \in S_k(\Gamma_1(N/\ell))$, and let T be one of the Hecke operators above. We must prove that $T(\iota f)$ and $T(V_\ell f)$ are in $S_k(\Gamma_1(N))^{\ell-\text{old}}$. Consider the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, which defines the operator $\langle d \rangle$ on $S_k(\Gamma_1(N))$ and on $S_k(\Gamma_1(N/\ell))$. This shows that $\langle d \rangle$ preserves $\iota S_k(\Gamma_1(N/\ell))$. Next, note that that

$$\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b\ell \\ c/\ell & d \end{pmatrix} \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}.$$

Since c/ℓ is an integer which is divisible by N/ℓ, the matrix $\left(\begin{smallmatrix} a & b\ell \\ c/\ell & d \end{smallmatrix}\right)$ defines the operator $\langle d \rangle$ on $S_k(\Gamma_1(N/\ell))$. Therefore the matrix equality above gives $\langle d \rangle (V_\ell f) = V_\ell(\langle d \rangle \iota f)$.

Next we prove that the operators T_p also preserve $S_k(\Gamma_1(N))^{\ell-\text{old}}$. If p does not divide N this is easy to show that T_p preserves both $V_\ell S_k(\Gamma_1(N/\ell))$ and $\iota S_k(\Gamma_1(N/\ell))$. When p does divide N but $p \neq \ell$, the same argument works. We now consider T_ℓ. Suppose that ℓ divides N exactly once. Then

$$T_\ell(\iota f) = \iota U_\ell f, \text{ and } \quad T_\ell(V_\ell f) = \iota f.$$

However, in $S_k(\Gamma_1(N/\ell))$ we have

$$\iota T_\ell f = T_\ell(\iota f) + \ell^{k-1} V_\ell(\langle \ell \rangle f), \text{ so } T_\ell(\iota f) = \iota T_\ell f - \ell^{k-1} V_\ell(\langle \ell \rangle f).$$

In particular we see that $T_\ell(\iota f)$ and $T_\ell(V_\ell f)$ are in $S_k(\Gamma_1(N))^{\ell-\text{old}}$.

Finally if ℓ^2 divides N then T_ℓ acts as U_ℓ in both $S_k(\Gamma_1(N/\ell))$ and $S_k(\Gamma_1(N))$, and hence

$$T_\ell \iota f = \iota T_\ell f, \quad T_\ell V_d f = \iota f.$$

It only remains to show that the adjoint of T_p preserves $S_k(\Gamma_1(N))^{\ell-\text{old}}$ when p divides N (when p does not divide N, the adjoints of Hecke operators are in the Hecke algebra and hence preserves the old subspace. In this case, consider the Fricke operator w_N acting on $S_k(\Gamma_1(N))$ by

$$f \mapsto f|_k W_N, \quad W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

(note that W_N normalizes $\Gamma_1(N)$). We can check:

$$(w_N f)(z) = z^{-k} f(-1/(Nz)).$$

Also, note that $W_N \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) W_N^{-1} = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and thus $T_p^* = w_N^{-1} T_p w_N$. One can then compute:

$$w_N \iota f = \ell^k V_\ell w_{N/\ell} f, \text{ and } w_N V_\ell f = \iota w_{N/\ell} f.$$

Therefore w_N (and hence T_p^*) preserves the old subspace. □

We say that $f \in S_k(\Gamma_1(N))^{\text{new}}$ is a if it is an *eigenform* for all Hecke operators, which is *normalized* so that the leading coefficient is 1.

Theorem 4.9. *Consider the space $S_k(\Gamma_1(N))^{new}$ for $N \geq 1$.*

1. *The space $S_k(\Gamma_1(N))^{new}$ has a basis of newforms.*
2. *If $f \in S_k(\Gamma_1(N))^{new}$ is an eigenvector for $\{T_q\}_{q \nmid N}$ then f is a scalar multiple of a newform, and hence an eigenvector for* all *the Hecke operators.*
3. *If $f \in S_k(\Gamma_1(N))^{new}$ and $g \in S_k(\Gamma_1(M))^{new}$ are both newforms satisfying $a_q(f) = a_q(g)$ for all but finitely many primes q, then $N = M$ and $f = g$.*

Proof. This was proven by Atkin–Lehner in 1970 and a partial proof can be found in [3]. □

Corollary 4.7.

1. *If f is a newform, then there is a Dirichlet character χ such that $f \in S_k(\Gamma_0(N), \chi)$.*
2. *If $\{\lambda_n\}_{(n,N)=1}$ is a system of eigenvalues for the T_n such that $(n, N) = 1$, then $\exists!$ newform $f \in S_k(\Gamma_1(M))^{new}$ for some $M \mid N$, such that $T_n f = \lambda_n f$ for all n satisfying $(n, N) = 1$.*

Finally, we see that the new subspaces give a complete description of $S_k(\Gamma_1(N))$ and $S_k(\Gamma_0(N))$.

Theorem 4.10. *There are direct sum decompositions*

$$S_k(\Gamma_1(N)) = \bigoplus_{M|N} \bigoplus_{dM|N} V_d \left(S_k(\Gamma_1(M))^{new} \right),$$

and

$$S_k(\Gamma_0(N)) = \bigoplus_{M|N} \bigoplus_{dM|N} V_d \left(S_k(\Gamma_0(M))^{new} \right).$$

Proof. Write $S_k(\Gamma_1(N)) = W_1 \oplus \cdots \oplus W_t$, where each of the W_i is a simultaneous eigenspace for $\{T_n\}_{(n,N)=1} \cup \{\langle n \rangle\}$. Each form $f \in W_i$ has the same "package" of eigenvalues $\{\lambda_n\}_{(n,N)=1}$. Therefore by Corollary 4.7 this f comes from a unique newform $f_i \in S_k(\Gamma_1(M_i))^{\text{new}}$ for some $M_i \mid N$. Therefore

$$W_i = \bigoplus_{dM_i|N} \mathbb{C} V_d(f_i)$$

as wanted. Since each of these spaces is stable under the diamond operators, we get the second decomposition by further taking the subspaces on which they act trivially. □

5 Eisenstein series

The conclusion of the previous chapter has been that $S_k(\Gamma_1(N))$ has a basis of eigenforms each of them new at some level dividing N. For a general congruence subgroup Γ, recall that the Petersson inner product allowed us to define an "orthogonal complement" to $S_k(\Gamma)$, the Eisenstein subspace

$$\mathcal{E}_k(\Gamma) = \{f \in M_k(\Gamma) \mid \langle f, g\rangle_\Gamma = 0 \quad \forall g \in S_k(\Gamma)\}.$$

The goal for this chapter is to find a natural basis for $\mathcal{E}_k(\Gamma)$.

5.1 Eisenstein series for congruence subgroups

Recall the Eisenstein series for $\mathrm{SL}_2(\mathbb{Z})$ that we saw at the beginning:

$$G_k(z) = \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(mz+n)^k}.$$

In order to generalize this construction, we need to put it in a more intrinsic form. Recall that the stabilizer of the cusp ∞ is

$$P_\infty = \mathrm{SL}_2(\mathbb{Z})_\infty = \{\pm \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \mid b \in \mathbb{Z}\}.$$

Write also $P_\infty^+ = \{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \mid b \in \mathbb{Z}\}$.

Lemma 5.1. *The map* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto (c, d)$ *induces a bijection*

$$P_\infty^+ \backslash \mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\sim} \{(c, d) \in \mathbb{Z}^2 \mid \gcd(c, d) = 1\}.$$

Proof. Surjectivity of the map follows from Bézout: given (c, d) with $\gcd(c, d) = 1$ we can find $a, b \in \mathbb{Z}$ such that $ad - bc = 1$. Moreover, any solution to the equation $xd - yc = 1$ is of the form

$$x = a + tc, y = b + td, \quad t \in \mathbb{Z}.$$

That is, the preimage of (c, d) consists of the set of matrices of the form

$$\begin{pmatrix} a + tc & b + td \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad t \in \mathbb{Z}.$$

□

This lemma allows us to rewrite $G_k(z)$ in a different way.

Proposition 5.1. *We have*

$$G_k(z) = \zeta(k) \sum_{\gamma \in P_\infty^+ \backslash \mathrm{SL}_2(\mathbb{Z})} j(\gamma, z)^{-k}.$$

Proof. Write a pair $(m, n) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ as (gc, gd), with $g = \gcd(m, n)$ and (c, d) coprime. Therefore

$$\begin{aligned} G_k(z) &= \sum_{g=1}^{\infty} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1}} \frac{1}{g^k (cz+d)^k} \\ &= \sum_{g=1}^{\infty} \frac{1}{g^k} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1}} \frac{1}{(cz+d)^k} = \zeta(k) \sum_{\gamma \in P_\infty^+ \backslash \mathrm{SL}_2(\mathbb{Z})} j(\gamma, z)^{-k}. \end{aligned}$$

□

Let now Γ be an arbitrary congruence subgroup, and define $\Gamma_\infty = \Gamma \cap P_\infty$ and $\Gamma_\infty^+ = \Gamma \cap P_\infty^+$.

Definition 5.1. The of weight k attached to Γ and to the cusp ∞ is

$$G_{k,\Gamma,\infty}(z) = \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} j(\gamma, z)^{-k}.$$

Since $j(h\gamma, z) = j(\gamma, z)$ whenever $h \in \Gamma_\infty^+$, the terms in the above sum are well-defined. Moreover, since $\Gamma_\infty^+ \backslash \Gamma$ injects in $P_\infty^+ \backslash \mathrm{SL}_2(\mathbb{Z})$, the series above is a sub-series of $G_k(z)$ and therefore it converges. So in particular, $G_{k,\Gamma,\infty}$ is holomorphic on $\mathbb{H}$.

Proposition 5.2. *If either*

1. *k is even, or*
2. *k is odd, $-I \notin \Gamma$ and ∞ is a regular cusp of Γ*

then $G_{k,\Gamma,\infty}$ belongs to $M_k(\Gamma)$. Moreover, $G_{k,\Gamma,\infty}(\infty) \neq 0$ and $G_{k,\Gamma,\infty}$ vanishes at all cusps $s \neq \infty$.

If k is odd and either $-I \in \Gamma$ or ∞ is an irregular cusp of Γ, then $G_{k,\Gamma,\infty} = 0$.

Proof. It is easy to show that $G_{k,\Gamma,\infty} = 0$ if the conditions stated in the proposition are satisfied. The computation showing that $G_{k,\Gamma,\infty}$ is weakly-modular of weight k for Γ is also straightforward, using the cocycle condition of $j(\gamma, z)$.

Next we compute the value $G_{k,\Gamma,\infty}(\infty)$. We need to understand how $j(\gamma, z)^{-k}$ behaves when $\Im z \longrightarrow \infty$. Suppose that $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then

$$\lim_{\Im z \longrightarrow \infty} j(\gamma, z)^{-k} = \lim_{\Im z \longrightarrow \infty} (cz + d)^{-k} = \begin{cases} d^{-k} & \text{if } c = 0, \\ 0 & \text{if } c \neq 0. \end{cases}$$

Note also that $c = 0 \iff \gamma \in \Gamma_\infty$. Therefore we may calculate

$$\begin{aligned} \lim_{\Im z \longrightarrow \infty} G_{k,\Gamma,\infty}(z) &= \lim_{\Im z \longrightarrow \infty} \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} j(\gamma, z)^{-k} \\ &= \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma_\infty} j(\gamma, z)^{-k} \\ &= \begin{cases} 1 & \text{if } \Gamma_\infty^+ = \Gamma_\infty, \\ 1 + (-1)^k & \text{if } [\Gamma_\infty \colon \Gamma_\infty^+] = 2. \end{cases} = \begin{cases} 1 & \text{if } \Gamma_\infty^+ = \Gamma_\infty, \\ 2 & \text{if } [\Gamma_\infty \colon \Gamma_\infty^+] = 2 \text{ and } k \text{ is even}, \\ 0 & \text{if } [\Gamma_\infty \colon \Gamma_\infty^+] = 2 \text{ and } k \text{ is odd}. \end{cases} \end{aligned}$$

The last case does not occur, by assumption. Hence $G_{k,\Gamma,\infty}(\infty) \in \{1, 2\}$ is nonzero.

Consider now a cusp s of Γ, different from ∞. Let $\gamma_s \in \mathrm{SL}_2(\mathbb{Z})$ satisfy $\gamma_s \infty = s$, so that $G_{k,\Gamma,\infty}(s) = (G_{k,\Gamma,\infty}|_k \gamma_s)(\infty)$. Note that

$$(G_{k,\Gamma,\infty}|_k \gamma_s)(z) = \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} j(\gamma, \gamma_s z)^{-k} j(\gamma_s, z)^{-k} = \sum_{\gamma \in \Gamma_\infty^+ \backslash \Gamma} j(\gamma\gamma_s, z)^{-k}.$$

Since $\gamma\gamma_s$ has nonzero bottom-left entry (otherwise $\gamma\gamma_s$ would stabilize infinity, which does not), then each of the terms approaches 0 as $\Im z \longrightarrow \infty$ and we obtain the desired vanishing. $\square$

The next goal is to construct Eisenstein series that are non-vanishing at each of the other cusps s of Γ (and vanish at the cusps $s' \neq s$). This is done by translating $G_{k,\Gamma,\infty}$ by the matrices γ_s.

Lemma 5.2. *Let s be a cusp of Γ and let $\gamma_s \in \mathrm{SL}_2(\mathbb{Z})$ be a matrix such that $\gamma_s \infty = s$. Define*

$$G_{k,\Gamma,s} = G_{k,\gamma_s^{-1}\Gamma\gamma_s,\infty}|_k \gamma_s^{-1} = \sum_{\gamma \in \Gamma_s^+ \backslash \Gamma} j(\gamma_s^{-1}\gamma, z), \quad \textit{where } \Gamma_s^+ = \{\gamma \in \Gamma \mid \gamma_s^{-1}\gamma\gamma_s = \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\}.$$

If k is odd, suppose that $-I \notin \Gamma$, and s is a regular cusp of Γ. Then $G_{k,\Gamma,s}$ belongs to $\mathcal{E}_k(\Gamma)$, does not vanish at s and vanishes at all other cusps $s' \neq s$ of Γ.

Although there is a choice of γ_s involved, the form $G_{k,\Gamma,s}$ is well defined when k is even, and well-defined up to sign when k is odd.

We next show that the Eisenstein series we have just introduced belong in fact to the Eisenstein subspace $\mathcal{E}_k(\Gamma)$.

Proposition 5.3. *Let Γ be a congruence subgroup, let $k \geq 3$ be an integer and let s be a cusp of Γ. Then $G_{k,\Gamma,s}$ belongs to $\mathcal{E}_k(\Gamma)$.*

Proof. We need to prove that for each $f \in S_k(\Gamma)$ we have $\langle f, G_{k,\Gamma,s}\rangle_\Gamma = 0$. From the definition of the Petersson inner product there is an equality

$$\langle f, g\rangle_\Gamma = \langle f|_k\gamma, g|_k\gamma\rangle_{\gamma^{-1}\Gamma\gamma}.$$

Thus we may reduce to showing $\langle f, G_{k,\Gamma,\infty}\rangle_\Gamma = 0$ for all $f \in S_k(\Gamma)$. Writing the definition of the pairing and exchanging the sum with the integral gives

$$\langle f, G_{k,\Gamma,\infty}\rangle_\Gamma = \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma} \int_{D_\Gamma} f(z)\overline{j(\gamma,z)^{-k}}\mathfrak{I}(z)^k d\mu(z).$$

Make the change of variables $w = \gamma z$, so

$$f(w) = j(\gamma,z)^k f(z), \quad \mathfrak{I}(w) = |j(\gamma,z)|^{-2}\mathfrak{I}(z).$$

This gives

$$\langle f, G_{k,\Gamma,\infty}\rangle_\Gamma = \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma} \int_{w\in\gamma D_\Gamma} f(w)y^k \frac{dxdy}{y^2} = \int_{w\in\Gamma_\infty^+\backslash\mathbb{H}} f(w)y^{k-2}dxdy.$$

Suppose now that ∞ has width h and that the q-expansion of f is $\sum a_n q_h^n$. Then

$$\begin{aligned}
\langle f, G_{k,\Gamma,\infty}\rangle_\Gamma &= \int_{\Gamma_\infty^+\backslash\mathbb{H}} \left(\sum_{n=1}^\infty a_n e^{2\pi i n w/h}\right) y^{k-2}dxdy \\
&= \int_{x=0}^h \int_{y=0}^\infty \left(\sum_{n=1}^\infty a_n e^{2\pi i n x/h} e^{-2\pi n y/h}\right) y^{k-2}dxdy \\
&= \sum_{n=1}^\infty a_n \int_{x=0}^h e^{2\pi i n x/h}dx \int_{y=0}^\infty e^{-2\pi n y/h} y^{k-2}dy.
\end{aligned}$$

Since $n \geq 1$, the integrals on x vanish and thus we get the result. □

We end the section by stating essentially that the Eisenstein series give a basis for $\mathcal{E}_k(\Gamma)$. We do this by giving the dimension of the Eisenstein space, and then exhibiting a the explicit basis.

Theorem 5.1. *Let Γ be a congruence subgroup, let k be an integer, let ε_Γ be the number of cusps of Γ and let $\varepsilon_\Gamma^{reg} \leq \varepsilon_\Gamma$ be the number of regular cusps. Then:*

$$\dim_{\mathbb{C}} \mathcal{E}_k(\Gamma) = \begin{cases} 0 & \text{if } k < 0, \text{ or } k \text{ odd and } -I \in \Gamma, \\ 1 & \text{if } k = 0, \\ \varepsilon_\Gamma^{reg}/2 & \text{if } k = 1 \text{ and } -I \notin \Gamma, \\ \varepsilon_\Gamma - 1 & \text{if } k = 2, \\ \varepsilon_\Gamma & \text{if } k \text{ even, and } k \geq 4, \\ \varepsilon_\Gamma^{reg} & \text{if } k \text{ odd, } k \geq 3, \text{ and } -I \notin \Gamma. \end{cases}$$

5.2 Eisenstein series for $\Gamma_1(N)$

We now specialize the above construction in the case where $\Gamma = \Gamma_1(N)$ for any positive integer N. In fact, we will construct a basis of Hecke eigenforms.

Recall that in Chapter 4 we introduced Dirichlet characters modulo N. Let M and N be positive integers with $M \mid N$. A Dirichlet character χ modulo M can be lifted to a Dirichlet character $\chi^{(N)}$ modulo N, by

$$\chi^{(N)}(m) = \begin{cases} \chi(m) & \text{if } \gcd(m, N) = 1, \\ 0 & \text{if } \gcd(m, N) > 1. \end{cases}$$

Definition 5.2. Let $\chi \colon \mathbb{Z} \longrightarrow \mathbb{C}$ be a Dirichlet character modulo N. The of χ is the smallest divisor M of N such that χ is the lift of a Dirichlet character modulo M. A Dirichlet character modulo N is if it has conductor N.

Example 5.1. The only character modulo one is $1 \colon \mathbb{Z} \longrightarrow \mathbb{C}$, the constant function 1. If N is any positive integer, the lift of 1 to a Dirichlet character modulo N is the function

$$1^{(N)} \colon \mathbb{Z} \longrightarrow \mathbb{C}, \quad m \mapsto \begin{cases} 1 & \gcd(m, N) = 1, \\ 0 & \gcd(m, N) > 1. \end{cases}$$

Example 5.2. For each prime number p, and each integer a we define the

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \mid a \text{ and } a \text{ is a square modulo } p, \\ -1 & \text{if } p \mid a \text{ and } a \text{ is not a square modulo } p, \end{cases}$$

Then $\left(\frac{\bullet}{p}\right)$ is a Dirichlet character modulo p. Its conductor is p if $p \neq 2$, and 1 if $p = 2$.

Example 5.3. Let χ_1 be a Dirichlet character modulo N_1 and let χ_2 be a Dirichlet character modulo N_2. If M is a common multiple of N_1 and N_2, one may consider the product $\chi = \chi_1\chi_2 = \chi_1^{(M)}\chi_2^{(M)}$. This is a character with modulus M. Note however that the conductor is not multiplicative: if χ is a quadratic character of conductor N, say, then χ^2 is the trivial character which will have conductor 1.

In order to give the q-expansions of the Eisenstein series attached to a pair of characters, we need some new notation. We will need the folloing generalization of the divisor function. If χ_1 and χ_2 are Dirichlet characters, define

$$\sigma_{k-1}^{\chi_1,\chi_2}(n) = \sum_{d|n} \chi_1(n/d)\chi_2(d)d^{k-1}.$$

The following theorem gives the q-expansions of Eisenstein series that will form a basis of eigenforms for the Eisenstein space.

Theorem 5.2. *Let χ_1, χ_2 be primitive Dirichlet characters modulo N_1 and N_2, respectively. Let $\chi = \chi_1\chi_2$ be the product as a character modulo N_1N_2 (not necessarily primitive). Let $k \geq 3$ be such that $\chi(-1) = (-1)^k$. Define*

$$\delta(\chi_1) = \begin{cases} 1 & \text{if } \chi_1 = 1_1, \\ 0 & \text{else.} \end{cases}$$

and let $L(\chi_2, s) = \sum_{n=1}^{\infty} \chi_2(n)n^{-s}$ be the L-series of χ_2. Then the function $E_k^{\chi_1,\chi_2}$ defined by

$$E_k^{\chi_1,\chi_2}(z) = \delta(\chi_1)L(\chi_2, 1-k) + 2\sum_{n=1}^{\infty} \sigma_{k-1}^{\chi_1,\chi_2}(n)q^n$$

belongs to $\mathcal{E}_k(\Gamma_1(N_1N_2))$. Moreover, it is a Hecke eigenform with character χ.

The modular form $E_k^{\chi_1,\chi_2}$ is called the *Eisenstein series of weight k associated to (χ_1, χ_2)*.

When $k = 1$ the theorem remains true, although in this case $E_1^{\chi_1,\chi_2} = E_1^{\chi_2,\chi_1}$. When $k = 2$, then we must require in addition that χ_1 and χ_2 must not be both trivial. If both χ_1 and χ_2 are trivial, then we know that $E_2(z) = 1 - 24\sum_{n\geq 1} \sigma_1(n)q^n$ is not a modular form. However, for any $N > 1$ the function

$$E_2^{(N)}(z) = E_2(z) - NE_2(Nz)$$

belongs to $M_2(\Gamma_1(N))$.

Theorem 5.3. *Let $k \geq 3$, let $N \geq 1$ and let χ be a Dirichlet character modulo N such that $\chi(-1) = (-1)^k$. Then there is a decomposition*

$$\mathcal{E}_k(\Gamma_0(N), \chi) = \bigoplus_{d|N} \bigoplus_{N_1N_2|\frac{N}{d}} \bigoplus_{\chi_1\chi_2=\chi} \mathbb{C}V_d(E_k^{\chi_1,\chi_2}),$$

where the inner sum runs through factorizations of χ into primitive Dirichlet characters χ_1 and χ_2 modulo N_1 and N_2.

6 L-functions

In this chapter we study the connection of modular forms with L-functions.

6.1 Basic definitions

Let $f \in M_k(\Gamma_1(N))$ be a modular form, given by a q-expansion $f = \sum_{n=0}^{\infty} a_n q^n$.

Definition 6.1. The of f is the function of $s \in \mathbb{C}$ given formally as

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

Proposition 6.1. *If $f \in S_k(\Gamma_1(N))$ is a cusp form then $L(f,s)$ converges absolutely for all s such that $\Re(s) > k/2 + 1$. If $f \in M_k(\Gamma_1(N))$ is not a cusp form then $L(f,s)$ converges absolutely for all s with $\Re(s) > k$.*

Proof. We have seen in Theorem 1.15 and Corollary 1.9 that $|a_n| \leq M n^{r(k)}$ for some constant M, where $r(k) = k/2$ when f is a cusp form and $r(k) = k-1$ when f is not a cusp form. Although those results were stated and proven only for level 1, they hold true (with essentially the same proofs) for higher levels. Therefore if $\Re(s) > r(k) + 1$ then

$$|\sum_{n\geq 0} a_n n^{-s}| \leq M \sum_{n \geq 0} n^{r(k)-\Re(s)} < \infty.$$

□

The L-functions attached to normalized eigenforms have a very remarkable decomposition, known as . In fact, having this property characterizes normalized eigenforms, as the following result states.

Theorem 6.1. *Let $f \in M_k(\Gamma_0(N), \chi)$ be a modular form with q-expansion $f = \sum_{n\geq 0} a_n q^n$. Then f is a normalized eigenform if and only if $L(f,s)$ has an Euler product expansion*

$$L(f,s) = \prod_{p \text{ prime}} (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1}.$$

Proof. By Proposition 4.5 we need to show that conditions (1), (2) and (3) of loc.cit. are equivalent to $L(f,s)$ having an Euler product. For a fixed prime p, condition (2) says

$$a_{p^r}(f) = a_p(f)a_{p^{r-1}}(f) - p^{k-1}\chi(p)a_{p^{r-2}}(f).$$

Multiplying by t^r and summing over all $r \geq 2$ we see that (2) is equivalent to

$$\sum_{r=2}^{\infty} a_{p^r}(f)t^r = a_p(f)t\sum_{r=1}^{\infty} a_{p^r}(f) - p^{k-1}\chi(p)t^2\sum_{r=0}^{\infty} a_{p^r}(f),$$

or

$$\left(\sum_{r\geq 0} a_{p^r}(f)t^r\right)(1 - a_p(f)t + \chi(p)p^{k-1}t^2) = a_1(f) + a_p(f)t(1 - a_1(f)).$$

Since we are assuming that $a_1(f) = 1$ we get, by substituting $t = p^{-s}$, the equality

$$\sum_{r=0}^{\infty} a_{p^r}(f)p^{-rs} = (1 - a_p(f)p^{-s} + \chi(p)p^{k-1-2s})^{-1}. \tag{6.1}$$

Conversely, if this equality holds then letting s approach ∞ we get $a_1(f) = 1$, and the other implications can also be reversed to show that Equation 6.1 is equivalent to conditions (1) and (2) for the $a_n(f)$'s.

The Fundamental Theorem of Arithmetic implies that if g is any function of prime powers, then

$$\prod_p \sum_{r=0}^{\infty} g(p^r) = \sum_{n=1}^{\infty} \prod_{p^r \| n} g(p^r).$$

Using this fact, it is easy to see that Equation 6.1 and condition (3) are equivalent to the existence of the Euler product, thus finishing the proof. □

6.2 L-functions of Eisenstein series

Let $\chi\colon \mathbb{Z} \longrightarrow \mathbb{C}$ be a primitive Dirichlet character modulo N. One can attach an L-function to χ via the formula

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n)n^{-s}, \quad \Re(s) > 1.$$

Proposition 6.2. *The L-function of χ extends to an entire function of on $\mathbb{C}$ unless $\chi = 1$, in which case $L(1,s) = \zeta(s)$ has a simple pole at $s = 1$.*

Proof. Omitted. □

We also have an Euler product:

Proposition 6.3. *There is an Euler product decomposition*

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

Proof. Exercise. □

We have defined the L-function of any modular form. In particular, if χ_1 and χ_2 are primitive Dirichlet characters modulo N_1 and N_2 respectively, then we can consider the L-function $L(E_k^{\chi_1,\chi_2}, s)$.

Example 6.1. Consider the Eisenstein series for the full modular group $E_k(z) \in M_k(\mathrm{SL}_2(\mathbb{Z}))$. In Proposition 4.4 we have seen that E_k is an eigenform for all the Hecke algebra, satisfying $T_p E_k = \sigma_{k-1}(p)E_k$. If we normalize E_k using its first coefficient (instead of the zero-th) and call the resulting Eisenstein series $\bar{E}_K$, then we have $a_p(\bar{E}_k) = \sigma_{k-1}(p) = 1 + p^{k-1}$. Therefore

$$\begin{aligned} L(\bar{E}_k, s) &= \prod_{p \text{ prime}} \frac{1}{1 - (1 + p^{k-1})p^{-s} + p^{k-1-2s}} \\ &= \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} \frac{1}{1 - p^{k-1-s}} = \zeta(s)\zeta(s - k + 1). \end{aligned}$$

The factorization of the example holds in much more generality. Denote by $\bar{E}_k^{\chi_1,\chi_2} = \frac{1}{2}E_k^{\chi_1,\chi_2}$, where $E_k^{\chi_1,\chi_2}$ were defined in Theorem 5.2.

Proposition 6.4. *The L-function attached to the Eisenstein series $\bar{E}_k^{\chi_1,\chi_2}$ has a factorization*

$$L(\bar{E}_k^{\chi_1,\chi_2}, s) = L(\chi_1, s)L(\chi_2, s - k + 1).$$

Proof. Exercise. □

The idea that one can extract from this is that the Eisenstein series are quite simple, and their L-functions are not too interesting since they can be understood from the (simpler) L-functions attached to characters. In stark contrast, the L-functions attached to cusp forms have much deeper connections.

6.3 L-functions of cusp forms

We focus from now on on cusp forms. The next striking property of L-functions of cusp forms is known as , a symmetry property of deep consequences. In order to state it precisely, we first define the , which appears often in number theory, as

$$\Gamma(s) = \int_0^\infty t^s e^{-t} \frac{dt}{t}.$$

Note that $\Gamma(n+1) = n!$ for all integers $n \geq 1$, so we can think of Γ as an analytic function interpolating the factorials. The Gamma-function enters also in the definition of another complex function, for which the symmetry property is more apparent.

Definition 6.2. The of $f \in S_k(\Gamma_1(N))$ is

$$\Lambda(f,s) = (2\pi)^{-s}\Gamma(s)L(f,s), \quad \Re(s) > k/2 + 1.$$

The next result gives an integral formula for the completed L-function.

Proposition 6.5. *We have*

$$\Lambda(f,s) = \int_0^\infty f(it)t^s \frac{dt}{t}, \quad \Re(s) > k/2 + 1.$$

This is called the of f.

Proof. We first remark that the integral makes sense, since

$$\left| \int_0^\infty f(it)t^s \frac{dt}{t} \right| < \int_0^\infty t^{-k/2+s} \frac{dt}{t},$$

which converges for $\Re(s) > k/2 + 1$. Now we compute

$$\Lambda(f,s) = (2\pi)^{-s} \left(\int_0^\infty t^s e^{-t} \frac{dt}{t} \right) \sum a_n n^{-s} = \sum_{n=1}^\infty a_n \int_0^\infty \left(\frac{t}{2\pi n} \right)^s e^{-t} \frac{dt}{t}.$$

By doing a change of variables $t \mapsto t/(2\pi n)$ in each term, the above expression becomes

$$\sum_{n=1}^\infty a_n \int_0^\infty t^s e^{-2\pi n t} \frac{dt}{t} = \int_0^\infty \left(\sum_{n=1}^\infty a_n e^{-2\pi n t} \right) t^s \frac{dt}{t} = \int_0^\infty f(it)t^s \frac{dt}{t},$$

which gives the desired equality. □

In order to extend $\Lambda(f,s)$ (and thus $L(f,s)$) to $s \in \mathbb{C}$ we need to avoid integrating near the real axis. We will also need to consider the operator W_N given by

$$W_N(f) = i^k N^{1-k/2} f|_k \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

It is an idempotent operator: $W_N^2 = W_N$, and one easily sees that it is self-adjoint: $\langle W_N f, g\rangle = \langle f, W_N g\rangle$ for $f, g \in S_k(\Gamma_1(N))$. Consider the + and −-eigenspaces

$$S_k(\Gamma_1(N))^{\pm} = \{f \in S_k(\Gamma_1(N)) \mid W_N f = \pm f\},$$

which gives an orthogonal decomposition of $S_k = S_k^+ \oplus S_k^-$.

Theorem 6.2. *Suppose that $f \in S_k(\Gamma_1(N))^{\pm}$. Then the function $\Lambda(f,s)$ extends to an entire function on $\mathbb{C}$, which satisfies the functional equation*

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

In particular, the L-function $L(f,s)$ has an analytic continuation to all of $\mathbb{C}$.

Proof. Define $\Lambda_N(s) = N^{s/2}\Lambda(f,s)$, and note that we must show that $\Lambda_N(s) = \pm\Lambda_N(k-s)$. By changing $t \mapsto t/\sqrt{N}$ we get

$$\Lambda_N(s) = N^{s/2}\int_0^\infty f(it)t^s\frac{dt}{t} = \int_0^\infty f(it/\sqrt{N})t^s\frac{dt}{t}.$$

We break the integral at $t = 1$. Note that the piece

$$\int_1^\infty f(it/\sqrt{N})t^s\frac{dt}{t}$$

converges to an entire function of s, because $f(it/\sqrt{N}) = O(e^{-2\pi t/\sqrt{N}})$ when $t \longrightarrow \infty$. As for the other part, use that $(W_N f)(i/(\sqrt{N}t)) = t^k f(it/\sqrt{N})$ to get

$$\int_0^1 f(it/\sqrt{N})t^s\frac{dt}{t} = \int_0^1 (W_N f)(i/(\sqrt{N}t))t^{s-k}\frac{dt}{t} = \int_1^\infty (W_N f)(it/\sqrt{N})t^{k-s}\frac{dt}{t}.$$

Again, since $W_n f = \pm f$ this converges to an entire function. As for the functional equation, note that we have obtained

$$\Lambda_N(s) = \int_1^\infty \left(f(it/\sqrt{N})t^s \pm f(it/\sqrt{N})t^{k-s}\right)\frac{dt}{t} = \pm\Lambda_N(k-s).$$

□

6.4 Relation to elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve. It can be thought of as the set cut out by an equation of the form

$$E\colon Y^2 = X^3 + AX + B, \quad A, B \in \mathbb{Z},$$

such that the discriminant Δ_E of $X^3 + AX + B$ is nonzero. The coefficients of this equation can be reduced modulo any prime p and the conductor N_E of E is an integer whose prime divisors are precisely the prime divisors of N_E (although in general $N_E \neq \Delta_E$. One can define an L-function attached to E via the following Euler product:

$$L(E, s) = \prod_{p | N_E} (1 - a_p(E)p^{-s})^{-1} \prod_{p \nmid N_E} (1 - a_p(E)p^{-s} + p^{1-2s})^{-1}, \quad \Re(s) > 3/2.$$

where $a_p(E) = 1 + p - \#E(\mathbb{F}_p)$. Here, by $E(\mathbb{F}_p)$ we mean the set of points of (the reduction of) E over the finite field $\mathbb{F}_p$, where we always include the "point at infinity".

It turns out that elliptic curves arise from modular forms, thanks to results of Eichler and Shimura.

Theorem 6.3. *Let $f \in S_2(\Gamma_0(N))$ be a normalized eigenform whose Fourier coefficients $a_n(f)$ are all integers. Then there exists an elliptic curve E_f defined over $\mathbb{Q}$ such that $L(E_f, s) = L(f, s)$.*

Proof. Construction of E_f. Consider the differential form $\omega_f = 2\pi i f(z)dz$, and write $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. To a point $\tau \in \mathbb{H}^*$ we attach the following complex number

$$\varphi(\tau) = \int_\infty^\tau \omega_f \in \mathbb{C}.$$

Let $\gamma \in \Gamma_0(N)$. Then note that

$$\beta_\gamma = \varphi(\gamma\tau) - \varphi(\tau) = \int_\tau^{\gamma_\tau} \omega_f$$

does not depend on τ:

$$\begin{aligned}
\int_\tau^{\gamma\tau} \omega_f &= \int_\tau^\infty \omega_f + \int_\infty^{\gamma\infty} \omega_f + \int_{\gamma\infty}^{\gamma\tau} \omega_f \\
&= \int_\tau^\infty \omega_f + \int_\infty^{\gamma\infty} \omega_f + \int_\infty^\tau \omega_f \\
&= \int_\infty^{\gamma\infty} \omega_f.
\end{aligned}$$

Therefore if denote by Λ_f the following subset of complex numbers

$$\Lambda_f = \left\{ \beta_\gamma = \int_\infty^{\gamma\infty} \omega_f \mid \gamma \in \Gamma_0(N) \right\} \subset \mathbb{C},$$

we get a well-defined map

$$\Gamma_0(N)\backslash\mathbb{H}^* \longrightarrow \mathbb{C}/\Lambda_f.$$

One can show that Λ_f is a lattice, and define E_f to be the elliptic curve corresponding to the complex torus $\mathbb{C}/\Lambda_f$. It is considerably harder to show that E_f is defined over $\mathbb{Q}$, and that $L(E_f, s) = L(f, s)$. □

We may wonder about a converse to the previous result. That is, given an elliptic curve E of conductor N_E, can we find a cusp form of level N_E having the same L-function as that of E? Let us give a name to the elliptic curves E satisfying this property.

Definition 6.3. We say that E is if there is a newform $f \in S_2(\Gamma_0(N_E))$ with $a_p(E) = a_p(f)$. Equivalently, if $L(E, s) = L(f, s)$.

The following theorem, which gives a positive answer to the question we asked, is one of the hallmarks of XX-century number theory. Its proof, spanning hundreds of pages of difficult mathematics, relies on breakthrough work of Andrew Wiles in the nineties, although the full proof needed extra work of Taylor–Wiles and Breuil–Conrad–Diamond–Taylor.

Theorem 6.4. *Let $E/\mathbb{Q}$ be an elliptic curve. Then E is modular.*

Thanks to the above theorem, the L-function of E extends to an entire function, which satisfies a functional equation relating $L(E, s)$ with $L(E, 2-s)$. In fact, there is no known proof of these two facts that does not need modularity of E. Finally, the Birch–Swinnerton-Dyer conjecture is a prediction about the behavior of $L(E, s)$ near $s = 1$. Recall that the set of points $E(\mathbb{Q})$ of E which have coordinates in the rational numbers has a structure of a finitely-generated group (this is the Mordell–Weil theorem).

Conjecture 6.1. *Let E be an elliptic curve defined over $\mathbb{Q}$. Let $L(E, s)$ be its L-function. Then*

$$\operatorname{ord}_{s=1} L(E, s) = \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}).$$

This conjectures is one of the ten "Millennium" problems proposed in 2000 by the Clay Mathematics Institute, and it is worth 1M$. Very little is known of it. For instance, one does not yet know how to show the particular case

$$L(E, 1) = 0 \overset{?}{\implies} E(\mathbb{Q}) \text{ infinite.}$$

However, thanks to work of B.Gross, D.Zagier and V.Kolyvagin, one has the following result.

Theorem 6.5. *Let $E/\mathbb{Q}$ be a modular elliptic curve.*

1. *Suppose that $L(E,1) \neq 0$. Then $E(\mathbb{Q})$ is finite.*
2. *Suppose that $L(E,1) = 0$ and $L'(E,1) \neq 0$. Then $E(\mathbb{Q})$ has rank one.*

That is, BSD holds if we assume a priori *that* $\operatorname{ord}_{s=1} L(E,s)$ *is at most one.*

The proof of this is also very difficult and uses crucially the modular form f_E attached to E by modularity. This is nowadays no restriction, since by the modularity theorem we know that all elliptic curves over $\mathbb{Q}$ are modular. However, the result of Gross–Zagier and Kolyvagin was proven in the eighties, *before* modularity was proven (or even thought to be attainable). A crucial ingredient that goes in the proof is to be able to produce, in the case of $L(E,1) = 0$, a point $P \in E(\mathbb{Q})$ which has infinite order, as predicted by BSD. It is an open problem to find a point of infinite order in $E(\mathbb{Q})$ knowing that $\operatorname{ord}_{s=1} L(E,s) \geq 2$. This is an example of the recurring phenomenon in mathematics: it is easy to construct objects that are uniquely defined, in what could be thought of as a perverse manifestation of the "axiom of choice".

7 Modular symbols

7.1 First definitions

Let A be an abelian group.

Definition 7.1. An A-valued is a function

$$m\colon \mathbb{P}_1(\mathbb{Q}) \times \mathbb{P}_1(\mathbb{Q}) \longrightarrow A, \quad (r,s) \mapsto m\{r \longrightarrow s\}$$

satisfying, for all r, s and t in $\mathbb{P}_1(\mathbb{Q})$,

1. $m\{r \longrightarrow s\} = -m\{s \longrightarrow r\}$,
2. $m\{r \longrightarrow s\} + m\{s \longrightarrow t\} = m\{r \longrightarrow t\}$.

Denote by $\mathcal{M}(A)$ the abelian group of all A-valued modular symbols. We will also write $\mathcal{M} = \mathcal{M}(\mathbb{C})$.

The group $\mathrm{GL}_2(\mathbb{Q})$ acts on $\mathcal{M}(A)$ on the left, by the rule

$$(\gamma m)\{r \longrightarrow s\} = m\{\gamma^{-1} r \longrightarrow \gamma^{-1} s\}.$$

We are interested in modular symbols invariant under a congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$ and, to simplify the exposition, we will concentrate on $\Gamma = \Gamma_0(N)$. The most important examples of modular symbols will arise from integrating modular forms. Let $f \in S_2(\Gamma_0(N))$ be a *newform*, and define

$$\lambda_f\{r \longrightarrow s\} = \int_r^s 2\pi i f(z)dz.$$

Note that since f is a cusp form the above integrals converge. Moreover, they can be explicitly computed: choose some $\tau \in \mathbb{H}$ and write

$$\int_r^s 2\pi i f(z)dz = \int_r^\tau 2\pi i f(z)dz + \int_\tau^s 2\pi i f(z)dz.$$

If $r = \infty$ then the integral from x to τ can be calculated with the formula

$$\int_\infty^\tau 2\pi i f(z)dz = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n \tau}.$$

Otherwise, choose a matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma\infty = r$ and reduce to the case above, using the change of variables

$$\int_r^\tau 2\pi i f(z)dz = \int_\infty^{\gamma^{-1}\tau} 2\pi i f(\gamma z)d(\gamma z) = \int_\infty^{\gamma^{-1}\tau} 2\pi i (f|_2\gamma)(z)dz.$$

A priori the modular symbol λ_f belongs to $\mathcal{M}(\mathbb{C})$, although a deep theorem of Shimura gives a much more precise description of its values. Define the plus-minus symbols

$$\lambda_f^\pm\{r \longrightarrow s\} = 2\pi i \left(\int_r^s f(z)dz \pm \int_{-r}^{-s} f(z)dz \right).$$

Theorem 7.1. *Let $f \in S_2(\Gamma_0(N))$ be a newform such that*

$$f(q) = \sum_{n=1}^\infty a_n q^n, \quad a_1 = 1, a_n \in \mathbb{Z}.$$

There exists $\Omega_f^+ \in \mathbb{R}$ and $\Omega_f^- \in i\mathbb{R}$ such that

$$\lambda_f^\pm\{r \longrightarrow s\} \in \Omega_f^\pm \mathbb{Z}.$$

Therefore $\frac{1}{\Omega_f^\pm}\lambda_f^\pm \in \mathcal{M}(\mathbb{Z})$.

A crucial property of λ_f and thus of $\lambda_f^\pm$ is their invariance with respect to $\Gamma_0(N)$:

Proposition 7.1. *We have, for all $\gamma \in \Gamma_0(N)$,*

$$\lambda_f\{\gamma r \longrightarrow \gamma s\} = \lambda_f\{r \longrightarrow s\}.$$

Proof. Write $\omega_f = 2\pi i f(z)dz$, and note that:

$$\lambda_f\{\gamma r \longrightarrow \gamma s\} = \int_{\gamma r}^{\gamma s} \omega_f = \int_r^s \omega_f|_2\gamma = \int_r^s \omega_f = \lambda_f\{r \longrightarrow s\}.$$

□

In the next section we will study the space of $\Gamma_0(N)$-invariant modular symbols in more detail.

7.2 The Eichler–Shimura isomorphism

Write $\mathcal{M}^{\Gamma_0(N)}$ for the space of $\Gamma_0(N)$-invariant modular symbols. It is equipped with an action of the Hecke operators T_p with $p \nmid N$, via the formula

$$(T_p m)\{r \longrightarrow s\} = m\{pr \longrightarrow ps\} + \sum_{j=0}^{p-1} m\left\{\frac{r+j}{p} \longrightarrow \frac{s+j}{p}\right\}.$$

Proposition 7.2. *The map $f \mapsto \lambda_f$ is an injective, $\mathbb{C}$-linear Hecke-equivariant map.*

Proof. Assuming that $\lambda_f = 0$, define the following holomorphic function on $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$:

$$F(\tau) = \int_\infty^\tau 2\pi i f(z) dz.$$

Note that $F(\gamma\tau) - F(\tau) = \lambda_f\{r \longrightarrow \gamma r\}$ for any choice of $r \in \mathbb{P}^1(\mathbb{Q})$. Since by assumption $\lambda_f\{r \longrightarrow \gamma r\}$ is zero, we get that F is $\Gamma_0(N)$-invariant. Therefore F is bounded on $\mathbb{H}$, and hence is constant by Liouville's theorem. Therefore $F'(\tau) = 0$. But note that by the fundamental theorem of Calculus $F'(\tau) = 2\pi i f(\tau)$. Hence $f = 0$. □

In order to investigate the image of $f \mapsto \lambda_f$, we first need to know the dimension of $\mathcal{M}^{\Gamma_0(N)}$. Let $g = \dim S_2(\Gamma_0(N))$ and let s be the number of cusps of $\Gamma_0(N)$.

Theorem 7.2. *The space $\mathcal{M}^{\Gamma_0(N)}$ has dimension $2g + s - 1$.*

Therefore the map $f \mapsto \lambda_f$ cannot be surjective, and in fact it will fail to be surjective in two ways. First, complex conjugation gives a natural action on $\mathcal{M}^{\Gamma_0(N)}$, by

$$\overline{m}\{r \longrightarrow s\} = \overline{m\{r \longrightarrow s\}}.$$

However $\overline{\lambda}_f$ is the modular symbol attached to $\overline{2\pi i f(z)dz} = -2\pi i \bar{f}(z) d\bar{z}$, which we didn't consider. Therefore we get a new homomorphism

$$\lambda\colon S_2(\Gamma_0(N)) \oplus \overline{S_2(\Gamma_0(N))} \longrightarrow \mathcal{M}^{\Gamma_0(N)},$$

which is still injective and its image has thus dimension $2g$ inside the $2g + s - 1$-dimensional space $\mathcal{M}^{\Gamma_0(N)}$.

Secondly, we need to consider the so-called .

Definition 7.2. A $\Gamma_0(N)$-invariant modular symbol m is called *Eisenstein* if there exists a $\Gamma_0(N)$-invariant function $M\colon \mathbb{P}^1(\mathbb{Q}) \longrightarrow \mathbb{C}$ such that

$$m\{r \longrightarrow s\} = M(s) - M(r), \quad r, s \in \mathbb{P}^1(\mathbb{Q}).$$

The space of Eisenstein modular symbols has dimension $s-1$ and is linearly disjoint from the image of λ above. This gives a complete description of $\mathcal{M}^{\Gamma_0(N)}$.

Theorem 7.3. *The map λ gives a Hecke-equivariant isomorphism*

$$M_2(\Gamma_0(N)) \oplus \overline{S_2(\Gamma_0(N))} \longrightarrow \mathcal{M}^{\Gamma_0(N)}.$$

7.3 Computation of modular symbols

One important feature of modular symbols is that they are computable. That is, we can calculate the space $\mathcal{M}^{\Gamma_0(N)}$ without using the Eichler–Shimura isomorphism and thus avoiding the computation of path integrals. The key to making this possible consists in noticing that a modular symbol m is determined by "a few" of its values $m\{r \longrightarrow s\}$.

Definition 7.3. Two elements a/b and c/d in $\mathbb{P}^1(\mathbb{Q})$ are if $ad - bc = \pm 1$. Here, we use the convention that these fractions are in reduced terms, and $\infty = 1/0$.

The following lemma is crucial in the algorithms for computing with modular symbols.

Lemma 7.1. *Any two elements a/b and c/d in $\mathbb{P}^1(\mathbb{Q})$ can be joined by a succession of paths between adjacent cusps.*

Proof. It is enough to see how to join a/b to ∞. We will find $t/a' \in \mathbb{P}_1(\mathbb{Q})$ such that:

$$\{a/b \longrightarrow \infty\} = \{a/b \longrightarrow t/a'\} + \{t/a' \longrightarrow \infty\}.$$

Choose a' satisfying

$$a'a \equiv 1 \pmod{b}, \quad |a'| \leq b/2.$$

Next, choose t such that

$$aa' - bt = 1.$$

Then $\{a/b \longrightarrow t/a'\}$ is a path joining adjacent cusps, and we reduced to a problem of smaller size, since $|a'| \leq b/2$. One can see how to adapt the Euclidean algorithm that computes the greatest common divisor of a and b to perform the above calculation. □

Example 7.1. Consider $a/b = 2/3$ and $c/d = 1/0 = \infty$. Then these are not adjacent, but note that $2/3$ is adjacent to $1/2$, that $1/2$ is adjacent to $1/1$, and $1/1$ is adjacent to $1/0$. Therefore we have have joined the cusps $2/3$ and ∞ with a chain of adjacent cusps.

$$2/3 \sim 1/2 \sim 1/0 \sim 1/0$$

Using the first defining property of modular symbols, the above proposition says that a modular symbol is determined by the values $m\{r \longrightarrow s\}$ where r and s are adjacent. That is, a modular symbol is completely determined by its values on

$$\Gamma_0(N)\backslash \left\{ \left(\frac{a}{b}, \frac{c}{d}\right) \mid ad - bc = 1 \right\}.$$

To study this set, define the projective line over $\mathbb{Z}/N\mathbb{Z}$ as

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) = \{(x : y) \in (\mathbb{Z}/N\mathbb{Z})^2 \mid \gcd(x, y, N) = 1\}/\sim,$$

where $(x : y) \sim (x' : y')$ if and only if there is $u \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $x' = ux$ and $y' = uy$.

Lemma 7.2. *The set* $\Gamma_0(N)\backslash \{(\frac{a}{b}, \frac{c}{d}) \mid ad - bc = 1\}$ *is in natural bijection with* $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.

Proof. First, note that the set $\{(\frac{a}{b}, \frac{c}{d}) \mid ad - bc = 1\}$ is in bijection with $\mathrm{SL}_2(\mathbb{Z})$ via $(a/b, c/d) \mapsto \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$. So to conclude the proof we need to show that the map $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto (c : d)$ induces a bijection

$$\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}).$$

To see this, note that the map is surjective, since given $(c : d) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ we can find a matrix in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ whose second row is (c, d). Using that $\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective we can lift this matrix to $\mathrm{SL}_2(\mathbb{Z})$. Secondly, if two matrices in $\mathrm{SL}_2(\mathbb{Z})$ map to the same element in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ then modulo N these matrices are of the form

$$\gamma_1 \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod N, \quad \gamma_2 \equiv \begin{pmatrix} au^{-1} & bu^{-1} \\ cu & du \end{pmatrix} \pmod N.$$

Then note that the product $\gamma_1\gamma_2^{-1}$ is $\gamma_1\gamma_2^{-1} \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod N$, and hence the matrices in $\mathrm{SL}_2(\mathbb{Z})$ are in the same coset for $\Gamma_0(N)$. □

Therefore a modular symbol m is determined by the function

$$[\cdot]_m : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathbb{C}, \quad [b : d]_m = m\{a/b \longrightarrow c/d\}, \quad ad - bc = 1.$$

In particular, the dimension of $\mathcal{M}^{\Gamma_0(N)}$ is finite, bounded by $\#\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.

Note, however, that not all functions $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathbb{C}$ represent a modular symbol. In fact, for such a function to be a modular symbol it has to satisfy some linear relations coming from the two axioms defining modular symbols.

Proposition 7.3. *A function* $\varphi : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathbb{C}$ *satisfies* $\varphi = [\cdot]_m$ *for some modular symbol* $m \in \mathcal{M}^{\Gamma_0(N)}$ *if and only if*

1. $\varphi(x) = -\varphi(\frac{-1}{x})$, *for all* $x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.
2. $\varphi(x) = \varphi(\frac{x}{x+1}) + \varphi(x + 1)$, *for all* $x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$.

Proof. Suppose that $\varphi = [\cdot]_m$ for some modular symbol $m \in \mathcal{M}^{\Gamma_0(N)}$, and let $x = [b\colon d] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Then

$$\begin{aligned}\varphi(x) = \varphi(b\colon d) = [b\colon d]_m &= m\left\{\frac{a}{b} \longrightarrow \frac{c}{d}\right\} \\ &= -m\left\{\frac{-c}{-d} \longrightarrow \frac{a}{b}\right\} = -[-d\colon b]_m = -\varphi(-1/x).\end{aligned}$$

Similarly, we compute

$$\begin{aligned}\varphi(x) = \varphi(b\colon d) = [b\colon d]_m &= m\left\{\frac{a}{b} \longrightarrow \frac{c}{d}\right\} = m\left\{\frac{a}{b} \longrightarrow \frac{a+c}{b+d}\right\} + m\left\{\frac{a+c}{b+d} \longrightarrow \frac{c}{d}\right\} \\ &= [b\colon b+d]_m + [b+d\colon d]_m = \varphi\left(\frac{x}{x+1}\right) + \varphi(x+1).\end{aligned}$$

□

The above proposition allows for an algorithm that computes the space $\mathcal{M}^{\Gamma_0(N)}$, by solving the linear system of equations for φ. Moreover, the Hecke action is also computable on this resulting representation. The details of this were worked out for the first time in [2].

7.4 A worked out example

We compute the space of modular symbols for $\Gamma_0(11)$. First we enumerate the elements of $\mathbb{P}^1(\mathbb{Z}/11\mathbb{Z})$:

$$\mathbb{P}^1(\mathbb{Z}/11\mathbb{Z}) = \{\infty, 0, 1, \ldots, 10\}.$$

Using the two-term relations of Proposition 7.3 we find that if $\varphi \in \mathbb{M}(\Gamma_0(11))$ then:

$$\varphi(\infty) = -\varphi(-1/\infty) = -\varphi(0).$$

Similarly, we find:

$$\begin{aligned}\varphi(1) &= -\varphi(10) \\ \varphi(2) &= -\varphi(5) \\ \varphi(3) &= -\varphi(7) \\ \varphi(4) &= -\varphi(8) \\ \varphi(6) &= -\varphi(9).\end{aligned}$$

Therefore an M-symbol φ is determined by its values on $0, 1, 2, 3, 4, 6$. Now we find the 3-term relations:

x	∞	0	1	2	3	4	5	6	7	8	9	10
$x+1$	∞	1	2	3	4	5	6	7	8	9	10	0
$\frac{x}{x+1}$	1	0	6	8	9	3	10	4	5	7	2	∞

The table above is to be read as follows. For example, the first column says $\varphi(\infty) = \varphi(\infty)+\varphi(1)$. The last column implies, in turn, $\varphi(10) = \varphi(0) + \varphi(\infty)$. We see from the first column that $\varphi(1) = 0$ (and thus $\varphi(10) = 0$). Column 3 gives then that $\varphi(6) = -\varphi(2)$, and Column 4 gives $\varphi(4) = \varphi(3) - \varphi(2)$. All the other columns are redundant, and so any modular symbol φ is (freely) determined by its values on 0, 2 and 3. We can write down a basis $\{f, g, h\}$ for $\mathbb{M}(\Gamma_0(11))$

	∞	0	1	2	3	4	5	6	7	8	9	10
f	-1	**1**	0	**0**	**0**	0	0	0	0	0	0	0
g	0	**0**	0	**1**	**0**	-1	-1	-1	0	1	1	0
h	0	**0**	0	**0**	**1**	1	0	0	-1	-1	0	0

Next we calculate T_2 acting on the basis $\{f, g, h\}$. Since we have only given the definition of T_p on modular symbols, we will need to relate the M-symbols $\{f, g, h\}$ to their corresponding modular symbols. We will abuse notation and use the same notation for those. Each element of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ can be lifted to a matrix in $\mathrm{SL}_2(\mathbb{Z})$. In fact, we can write the following table:

$x = (c\colon d) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$	$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$	$\frac{a}{c} \longrightarrow \frac{b}{d}$
0	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	$\infty \longrightarrow 0$
2	$\left(\begin{smallmatrix} -1 & -1 \\ 2 & 1 \end{smallmatrix}\right)$	$-1/2 \longrightarrow -1$
3	$\left(\begin{smallmatrix} -2 & -1 \\ 3 & 1 \end{smallmatrix}\right)$	$-2/3 \longrightarrow -1$

Let us write $T_2 f = af + bg + ch$, with a, b, c to be determined. Note that $a = (T_2 f)(0)$, and thus we compute:

$$\begin{aligned}
[0]_{T_2(m)} &= (T_2 m)\{\infty \longrightarrow 0\} \\
&= m\{\frac{2}{0} \longrightarrow \frac{0}{1}\} + m\{\frac{\infty+0}{2} \longrightarrow \frac{0+0}{2}\} + m\{\frac{\infty+1}{2} \longrightarrow \frac{0+1}{2}\} \\
&= m\{\infty \longrightarrow 0\} + m\{\infty \longrightarrow 0\} + m\{\infty \longrightarrow \frac{1}{2}\} \\
&= 2m\{\infty \longrightarrow 0\} + m\{\infty \longrightarrow 1\} + m\{1 \longrightarrow \frac{1}{2}\} \\
&= 2[0]_m + [(0\colon 1)]_m + [1\colon 2]_m \\
&= 3[0]_m + [1/2]_m = 3[0]_m + [6]_m.
\end{aligned}$$

Analogous computations give

$$[2]_{T_2(m)} = [1]_m + [4]_m + [5]_m + [7]_m, \quad [3]_{T_2(m)} = [1]_m + [6]_m + [7]_m + [8]_m$$

Note that we could express the resulting values in other ways using the relations for M-symbols, so the above equations are not unique. In any way, this allows us to find that

$$T_2 f = 3f, \quad T_2 g = -f - 2g, \quad T_2 h = -2h.$$

We find then that the matrix of T_2 in the basis $\{f, g, h\}$ is

$$[T_2] = \begin{pmatrix} 3 & -1 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix},$$

whose eigenvalues are 3 and -2 (the eigenvalue -2 with multiplicity 2). Since we have a decomposition $\mathcal{M}(\Gamma_0(11)) \cong \mathcal{E} \oplus S_2(\Gamma_0(11)) \oplus \overline{S_2(\Gamma_0(11))}$, we deduce that $\dim S_2(\Gamma_0(11)) = 1$ (and also $\dim \mathcal{E} = 1$). Moreover, if $F \in S_2(\Gamma_0(11))$ is any nonzero cusp form, then we know that $T_2 F = -2F$, so $a_2(F) = -2$.

Similar computations would give us the Hecke eigenvalues for all T_p operators (with $p \neq 11$). By the Eichler–Shimura construction, these numbers are telling us the number of points of a certain elliptic curve. In fact, let E be the elliptic curve of conductor 11 given by the equation

$$E_{/\mathbb{Q}} \colon y^2 + y = x^3 - x^2 - 10x - 20.$$

When reduced modulo 2, we get $\overline{E}$:

$$\overline{E}_{\mathbb{F}_2} \colon y^2 + y = x^3 + x^2.$$

Note that

$$\#\overline{E}(\mathbb{F}_2) = \#\{\infty, (0,0), (0,1), (1,0), (1,1)\} = 5,$$

which matches with the prediction from the modular symbols computation: we expected $p + 1 - \#E(\mathbb{F}_p) = a_p$ and, in fact: $2 + 1 - 5 = -2$.

Bibliography

[1] Jan Hendrik Bruinier et al. *The 1-2-3 of modular forms*. Ed. by Kristian Ranestad. Universitext. Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004. Springer-Verlag, Berlin, 2008, pp. x+266. isbn: 978-3-540-74117-6. doi: 10.1007/978-3-540-74119-0. url: https://doi.org/10.1007/978-3-540-74119-0.

[2] J. E. Cremona. *Algorithms for modular elliptic curves*. Second. Cambridge University Press, Cambridge, 1997, pp. vi+376. isbn: 0-521-59820-6.

[3] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*. Vol. 228. Springer, 2005.

[4] Jean-Pierre Serre. *A course in arithmetic*. Vol. 7. Springer Science & Business Media, 2012.

Index