Modular Forms

Sarah Zerbes

Spring semester 2021/22

Contents

0 Prologue

Example 0.0.1. Let $z \in \mathbb{C}$, $\Im(z) > 0$. Let $q = e^{2\pi i z}$ and define **Ramanujan's tau function**

$$\Delta(z) = q \cdot \prod_{n \in \mathbb{N}} (1 - q^n)^{24}.$$

This is one of the simplest examples of a modular form. Note that we can "multiply out" the product above which leads us to

$$\Delta(z) = \sum_{n \in \mathbb{N}} \tau(n) q^n$$

for some integers $\tau(n)$.

Facts 0.0.2.

(1) Known to Weierstrass, 1850:

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

(2) Ramanujan proved in 1916 that the integers $\tau(n)$ satisfy the equation

$$\tau(n) = \sum_{d|n} d^{11} \mod 691.$$

(3) Ramanujan also conjectured $\tau(nm) = \tau(n)\tau(m)$ for n, m coprime. This was proved by Mordell in 1917.

(4) In 1972 Swinnerton-Dyer proved $\tau(n)$ satisfies congruences like (2) modulo 2, 3, 5, 7, 23 and 691 but no other primes.

(5) Ramanujan conjectured in 1916 for p prime holds $|\tau(p)| < 2\, p^{11/2}$. This was proved in 1974 by Deligne.

(6) The quantity

$$\frac{\tau(p)}{2p^{11/2}} \in [-1, 1]$$

is distributed in the interval $[-1, 1]$ with density function proportional to $\sqrt{1 - x^2}$. This was conjectured by Sato and Tate (1960s) and proved by Barnet-Lamb, Geraghty, Harris and Taylor in 2009 using Bau Chau Ngo's *Fundamental Lemma* which got Ngo the 2010 Fields Medal.

Example 0.0.3. We now consider another modular form

$$\begin{aligned} f(z) &= q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 + \dots \\ &= \sum_{n=1}^{\infty} a(n)q^n \qquad ' \qquad \text{with } a(n) \in \mathbb{N} \end{aligned}$$

We will later prove the following results:

Theorem.

1. *We have $a(mn) = a(m)(n)$ for all $m, n \geq 1$ with $(m, n) = 1$.*
2. *We have $|a(p)| \leq 2\sqrt{p}$ for all primes p.*

It turns out that this modular form is closely related to the elliptic curve

$$E : Y^2 + Y = X^3 - X^2 - 10X - 20.$$

For p prime, denote by $N(p)$ the number of points on the elliptic curve in $\mathbb{F}_p$. It is easy to see heuristically tat $N(p) \simeq p$.

Theorem. *(Hasse) We have*

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

The theory of modular forms allows one to prove that the elliptic curve E and the modular form f 'correspond' to each other in the following sense:

Theorem. *For all primes p, we have*

$$a(p) = p - N(p).$$

In particular, using the properties of the modular form f, we can easily calculate the quantity $N(p)$ for all p, so f 'knows' about the behaviour of the elliptic curve over $\mathbb{F}_p$. We say that the elliptic curve E is **modular**. It is generally not too difficult to attach an elliptic curve to a modular form (this is called "Eichler–Shimura"); however, it is very difficult indeed to reverse this process, and this is the basis of Andrew Wiles' work on Fermat's Last Theorem. The proof of this result was later completed by Breuil–Conrad–Diamond–Taylor. I will talk a bit more about this when we discuss L-functions of modular forms.

1 The modular group

1.1 The upper half-plane

Definition 1.1.1. Let $\mathcal{H} = \{z \in \mathbb{C} \colon \Im(z) > 0\}$ the **upper half-plane**.

Proposition 1.1.2. *The* ***special linear group*** $\mathrm{SL}_2(\mathbb{R}) = \{A \in \mathrm{GL}_2(\mathbb{R}) \colon \det(A) = 1\}$ *acts on* $\mathcal{H}$ *via*

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

Proof. For $z \in \mathcal{H}$ is $\Im(z) > 0$ and either c or d is nonzero, so $cz + d \neq 0$. Moreover

$$\Im\left(\frac{az+b}{cz+d}\right) = \frac{1}{|cz+d|^2} \Im\left((az+b)(c\overline{z}+d)\right).$$

Say $z = x + iy$ for $x, y \in \mathbb{R}$.

$$\begin{aligned} \Im\left(\frac{az+b}{cz+d}\right) &= \frac{1}{|cz+d|^2} \Im\Big(\underbrace{(ax+b)(cx+d)+acy^2}_{\in\mathbb{R}} + i\underbrace{(ad-bc)}_{=1} y\Big) \\ &= \frac{1}{|cz+d|^2} \Im(z) \ > \ 0 \end{aligned}$$

Therefore $\frac{az+b}{cz+d} \in \mathcal{H}$ for any $z \in \mathcal{H}$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$.

Also it is easy to check that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) z = z$ and $A(Bz) = (AB)z$ for any $z \in \mathcal{H}$ and for any $A, B \in \mathrm{SL}_2(\mathbb{R})$. Thus $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{H}$. □

Note 1.1.3. The matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ acts trivially on $\mathcal{H}$, so the action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}$ factors through the quotient $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/(\pm 1)$, the **projective special linear group**.

Definition 1.1.4. The *automorphy factor* is the function

$$\begin{aligned} j \, : \, \mathrm{SL}_2(\mathbb{R}) \times \mathcal{H} &\to \mathbb{C}, \\ (g, z) &\mapsto cz + d \qquad\qquad \text{for } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{aligned}$$

Proposition 1.1.5. *For any* $k \in \mathbb{Z}$, *we can define a right action of* $\mathrm{SL}_2(\mathbb{R})$ *on the set of holomorphic functions* $\mathcal{H} \to \mathbb{C}$ *given by*

$$(f|_k g)(z) := j(g,z)^{-k} \ f(gz)$$

where $f \colon \mathcal{H} \to \mathbb{C}$ *holomorphic,* $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{R})$. *We will call this the* ***weight k action***.

Proof. Firstly we need to show that $f|_k g$ is a well-defined holomorphic function $\mathcal{H} \to \mathbb{C}$. But this is obvious since $cz + d \neq 0$ and $gz \in \mathcal{H}$ for all $z \in \mathcal{H}$. Clearly also the equation $f|_k 1 = f$ holds. Therefore it remains to show $(f|_k g)|_k h = f|_k(gh)$ for arbitrary $g, h \in \mathrm{SL}_2(\mathbb{R})$. The left hand side of the equation can be rewritten as

$$\begin{aligned}(f|_k g)|_k h &= j(h,z)^{-k}\left((f|_k g)(hz)\right)\\ &= j(h,z)^{-k} j(g,hz)^{-k} f(g(hz))\end{aligned}$$

and the right hand side results in

$$f|_k(gh) = j(gh,z)^{-k} f((gh)z).$$

We already know $(gh)z = g(hz)$. So it remains to show $j(gh,z) = j(h,z)j(g,hz)$. This is the so called **cocycle relation** and can be checked easily. $\square$

1.2 The modular group

Definition 1.2.1. The **modular group** is the group

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\,;\, a,b,c,d \in \mathbb{Z},\ \det(A) = 1 \right\}.$$

The **projective modular group** is $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/(\pm 1)$.

Theorem 1.2.2. *(a) The group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by* $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ *and* $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

(b) Every orbit of $\mathrm{SL}_2(\mathbb{Z})$ *acting on* $\mathcal{H}$ *contains a point of the set* D *defined by*

$$D = \left\{ z \in \mathcal{H}\colon\ -\frac{1}{2} \leq \Re(z) \leq \frac{1}{2} \text{ and } |z| \geq 1 \right\}.$$

(c) If $z \in D$ *and* $gz \in D$ *for some* $g \in \mathrm{SL}_2(\mathbb{Z})$, *then either* $g = \pm 1$ *and* $gz = z$ *or* z *lies on the boundary of* D.

(d) The stabilizer of $z \in \mathcal{H}$ *in* $\mathrm{PSL}_2(\mathbb{Z})$ *is trivial unless* z *is in the orbit of* i *or in the orbit of* $\rho = e^{2\pi i/3}$.

Proof. We will prove all of these statements in 4 steps using a very elegant argument of Serre. Let $G = \mathrm{SL}_2(\mathbb{Z})$ and $G' = \langle S, T\rangle \leq G$.

Step 1. Every G' orbit in $\mathcal{H}$ contains a point of D.

Proof of Step 1. Let $z \in \mathcal{H}$. Since $|cz+d| \geq |c\,\Im(z)|$ and $|cz+d| \geq |c\,\Re(z)+d|$ there exist only finitely many $(c,d) \in \mathbb{Z}^2$ such that $|cz+d| < 1$. Recall $\Im(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)z) = |cz+d|^{-2}\,\Im(z)$. This implies there are only finitely many $g \in G'$ such that $\Im(gz) > \Im(z)$. So the G' orbit of z contains a point of maximal imaginary part. Let this point be z.

We can assume $\Re(z) \in [-\frac{1}{2}, \frac{1}{2}]$ since $Tz = z + 1$. Moreover $\Im(Sz) = |z|^{-2}\,\Im(z)$. But z is a point of maximal imaginary part in the orbit of G', so we get $|z|^{-2}\,\Im(z) \leq \Im(z)$ implying $|z| \geq 1$. Thus $z \in D$. Clearly this proves part (b) of the theorem. $\square$

Step 2. If $z \in D$ and $gz \in D$, where $g \in G$, then one of the following holds:

1. $g = \pm \mathrm{Id}$
2. $g = \pm S$ and $|z| = 1$
3. $g = \pm T$ and $\Re(z) = -\frac{1}{2}$, or $g = \pm T^{-1}$ and $\Re(z) = \frac{1}{2}$
4. $g = \pm ST = \pm\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ or $g = \pm T^{-1}S = \pm\left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ or $g = \pm ST^{-1}S = \pm\left(\begin{smallmatrix} -1 & 0 \\ -1 & -1 \end{smallmatrix}\right)$ and $z = \rho$
5. $g = \pm TS = \pm\left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ or $g = \pm ST^{-1} = \pm\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ or $g = \pm STS = \pm\left(\begin{smallmatrix} -1 & 0 \\ 1 & -1 \end{smallmatrix}\right)$ and $z = \rho + 1$

Proof of Step 2. Let $z \in D$ and $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ such that $z' = gz \in D$. Being free to replace g by g^{-1} and z by z' we can assume that $\Im(z') \geq \Im(z)$. Again recalling $\Im(gz) = |cz + d|^{-2}\, \Im(z)$ we gain $|cz + d| \leq 1$. Furthermore we have

$$|cz + d| \geq |c|\ \Im(z) \geq |c|\ \Im(\rho) = \frac{\sqrt{3}}{2}|c|.$$

Thus $|c| \leq 2/\sqrt{3} < 2$. As $c \in \mathbb{Z}$ we get $c = 0$ or $c = \pm 1$.

- Let $c = 0$. Since $1 \geq |cz + d| = |d|$ we have $d = 0$ or $d = \pm 1$. But $c = d = 0$ is impossible. So $d = \pm 1$ and hence $a = \pm 1$. Therefore $g = \left(\begin{smallmatrix} \pm 1 & b \\ 0 & \pm 1 \end{smallmatrix}\right)$ is the translation by b. But since
$$\Re(z),\, \Re(gz) \in \left[-\frac{1}{2}, \frac{1}{2}\right],$$
this implies that $b = 0$ or $b = \pm 1$. So either $g = \pm \mathrm{Id}$ (case 1) or $g = \pm T$ and $\Re(z) = -\frac{1}{2}$ or $g = \pm T^{-1}$ and $\Re(z) = \frac{1}{2}$.

- Let $c = 1$. Assuming $|d| \geq 2$ leads to the following contradiction:
$$1 \geq |cz + d| = |z + d| \geq |d| - \Re(z) \geq |d| - \frac{1}{2} \geq \frac{3}{2}$$
Thus we have $d = 0$ or $d = \pm 1$.

  Let $d = 0$. Then $1 \geq |cz + d| = |z|$. On the other hand $|z| \geq 1$ as $z \in D$ and therefore $|z| = 1$ (cases 2, 4 or 5 – exercise sheet 1).

  Let $d = 1$. Then $1 \geq |z + 1|$. This is only possible for $z \in D$ if $z = \rho$ (exercise). Since $a - b = 1$, we deduce that wither $(a, b) = (1, 0)$ or $(a, b) = (0, -1)$ (case 4).

  Analogue $d = -1$ implies $z = \rho + 1$ (case 5).

- The case $c = -1$ is analogous to the case $c = 1$.

Since there are no further cases this shows Step 2 (it remains to check the matrices in case 4 and 5 – see exercise sheet 1) and therefore part (c) of the theorem. □

Step 3. Let $z \in D$ such that the stabilizer G_z of z is not $\pm\mathrm{Id}$. Then $z = i$, $z = \rho$ or $z = \rho + 1$.

Proof of Step 3. This follows directly from Step 2 by checking $gz = z$ for all possible g's. Step 3 proves part (d) of the theorem. $\square$

Step 4. It remains to show that $SL_2(\mathbb{Z})$ is generated by S and T.

Proof of Step 4. Let $g \in G$ and let z be an arbitrary point of the interior of D. Then $gz \in \mathcal{H}$ and by Step 1 exists $g' \in G'$ such that $g'(gz) \in D$. Moreover Step 2 implies that either $g'g \in \{\pm\,\mathrm{Id}\}$ or z is on the boundary of D which is by assumption not the case. Thus either $g'g = \mathrm{Id}$ or $g'g = -\,\mathrm{Id}$. Since $S^2 = -\,\mathrm{Id} \in G'$, we deduce that $g \in G'$, so $\mathrm{SL}_2(\mathbb{Z})$ is generated by S and T. This proves part (a) of the theorem. $\square$

Therefore the theorem is proved. $\square$

Remark 1.2.3. We have seen in the proof of Theorem 1.2.2 that $\mathrm{SL}_2(\mathbb{Z})$ is generated by the elements S and T. These satisfy the relations

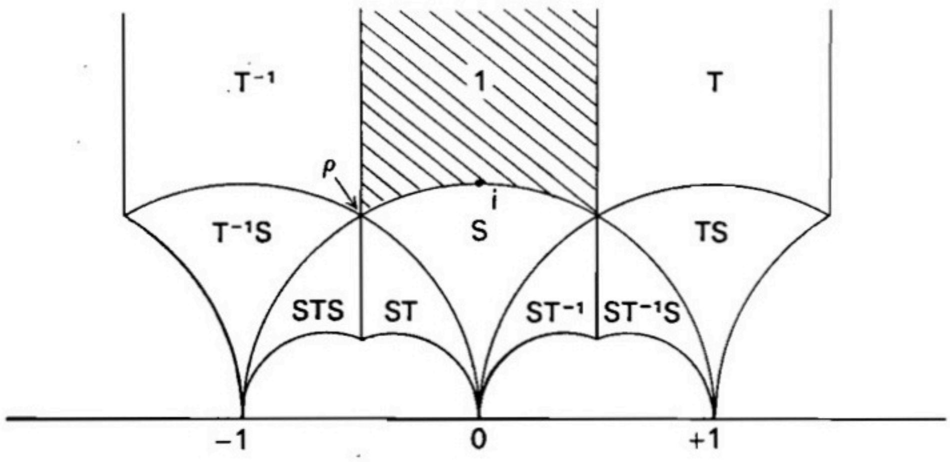
$$S^4 = \mathrm{Id} \quad (ST)^3 = S^2,$$

and one can show that these generate all the relations, i.e. that

$$\langle S, T \mid S^4,\, S^{-2}(ST)^3 \rangle$$

is a presentation of the group $\mathrm{SL}_2(\mathbb{Z})$.

Remark 1.2.4. The set D is called the **fundamental domain**. The figure below represents D itself and the transforms of D by some group elements of $\mathrm{SL}_2(\mathbb{Z})$. Part (c) of the theorem shows that two sets gD and $g'D$ where $g, g' \in \mathrm{SL}_2(\mathbb{Z})$ are either equal (if $g' = \pm g$) or only intersect along their edges. Furthermore part (a) implies that $\mathcal{H}$ is covered by the sets $\{gD \colon g \in \mathrm{SL}_2(\mathbb{Z})\}$: they form a **tesselation** of $\mathcal{H}$.



1.3 Modular forms and modular functions

Definition 1.3.1. A **weakly modular function of weight** k **and level 1** is a meromorphic function $\mathcal{H} \to \mathbb{C}$ such that $f|_k\alpha = f$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, or equivalent

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k \; f(z)$$

for all $z \in \mathcal{H}$ and for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Note 1.3.2. Since $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices S and T, it is sufficient to check invariance under these two matrices, i.e. that

$$f(z+1) = f(z) \qquad \text{and} \qquad f(-1/z) = z^k f(z)$$

for all $z \in \mathcal{H}$.

Lemma 1.3.3. *There are no nonzero weakly modular functions of odd weight.*

Proof. Let k be odd and let f be a weakly modular function of weight k. As shown in (2) we have $f(z) = f(z+1)$ for all $z \in \mathcal{H}$. Moreover we get $f(z) = -f(z+1)$ for all $z \in \mathcal{H}$, since $f|_k\left(\begin{smallmatrix} -1 & -1 \\ 0 & -1 \end{smallmatrix}\right) = -f(\cdot + 1)$. So $f(z) = -f(z)$ and thus $f(z) = 0$ for all $z \in \mathcal{H}$. $\square$

Define the function

$$\begin{aligned} q : \mathcal{H} &\to \mathbb{C}, \\ z &\mapsto \exp(2\pi i z). \end{aligned}$$

Note 1.3.4. Now let f be weakly periodic of weight k. Then f is periodic with period 1, so it can be written in the form

$$f(z) = \tilde{f}(\exp(2\pi i z)),$$

where $\tilde{f}$ is a meromorphic function on the punctured unit disk

$$\mathbb{D}^* = \{q \in \mathbb{C} : \; 0 < |q| < 1\}.$$

Note 1.3.5. The function $\tilde{f}$ is defined by

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

Observe that the logarithm is multi-valued, but choosing a different value of the logarithm is the same as adding an integer to $\frac{\log q}{2\pi i}$. The periodicity of f hence implies that $\tilde{f}(q)$ does not depend on the chosen value of the logarithm.

Note 1.3.6. Any weakly modular function can be written as

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n$$

for some $a_n \in \mathbb{C}$ where $q = e^{2\pi i z}$; we call this the *q-expansion of f*. This is just the Laurent series of $\tilde{f}$ around $q = 0$, which converges for $0 < |q| < \varepsilon$ for ε sufficiently small ($\Leftrightarrow \Im(z) \gg 0$)

Definition 1.3.7.

- We say that f is meromorphic at ∞ if $a_n = 0$ for $n < -N$ and some $N \in \mathbb{N}$.
- We say that f is holomorphic at ∞ if $a_n = 0$ for $n < 0$. In this case, we define the value of f at ∞ to be $f(\infty) = \tilde{f}(0) = a_0$.

Definition 1.3.8. Let f be a weakly modular function of weight k and level 1.

1. If f is meromorphic on $\mathcal{H} \cup \{\infty\}$ we say f is a **modular function** (of weight k and level 1).
2. If f is holomorphic on $\mathcal{H} \cup \{\infty\}$ we say f is a **modular form** (of weight k and level 1).
3. If f is holomorphic on $\mathcal{H} \cup \{\infty\}$ and $f(\infty) = 0$ we say f is a **cuspidal modular form** or **cusp form**.

Note 1.3.9. If f and g are modular forms (resp. modular functions) of level 1 and weights k and ℓ, then the product fg is a modular form (resp. modular function) of weight $k + \ell$.

1.4 Eisenstein series

Definition 1.4.1. Let $k \geq 4$ even. Define the **Eisenstein series of weight** k to be the function $G_k \colon \mathcal{H} \to \mathbb{C}$ given by

$$G_k(z) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{0\}} \frac{1}{(mz+n)^k}. \tag{1.1}$$

Recall the following result from complex analysis:

Proposition 1.4.2. *Let U be an open subset of $\mathbb{C}$, and let $(f_n)_n \geq 0$ be a sequence of holomorphic functions on U that converges uniformly on compact subsets of U. Then the limit function $U \to \mathbb{C}$ is holomorphic.*

Lemma 1.4.3. *The series defining $G_k(z)$ converges absolutely and uniformly on subsets of $\mathcal{H}$ of the form*

$$R_{r,s} = \{x + iy : |x| \le r, \, y \ge s\}.$$

It hence converges to a holomorphic function on $\mathcal{H}$.

Proof. Let $z = x + iy \in R_{r,s}$. We have

$$|mz + n|^2 = (mx + n)^2 + m^2y^2 \ge (mx + n)^2 + m^2s^2.$$

For fixed m and n, we distinguish the cases $|n| \le 2r|m|$ and $|n| \ge 2r|m|$. In the first case, we have

$$|mz + n|^2 \ge m^2s^2 \ge \frac{s^2}{2}m^2 + \frac{s^2}{2(2r)^2}n^2 \ge \min\left\{\frac{s^2}{2}, \frac{s^2}{8r^2}\right\} \cdot (m^2 + n^2).$$

In the second case, the triangle inequality implies

$$|mz + n|^2 \ge (|mx| - |n|)^2 + m^2s^2 \ge \left(\frac{|n|}{2}\right)^2 + m^2s^2 \ge \min\left\{\frac{1}{4}, s^2\right\} \cdot (m^2 + n^2).$$

Combining both cases and putting

$$c = \min\left\{\frac{s^2}{2}, \frac{s^2}{8r^2}, \frac{1}{4}, s^2\right\},$$

we get the inequality

$$|mz + n| \ge c^{1/2}(m^2 + n^2)^{1/2} \quad \text{for all } m, n \in \mathbb{Z}, \ z \in R_{r,s}.$$

Hence for all $z \in R_{r,s}$, we have

$$G_k(z) \le \frac{1}{c^{k/2}} \sum_{(m,n)\ne(0,0)} \frac{1}{(m^2 + n^2)^{k/2}}.$$

We rearrange the sum by grouping together, for each fixed $j = 1, 2, 3, \ldots$, all pairs (m, n) with $\max\{|m|, |n|\} = j$. We note that for each j there are $8j$ such pairs (m, n), each of which satisfies

$$j^2 \le m^2 + n^2.$$

Hence

$$|G_k(z)| \le \frac{1}{c^{k/2}} \sum_{j=1}^{\infty} \frac{8j}{j^k} = \frac{8}{c^{k/2}} \sum_{j=1}^{\infty} \frac{1}{j^{k-1}},$$

which is finite and independent of $z \in R_{r,s}$, so $G_k(z)$ converges absolutely and uniformly on $R_{r,s}$. Since every compact subset of $\mathcal{H}$ is contained in some $R_{r,s}$, this finishes the proof by Proposition 1.4.2. □

Remark 1.4.4. This proof clearly fails for $k = 2$. One can show that for $k = 2$, the series (1.1) is conditionally but not absolutely convergent. We will come back to this issue later in the course.

Proposition 1.4.5. *For every even integer $k \geq 4$, the function G_k is a modular form of weight k and level 1. The q-expansion of G_k is given by*

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

where $\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$ (the Riemann zeta function) and $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$.

Proof. One easily checks that $G_k(z+1) = G_k(z)$. Moreover, we have

$$\begin{aligned} G_k\left(-\frac{1}{z}\right) &= \sum_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} \frac{1}{(m(-\frac{1}{z})+n)^k} \\ &= z^k \sum_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} \frac{1}{(-m+nz)^k} \\ &= z^k\, G_k(z). \end{aligned}$$

Hence $G_k|_k S = G_k$ and $G_k|_k T = G_k$, so $G_k|_k \alpha = G_k$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ by Theorem 1.2.2 (a). Thus G_k is a weakly modular function of weight k and level 1.

It remains to show that G_k is holomorphic at ∞. Therefore we will determine the q-expansion of G_k. Consider the formula $\sum_{n\in\mathbb{Z}} \frac{1}{z+n} = \pi \cdot \cot(\pi z)$. Thus we obtain

$$\sum_{n\in\mathbb{Z}} \frac{1}{z+n} = \pi \cdot \cot(\pi z) = i\pi \left(\frac{e^{2\pi i z}+1}{e^{2\pi i z}-1}\right) = i\pi \left(1 + \frac{2}{q-1}\right) = i\pi - 2\pi i \sum_{n=0}^{\infty} q^n,$$

where $q = e^{2\pi i z}$. Differentiating $(k-1)$ times with respect to z, and using that $\frac{\partial}{\partial z} = 2\pi i q \frac{\partial}{\partial q}$, leads to

$$\begin{aligned} \sum_{n\in\mathbb{Z}} \frac{-(k-1)!}{(z+n)^k} &= \frac{\partial^{k-1}}{\partial z^{k-1}} \left(i\pi - 2\pi i \sum_{n=0}^{\infty} q^n \right) \\ &= -2\pi i \sum_{n=1}^{\infty} (2\pi i n)^{k-1} q^n \\ &= -(2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} q^n \end{aligned}$$

(We are using here that k is even; for k odd we get an additional $-$ sign.)

Hence we get

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

Now we can split up the original sum of the function G_k into two parts, one where $m = 0$ and one where $m \neq 0$. Afterwards we will simplify both parts using symmetry (remember again that k is even) of the sums and the above formula:

$$\begin{aligned}
G_k(z) &= \sum_{n\in\mathbb{Z}\setminus\{0\}} \frac{1}{n^k} + \sum_{m\in\mathbb{Z}\setminus\{0\}} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^k} \\
&= 2\sum_{n=1}^{\infty} \frac{1}{n^k} + 2\sum_{m=1}^{\infty} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^k} \\
&= 2\zeta(k) + 2\sum_{m=1}^{\infty} t_k(mz) \\
&= 2\zeta(k) + 2\sum_{m=1}^{\infty} \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} e^{2\pi i n m z} \\
&= 2\zeta(k) + \frac{2\cdot(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} n^{k-1} q^{nm}
\end{aligned}$$

From there we obtain the proposed q-expansion by resorting the last sum:

$$G_k(z) = 2\zeta(k) + \frac{2\cdot(2\pi i)^k}{(k-1)!} \sum_{l=1}^{\infty} \underbrace{\sum_{d\mid l} d^{k-1}}_{\sigma_{k-1}(l)} q^l$$

And since G_k has a q-expansion without any negative powers of q, G_k is holomorphic at ∞. Thus G_k is indeed a modular form. $\square$

Definition 1.4.6. The Bernoulli numbers are the rational numbers B_k, for $k \geq 0$, defined by the equation

$$\frac{t}{\exp(t)-1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} t^k \in \mathbb{Q}[[t]].$$

Remark 1.4.7. The Bernoulli numbers are of great importance in mathematics. Barry Mazur once said: *"When a Bernoulli number sneezes, the tremors can be felt in all of mathematics."*

Lemma 1.4.8. *We have*

$$B_k \neq 0 \qquad \Leftrightarrow \qquad k = 1 \text{ or } k \text{ is even.}$$

Proof. Exercise sheet 2. $\square$

Example 1.4.9. The first few non-zero Bernoulli numbers

$$B_0 = 0, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{3}, \quad B_6 = \frac{1}{42},$$
$$B_8 = -\frac{1}{30}, \quad B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2730}.$$

Lemma 1.4.10. *If $k \geq 2$ is an even integer, then*

$$\zeta(k) = -\frac{(2\pi i)^k B_k}{2 \cdot k!}.$$

Proof. Exercise sheet 2. □

Definition 1.4.11. Let $k \geq 4$ be even. The normalised **Eisenstein series** of weight k is given by

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

1.5 The valence formula

Definition 1.5.1. Let $f \neq 0$ be a meromorphic function $\mathcal{H} \to \mathbb{C}$ and let $P \in \mathcal{H}$. The unique integer n such that $(z-P)^{-n} f(z)$ is holomorphic and non-vanishing at P is called the **order of f at P** and denoted by $v_P(f)$. We say f has a **zero of order n at P** if n is positive, and f has a **pole of order n at P** if n is negative.

Definition 1.5.2. Consider the Laurent expansion of f around P

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

Then the **residue of f at P** is $\mathrm{Res}_P(f) = c_{-1} \in \mathbb{C}$.

Lemma 1.5.3. *If f is meromorphic around a point P, then*

$$\mathrm{Res}_P(f/f') = v_P(f).$$

Proof. Exercise. □

We recall without proof the following results from complex analysis:

Theorem 1.5.4. *(Cauchy's integral formula) Let g be a holomorphic function on an open subset $U \subseteq \mathbb{C}$ and let C be a contour in U. Then for each $P \in U$, we have*

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

Corollary 1.5.5. *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*

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

(Here, we integrate counterclockwise.)

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

Theorem 1.5.6. *(Argument principle) 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*
$$\int_C \frac{f'(z)}{f(z)} dz = 2\pi i \sum_{P \in \mathrm{int}(C)} v_P(f).$$

Note 1.5.7. By Lemma 1.5.3, we have
$$\int_C \frac{f'(z)}{f(z)} dz = 2\pi i \sum_{P \in \mathrm{int}(C)} \mathrm{Res}_P(f'/f). \tag{1.2}$$

Corollary 1.5.8. *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*
$$\lim_{r \to 0} \int_{C(P,r,\alpha)} \frac{f'(z)}{f(z)} dz = \alpha i \cdot v_P(f).$$

Now assume that f is a weakly modular funktion (of weight k and level 1).

Remark 1.5.9. Since $f|_k \alpha = f$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, we have $v_{\alpha P}(f) = v_p(f)$. Hence $v_P(f)$ is well-defined for P being a $\mathrm{SL}_2(\mathbb{Z})$ orbit in $\mathcal{H}$.

Moreover, if f is meromorphic at ∞, we can define the order of f at ∞ by
$$v_\infty(f) := v_0(\tilde{f}).$$

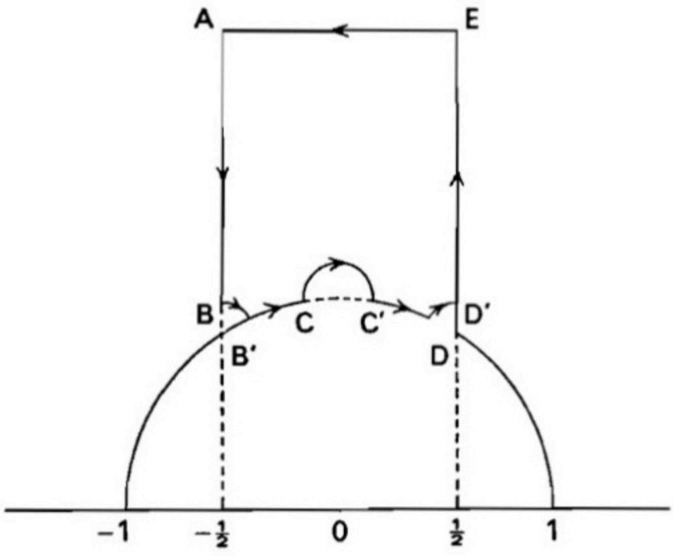
The following theorem is fundamental for studying the spaces of modular forms:

Theorem 1.5.10. *(The valence formula) Let $f \neq 0$ be a modularfunction of weight k and level 1. Then f has finitely many $\mathrm{SL}_2(\mathbb{Z})$-orbits of zeros and poles in $\mathcal{H}$, and*
$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{P \in W} v_P(f) = \frac{k}{12}, \tag{1.3}$$
where $\rho = e^{2\pi i/3}$ and W is the set of all $\mathrm{SL}_2(\mathbb{Z})$-orbits in $\mathcal{H}$ except the orbits of i and ρ.

Proof. Recall the fundamental domain from 1.2.2 and let $\mathcal{C}$ be the contour as shown in the figure below. Here $\Im(A) = \Im(E) = R$ (we will later let $R \to +\infty$) and the three small circles have radius r. We assume that R is sufficiently large and r sufficiently small that the interior of $\mathcal{C}$ contains all the zeros and poles of f except those at i, ρ, $\rho + 1$ and ∞.

Simplifying assumption: We assume for simplicity f has no zeros or poles on the boundary of the fundamental domain, except possibly at i and ρ. (In the case where it does contain zeros or poles of f, the contour has to be modified using additional small arcs going around these zeros or poles in the counterclockwise direction.)

We will now calculate $\int_{\mathcal{C}} \frac{f'(z)}{f(z)} dz$ in two different ways and compose the results afterwards.



(1) Computing the integral using Theorem 1.5.6, we get

$$\int_{\mathcal{C}} \frac{f'(z)}{f(z)} dz = 2\pi i \sum_{P \in \text{interior}(\mathcal{C})} v_P(f) = 2\pi i \sum_{P \in W} v_P(f),$$

where W is the set described in the stated theorem. The last equality is satisfied by the simplifying assumption, so the interior of the fundamental domain contains exactly one representative of every pole or zero $\mathrm{SL}_2(\mathbb{Z})$-orbit of $\mathcal{H}$.

(2) Secondly, we estimate the integral by splitting up the contour in 8 parts. Let $\mathcal{C}_1$ be the part from E to A, $\mathcal{C}_2$ be the part from A to B, and so on, such that in the end $\mathcal{C}_8$ is the part from D' to E.

(i) Note that since f is a modular function, we have $f(z) = f(z+1)$. Hence also $f'(z) = f'(z+1)$, and we have

$$\int_{\mathcal{C}_2} \frac{f'(z)}{f(z)} dz = \int_{\mathcal{C}_2} \frac{f'(z+1)}{f(z+1)} dz = -\int_{\mathcal{C}_8} \frac{f'(z)}{f(z)} dz,$$

so

$$\int_{\mathcal{C}_2} \frac{f'(z)}{f(z)} dz + \int_{\mathcal{C}_8} \frac{f'(z)}{f(z)} dz = 0.$$

(ii) Now we consider $\mathcal{C}_1$ and change the variable by $q(z) = e^{2\pi i z}$. This maps $\mathcal{C}_1$ to a clockwise oriented circle around the origin with radius $e^{-2\pi R}$. Furthermore we have $f(z) = \tilde{f}(q(z))$, thus $f'(z) = \tilde{f}'(q(z))\, q'(z)$ and since f is a modular function, $\tilde{f}$ is meromorphic at 0. Therefore

$$\begin{aligned}\int_{\mathcal{C}_1} \frac{f'(z)}{f(z)} dz &= \int_{\mathcal{C}_1} \frac{\tilde{f}'(q(z))q'(z)}{\tilde{f}(q(z))} dz \\ &= \int_{q(\mathcal{C}_1)} \frac{\tilde{f}'(q)}{\tilde{f}(q)} dq \\ &= -2\pi i \operatorname{Res}_0 \left(\frac{\tilde{f}'}{\tilde{f}}\right) \\ &= -2\pi i \ v_0(\tilde{f}) \\ &= -2\pi i \ v_\infty(f).\end{aligned}$$

(iii) $\mathcal{C}_5$ is half of a circle around i. We deduce from Corollary 1.5.8 that

$$\lim_{r\to 0} \int_{\mathcal{C}_5} \frac{f'(z)}{f(z)} dz = -\frac{1}{2} \ 2\pi i \ v_i(f).$$

Similarly we get

$$\begin{aligned}\lim_{r\to 0} \int_{\mathcal{C}_3} \frac{f'(z)}{f(z)} dz &= -\frac{1}{6} \ 2\pi i \ v_\rho(f) \\ \lim_{r\to 0} \int_{\mathcal{C}_7} \frac{f'(z)}{f(z)} dz &= -\frac{1}{6} \ 2\pi i \ v_{\rho+1}(f) = -\frac{1}{6} \ 2\pi i \ v_\rho(f).\end{aligned}$$

(iv) So it remains to study $\mathcal{C}_4$ and $\mathcal{C}_6$. Therefore consider $u(z) = -\frac{1}{z}$. This maps $\mathcal{C}_6$ to $-\mathcal{C}_4$ and we have $f(z) = z^{-k} f(u(z))$, hence

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

So

$$\begin{aligned}\int_{\mathcal{C}_4} \frac{f'(z)}{f(z)} dz &= \int_{\mathcal{C}_4} \frac{-k}{z} dz + \int_{\mathcal{C}_4} \frac{f'(u(z))u'(z)}{f(u(z))} dz \\ &= \frac{2\pi i k}{12} + \int_{u(\mathcal{C}_4)} \frac{f'(u)}{f(u)} du \\ &= \frac{2\pi i k}{12} - \int_{\mathcal{C}_6} \frac{f'(u)}{f(u)} du\end{aligned}$$

and thus

$$\int_{\mathcal{C}_4} \frac{f'(z)}{f(z)} dz + \int_{\mathcal{C}_6} \frac{f'(z)}{f(z)} dz = 2\pi i \frac{k}{12}.$$

Composing (i) to (iv) yields

$$\int_{\mathcal{C}} \frac{f'(z)}{f(z)} dz = 2\pi i \left(\frac{k}{12} - \frac{1}{3} v_\rho(f) - \frac{1}{2} v_i(f) - v_\infty(f)\right).$$

Combining this with the result in (1) gives us exactly the proposed formula. $\square$

1.6 Applications to modular forms

The valence formula provides some interesting consequences to spaces of modular forms which we will investigate below.

Definition 1.6.1. Let M_k be the set of all modular forms of weight k and level 1 and let S_k be the set of all cusp forms of weight k and level 1.

Remark 1.6.2. It can be easily checked that these are both vector spaces over $\mathbb{C}$.

Lemma 1.6.3.

(a) $M_k = \{0\}$ *for* $k < 0$ *and* $k = 2$.

(b) $S_k = \{0\}$ *for* $k < 12$.

(c) M_0 *is the set of all constant functions* $\mathcal{H} \to \mathbb{C}$ *and thus isomorphic to* $\mathbb{C}$.

Proof. (a) Let $f \in M_k$, $f \neq 0$. Then $v_z(f) \geq 0$ for all $z \in \mathcal{H} \cup \{\infty\}$. So by the valence formula we get $k \geq 0$. Moreover a sum of non-negative integer multiples of $\frac{1}{2}$ and $\frac{1}{3}$ can't equal $\frac{1}{6}$. Thus $k \neq 2$.

(b) Let $f \in S_k$, $f \neq 0$. Then $v_\infty(f) \geq 1$, hence $k \geq 12$ by valence formula.

(c) Let $f \in M_0$. Then the constant function $g := f(\infty)$ is also in M_0, so $f - g \in S_0$ and therefore $f = g$ since $S_0 = \{0\}$.

□

Definition 1.6.4. Define

$$\Delta = \frac{E_4^3 - E_6^2}{1728}.$$

Remark 1.6.5. In the prologue of this lecture we defined $\Delta = q \cdot \prod_{n \in \mathbb{N}} (1 - q^n)^{24}$. We will prove later that this is indeed the same Δ as the one in Definition 1.6.4.

Note 1.6.6. Since E_4 and E_6 are modular forms of weight 4 and 6, respectively, Δ is a modular form of weight 12. Since the q-expansion has zero constant coefficient, it is indeed a cusp form.

Lemma 1.6.7. *The modular form* Δ *has a simple zero at* ∞ *and no other zeros.*

Proof. Using the known q-expansions of E_4 and E_6, one can compute the q-expansion of Δ as

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + \dots,$$

so Δ has a simple zero at ∞. Now since Δ is a modular form, all the quantities $v_\star(\Delta)$ occurring in Theorem 1.5.10 are non-negative, so the only way to get equality is if there are no zeros apart from the one at ∞. □

Proposition 1.6.8. *S_{12} is one-dimensional over $\mathbb{C}$ and spanned by Δ.*

Proof. Let $f \in S_{12}$ and define a function g by

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

This function is well-defined since Δ does not vanish on $\mathcal{H}$, so $\Delta(i) \neq 0$. Clearly $g \in S_{12}$ and $g(i) = 0$. Using the valence formula yields

$$v_\infty(g) + \frac{1}{2}v_i(g) + \frac{1}{3}v_\rho(g) + \sum_{p\in W} v_p(g) = 1.$$

But this is a contradiction since $v_\infty(g) \geq 1$ and $v_i(g) \geq 1$. Therefore g has to be zero and

$$f = \frac{f(i)}{\Delta(i)}\Delta \in \mathbb{C}\cdot\Delta.$$

□

Corollary 1.6.9.

1. *For all $k \in \mathbb{Z}$, the map*
$$M_k \to S_{k+12},\ f \mapsto f\cdot\Delta$$
is an isomorphism.

2. *For $k \geq 4$ we have $M_k = S_k \oplus (\mathbb{C}\cdot E_k)$.*

Proof. The first statement is trivial for $k < 0$ since then $M_k = S_{k+12} = \{0\}$ by Lemma 1.6.3 (a), (b). So let $k \geq 0$. As Δ is non-vanishing the given map is clearly an injection. Now let $g \in S_{k+12}$. Then $\frac{g}{\Delta}$ is weakly modular of weight $(k+12) - 12 = k$ and holomorphic on $\mathcal{H}$ since Δ is non-vanishing. Furthermore $v_\infty(g) \geq 1$ by assumption, so

$$v_\infty\left(\frac{g}{\Delta}\right) = v_\infty(g) - v_\infty(\Delta) = v_\infty(g) - 1 \geq 0.$$

So $\frac{g}{\Delta} \in M_k$. Therefore the given map is also onto, thus bijectiv.

For the second part of the corollary we just have to note that S_k is the kernel of the linear map $M_k \to \mathbb{C},\ f \mapsto f(\infty)$. Thus we have $\dim(M_k/S_k) \leq 1$. On the other hand we know that $E_k \in M_k \setminus S_K$ since $E_k(\infty) \neq 0$. So $M_k = S_k \oplus (\mathbb{C}\ E_k)$. □

Theorem 1.6.10.

(a) The space M_k is finite dimensional over $\mathbb{C}$ for all $k \in \mathbb{Z}$.

(b) Let $k \geq 0$ even. Then

$$\dim(M_k) = \begin{cases} 1 + \left\lfloor \frac{k}{12} \right\rfloor, & k \neq 2 \mod 12, \\ \left\lfloor \frac{k}{12} \right\rfloor, & k = 2 \mod 12. \end{cases}$$

Otherwise $M_k = \{0\}$.

(c) A basis for M_k is given by $\{E_4^a E_6^b \colon a, b \in \mathbb{N}_0, 4a + 6b = k\}$.

Proof. (a) This is a consequence of part (b).

(b) We will prove this by induction on k. First of all note that the statement is clear for odd k since there aren't any nonzero weakly modular functions of odd weight. Moreover we already know that $\dim(M_0) = 1$, $\dim(M_2) = 0$ and $\dim(M_k) = 0$ for $k < 0$ by Lemma 1.6.3 (a) and (c). In addition we have $\dim(M_k) = 1$ for $k = 4, \ldots, 10$ since $\dim(M_k) = \dim(S_k) + 1$ by Corollary 1.6.9 and $S_k = \{0\}$ for these k's by Lemma 1.6.3 (b). Hence the statement is true for $k = 0, \ldots, 10$.

Let now $k \geq 12$. Then

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

since $\dim(S_k) = \dim(M_{k-12})$ by Corollary 1.6.9. So the statement is true for all k by induction in steps of 12.

(c) We will use again induction to prove the statement. Note that there is nothing to show for odd k, $k < 0$ and $k = 2$ since in these cases $M_k = \{0\}$. The case $k = 0$ is also trivial because M_0 is the set of all constant functions, hence generated by $1 = E_4^0 E_6^0$.

Let now $k \geq 4$ be even. Obviously there is always a pair (a, b) such that $a, b \in \mathbb{Z}_{\geq 0}$ and $4a + 6b = k$. Pick such a pair. Let $f \in M_k$. Then f can be written in the form

$$f = \lambda \, E_4^a E_6^b + g$$

for some $\lambda \in \mathbb{C}$ and $g \in S_k$ since the modular form $E_4^a E_6^b$ is in M_k and does not vanish at infinity. So there is an $h \in M_{k-12}$ such that $g = h \cdot \Delta$ by corollary 1.6.9 and by induction we may assume h to be a linear combination of $E_4^r E_6^s$ where $r, s \in \mathbb{Z}_{\geq 0}$ and $4r + 6s = k - 12$. Hence

$$h \cdot \Delta = h \cdot \left(\frac{E_4^3 - E_6^2}{1726} \right)$$

is a linear combination of $E_4^{r+3} E_6^s$ and $E_4^r E_6^{s+2}$ and since

$$4(r + 3) + 6s = 4r + 6(s + 2) = k$$

the function h is a linear combination of $E_4^p E_6^q$ with $4p + 6q = k$. So the linear span of these functions contains g and hence also f. Therefore

$$M_k = \operatorname{span}\{E_4^a E_6^b \colon a, b \in \mathbb{N}_0, 4a + 6b = k\}.$$

To show that the given set is indeed a basis of M_k it suffices to check that

$$\left| \left\{ (a, b) \in \mathbb{Z}_{\geq 0}^2 \colon 4a + 6b = k \right\} \right| = \dim(M_k).$$

This can again be easily seen by induction in steps of 12 (exercise).

$\square$

Example 1.6.11. For the first few values of k, the dimensions of M_k and S_k are given by

k	$\dim M_k$	$\dim S_k$
0	1	0
2	0	0
4	1	0
6	1	0
8	1	0
10	1	0
12	2	1
14	1	0
16	2	1

Example 1.6.12. Both, E_4^2 and E_8 are in M_8. But $\dim(M_8) = 1$ by Theorem 1.6.10 (b). Hence E_4^2 and E_8 are linearly dependent and as both are 1 at infinity, we can conclude that E_4^2 and E_8 are equal. So

$$\left(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n\right)^2 = E_4^2 = E_8 = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n$$

, so

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

This is very hard to prove (or even conjecture!) without using the theory of modular forms.

Example 1.6.13. From the theorem, we deduce that

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

I claim that another basis for the same space is given by

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

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

The following theorem is a very useful consequence of the fact that the spaces of modular forms are finite-dimensional:

Theorem 1.6.14. *Let f be a modular form of weight k and level 1 with q-expansion $\sum_{n=0}^{\infty} a_n q^n$. Suppose that*

$$a_j = 0 \qquad \text{for all } j = 0, \ldots, \lfloor k/12 \rfloor.$$

Then $f = 0$.

Proof. Suppose that $f \neq 0$. Then the hypothesis implies that

$$v_\infty(f) \geq \lfloor k/12 \rfloor + 1 > k/12.$$

Hence the left-hand side of (1.3) is strictly greater than $k/12$, which gives a contradiction. $\square$

Corollary 1.6.15. *Let f, g be modular forms of the same weight k and level 1, with q-expansions $\sum_{n=0}^{\infty} a_n q^n$ and $\sum_{n=0}^{\infty} b_n q^n$, respectively. Suppose that*

$$a_j = b_j \qquad \text{for all } j = 0, ..., \lfloor k/12 \rfloor.$$

Then $f = g$.

Corollary 1.6.15 is a very powerful tool: it allows us to conclude that two modular forms are identical if we only know a priori that their q-expansions agree to a certain finite precision.

1.7 The q-expansion of Δ

The aim of this section is to prove the product formula for the q-expansion of Δ. We start with the following definition:

Definition 1.7.1. We define

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

and $E_2(z) = \frac{3}{\pi^2} \cdot G_2(z)$.

Lemma 1.7.2.

1. *The series in Definition 1.7.1 is convergent, but not absolutely convergent, and defines a holomorphic function on $\mathcal{H}$*[1].
2. *We have*

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

Proof. 1. Exercise.
2. Argue as in the proof of proposition 1.4.5. $\square$

Proposition 1.7.3. *The functions G_2 and E_2 satisfies the transformation property*

$$z^{-2} G_2\left(-\frac{1}{z}\right) = G_2(z) - 2\pi i z, \tag{1.4}$$

$$z^{-2} E_2\left(-\frac{1}{z}\right) = E_2(z) - \frac{6i}{\pi z}. \tag{1.5}$$

[1]It is not a modular form, however: it can't be, since $M_2 = \{0\}$.

The proof of this result is based on the following lemma, which gives an example of two double series that contain the same terms but sum to different values due to the order of summation being different.

Lemma 1.7.4. *For all $z \in \mathcal{H}$, we have*

$$\sum_{m\neq 0}\sum_{n\in\mathbb{Z}}\left(\frac{1}{mz+n}-\frac{1}{mz+n+1}\right)=0, \tag{1.6}$$

$$\sum_{n\in\mathbb{Z}}\sum_{m\neq 0}\left(\frac{1}{mz+n}-\frac{1}{mz+n+1}\right)=-\frac{2\pi i}{z}. \tag{1.7}$$

Proof. We start with the sum

$$\sum_{-N\leq n<N}\left(\frac{1}{mz+n}-\frac{1}{mz+n+1}\right)=\frac{1}{mz-N}-\frac{1}{mz+N}.$$

Using this, we compute the inner sum of (1.6) as

$$\sum_{n\in\mathbb{Z}}\left(\frac{1}{mz+n}-\frac{1}{mz+n+1}\right)=\lim_{N\to\infty}\sum_{-N\leq n<N}\left(\frac{1}{mz+n}-\frac{1}{mz+n+1}\right) \tag{1.8}$$

$$=\lim_{N\to\infty}\frac{1}{mz-N}-\frac{1}{mz+N}. \tag{1.9}$$

$$=0, \tag{1.10}$$

which implies (1.6).

The proof of the second formula is more complicated, and I will not give the proof here. For a reference, see Serre's "A course in Arithmetic". ☐

We can now prove Proposition 1.7.3:

Proof. Recall that

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

Subtracting (1.6) and simplifying, we obtain the alternative expression

$$G_2(z)=2\zeta(2)+\sum_{m\neq 0}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^2(mz+n+1)}. \tag{1.11}$$

Also, we have

$$z^{-2}G_2(-1/z)=2\zeta(2)z^{-2}+\sum_{m\neq 0}\sum_{n\in\mathbb{Z}}\frac{1}{(nz-m)^2} \tag{1.12}$$

$$=2\zeta(2)+\sum_{m\in\mathbb{Z}}\sum_{n\neq 0}\frac{1}{(nz-m)^2} \tag{1.13}$$

$$=2\zeta(2)+\sum_{n\in\mathbb{Z}}\sum_{m\neq 0}\frac{1}{(mz+n)^2}; \tag{1.14}$$

note that in the second equality we just relabelled the parameters, but did not change the order of summation.

Subtracting (1.7) and simplifying, we obtain

$$z^{-2}G_2(-1/z) + \frac{2\pi i}{z} = 2\zeta(2) + \sum_{n\in\mathbb{Z}}\sum_{m\neq 0}\frac{1}{(mz+n)^2(mz+n+1)}, \tag{1.15}$$

and by imitating the proof of Lemma 1.4.3 one can show that the sum on the right-hand side is absolutely convergent. We can hence change the order of summation, and we see that (1.15) is equal to (1.11). □

Corollary 1.7.5. *The q-expansion of Δ is given by*

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

Proof. Let $D(z) = q\prod_{n\geq 1}(1-q^n)^{24}$.

Let $D(z) = q\cdot\prod_{n=1}^{\infty}(1-q^n)^{24}$ where $q = e^{2\pi iz}$ as usual. We can check that this product converges sufficiently fast for D to be defined and holomorphic on $\mathcal{H}$. Evidently $D(z+1) = D(z)$ and $D(z)\to 0$ as $\Im(z)\to\infty$. So to check that it is a modular form of weight 12 (clearly cuspidal), it suffices to show that $D(-\frac{1}{z}) = z^{12}D(z)$. The result then follow immediately, since we already know that S_{12} is 1-dimensional.

Recall that $\frac{\partial d}{\partial z} = 2\pi iq\frac{\partial}{\partial q}$. Then

$$\begin{aligned}
\frac{\partial}{\partial z}(\log(D(z))) &= \frac{\partial}{\partial z}\left(\log(q) + \sum_{n=1}^{\infty}24\log(1-q^n)\right)\\
&= 2\pi i + 24\sum_{n=1}^{\infty}\frac{-2\pi inq^n}{1-q^n}\\
&= 2\pi i\left(1 - 24\sum_{n=1}^{\infty}nq^n\sum_{r=0}^{\infty}q^r\right)\\
&= 2\pi i\left(1 - 24\sum_{n=1}^{\infty}\sum_{r=0}^{\infty}nq^{nr}\right)\\
&= 2\pi i\left(1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n\right)\\
&= 2\pi i\ E_2(z).
\end{aligned}$$

Hence finally

$$\begin{aligned}
\frac{\partial}{\partial z}\left(\log\left(\frac{D(-1/z)}{z^{12}D(z)}\right)\right) &= \frac{1}{z^2}2\pi i\ E_2\left(-\frac{1}{z}\right) - \frac{12}{z} - 2\pi i\ E_2(z)\\
&= \frac{2\pi i}{z^2}\left(E_2\left(-\frac{1}{z}\right) - \left(z^2E_2(z) + \frac{6z}{i\pi}\right)\right)\\
&= 0.
\end{aligned}$$

So there is a constant λ sucht that $D(-\frac{1}{z}) = \lambda z^{12} D(z)$ for all $z \in \mathcal{H}$. For $z = i$ solves this to $D(i) = D(-\frac{1}{i}) = \lambda D(i)$, and since $D(i) \neq 0$ we have $\lambda = 1$, and therefore $D(-\frac{1}{z}) = z^{12} D(z)$. $\square$

We can now expand the product formula for $\Delta(z)$ as

$$\Delta(z) = \sum_{n \geq 1} \tau(n) q^n \qquad \text{for some } \tau(n) \in \mathbb{Z}.$$

Conjecture 1.7.6. *(Ramanujan, 1916)*

1. *For m, n coprime, we have $\tau(mn) = \tau(m)\tau(n)$.*
2. *For p prime and $n > 0$, we have*

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^1 1 \tau(p^{n-1}).$$

3. *We have $|\tau(p)| \leq 2p^{\frac{11}{2}}$ for all primes p.*

We will see a proof of properties 1) and 2) later in the course, in the section on Hecke operators. Property 3) was proved by Deligne in 1974 as a consequence of his proof of the Weil conjectures, for which he was awarded the Fields medal in 1978.

2 Modular forms of higher level

The idea is to look at functions transforming nicely under subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

2.1 Congruence subgroups

Definition 2.1.1. For $N \in \mathbb{N}$ define the subgroup

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

We will call this group the **principal congruence subgroup of level** N.

Note 2.1.2. $\Gamma(N)$ is the kernel of the group homomorphism induced by the reduction map $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$:

$$\pi_N : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

It is hence a normal subgroup of finite index. (Ex: show that π_N is sujective. This statement goes by the name of "strong approximation for SL_2". It can be shown to be false for $\mathrm{GL}_2(\mathbb{Z})$.)

Definition 2.1.3. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a **congruence subgroup** if there exists $N \geq 1$ such that $\Gamma(N) \subseteq \Gamma$. The least such N is called the **level** of Γ.

Lemma 2.1.4. *Any congruence subgroup has finite index in* $\mathrm{SL}_2(\mathbb{Z})$.

Proof. It sufficies to show that $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] < \infty$ for all $N \in \mathbb{N}$. But this is clear as $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \hookrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is finite. □

Remark 2.1.5. The converse to Lemma 2.1.4 is false. There exist finite index $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ which don't contain $\Gamma(N)$ for any N. (For example there is one of index 7.) But every finite index subgroup of $\mathrm{SL}_n(\mathbb{Z})$ is congruence for $n \geq 3$. So SL_2 is quite unusual. (Bass-Serre-Milnor theorem)

Definition 2.1.6. Other standard congruence subgroups of level N are given by

- $\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})\colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}$,
- $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})\colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$.

Note 2.1.7. We have a chain of inclusions

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z}).$$

These inclusions are in general strict; however, all of them are equalities for $N = 1$, and $\Gamma_0(2) = \Gamma_1(2)$.

Lemma 2.1.8. *For $N \geq 1$, we have*

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

Definition 2.1.9. Let Γ be a congruence subgroup. We say that Γ is even (resp. odd) if $-\mathrm{Id} \in \Gamma$ (resp. $\mathrm{Id} \notin \Gamma$). We define the projective index of Γ to be

$$d_\Gamma = [\mathrm{PSL}_2(\mathbb{Z}) : \bar{\Gamma}],$$

where $\bar{\Gamma}$ is the image of Γ in $\mathrm{PSL}_2(\mathbb{Z})$.

2.2 Fundamental domains and cusps

Proposition 2.2.1. *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and let R be a set of coset representatives for the quotient $\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$. Then the set*

$$D_\Gamma = \bigcup_{\gamma \in R} \gamma D$$

*has the property that for any $z \in \mathcal{H}$ there exists $\gamma \in \Gamma$ such that $\gamma z \in D_\Gamma$. Furthermore, γ is unique up to multiplication by an element of $\Gamma \cap \{\pm \mathrm{Id}\}$, except possibly if γz lies on the boundary of D. We call D_Γ a **fundamental domain for** Γ.*

Proof. If $z \in \mathcal{H}$, thern there exists $g \in \mathrm{SL}_2(\mathbb{Z})$ and $z_0 \in D$ such that $g.z = z_0$. The coset decomposition implies that we can express g uniquely as $\gamma^{-1}\gamma'$ with $\gamma \in \Gamma$ and $\gamma' \in R$. We now have

$$\gamma.z = \gamma g.z_0 = \gamma'.z_0 \in D_\Gamma.$$

The uniqueness is left as an exercise. □

Example 2.2.2. Let $\Gamma = \Gamma_0(2)$. A system of representatives for the quotient $\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$ is

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \right\} = \{\mathrm{Id}, S, ST\}.$$

Using this, one can draw the fundamental domain for Γ.

Note that there are now two points in its closure which do not belong to $\mathcal{H}$: the cusp ∞, as well as 0.

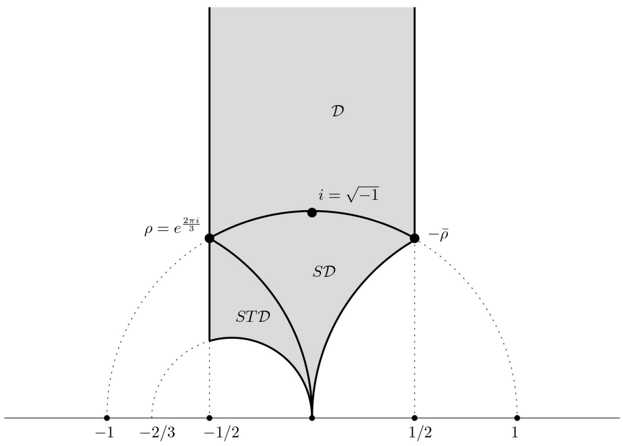


Figure 2.1: A fundamental domain for $\Gamma_0(2)$

Definition 2.2.3. The set $\mathbb{P}^1(\mathbb{Q})$, the **projective line over** $\mathbb{Q}$, consists of $\mathbb{Q} \cup \{\infty\}$. We give this an action of $\mathrm{SL}_2(\mathbb{Z})$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} .x = \frac{ax+b}{cx+d}$$

where the right-hand-side is interpreted as $\frac{a}{c}$ if $x = \infty$, and as ∞ if $cx + d = 0$.

Proposition 2.2.4. $\mathrm{SL}_2(\mathbb{Z})$ *acts transitively on* $\mathbb{P}^1(\mathbb{Q})$.

Proof. Clearly it sufficies to show that for any $x \in \mathbb{P}^1(\mathbb{Q})$ we can map ∞ to x. For $x = \infty$ we have $\infty.1 = \infty$. So let $x = \frac{a}{c}$ with $a, c \in \mathbb{Z}$ coprime. Then there are $r, s \in \mathbb{Z}$ such that $ar + cs = 1$, thus $\left(\begin{smallmatrix} a & -s \\ c & r \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\left(\begin{smallmatrix} a & -s \\ c & r \end{smallmatrix}\right).\infty = x$. $\square$

Note 2.2.5. An easy computation shows that the stabiliser of ∞ in $\mathrm{SL}_2(\mathbb{Z})$ is the subgroup

$$\mathrm{SL}_2(\mathbb{Z})_\infty = \left\{ \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}.$$

It follows from Proposition 2.2.4 that we hence have a bijection

$$\begin{aligned} \mathrm{SL}_2(\mathbb{Z}) / \mathrm{SL}_2(\mathbb{Z})_\infty &\to \mathbb{P}^1(\mathbb{Q}), \\ \gamma \, \mathrm{SL}_2(\mathbb{Z})_\infty &\mapsto \gamma\infty. \end{aligned}$$

Definition 2.2.6. For $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index we define **the set of cusps of** Γ, denoted by $\mathrm{Cusps}(\Gamma)$, as the set of Γ-orbits in $\mathbb{P}^1_{\mathbb{Q}}$.

Example 2.2.7. Let p be prime. Then $\mathrm{Cusps}(\Gamma_0(p)) = \{[\infty], [0]\}$.

Proof. Let $\frac{u}{v} \in \mathbb{Q}$ with $u, v \in \mathbb{Z}$ coprime. Then there are $r, s \in \mathbb{Z}$ such that $ur + vs = 1$, so $\left(\begin{smallmatrix} u & -s \\ v & r \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\left(\begin{smallmatrix} u & -s \\ v & r \end{smallmatrix}\right).\infty = \frac{u}{v}$. We will distinguish two cases:

(1) If p divides v then $\left(\begin{smallmatrix} u & -s \\ v & r \end{smallmatrix}\right) \in \Gamma_0(p)$, so $\frac{u}{v} \in [\infty]$. Conversly, if $\gamma \in \Gamma_0(p)$ then p divides the denominator of $\gamma.\infty$ by definition. So the orbit of ∞ is given by all fractions $\frac{u}{v}$ with p dividing the denominator v.

(2) If v is not divisible by p we can note that

$$u(r + \lambda v) + v(s - \lambda u) = 1$$

and since p is not a divisor of v we find $\lambda \in \mathbb{Z}$ such that $r' = r + \lambda v \in p\mathbb{Z}$. Therefore $\left(\begin{smallmatrix} s' & u \\ -r' & v \end{smallmatrix}\right) \in \Gamma_0(p)$ where $s' = s - \lambda u$ and $\left(\begin{smallmatrix} s' & u \\ -r' & v \end{smallmatrix}\right).0 = \frac{u}{v}$ by definition. So $\frac{u}{v} \in [0]$. Conversely, if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(p)$ then p does not divide d since $ad - bc = 1$. Thus p cannot divide the denominator of $\gamma.0$. Therefore the orbit of 0 is given by all fractions $\frac{u}{v}$ with p not dividing the denominator v.

So this is everything and there are exactly two distinct orbits as claimed. □

Note 2.2.8. By Note 2.2.5, we see that

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

In particular, we have a sujective map

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

Definition 2.2.9. If $P = [t] \in \mathrm{Cusps}(\Gamma)$, denote by Γ_t the stabilizer for t in Γ.

Lemma 2.2.10. *Choose $\gamma_t \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_t(\infty) = t$. Then*

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

Proof. Let $h \in \Gamma$. Then

$$\begin{aligned} h \in \Gamma_t \quad &\Leftrightarrow \quad h.t = t \\ &\Leftrightarrow \quad h\gamma_t(\infty) = \gamma_t(\infty) \\ &\Leftrightarrow \quad \gamma_t^{-1} h \gamma_t(\infty) = \infty \\ &\Leftrightarrow \quad \gamma_t^{-1} h \gamma_t \in \mathrm{SL}_2(\mathbb{Z})_\infty \\ &\Leftrightarrow \quad h \in \gamma_t \, \mathrm{SL}_2(\mathbb{Z})_\infty \gamma_P t{-}1. \end{aligned}$$

□

Note 2.2.11. It follows from the proof that we have an injection

$$\Gamma_t \backslash (\gamma_t^{-1} \, \mathrm{SL}_2(\mathbb{Z})_\infty \gamma_t) \hookrightarrow \Gamma \backslash \mathrm{SL}_2(\mathbb{Z}),$$

so Γ_t has finite index in $\gamma_t^{-1} \, \mathrm{SL}_2(\mathbb{Z})_\infty \gamma_t$.

Lemma 2.2.12. *The subgroup*

$$H_P = \gamma_t^{-1}\Gamma\gamma_t \cap \mathrm{SL}_2(\mathbb{Z})_\infty \subseteq \mathrm{SL}_2(\mathbb{Z})$$

does not depend on the choice of representative for P, and it has finite index in $\mathrm{SL}_2(\mathbb{Z})_\infty$.

Proof. We first show that if we have elements γ_t and $\tilde{\gamma}_t$ in $\mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_t.\infty = t$ and $\tilde{\gamma}_t.\infty = t$, then

$$\gamma_t^{-1}\Gamma\gamma_t \cap \mathrm{SL}_2(\mathbb{Z})_\infty = \tilde{\gamma}_t^{-1}\Gamma\tilde{\gamma}_t \cap \mathrm{SL}_2(\mathbb{Z})_\infty.$$

Note that $\gamma_t^{-1}\tilde{\gamma}_t$ fixes ∞, so it is an element in $\mathrm{SL}_2(\mathbb{Z})_\infty$, say $\gamma_t^{-1}\tilde{\gamma}_t = g \in \mathrm{SL}_2(\mathbb{Z})_\infty$. Then

$$\begin{aligned}\tilde{\gamma}_t^{-1}\Gamma\tilde{\gamma}_t \cap \mathrm{SL}_2(\mathbb{Z})_\infty &= g^{-1}\gamma_t^{-1}\Gamma\gamma_t g \cap \mathrm{SL}_2(\mathbb{Z})_\infty \\ &= g^{-1}\left(\gamma_t^{-1}\Gamma\gamma_t \cap g\,\mathrm{SL}_2(\mathbb{Z})_\infty g^{-1}\right) g \\ &= \gamma_t^{-1}\Gamma\gamma_t \cap \mathrm{SL}_2(\mathbb{Z})_\infty.\end{aligned}$$

Here, we get the last equality since $\gamma_t^{-1}\Gamma\gamma_t \cap g\,\mathrm{SL}_2(\mathbb{Z})_\infty g^{-1} \subseteq \mathrm{SL}_2(\mathbb{Z})_\infty$ and hence is commutative, so in particular its elements commute with g.

Suppose now that we choose another element t in the Γ-orbit of t, and let $\gamma_{t'} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_{t'}.\infty = t'$. Then we can write $\gamma_{t'} = g\gamma_t$ for some $g \in \Gamma$ which satisfies $g.t = t'$. Then

$$\gamma_{t'}^{-1}\Gamma\gamma_{t'} = \gamma_t^{-1}g^{-1}\Gamma g\gamma_t = \gamma_t^{-1}\Gamma\gamma_t^{-1},$$

and hence

$$\gamma_{t'}^{-1}\Gamma\gamma_t \cap \mathrm{SL}_2(\mathbb{Z})_\infty = \gamma_t^{-1}\Gamma\gamma_{t'} \cap \mathrm{SL}_2(\mathbb{Z})_\infty.$$

□

Lemma 2.2.13. *Let H be a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})_\infty$, and let h be the index of $\pm H$ in $\mathrm{SL}_2(\mathbb{Z})_\infty$. Then H is one of the following:*

$$H = \begin{cases} \langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \rangle \\ \left\langle \left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right) \right\rangle = \{(-1)^t \left(\begin{smallmatrix} 1 & th \\ 0 & 1 \end{smallmatrix}\right) : t \in \mathbb{Z}\} \\ \{\pm \mathrm{Id}\} \times \langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \rangle \end{cases}$$

Proof. Exercise. □

Definition 2.2.14. For $H = H_P$, the integer $h_\Gamma(P) = h$ in Lemma 2.2.13 is called the **width of the cusp** P for Γ. The cusp P is

- **irregular** if H_P is of the form $\left\langle \left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right) \right\rangle$ (then Γ is necessarily odd),
- **regular** if H_P is of the form $\langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \rangle$ (so Γ is odd), of if H_P is of the form $\{\pm \mathrm{Id}\} \times \langle \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \rangle$ (so Γ is even).

Remark 2.2.15. If Γ is normal in $\mathrm{SL}_2(\mathbb{Z})$, the subgroup H_P does not depend on the cusp P, and hence all the cusps have the same width and regularity.

Example 2.2.16. Let us determine the width of the two cusps in $\mathrm{Cusps}(\Gamma_0(p))$.

- $c = [\infty]$: we need to determine the smallest $h \geq 1$ such that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right)$ are in $\Gamma_0(p)$. Hence $h_{\Gamma_0(p)}(\infty) = 1$, since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(p)$.
- $c = [0]$: note that $g.\infty = 0$ for $g = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Moreover

$$g \begin{pmatrix} a & b \\ c & d \end{pmatrix} g^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix},$$

so $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in g^{-1}\Gamma_0(p)g$ if and only if $b = 0 \mod p$. In particular,

$$(\Gamma_0(p))_{[0]} = \left(g^{-1}\Gamma_0(p)g\right) \cap P_\infty = \pm \begin{pmatrix} 1 & p\mathbb{Z} \\ 0 & 1 \end{pmatrix}.$$

So the width of the cusp 0 is p.

We now want to count the number of cusps for a given congruence subgroup. We need the following group-theoretic result:

Proposition 2.2.17. *Let G be a group acting transitively on a set X, and let H be a subgroup of finite index in G.*

(i) For any $x \in X$, $\mathrm{Stab}_H(x)$ has finite index in $\mathrm{Stab}_G(x)$, and we have an injection

$$\mathrm{Stab}_H(x)\backslash \mathrm{Stab}_G(x) \hookrightarrow H\backslash G$$

with image $H\backslash H\,\mathrm{Stab}_G(x)$.

(ii) Let $x_0 \in X$. Then there is a surjective map

$$\begin{aligned} H\backslash G &\twoheadrightarrow H\backslash X, \\ Hg &\mapsto Hg.x_0 \end{aligned}$$

and for each $x \in X$, the cardinality of the fibre of this map over Hx equals the index $[\mathrm{Stab}_G(x) : \mathrm{Stab}_H(x)]$.

(iii) If R is a set of orbit representatives for the quotient $H\backslash X$, we have

$$\sum_{x \in R} [\mathrm{Stab}_G(x) : \mathrm{Stab}_H(x)] = [G : H].$$

Proof. (i) is standard.

For (ii), the transitivity of the G-action on X implies that for all $x \in X$, we can choose an element $g_x \in G$ such that $g_x.x_0 = x$, so the map $H\backslash G \to H\backslash X$ is surjective. Denote by T_{Hx} the fibre of this map over Hx, i.e.

$$T_{Hx} = \{Hg \in H\backslash G \mid Hg.x_0 = H.x\}\,.$$

Writing g as $g'g_x$, we obtain a bijection

$$\begin{aligned} T_{Hx} &\cong \{Hg' \in H\backslash G \mid Hg'g_x.x_0 = H.x\} \\ &= \{Hg' \in H\backslash G \mid Hg'.x = Hx\} \\ &= H\backslash(H \operatorname{Stab}_G(x)) \\ &\cong \operatorname{Stab}_H(x)\backslash \operatorname{Stab}_G(x), \end{aligned}$$

where the last equality follows from (i).

(iii) Summing over R and using (ii), we obtain

$$[G:H] = |H\backslash G| = \sum_{x\in R} |T_{Hx}| = \sum_{r\in R} [\operatorname{Stab}_G(x) : \operatorname{Stab}_H(x)],$$

which finishes the proof. □

Corollary 2.2.18. *Let* Γ *be a congruence subgroup. Then*

$$\sum_{P\in\operatorname{Cusps}(\Gamma)} h_\Gamma(P) = d_\Gamma.$$

Proof. Apply Proposition 2.2.17 to $G = \mathrm{PSL}_2(\mathbb{Z})$, $H = \bar{\Gamma}$ and $X = \mathbb{P}^1(\mathbb{Q})$. □

2.3 Weakly modular forms for congruence subgroups

Definition 2.3.1. Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup, and let $k \in \mathbb{Z}$. A function $f : \mathcal{H} \to \mathbb{C}$ is **a weakly modular function of weight** k **and level** Γ if f is meromorphic on $\mathcal{H}$ and $f|_k\gamma = f$ for all $\gamma \in \Gamma$.

Remark 2.3.2. Let k be odd and Γ be even. Let f be a weakly modular function of weight k and level Γ. By Lemmas 2.2.12 and 2.2.13 there is $h \in \mathbb{N}$ such that $\pm\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$, so

$$f = f|_k\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) = f(\cdot + h) \qquad \text{and} \qquad f = f|_k\left(\begin{smallmatrix} -1 & -h \\ 0 & -1 \end{smallmatrix}\right) = -f(\cdot + h).$$

Hence $f(z) = -f(z)$ for all $z \in \mathcal{H}$ and therefore $f = 0$.

Example 2.3.3. Let f be weakly modular of level $\mathrm{SL}_2(\mathbb{Z})$ and weight k. Then $f(Nz)$ is weakly modular of level $\Gamma_0(N)$ and weight k.

Proof. We have

$$f\left(N\frac{az+b}{cz+d}\right) = f\left(\frac{aNz+bN}{cz+d}\right) = f\left(\frac{aNz+bN}{\frac{c}{N}Nz+d}\right).$$

If $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ then $\left(\begin{smallmatrix} a & Nb \\ c/N & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and hence

$$f\left(\frac{aNz+bN}{\frac{c}{N}Nz+d}\right) = \left(\left(\frac{c}{N}\right)(Nz)+d\right)^k f(Nz) = (cz+d)^k f(Nz)$$

as required. So $z \mapsto f(Nz)$ is weakly modular of level $\Gamma_0(N)$. □

2.4 q-expansion at ∞

Proposition 2.4.1. *Let $f\colon \mathcal{H} \to \mathbb{C}$ be weakly modular of weight k and level Γ and let $h = h_\Gamma(\infty)$.*

- *If k is even or if k is odd, Γ is odd and ∞ is a regular cusp, then there is a meromorphic function $\tilde{f}$ on the punctured disc $\mathbb{D}^*$ such that $f(z) = \tilde{f}(q_h(z))$ for all $z \in B$ where $q_h(z) = e^{2\pi i z/h}$.*
- *If k is odd, Γ is odd and ∞ is irregular, then there is a meromorphic function $\tilde{F}$ on $\mathbb{D}^*$ such that $f(z) = e^{\pi i z/h}\tilde{F}(q_h(z))$ for all $z \in \mathcal{H}$ where $q_h(z) = e^{2\pi i z/h}$.*

Proof. By Lemma 2.2.13, at least one of $\pm\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ lies in Γ, so

$$f(z) = \left(f|_k \pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)\right)(z) = (\pm 1)^k f(z+h)$$

for all $z \in \mathcal{H}$.

If k is even then $(\pm 1)^k = 1$, so $f = f(\cdot + h)$, and if Γ is odd and ∞ is regular, then $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$, so we also have $f = f(\cdot + h)$. In both cases we can argue as in section 1.3.

If k is odd and Γ is odd but ∞ is irregular, then $-\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ and therefore

$$f(z) = -f(z+h) \quad \forall z \in \mathcal{H}.$$

Define a function F on $\mathcal{H}$ by $F(z) = f(z)e^{-\pi i z/h}$. Then

$$F(z+h) = e^{-\pi i} f(z+h)e^{-\pi i z/h} = f(z)e^{-\pi i z/h} = F(z).$$

So we can argue for F as before and get $f(z) = e^{\pi i z/h}\tilde{F}(q_h(z))$. □

Remark 2.4.2. We can hence write $f(z)$ as a q-expansion at ∞:

$$f(z) = \begin{cases} \sum_{n\in\mathbb{Z}} a_{\infty,n} q_h^n & \text{if } k \text{ is even or if } k \text{ is odd and } \Gamma \text{ is odd and regular at } \infty \\ \sum_{n\in\frac{1}{2}+\mathbb{Z}} a_{\infty,n} q_h^n & \text{if } k \text{ is odd and } \Gamma \text{ is odd and irregular at } \infty \end{cases}$$

Definition 2.4.3. Let $f\colon \mathcal{H} \to \mathbb{C}$ be weakly modular of weight k and level Γ. We say that f is **meromorphic at** ∞ if $\tilde{f}$ is meromorphic at 0. Similarly we define f to be **holomorphic at** ∞ if $\tilde{f}$ is holomorphic at 0. If f is meromorphic at ∞, we define

$$v_{\infty,\Gamma}(f) = \min\{n \in \frac{1}{2}\mathbb{Z} : a_{\infty,n} \neq 0.\}$$

We then say f is **vanishing at** ∞ if $v_{\infty,\Gamma}(f) > 0$. If f is holomorphic at ∞ we define

$$f(\infty) = \begin{cases} \tilde{f}(0) & \text{if } k \text{ is even or if } k \text{ is odd, } \Gamma \text{ is odd and } \infty \text{ is regular} \\ 0, & \text{if } k \text{ is odd and } \Gamma \text{ is odd and irregular at } \infty. \end{cases}$$

Remark 2.4.4. To motivate the definition $v_{\infty,\Gamma}(f) = v_0(\tilde{F}) + \frac{1}{2}$ in the irregular case note that the additional $\frac{1}{2}$ term ensures

$$v_{\infty,\Gamma}(fg) = v_{\infty,\Gamma}(f) + v_{\infty,\Gamma}(g)$$

since this would fail for f, g with $f(z) = e^{\pi i z/h}\tilde{f}(q_h)$ and $g(z) = e^{\pi i z/h}\tilde{g}(q_h)$ without this extra term. Moreover, note that in the irregular case f being holomorphic at ∞ implies f vanishes at ∞.

2.5 q-expansion at a cusp

To define the q-expansion at a general cusp, we need the following result:

Lemma 2.5.1. *Let $f\colon \mathcal{H} \to \mathbb{C}$ be weakly modular of weight k and level Γ and let $g \in \mathrm{SL}_2(\mathbb{Z})_\infty$ but not necessarily in H_∞. Then $f|_k g$ is meromorphic at ∞ if and only if f is. Moreover $v_{\infty,g^{-1}\Gamma g}(f|_k g) = v_{\infty,\Gamma}(f)$ and $(f|_k g)(\infty) = f(\infty)$ if defined and if k is even.*

Proof. We check that $f|_k g$ is indeed weakly modular of weight k and level $g^{-1}\Gamma g$ since

$$(f|_k g)\,|_k \left(g^{-1}\gamma g\right) = (f|_k \gamma)\,|_k g = f|_k g.$$

Moreover we have

$$h_{g^{-1}\Gamma g}(\infty) = \left[\overline{\mathrm{SL}_2(\mathbb{Z})_\infty} : \overline{g^{-1}H_\infty g}\right] = \left[\overline{\mathrm{SL}_2(\mathbb{Z})_\infty} : \overline{H}_\infty\right]$$

since $\overline{\mathrm{SL}_2(\mathbb{Z})_\infty}$ is abelian and $g \in \mathrm{SL}_2(\mathbb{Z})_\infty$.

Now let $g = \pm\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$. Then

$$(f|_k g)(z) = \begin{cases} (\pm 1)^k \tilde{f}\left(e^{2\pi i t/h} q\right), & \text{if } k \text{ is even or if } k \text{ is odd, } \Gamma \text{ is odd and } \infty \text{ is regular,} \\ (\pm 1)^k e^{it/h} \tilde{F}\left(e^{2\pi i t/h} q\right), & \text{if } k \text{ is odd and } \Gamma \text{ is odd and irregular at } \infty. \end{cases}.$$

So $f|_k g$ is meromorphic or holomorphic at ∞ if and only if so is f, and the orders of vanishing are equal. ☐

Definition 2.5.2. Let f be weakly modular of weight k and level Γ. Let $P \in \text{Cusps}(\Gamma)$ be represented by an element $t \in \mathbb{P}^1(\mathbb{Q})$ and choose some $\gamma_t \in \text{SL}_2(\mathbb{Z})$ such that $\gamma_t.\infty = t$. Define $v_{P,\Gamma}(f) = v_{\infty,\gamma_t^{-1}\Gamma\gamma_t}(f|_k\gamma_t)$.

The following proposition shows that $v_{P,\Gamma}(f)$ is well-defined.

Proposition 2.5.3. *$v_{P,\Gamma}(P)$ is well-defined.*

Proof. Suppose that $\gamma_t' \in \text{SL}_2(\mathbb{Z})$ also satisfies $\gamma_t'.\infty = t$. then $\gamma_t^{-1}\gamma_t' \in \text{SL}_2(\mathbb{Z})_\infty$, so by Lemma 2.5.1 applied to $F|_k\gamma_t$ we deduce that $(f|k\gamma_t)|_k\gamma_t^{-1}\gamma_t' = f|_k\gamma_t'$ is meromorphic at ∞ if and only if so $f|k\gamma_t$, with the same order of vanishing.

Now let s be another representative of P, and let $\gamma_s \in \text{SL}_2(\mathbb{Z})$ such that $\gamma_s.\infty = s$. Then there exists $g \in \Gamma$ such that $g.s = t$, so $g.\gamma_s.\infty = t$, so $f_k\gamma_t$ is meromorphic at ∞ if and only if so is $f|_k(g\gamma_s) = f_k\gamma_s$, with the same order of vanishing. $\square$

Note 2.5.4. Note that we can define $f(P) = (f|_kg)(\infty)$ if f is holomorphic at P and if k is even, but if k is odd, then $f(P)$ is only defined up to change of sign.

Definition 2.5.5. We say that f **is holomorphic at** P if $v_{P,\Gamma}(f) \geq 0$ and that f **is vanishing at** P if $v_{P,\Gamma}(f) > 0$.

Definition 2.5.6. We say f is a **modular function** if f is meromorphic at every cusp, f is a **modular form** if f is holomorphic on $\mathcal{H}$ and at every cusp, and f is a **cusp form** if f is holomorphic on $\mathcal{H}$ and vanishes at every cusp.

Definition 2.5.7. Define $M_k(\Gamma)$ to be the space of modular forms of level Γ and $S_k(\Gamma)$ to be the space of cusp forms of level Γ.

Clearly they are both complex vector spaces.

2.6 The valence formula in arbitrary levels

Definition 2.6.1. For $z \in \mathcal{H}$ and $\Gamma \leq \text{SL}_2(\mathbb{Z})$ of finite index we let

$$n_\Gamma(z) = \left|\text{stab}_{\overline{\Gamma}}(z)\right|.$$

If $n_\Gamma(z) > 1$, we say z is an **elliptic point of** Γ.

Note 2.6.2. Clearly $n_\Gamma(z)$ is 1, 2 or 3, and it is 1 unless $z \in \text{SL}_2(\mathbb{Z})$-orbit of i or ρ. There exist only finitely many Γ-orbits of elliptic points for any Γ, often even none at all, for example for $\Gamma_1(N)$ if $N \geq 4$.

Theorem 2.6.3 (The valence formula)**.** *If f is a modular function of weight k and level Γ and $f \neq 0$ then*

$$\sum_{z \in \Gamma\backslash\mathcal{H}} \frac{v_z(f)}{n_\Gamma(z)} + \sum_{P \in \text{Cusps}(\Gamma)} v_{P,\Gamma}(f) = \frac{k\, d_\Gamma}{12}.$$

Here, d_Γ is the projective index as defined in Definition 2.1.9.

The proof of this will take us a while.

Definition 2.6.4. Let $V_\Gamma(f) = \sum_{z\in\Gamma\backslash\mathcal{H}} \frac{v_z(f)}{n_\Gamma(z)} + \sum_{P\in\mathrm{Cusps}(\Gamma)} v_{P,\Gamma}(f)$.

Lemma 2.6.5. *Let f be a modular function of level Γ, $f\neq 0$, and let $\Gamma' \leq \Gamma$ be another finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Then*

$$V_{\Gamma'}(f) = \frac{d_{\Gamma'}}{d_\Gamma}\cdot V_\Gamma(f).$$

Proof. Let $z\in\mathcal{H}$. We apply Proposition 2.2.17 with X being the Γ-orbit of z, $G=\Gamma$ and $H=\Gamma'$. This yields

$$\begin{aligned}\sum_{\substack{w\in\Gamma'\backslash\mathcal{H}\\ [w]=[z] \mod \Gamma}} \frac{n_\Gamma(w)}{n_{\Gamma'}(w)} &= \sum_{w\in H\backslash X} \frac{|\operatorname{stab}_{\overline{\Gamma}}(w)|}{|\operatorname{stab}_{\overline{\Gamma}'}(w)|}\\ &= \sum_{w\in H\backslash X} \left[\operatorname{stab}_{\overline{\Gamma}}(w) : \operatorname{stab}_{\overline{\Gamma}'}(w)\right] = \left[\overline{\Gamma} : \overline{\Gamma}'\right] = \frac{d_{\Gamma'}}{d_\Gamma},\end{aligned}$$

and since $n_\Gamma(w) = n_\Gamma(z)$ for all $w\in R_z$, we have

$$\sum_{w\in R_z} \frac{1}{n_{\Gamma'}(w)} = \frac{1}{n_\Gamma(z)}\,\frac{d_{\Gamma'}}{d_\Gamma}.$$

Hence we have

$$\sum_{w\in H\backslash X} \frac{v_w(f)}{n_{\Gamma'}(w)} = \sum_{z\in\Gamma\backslash H}\left(v_z(f) \sum_{\substack{w\in\Gamma'\backslash\mathcal{H}\\ [w]=[z] \mod \Gamma}} \frac{1}{n_{\Gamma'}(w)}\right) = \frac{d_{\Gamma'}}{d_\Gamma}\sum_{z\in\Gamma\backslash H}\frac{v_z(f)}{n_\Gamma(z)}.$$

Similarily we can argue at the cusps: If $P\in\mathrm{Cusps}(\Gamma)$ and $Q\in\mathrm{Cusps}(\Gamma')$ which maps to P under the natural map $\mathrm{Cusps}(\Gamma')\to\mathrm{Cusps}(\Gamma)$, then we have by definition

$$v_{Q,\Gamma'}(f) = \frac{h_{\Gamma'}(Q)}{h_\Gamma(P)} v_{P,\Gamma}(f).$$

Therefore we get again by Proposition 2.2.17

$$\sum_{\substack{Q\in\mathrm{Cusps}(\Gamma')\\ Q=P \text{ in } \mathrm{Cusps}(\Gamma)}} v_{Q,\Gamma'}(f) = v_{P,\Gamma}(f) \sum_{\substack{Q\in\mathrm{Cusps}(\Gamma')\\ Q=P \text{ in } \mathrm{Cusps}(\Gamma)}} \frac{h_{\Gamma'}(Q)}{h_\Gamma(P)} = v_{P,\Gamma}(f)\frac{d_{\Gamma'}}{d_\Gamma}.$$

and thus

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

This finishes the proof. □

Lemma 2.6.6. *For any $g \in \mathrm{SL}_2(\mathbb{Z})$ we have*

$$V_{g^{-1}\Gamma g}(f|_k g) = V_\Gamma(f).$$

Proof. We clearly have $v_z(f|_k g) = v_{gz}(f)$ for any $z \in \mathcal{H}$ and $n_{g^{-1}\Gamma g}(z) = n_\Gamma(gz)$ since $\mathrm{stab}_\Gamma(gz) = g(\mathrm{stab}_{g^{-1}\Gamma g}(z))g^{-1}$. Hence

$$\sum_{z \in (g^{-1}\Gamma g)\backslash\mathcal{H}} \frac{v_z(f|_k g)}{n_{g^{-1}\Gamma g}(z)} = \sum_{gz \in \Gamma\backslash\mathcal{H}} \frac{v_{gz}(f)}{n_\Gamma(gz)}.$$

This deals with the non-cusp terms in the valence formular. But similarily we can check that $v_P(f|_k g) = v_{gP}(f)$ for all $P \in \mathrm{Cusps}(\Gamma)$, so the cusp terms in $V_{g^{-1}\Gamma g}(f|_k g)$ and $V_\Gamma(f)$ are also equal. □

Now we can finally proof the valence formula.

Proof of theorem 2.6.3. Let Γ' be any finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ which is normal and contained in Γ. (Note that such a group exists since Γ is a congruence subgroup.) Then

$$V_\Gamma(f) = \frac{d_\Gamma}{d_{\Gamma'}} \cdot V_{\Gamma'}(f)$$

by Lemma 2.6.5. Let $d = d_{\Gamma'}$ and choose $g_1, \ldots, g_d \in \mathrm{SL}_2(\mathbb{Z})$ such that $\overline{g_1}, \ldots, \overline{g_d}$ are coset representatives for $\mathrm{PSL}_2(\mathbb{Z})/\overline{\Gamma'}$. Define

$$F(z) = \prod_{i=1}^{d} (f|_k g_i)(z).$$

Then F is weakly modular of weight dk for the full modular group $\mathrm{SL}_2(\mathbb{Z})$, and meromorphic at ∞. Hence by Theorem 1.5.10, we have

$$V_{\mathrm{SL}_2(\mathbb{Z})}(F) = \frac{dk}{12} \quad \Rightarrow \quad V_{\Gamma'}(F) = d^2 \frac{k}{12}$$

since $V_{\Gamma'}(F) = d\ V_{\mathrm{SL}_2(\mathbb{Z})}(F)$ by Lemma 2.6.5 But we can easily check that

$$V_{\Gamma'}(F) = \sum_{i=1}^{d} V_{\Gamma'}(f|_k g_i) = \sum_{i=1}^{d} V_{g_i^{-1}\Gamma' g_i}(f|_k g_i) = dV_{\Gamma'}(f)$$

where we obtain the last two equalities since Γ' is normal and applying Lemma 2.6.6. Hence

$$V_{\Gamma'}(f) = \frac{dk}{12} \quad \Rightarrow \quad V_\Gamma(f) = \frac{kd_\Gamma}{12},$$

which finishes the proof. □

Corollary 2.6.7. *$M_k(\Gamma)$ is empty for any $k < 0$ and for any Γ.*

Proof. Clear since the left hand side of the valence formula must be non-negative. □

Corollary 2.6.8 ("The unreasonable effectiveness of modular forms in number theory"). *Let $k \in \mathbb{Z}$ and suppose f and g are modular forms of weight k and level Γ, and their q-expansions agree up to degree $\frac{k\,d_\Gamma}{12}$, so up to and including q_h^m where $m = \lfloor \frac{k\,d_\Gamma}{12} \rfloor$ and $h = h_\infty(\Gamma)$. Then $f = g$.*

Proof. We have $v_{\infty,\Gamma}(f-g) \geq 1 + \lfloor \frac{k\,d_\Gamma}{12} \rfloor > \frac{k\,d_\Gamma}{12}$, which yields a contradiction to Theorem 2.6.3 unless $f - g = 0$. □

Corollary 2.6.9. *For any $k \geq 0$ and any finite index subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ we have*

$$\dim\left(M_k(\Gamma)\right) \leq 1 + \left\lfloor \frac{k\,d_\Gamma}{12} \right\rfloor.$$

In particular $M_k(\Gamma)$ is finite dimensional.

Proof. Let $m = \lfloor \frac{k\,d_\Gamma}{12} \rfloor$ and $h = h_\infty(\Gamma)$. Consider the linear map $M_k(\Gamma) \to \mathbb{C}^{m+1}$ mapping f to the coefficients up to q_h^m in its q-expansion. By Corollary 2.6.8 this map is injective, hence $\dim(M_k(\Gamma)) \leq m+1$. □

Remark 2.6.10.

(i) It can be shown that if $-1 \in \Gamma$ and k is any non-negative even integer or if Γ is odd and k is any non-negative integer then

$$\dim(M_k(\Gamma)) \geq \left(\frac{k}{12} - 1\right)d_\Gamma.$$

(ii) In Diamond & Shurman there are precise formulae for the dimsion of $M_k(\Gamma)$.

2.7 Eisenstein series revisited

Recall that $\mathrm{SL}_2(\mathbb{Z})_\infty = \pm\left(\begin{smallmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right)$, and let $\mathrm{SL}_2(\mathbb{Z})_\infty^+ = \left(\begin{smallmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right) \subseteq \mathrm{SL}_2(\mathbb{Z})_\infty$.

Proposition 2.7.1. *(a) Let $g, g' \in \mathrm{SL}_2(\mathbb{Z})$, $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $g' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$. Then $c = c'$ and $d = d'$ if and only if there is an $g_\infty \in \mathrm{SL}_2(\mathbb{Z})_\infty^+$ such that $g' = g_\infty g$.*

(b) For $(c,d) \in \mathbb{Z}^2$ there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with bottom row (c,d) if and only if $\gcd(c,d) = 1$.

Proof. For (a) note that

$$g'g^{-1} = \begin{pmatrix} a' & b' \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} a'd - b'c & -a'b + b'a \\ 0 & -cb + da \end{pmatrix} = \begin{pmatrix} 1 & ab' - a'b \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})_\infty^+.$$

Part (b) is clear since $\gcd(c,d)$ divides $\det(\gamma)$. □

Corollary 2.7.2. *The mapping $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto (c,d)$ gives a bijection*

$$\mathrm{SL}_2(\mathbb{Z})_\infty^+ \backslash \mathrm{SL}_2(\mathbb{Z}) \to \{(c,d) \in \mathbb{Z}^2 \colon \gcd(c,d) = 1\}.$$

We will now motivate the definition of a generalised Eisenstein series using this bijection.

Note 2.7.3. Observe that $1|_k\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = (cz+d)^{-k}$, so 1 is $\mathrm{SL}_2(\mathbb{Z})^+_\infty$-invariant. Hence the unnormalised level 1 Eisenstenstein series $G_k(z)$ can be written as

$$\begin{aligned}
\sum_{(c,d)\in\mathbb{Z}^2\setminus\{0\}} \frac{1}{(cz+d)^k} &= \sum_{r=1}^{\infty} \left(\sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=r}} \frac{1}{(cz+d)^k} \right) \\
&= \sum_{r=1}^{\infty} \left(\frac{1}{r^k} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1}} \frac{1}{(cz+d)^k} \right) \\
&= \left(\sum_{r=1}^{\infty} \frac{1}{r^k} \right) \left(\sum_{[\gamma]\in \mathrm{SL}_2(\mathbb{Z})^+_\infty \setminus \mathrm{SL}_2(\mathbb{Z})} j(\gamma,z)^{-k} \right) \\
&= \zeta(k) \sum_{[\gamma]\in \mathrm{SL}_2(\mathbb{Z})^+_\infty \setminus \mathrm{SL}_2(\mathbb{Z})} j(\gamma,z)^{-k}.
\end{aligned}$$

Definition 2.7.4. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and let $\Gamma^+_\infty = \Gamma \cap \mathrm{SL}_2(\mathbb{Z})^+_\infty$. For $k \geq 3$, define

$$G_{k,\Gamma,\infty} = \sum_{\gamma \in \Gamma^+_\infty \setminus \Gamma} j(\gamma,z)^{-k}.$$

Proposition 2.7.5. *The function $G_{k,\Gamma,\infty}$ is a weakly modular function of weight k and level Γ.*

Proof. It can be shown that the sum defining $G_{k,\Gamma,\infty}$ converges absolutely and uniformly on compact subsets of $\mathcal{H}$. Thus $G_{k,\Gamma,\infty}$ is well-defined and holomorphic. Moreover, $G_{k,\Gamma,\infty}$ is also clearly Γ-invariant under the weight k action. $\square$

Proposition 2.7.6. *If either k is even or if k is odd and Γ is regular at ∞, then $G_{k,\Gamma,\infty}$ is a modular form of weight k and level Γ, which does not vanish at ∞, but at all other cusps. Conversly, if k is odd and Γ is irregular at ∞, then $G_{k,\Gamma,\infty} = 0$.*

Proof. First suppose that k is odd and Γ is odd and irregular at ∞, so $g = \left(\begin{smallmatrix} -1 & n \\ 0 & -1 \end{smallmatrix}\right) \in \Gamma$ for some $n \in \mathbb{Z}$. Then $g \notin \Gamma^+_\infty$ and

$$j(\gamma,z)^{-k} + j(g\gamma,z)^{-k} = (cz+d)^k + (-1)^k(cz+d)^k = 0$$

for all $\gamma \in \Gamma$. Hence the terms in the sum defining $G_{k,\Gamma,\infty}$ cancel out, so $G_{k,\Gamma,\infty} = 0$.

Now let k be even or let k be odd and Γ regular at ∞. We compute $G_{k,\Gamma,\infty}(\infty)$. We have

$$\lim_{\Im(z)\to\infty} (cz+d)^{-k} = \begin{cases} d^{-k} & \text{if } c = 0 \\ 0 & \text{if } c \neq 0 \end{cases} \tag{2.1}$$

Note also that for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we have $c = 0$ if and only if $\gamma \in \Gamma_\infty$. Thus

$$\begin{aligned} G_{k,\Gamma,\infty}(\infty) &= \lim_{\Im(z)\to\infty} G_{k,\Gamma,\infty}(z) \\ &= \lim_{\Im(z)\to\infty} \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma_\infty} j(\gamma, z)^{-k} \end{aligned}$$

which takes the following values:

	Γ even	Γ odd ∞ regular	Γ odd ∞ irregular
k even	2	1	2
k odd	0	1	0
$\Gamma_\infty^+\backslash\Gamma_\infty$	$\pm\,\mathrm{Id}$	Id	$(\mathrm{Id}, \left(\begin{smallmatrix} -1 & h \\ & 1 \end{smallmatrix}\right))$

Now let P be a cusp different from ∞. Let t be a representative of P, and choose $\gamma_t \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_t.\infty = t$.

Then by definition, we have

$$G_{k,\Gamma,\infty}(P) = (G_{k,\Gamma,\infty}|_k\gamma_t)\,(\infty).$$

But

$$(G_{k,\Gamma,\infty}|_k\gamma_t)\,(z) = \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma} j(\gamma\gamma_t, z)^{-k} = \sum_{\gamma\in\Gamma_\infty^+\backslash\Gamma\gamma_t} j(\gamma, z)^{-k}.$$

Claim: any $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma\gamma_t$ has $c \neq 0$.

Proof of claim: if $g = \gamma\gamma_t$ had $c = 0$, then $g \in \mathrm{SL}_2(\mathbb{Z})_\infty$, so $\gamma \in \mathrm{SL}_2(\mathbb{Z})_\infty\gamma_t^{-1} \cap \Gamma$. But any element in $\mathrm{SL}_2(\mathbb{Z})_\infty\gamma_t^{-1}$ maps t to ∞, which gives a contradicton since $P \neq \infty$, i.e. t does not lie in the Γ-orbit of ∞. We therefore deduce from (2.1) that

$$G_{k,\Gamma,\infty}(P) = (G_{k,\Gamma,\infty}|_k\gamma_t)\,(\infty) = 0.$$

In particular $G_{k,\Gamma,\infty}|_k g$ is bounded as $\Im(z) \to \infty$ for all $g \in \mathrm{SL}_2(\mathbb{Z})$, so $G_{k,\Gamma,\infty}$ is indeed a modular form. □

Note 2.7.7. We have constructed a modular form that doesn't vanish at ∞ for all pairs (k, Γ) where this isn't trivially impossible.

Corollary 2.7.8. *Let Γ be a congruence subgroup, let $P \in \mathrm{Cusps}(\Gamma)$, and let $k \geq 3$. If k is odd, assume that P is regular and that Γ is odd. Then there is a modular form in $M_k(\Gamma)$ does not vanish at P but at all other cusps.*

Proof. Let t be a representative of P, and choose $\gamma_t \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_t.\infty = t$. Define

$$G_{k,\Gamma,P} = G_{k,g^{-1}\Gamma g,\infty}\ |_k\ g^{-1}.$$

Then $G_{k,\Gamma,P}$ is a modular form of weight k and level Γ which does not vanish at P but at all other cusps, by Proposition 2.7.6. □

Note 2.7.9. The Eisenstein series $G_{k,\Gamma,P}$ is well-defined if k is even, and in this case independent of the choice of t. But if k is odd $G_{k,\Gamma,P}$ is only well-defined up to sign.

Definition 2.7.10. We define $\mathcal{E}_k(\Gamma)$ as the subspace of $M_k(\Gamma)$ spanned by the $G_{k,\Gamma,P}$'s.

Note 2.7.11. We have

$$\dim(\mathcal{E}_k(\Gamma)) = \begin{cases} |\operatorname{Cusps}(\Gamma)|, & \text{if } k \text{ is even} \\ |\operatorname{Cusps}_{\text{reg}}(\Gamma)|, & \text{if } k \text{ is odd and } \Gamma \text{ is odd} \end{cases}.$$

Example 2.7.12. Let p be prime and $\Gamma = \Gamma_0(p)$. Then $\operatorname{Cusps}(\Gamma) = \{0, \infty\}$, both cusps are regular (see Example 2.2.16), and Γ is even. So the case k odd is trivial. For $k \geq 4$ an even integer there are two Eisenstein series: $G_{k,\Gamma,\infty}$ and $G_{k,\Gamma,0}$.

- $G_{k,\Gamma,\infty}$: by the definition of $\Gamma_0(p)$ and Proposition 2.7.1 we have

$$G_{k,\Gamma,\infty} = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p|c}} \frac{1}{(cz+d)^k}.$$

- $G_{k,\Gamma,0}$: note that we have $S.\infty = 0$ for $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and

$$S^{-1}\Gamma S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : p \text{ didivdes } b \right\} =: \Gamma^0(p).$$

  Now clearly

$$\Gamma^0(p)^+_\infty = \left\{ \left(\begin{smallmatrix} 1 & p\star \\ 0 & 1 \end{smallmatrix}\right) \right\},$$

  and $\Gamma^0(p)^+_\infty \backslash \Gamma^0(p)$ can be identified with the set

$$\left\{ (c,d) \in \mathbb{Z}^2 - \{0\} : \gcd(c,d) = 1,\ p \nmid d \right\}$$

  Hence

$$\begin{aligned} G_{k,\Gamma,0}(z) &= \left(G_{k,\Gamma^0(p),\infty}|_k \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right)(z) \\ &= z^{-k} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p\nmid d}} \frac{1}{(-cz^{-1}+d)^k} \\ &= \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p\nmid d}} \frac{1}{(-c+dz)^k} \\ &= \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p\nmid c}} \frac{1}{(cz+d)^k}. \end{aligned}$$

Thus we have

$$G_{k,\Gamma,\infty}(z) + G_{k,\Gamma,0}(z) = G_{k,\mathrm{SL}_2(\mathbb{Z}),\infty}(z) = 2E_k(z).$$

Finally consider

$$2E_k(pz) = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1}} \frac{1}{(cpz+d)^k}.$$

Note that if $(c,d) \in \mathbb{Z}^2$ with $\gcd(c,d) = 1$, then $\gcd(pc,d) = 1$ unless p divides d. So

$$2E_k(pz) = \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p|c}} \frac{1}{(cz+d)^k} + \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p|d}} \frac{1}{(pcz+d)^k}.$$

We can check that

$$\{(pc,d)\colon\ \gcd(c,d)=1, p|d\} = \{(pc,pd)\colon\ \gcd(c,d)=1, p\nmid c\},$$

which gives us

$$2E_k(pz) = G_{k,\Gamma,\infty} + \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1 \\ p\nmid c}} \frac{1}{(pcz+pd)^k} = G_{k,\Gamma,\infty} + p^{-k}G_{k,\Gamma,0}.$$

Hence $\mathcal{E}_k(\Gamma)$ is spanned by $E_k(z)$ and $E_k(pz)$. Note that we have also shown that $E_k(pz)$ is p^{-k} at cusp 0.

3 Hecke operators

3.1 Double cost operators

It turns out that the space $M_K(\Gamma)$ has a very interesting structure: it is a module over a commutative ring, classed the **Hecke algebra**.

Lemma 3.1.1.

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

2. *Any two congruence subgroups are* ***commensurable****: we have*

$$[\Gamma_1 : \Gamma_1 \cap \Gamma_2] < \infty \qquad \textit{and} \qquad [\Gamma_2 : \Gamma_1 \cap \Gamma_2].$$

Proof. 1. Let $N \geq 1$ such that $\Gamma(N) \subseteq \Gamma$, and such that $N\alpha \in M_2(\mathbb{Z})$ and $N\alpha^{-1} \in M_2(\mathbb{Z})$. Then one can check that

$$\alpha\Gamma(N^3)\alpha^{-1} \subseteq \Gamma(N) \subseteq \Gamma,$$

so $\Gamma(N^3) \subseteq \alpha^{-1}\Gamma\alpha$.

2. Note that there is some $M \geq 1$ such that $\Gamma(M) \subseteq \Gamma_1 \cap \Gamma_2$. $\square$

Definition 3.1.2. Let $\mathrm{GL}_2^+(\mathbb{Q})$ denote the set of invertible 2×2 matrices over $\mathbb{Q}$ with positive determinant. Let Γ_1, Γ_2 be congruence subgroups, and let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. The double coset $\Gamma_1\alpha\Gamma_2$ is the set

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

Note 3.1.3. Multiplication gives a left (resp. right) action by Γ_1 (resp. by Γ_2) on $\Gamma_1\alpha\Gamma_2$. We can hence decompose the double coset into Γ_1-orbits:

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

We will see in a moment that this decomposition is finite.

Proposition 3.1.4. *Let Γ_1, Γ_2 be congruence subgroups, and let $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$. Let*

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

Then 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

$$\Gamma_2 \to \Gamma_2\backslash(\Gamma_1\alpha\Gamma_2), \qquad \gamma_2 \mapsto \Gamma_1\alpha\gamma_2.$$

The map is clearly surjective, and two elements γ_2, γ_2' get mapped to the same element if and only if

$$\Gamma_1\alpha\gamma_2 = \Gamma_1\alpha\gamma_2' \qquad \Leftrightarrow \qquad \gamma_2'\gamma_2^{-1} \in \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2.$$

□

Note 3.1.5. By Lemma 3.1.1 (2), we have $[\Gamma_2 : \Gamma_3] < \infty$.

Corollary 3.1.6. *Let $\Gamma_2 = \bigcup \Gamma_3\gamma_j$ be a coset decomposition of $\Gamma_3\backslash\Gamma_2$. Then*

$$\Gamma_1\alpha\Gamma_2 = \bigcup \Gamma_1\alpha\gamma_j$$

is an orbit decomposition (so $\Gamma_1\alpha\gamma_i \cap \Gamma_1\alpha\gamma_j = \emptyset$ if $i \neq j$). In particular, the number of orbits of $\Gamma_1\alpha\Gamma_2$ under the action of Γ_1 is finite.

Note 3.1.7. Note that the action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}$ extends naturally to $\mathrm{GL}_2^+(\mathbb{R})$.

Definition 3.1.8.

(i) Let $k \in \mathbb{Z}$. For a function $f\colon \mathcal{H} \to \mathbb{C}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$ we define

$$\left(f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)(z) = (ad-bc)^{k-1}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right).$$

(ii) Let $\Gamma_1, \Gamma_2 \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index, $g \in \mathrm{GL}_2^+(\mathbb{Q})$ and let $\beta_1, \ldots, \beta_r \in \mathrm{GL}_2(\mathbb{Q})^+$ be an orbit decomposition $\Gamma_1 g\Gamma_2 = \bigcup \Gamma_1\beta_i$ as in Corollary 3.1.6. For f weakly modular of weight k and level Γ_1 we define

$$f|_k\,[\Gamma_1 g\Gamma_2] = \sum_{i=1}^{r} f|_k\beta_i.$$

Proposition 3.1.9. *$f|_k[\Gamma_1 g\Gamma_2]$ is independent of the choice of the β_i's, and it is weakly modular of weight k and level Γ_2.*

Proof. If $\beta_1', \ldots, \beta_s'$ is another set of coset representatives then we see that $s = r$. So we can reorder such that $\beta_i = \gamma_i\beta_i'$ for some $\gamma_i \in \Gamma_1$. Hence $f|_k\beta_i = f|_k\beta_i'$, so $f|_k[\Gamma_1 g\Gamma_2]$ is independent of the choice of the β_i's.

In particular, if $\beta_1, \ldots, \beta_r$ is one such choice then so is $\beta_1\gamma, \ldots, \beta_r\gamma_2$ for any $\gamma_2 \in \Gamma_2$. Hence the sum

$$\sum_{i=1}^{r} f|_k\beta_i = \sum_{i=1}^{r} f|_k(\beta_i\gamma) = (\sum_{i=1}^{r} f|_k\beta_i)|_k\gamma,$$

so $\sum_{i=1}^{r} f|_k\beta_i$ is weakly modular of weight k and level Γ_2. □

Note 3.1.10. Note that acting on the right of $f|_k[\Gamma_1 g \Gamma_2]$ by Γ_2 is effectively permuting summands.

Proposition 3.1.11. *If f is a a modular form or a cusp form of level Γ_1 then so is $f|_k[\Gamma_1 g\Gamma_2]$ of level Γ_2.*

Proof. If f is a modular function, a modular form or a cusp form of level Γ_1 then so is each term $f|_k\beta_i$ of level $\beta_i^{-1}\Gamma_1\beta_i \cap \mathrm{SL}_2(\mathbb{Z})$. Hence all the $f|_k\beta_i$ are of the same type of level $\Gamma' := \mathrm{SL}_2(\mathbb{Z}) \cap \bigcap_{i=1}^r \beta_i^{-1}\Gamma_1\beta_i \cap \Gamma_2$ and thus so is $f|_k[\Gamma_1 g\Gamma_2]$.

But all of the properties for a function being a modular function, a modular form or a cusp form of some level Γ are satisfied ifthese properties are already satisfied at any smaller level $\Gamma' \subseteq \Gamma$ of finite index. So we can descend from Γ' to Γ_2. $\square$

Remark 3.1.12. We thus have a map

$$M_k(\Gamma_1) \xrightarrow{[\Gamma_1 g\Gamma_2]} M_k(\Gamma_2).$$

This map preserves cusp forms and hence induces a map

$$M_k(\Gamma_1)/S_k(\Gamma_1) \to M_k(\Gamma_2)/S_k(\Gamma_2).$$

Examples 3.1.13. (1) If $g^{-1}\Gamma_1 g = \Gamma_2$ then $\Gamma_1 g\Gamma_2 = \Gamma_1 g = g\Gamma_2$. So the map $f \mapsto f|_k[\Gamma_1 g\Gamma_2]$ is just $f \mapsto f|_k g$.

(2) More generally, if $g^{-1}\Gamma_1 g \supseteq \Gamma_2$ then this map is still $f \mapsto f|_k g$, but it is not an isomorphism anymore.

(3) If $\Gamma_1 \supset \Gamma_2$ and $g = \mathrm{Id}$, then $\Gamma_1 g\Gamma_2 = \Gamma_1$, and $\Gamma_1 = \Gamma_1.\mathrm{Id}$ is an orbit decomposition. Then $f_k|[\Gamma_1 g\Gamma_2] = f_K\,\mathrm{Id} = f$. This just says that $M(\Gamma_1)$ is a subgpace of $M(\Gamma_2)$.

(4) Suppose $\Gamma_1 \subseteq \Gamma_2$ and $g = 1$. Then the α_i's are just coset representatives for $\Gamma_1\backslash\Gamma_2$ and we are sending

$$f \mapsto \sum_{\gamma \in \Gamma_1\backslash\Gamma_2} f|_k\gamma.$$

This is a surjective map $M_k(\Gamma_1) \to M_k(\Gamma_2)$. The restriction of this map to $M_k(\Gamma_2) \subseteq M_k(\Gamma_1)$ is just the multiplication by the index $[\Gamma_2 : \Gamma_1]$. (The map is called the "trace map" from level Γ_1 to level Γ_2.)

(5) The last example is a much more subtle one. Let $\Gamma = \Gamma_1 = \Gamma_2 = \mathrm{SL}_2(\mathbb{Z})$ and $g = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ for some prime p. Then

$$\Gamma \cap \left(g^{-1}\Gamma g\right) = \Gamma^0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : p \text{ divdes } b \right\}.$$

One can check that $\Gamma^0(p)\backslash\Gamma$ is given by the coset representatives $\left(\begin{smallmatrix}1 & j\\ 0 & 1\end{smallmatrix}\right)_{j=0,\dots,p-1}$ and $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$. So for $f \in M_k(\Gamma)$ we have

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

But f is a modular form of level $\mathrm{SL}_2(\mathbb{Z})$, so

$$
(pz)^{-k} f\left(-\frac{1}{pz}\right) = \left(f|_k \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right)(pz) = f(pz).
$$

Therefore we get

$$
f|_k[\Gamma g\Gamma] = \frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) + p^{k-1} f(pz).
$$

We extract the following lemma from Example (5).

Lemma 3.1.14. *Let H be the subgroup of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ consisting of the lower-triangular matrices. Then we have*

$$
H\backslash \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = \bigsqcup_{j=0}^{p-1} H\bar{\alpha}_j \sqcup H\bar{\beta},
$$

where $\bar{\alpha}_j = \left(\begin{smallmatrix}1 & j\\ 0 & 1\end{smallmatrix}\right)$ for $j = 0, \dots, p-1$ and $\bar{\beta} = \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$.

Definition 3.1.15. (a) Let $\Gamma_1, \Gamma_2 \le \mathrm{SL}_2(\mathbb{Z})$ of finite index. We define $\mathcal{R}(\Gamma_1, \Gamma_2)$ to be the $\mathbb{C}$-vector space with basis the symbols $[\Gamma_1 g \Gamma_2]$ for each $g \in \Gamma_1\backslash \mathrm{GL}_2^+(\mathbb{Q})/\Gamma_2$.

(b) Let $\Gamma_1, \Gamma_2, \Gamma_3 \le \mathrm{SL}_2(\mathbb{Z})$ of finite index. We define a multiplication

$$
\mathcal{R}(\Gamma_1, \Gamma_2) \times \mathcal{R}(\Gamma_2, \Gamma_3) \to \mathcal{R}(\Gamma_1, \Gamma_3).
$$

For $[\Gamma_1 g \Gamma_2] \in \mathcal{R}(\Gamma_1, \Gamma_2)$ and $[\Gamma_2 h \Gamma_3] \in \mathcal{R}(\Gamma_2, \Gamma_3)$ write

$$
\Gamma_1 g \Gamma_2 = \coprod_{i=1}^{s} \Gamma_1 \lambda_i \quad \text{and} \quad \Gamma_2 h \Gamma_3 = \coprod_{j=1}^{t} \Gamma_2 \mu_j.
$$

We define

$$
[\Gamma_1 g \Gamma_2] \times [\Gamma_2 h \Gamma_3] := \sum_{\gamma \in \Gamma_1\backslash \mathrm{GL}_2^+(\mathbb{Q})/\Gamma_3} c_\gamma \cdot [\Gamma_1 \gamma \Gamma_3]
$$

where

$$
c_\gamma := \left|\{(i,j) \in \{1,\dots,s\} \times \{1,\dots,t\} \colon \lambda_i \mu_j \in \Gamma_1 \gamma\}\right|.
$$

Remark 3.1.16. It is tedious to check that this definition is indeed well-defined, so independent of the choice of λ_i and μ_j, and that this multiplication is associative, so

$$[\Gamma_1 g\Gamma_2] \times \Big([\Gamma_2 h\Gamma_3] \times [\Gamma_3 j\Gamma_4]\Big) = \Big([\Gamma_1 g\Gamma_2] \times [\Gamma_2 h\Gamma_3]\Big) \times [\Gamma_3 j\Gamma_4].$$

Moreover, we have to check that the introduced multiplication satisfies

$$f|_k\Big([\Gamma_1 g\Gamma_2] \times [\Gamma_2 h\Gamma_3]\Big) = \Big(f|_k[\Gamma_1 g\Gamma_2]\Big)|_k[\Gamma_2 h\Gamma_3].$$

In particular, $\mathcal{R}(\Gamma) := \mathcal{R}(\Gamma, \Gamma)$ is a ring and $M_k(\Gamma)$ and $S_k(\Gamma)$ are right modules over it.

3.2 The Hecke algebra of $\Gamma_1(N)$

Lemma 3.2.1. *Let Γ be any congruence subgroup containing $\Gamma(N)$. If p is a prime which is comprime to N, then Γ surjects onto $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ under reduction $\pmod p$.*

Proof. It is clearly sufficient to prove the result for $\Gamma = \Gamma(N)$. We know by Strong Approximation (Question Sheet 4) that the map

$$\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/Np\mathbb{Z})$$

is sujective. Since N and p are coprime, we have

$$\mathrm{SL}_2(\mathbb{Z}/Np\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}),$$

so we deduce that the map

$$\mathrm{SL}_2(\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), \qquad x \mapsto (x \pmod N, x \pmod p))$$

is surjective. It follows that for any element $\bar{A} \in \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ there exists $A \in \mathrm{SL}_2(\mathbb{Z})$ which maps to $(\mathrm{Id}, \bar{A})$. Since

$$\Gamma(N) = \ker\left(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\right),$$

this finishes the proof. $\square$

Proposition 3.2.2. *Let p be prime, $N \geq 1$ and $\Gamma = \Gamma_0(N)$ or $\Gamma = \Gamma_1(N)$.*

(i) If p divides N then

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma = \coprod_{i=0}^{p-1} \Gamma \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix}.$$

(ii) If p does not divide N then

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma = \coprod_{i=0}^{p-1} \Gamma \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} \sqcup \Gamma\gamma \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

where $\gamma = 1$ in the case of $\Gamma_0(N)$ and $\gamma = \left(\begin{smallmatrix} a & b \\ N & p \end{smallmatrix}\right)$ in the case of $\Gamma_1(N)$ with a, b being any integers such that $ap - bN = 1$.

Proof. Let $g = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. For $\Gamma = \Gamma_0(N)$ or $\Gamma = \Gamma_1(N)$, let

$$\Gamma' = \Gamma \cap \left(g^{-1}\Gamma g\right).$$

We need to find representatives for the quotient $\Gamma' \backslash \Gamma$.

1. Assume $p \nmid N$.

   Now for $\Gamma = \Gamma_0(N)$, we have

   $$\Gamma' = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : p \text{ divides } b,\ N \text{ divides } c \right\}$$

   and for $\Gamma = \Gamma_1(N)$ that

   $$\Gamma' = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{matrix} p \text{ divides } b,\ N \text{ divides } c \\ a = d = 1 \mod N \end{matrix} \right\}.$$

   Hence in both cases the image $\bar{\Gamma}' = \Gamma' \pmod p$ is $\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right) \subset \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, and by Lemma 3.1.14 we have

   $$\bar{\Gamma}' \backslash \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = \bigsqcup_{j=0}^{p-1} \bar{\Gamma}' \bar{\alpha}_j \sqcup \bar{\Gamma}' \bar{\beta},$$

   By Lemma 3.2.1, we know that there exists lifts of the coset representatives to Γ. For $\bar{\alpha}_j$, this is easy: we take the lift $\alpha_j = \left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right)$.
   For $\bar{\Gamma}'\bar{\beta}$, we need to find an element β of $\Gamma_0(N)$ or $\Gamma_1(N)$ whose reduction $\pmod p$ lies in the coset

   $$\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & \star \\ \star & \star \end{smallmatrix}\right) \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}).$$

   This will be satisfied by any matrix $\beta \in \Gamma$ which

   - for $\Gamma = \Gamma_0(N)$, is of the form $\left(\begin{smallmatrix} pa & b \\ Nc & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}$ such that $pad - Nbc = 1$;
   - for $\Gamma = \Gamma_1(N)$, is of the form $\left(\begin{smallmatrix} pa & b \\ Nc & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}$ such that $pad - Nbc = 1$, and such that

     $$pa = d = 1 \pmod N.$$

     We make the spicific choice that $c = d = 1$; it is then easy to see that we can find a, b which satisfy $pa - Nb = 1$; note that this automatically implies that $pa = 1 \pmod N$.

   Hence we obtain the decomposition

   $$\begin{aligned} \Gamma' \backslash \Gamma &= \bigcup_{j=0}^{p-1} \Gamma' \alpha_j \sqcup \Gamma' \beta \\ \Rightarrow \qquad \Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma &= \bigcup_{j=0}^{p-1} \Gamma' \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \alpha_i \sqcup \Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \beta. \end{aligned}$$

Now write

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} pa & b \\ Nc & d \end{pmatrix} = \begin{pmatrix} a & b \\ Nc & pd \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix},$$

so we can write

$$\Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \beta = \Gamma \begin{pmatrix} a & b \\ Nc & pd \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

In the case $\Gamma = \Gamma_0(N)$, the matrix $\begin{pmatrix} a & b \\ Nc & pd \end{pmatrix}$ is an element of Γ, so we have

$$\Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \beta = \Gamma \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

For $\Gamma = \Gamma_1(N)$ and our choice $c = d = 1$, we get the claimed result.

2. Assume $p|N$. Then one can check that $\left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right)_{j=0,\dots,p-1}$ is a set of coset representatives for $(\Gamma \cap g^{-1}\Gamma g)\backslash\Gamma$, so we don't need α_p since any element of Γ has diagonal entries coprime to p.

$\square$

Corollary 3.2.3. *Let $\Gamma = \Gamma_0(N)$ or $\Gamma = \Gamma_1(N)$, and let $f \in M_k(\Gamma)$.*

1. *If p divides N, then*

$$\left[\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma\right](f) = \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right)$$

2. *If p does not divide N, then*

$$\left[\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma\right](f) = \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) + p^{k-1}\left(f|_k\gamma\right)(pz),$$

where γ is as in Proposition 3.2.2. In particular, in the case $\Gamma = \Gamma_0(N)$ the term $f|_k\gamma$ reduces to f.

Definition 3.2.4. Write T_p for the operator $\left[\Gamma_1(n) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)\right]$.

3.2.1 Diamond operators

Definition 3.2.5. Let $N \geq 1$. A **Dirichlet charachter mod** N is a homomorphism $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$.

Example 3.2.6. The map

$$(\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times,\ 1 \mapsto 1,\ 3 \mapsto -1$$

is a Dirichlet character mod 4. In particular, it is the only non-trivial character mod 4. An example of a character mod 13 is the map

$$(\mathbb{Z}/13\mathbb{Z})^\times \to \mathbb{C}^\times,\ 2 \mapsto e^{2\pi i/12},$$

which is well-defined since 2 generates $(\mathbb{Z}/13\mathbb{Z})^\times$.

Note 3.2.7. If M divides N any Dirichlet character mod M induces a character mod N.

Definition 3.2.8. We say a character χ is **primitive** if it is not induced from a character (mod M) for any M dividing N, $M < N$.

Example 3.2.9. The characters in Example 3.2.6 above are primitive characters. However, the character

$$\chi : (\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}^\times,\ 1, 5 \mapsto 1,\ 3, 7 \mapsto -1$$

is not primitve since it comes from the above character mod 4.

Note 3.2.10. If χ is a Dirichlet character $\pmod N$, it can be extended to a map $\chi : \mathbb{Z} \to \mathbb{C}$ by the recipe

$$\chi(d) = \begin{cases} \chi(d \pmod N) & \text{if } (d, N) = 1 \\ 0 & \text{if } (d, N) > 1 \end{cases}$$

The resulting function is multiplicative: it satisfies

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

Lemma 3.2.11. *The map*

$$\iota : \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times, \qquad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d \pmod N$$

is well-defined, and it induces an isomorphism

$$\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times.$$

Definition 3.2.12. Let $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, and let $g \in \Gamma_0(N)$ such that $\iota(g) = d \pmod N$. Then the diamond operator $\langle d \rangle$ is the double coset operator $\Gamma_1(N)g\Gamma_1(N) \in \mathcal{R}(\Gamma_1(N))$.

Note 3.2.13. Since $\Gamma_1(N)$ is normal in $\Gamma_0(N)$, we have

$$\Gamma_1(N)g\Gamma_1(N) = \Gamma_1(N)g = g\Gamma_1(N).$$

The map

$$(\mathbb{Z}/N\mathbb{Z})^\times \to \mathcal{R}(\Gamma_1(N)), \qquad d \mapsto \langle d \rangle$$

is hence a group homomorphism, and we get an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ by linear operators on $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$.

Recall the following result from the representation theory of finite groups:

Proposition 3.2.14. *Let V be any complex vector space with an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ by linear operators. Then*

$$V = \bigoplus_{\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} V^\chi$$

where

$$V^\chi = \left\{ v \in V : g.v = \chi(g)\cdot v \text{ for all } g \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

Definition 3.2.15. Let χ be a Dirichlet character. We define $M_k(\Gamma_1(N), \chi)$ as the χ-eigenspace $M_k(\Gamma_1(N))^\chi$ for the action of $(\mathbb{Z}/N\mathbb{Z})^\times$. In other words,

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

This is called **the space of modular forms of weight k, level N and character χ.**

We similarly define $S_k(\Gamma_1(N), \chi)$.

Example 3.2.16. If $\mathbb{1}_N$ is the trivial character mod N then

$$M_k(\Gamma_1(N), \mathbb{1}_N) = M_k(\Gamma_0(N)).$$

To see this consider $f \in M_k(\Gamma_1(N), \mathbb{1}_N)$. Then for all $g \in \Gamma_0(N)$ we have

$$f|_k g = \langle \iota(g) \rangle f = f.$$

Note 3.2.17. We have $M_k(\Gamma_1(N), \chi) = \{0\}$ unless $\chi(-1) = (-1)^k$.

3.2.2 Hecke operators on q-expansions

Definition 3.2.18. Define the following two operators on formal q-expansions: let $q = e^{2\pi i z}$, and define

$$U_p.f = \sum a_{np} q^n,$$
$$V_p.f = \sum a_n q^{np}$$

Lemma 3.2.19. *If $f = \sum_{n=0}^\infty a_n q^n$, then*

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

Proof. Note that if $\zeta_p = e^{\frac{2\pi i}{p}}$, then

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

Now

$$\begin{aligned} \sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} &= p^{k-1}p^{-k} \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) \\ &= \frac{1}{p} \sum_{j=0}^{p-1} \sum_{n=0}^{\infty} a_n e^{2\pi i n \frac{z+j}{p}} \\ &= \sum_{n=0}^{\infty} a_n e^{\frac{2\pi i n z}{p}} \left(\frac{1}{p} \sum_{j=0}^{p-1} \zeta_p^{nj}\right) \\ &= U_p.f \end{aligned}$$

by Lemma 3.2.19. The statement for V_p is clear. □

Theorem 3.2.20. *If $f \in M_k(\Gamma_1(N))$, then*

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

Proof. Immediate from Corollary 3.2.3 and Lemma 3.2.19. □

Corollary 3.2.21. *If $f \in M_k(\Gamma_1(N), \chi)$, then for all p we have*

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

Note 3.2.22. Recall that $\chi(p) = 0$ if $p \mid N$.

Example 3.2.23. Consider the Eisenstein series

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

Claim. $E_k(z)$ is an eigenform **for all** T_p, and

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

Proof of claim. By Theorem 3.2.20, we have for any $f \in M_k(\Gamma_1(1))$

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

where we understand that $a_{n/p}(f) = 0$ if $p \nmid f$. Hence

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

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 $\sigma_{k-1}(n/p) = 0$ if $p \nmid n$. We now want to show that

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

- For $p \nmid p$, this is just the multiplicativity of σ_{k-1}.
- if $p|n$, write $n = p^e m$ with $p \nmid m$. Then we need to show that

$$\begin{aligned} & \sigma_{k-1}(p^{e+1}m) + p^{k-1}\sigma_{k-1}(p^{e-1}m) = \sigma_{k-1}(p)\sigma_{k-1}(p^e m) \\ \Leftrightarrow\quad & \sigma_{k-1}(p^{e+1}) + p^{k-1}\sigma_{k-1}(p^{e-1}) = \sigma_{k-1}(p)\sigma_{k-1}(p^e). \end{aligned} \tag{3.1}$$

  since p and m are coprime. But (3.1) can easily seen to be true.

3.2.3 The Hecke algebra

Definition 3.2.24. For $\lambda \in \mathbb{Q}^\times$ write R_λ for the Hecke operator $\left[\Gamma_1(N)\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right)\Gamma_1(N)\right]$. Define $\mathcal{T}(\Gamma_1(N))$ as the subalgebra of $\mathcal{R}(\Gamma_1(N))$ generated by the operators T_p, R_λ and $\langle d\rangle$ for all primes p, $\lambda \in \mathbb{Q}^\times$ and $d \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Proposition 3.2.25. *The algebra $\mathcal{T}(\Gamma_1(N))$ is commutative.*

We will only sketch the proof:

Proof. The R_λ's commute with everything since $\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right)$ is central in $\mathrm{GL}_2^+(\mathbb{Q})$ and the $\langle d\rangle$'s commute with each other. So it remains to show that the T_p's commute with each other and with the $\langle d\rangle$'s.

We will first show that for p, q distinct primes, we have

$$T_pT_q = T_qT_p = \Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & pq\end{pmatrix}\Gamma_1(N).$$

To simplify the notation, let $\Gamma = \Gamma_1(N)$. Recall the multiplication in $\mathcal{R}(\Gamma)$: write $T_p = \bigsqcup \Gamma\alpha_i$, $T_q = \bigsqcup \Gamma\beta_j$, with $\alpha_i \in \Gamma\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma$, $\beta_j \in \Gamma\left(\begin{smallmatrix}1 & 0\\ 0 & q\end{smallmatrix}\right)\Gamma$. (Of course we know what the α_i, β_j are explicitly, but we do not use that here.) Then

$$T_pT_q = \sum_{\gamma \in \Gamma\backslash \mathrm{GL}_2^+(\mathbb{Q})/\Gamma} c_\gamma \cdot [\Gamma\gamma\Gamma],$$

where $c_\gamma := |\{(i,j)\colon \alpha_i\beta_j \in \Gamma\gamma\}|$.

Claim. For all $\alpha \in \Gamma\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma$, $\beta \in \Gamma\left(\begin{smallmatrix}1 & 0\\ 0 & q\end{smallmatrix}\right)\Gamma$, we have

$$\alpha\beta \in \Gamma\left(\begin{smallmatrix}1 & 0\\ 0 & pq\end{smallmatrix}\right).$$

Proof of claim. Note that $\alpha\beta$ has determinant pq, so by the Smith normal form we have $\alpha\beta \in \mathrm{SL}_2(\mathbb{Z})\left(\begin{smallmatrix} 1 & 0 \\ 0 & pq \end{smallmatrix}\right)\mathrm{SL}_2(\mathbb{Z})$. One can show that since $\alpha\beta = \left(\begin{smallmatrix} 1 & * \\ 0 & pq \end{smallmatrix}\right) \bmod N$ we in fact have

$$\alpha\beta \in \Gamma \begin{pmatrix} 1 & * \\ 0 & pq \end{pmatrix} \Gamma.$$

This proves that the product T_pT_q is a constant multiple of $\Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & pq \end{smallmatrix}\right)\Gamma_1(N)$ and one can check that this constant is indeed one.

It remains to check that $T_p\langle d\rangle = \langle d\rangle T_p$. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ as in the definition of $\langle d\rangle$. Note that since $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ we have

$$\begin{aligned}
\langle d\rangle\, T_p &= (\Gamma_1(N)\gamma)\left[\Gamma_1(N)\gamma\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\gamma^{-1}\Gamma_1(N)\right] \\
&= \Gamma_1(N)\left(\gamma\Gamma_1(N)\gamma^{-1}\right)\left(\gamma\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\gamma^{-1}\right)\gamma\Gamma_1(N) \\
&= \left[\Gamma_1(N)\gamma\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\gamma^{-1}\Gamma_1(N)\right]\langle d\rangle\,.
\end{aligned}$$

But $\gamma\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\gamma^{-1}$ has determinant p and is $\left(\begin{smallmatrix} 1 & * \\ 0 & p \end{smallmatrix}\right)$ mod N. By multiplying on the right by some power of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$ we can make this be $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ mod N. So it is in $\Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_1(N)$ and thus $T_p\,\langle d\rangle = \langle d\rangle\, T_p$. □

Definition 3.2.26. For a prime power $n = p^r$, $r \geq 2$, we define T_n by

$$T_{p^r} = \begin{cases} (T_p)^r, & \text{if } p \text{ divides } N, \\ T_{p^{r-1}}T_p - p\,R_pT_{p^{r-2}}\,\langle p\rangle\,, & \text{if } p \text{ does not divide } N. \end{cases}$$

For general $n = p_1^{r_1}\dots p_k^{r_k}$ we define $T_n = T_{p_1^{r_1}}\dots T_{p_k^{r_k}}$.

Note 3.2.27. We have $T_n \in \mathcal{T}(\Gamma_1(N))$ for all $n \in \mathbb{N}$ by definition. In particular all T_n's commute.

Proposition 3.2.28. *Let $f \in M_k(\Gamma_1(N))$, and let m, n be comprime. Then $a_m(T_nf) = a_{mn}(f)$. In particular, we have $a_1(T_nf) = a_n(f)$.*

Proof. First a prime power $n = p^r$. By induction and using proposition 3.2.20 we get

$$\begin{aligned}
T_{p^r}(f) = \sum_{n=0}^{\infty} a_{np^r}(f)q^n \;&+\; p^{k-1}\sum_{n=0}^{\infty} a_{np^{r-1}}\left(\langle p\rangle\, f\right)q^{np} \\
&+\; p^{2(k-1)}\sum_{n=0}^{\infty} a_{np^{r-2}}\left(\langle p\rangle^2\, f\right)q^{np^2} \\
&+\;\dots\;+\; p^{r(k-1)}\sum_{n=0}^{\infty} a_n\left(\langle p\rangle^r\, f\right)q^{np^r}.
\end{aligned}$$

If $n = p_1^{r_1} \dots p_k^{r_k}$ with $\gcd(n, m) = 1$, then

$$a_m(T_n f) = a_m(T_{p_1^{r_1}} \dots T_{p_k^{r_k}} f) = a_{mp_1^{r_1}}((T_{p_2^{r_2}} \dots T_{p_k^{r_k}} f) = \dots = a_{mp_1^{r_1} \dots m_k^{r_k}}(f).$$

□

Remark 3.2.29. For general m, n (not necessarily comprime), one can show (exercise) that

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

Proposition 3.2.30. *For all χ mod N the operators T_n preserve the subspaces $M_k(\Gamma_1(N), \chi)$ and $S_k(\Gamma_1(N), \chi)$ of $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$.*

Proof. This follows from the commutativity of $\mathcal{T}(\Gamma_1(N))$ as commuting operators preserve each others eigenspaces. □

Definition 3.2.31. We say $f \in M_k(\Gamma_1(N))$ is an **Hecke eigenform** (or just eigenform) if it is a simultaneous eigenvector for all the operators in $\mathcal{T}(\Gamma_1(N))$ (i.e. for all the $T_n's$ and $\langle d \rangle$'s).

A normalized Hecke eigenform is an eigenform satisfying $a_1(f) = 1$.

Note 3.2.32. Let $f \in M_k(\Gamma_1(N))$ be an eigenform, say $T_n.f = \lambda_n f$ for all n. Then

$$a_n(f) = a_1(T_n f) = \lambda_n a_1(f) \qquad \forall n \geq 1.$$

It follows that if $a_1(f) = 0$, then $a_n(f) = 0$ for all $n \geq 1$, so f is constant. Therefore a non-constant eigenform must have $a_1(f) \neq 0$, and it may be scaled to be a normalized eigenform.

Theorem 3.2.33. *Let $f \in M_k(\Gamma_1(N))$ be a normalized eigenform. Then the eigenvalues of the Hecke operators T_n on f are the coefficients of the q-expansion of f at the cusp ∞: we have*

$$T_n.f = a_n(f) \cdot f \qquad \forall\, n \geq 1.$$

Proposition 3.2.34. *Let $f \in M_k(\Gamma_1(N), \chi)$ be a modular form with q-expansion $\sum_{n \geq 0} a_n(f) q^n$ at ∞. Then f is a normalized eigenform if and only if*

i $a_1(f) = 1$;

ii $a_{mn}(f) = a_m(f) a_n(f)$ *for all m, n comprime;*

iii $a_{p^r}(f) = a_p(f) a_{p^{r-1}}(f) - p^{k-1} \chi(p) a_{p^{r-2}}(f)$ *for all primes p and all $r \geq 2$.*

Proof. The implication $\Rightarrow$ follows directly from Definition 3.2.26 and Theorem 3.2.33. Conversely, if $f \in M_k(\Gamma_1(N), \chi)$ satisfies properties (i)-(iii), then f is already normalized, so we need to show that it satisfies

$$a_m(T_p.f) = a_p(f) a_m(f) \qquad \forall\, p \text{ prime}, \forall m \geq 1.$$

If $p \nmid m$, then it follows from Proposition 3.2.28 that $a_m(T_p.f) = a_{mp}(f)$, which by (ii) is equal to $a_m(f)a_p(f)$. If $m = p^r m'$ with $p \nmid m'$, then by Remark 3.2.29 we have

$$a_m(T_p.f) = a_{p^{r+1}m'}(f) + \chi(p)p^{k-1}a_{p^{r-1}m'}(f).$$

Using (ii) and (ii), this can be shown to be equal to $a_p(f)a_m(f)$ as required. □

Question. Do such normalized eigenforms actually exist?

Example 3.2.35.

1. A non-Eisenstein eigenform is given by $\Delta \in S_{12}(\mathrm{SL}_2(\mathbb{Z}))$. This is clear since all T_n preserve S_{12} and S_{12} is spanned by Δ. Moreover Δ is obviously normalized. Let $\tau(n) = a_n(\Delta)$. Then
$$\tau(mn) = \tau(m)\tau(n)$$
for m and n coprime by Proposition 3.2.34. This shows a statement which was made in the prologue of this lecture.

2. Similarly we can show that the cusp forms $E_4\Delta$, $E_6\Delta$, $E_4^2\Delta$, $E_4E_6\Delta$ and $E_4^2E_6\Delta$ of level $(\mathrm{SL}_2(\mathbb{Z}))$ and weight 16, 18, 20, 22 and 26 are normalized eigenforms since the corresponding spaces of cusp forms are one-dimensional.

3. More interesting is the case $k = 24$ since $S_{24}(\mathrm{SL}_2(\mathbb{Z}))$ is two-dimensional. It can easily be shown that $S_{24}(\mathrm{SL}_2(\mathbb{Z}))$ is spanned by $f_1 = E_4^3\Delta$ and $f_2 = \Delta^2$. The q-expansion of these are given by
$$\begin{aligned} f_1 &= q + 696q^2 + 162252q^3 + 128318089q^4 + \dots \\ f_1 &= q^2 - 48q^3 + 1080q^4 + \dots. \end{aligned}$$
We want to know how T_2 acts on this basis. By the formula in the proof of Proposition 3.2.28, we have
$$\begin{aligned} T_2(f_1) &= \left(696q + 128318089q^2 + \dots\right) + 2^{23}\left(q^2 + 696q^4 + \dots\right) \\ &= 696q + 136706697q^2 + \dots \end{aligned}$$
and
$$\begin{aligned} T_2(f_2) &= \left(q + 1080q^2 + \dots\right) + 2^{23}\left(q^4 + \dots\right) \\ &= q + 1080q^2 + \dots \end{aligned}$$
In terms of the given basis we therefore have
$$\begin{aligned} T_2(f_1) &= 696f_1 + 136222281f_2 \\ T_2(f_2) &= f_1 + 384f_2. \end{aligned}$$
Thus T_2 is given by the matrix
$$\begin{pmatrix} 696 & 1 \\ 136222281 & 384 \end{pmatrix}.$$

Open conjecture (Maeda's conjecture)**.** *The Galois group of the splitting field of the characteristic polynomial of T_2 on $S_k(\mathrm{SL}_2(\mathbb{Z}))$ is as large as possible, so isomorphic to the symmetric group* $\mathrm{Sym}(d)$ *where* $d = \dim(S_k)$.