

Modular forms and their combinatorial variants

Henrik Bachmann

Nagoya University

Topics in Mathematical Science IV, Spring 2023

Contact: Math. Building Room 457, henrik.bachmann@math.nagoya-u.ac.jp

Lecture notes and Exercises are available at: http://www.henrikbachmann.com/mf_2023.html

🔔 **These notes are under construction and therefore may contain mistakes and change without notice. If you find any typos/errors or have any suggestion, please let me know!**

Contents

1	Introduction & Motivation	2
1.1	The four square theorem	3
1.2	Sum of divisors and the Hurwitz identity	5
2	Modular forms for $SL_2(\mathbb{Z})$	7
2.1	The modular group and fundamental domains	7
2.2	Modular functions and modular forms	9
2.3	Eisenstein series	12
2.4	Cusp forms and the discriminant function Δ	15
2.5	Structure of the space of modular forms	17
3	Modular forms for congruence subgroups	23
3.1	Congruence subgroups	23
3.2	Modular forms for congruence subgroups	24
	References	25

1 Introduction & Motivation

Modular forms are functions appearing in several areas of mathematics as well as mathematical physics. We start directly with a rough definition of modular forms and give some explicit applications of them. In this lecture, a **modular form** of weight $k \in \mathbb{Z}$ for some subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ of the **modular group**

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

is a holomorphic function $f \in \mathcal{O}(\mathbb{H})$ in the complex upper half-plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$, which satisfies the **modular transformation property**

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \tag{1.1}$$

for all $\tau \in \mathbb{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ together with certain growth conditions ("holomorphicity at the cusps"). We will make this notion precise later, but in the case $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ this just means that $f(it)$ is bounded as $t \rightarrow \infty$. By $M_k(\Gamma)$ we denote the \mathbb{C} -vector space spanned by all modular forms of weight $k \in \mathbb{Z}$ for the subgroup Γ . A common example for subgroups Γ are given for $N \geq 1$ (the **level**) by the **congruence subgroups**

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}. \tag{1.2}$$

Notice that in the level $N = 1$ case we have $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$. One important fact is that (1.1) just needs to be checked for the generators of Γ . For example, $\mathrm{SL}_2(\mathbb{Z})$ is generated by the two matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Therefore, a holomorphic function f (bounded at $i\infty$) satisfying

$$f(\tau + 1) = f(\tau), \quad f\left(-\frac{1}{\tau}\right) = \tau^k f(\tau)$$

is already a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$.

In general, if $T \in \Gamma$ then $f(\tau + 1) = f(\tau)$ and $f \in M_k(\Gamma)$ has a **Fourier expansion**

$$f(\tau) = \sum_{n \geq 0} a_n q^n, \quad (q = e^{2\pi i \tau})$$

for some $a_n \in \mathbb{C}$, which are called the **Fourier coefficients**. That this sum starts at $n = 0$ is a consequence of f being bounded at $i\infty$. One of the many reasons why modular forms are interesting/powerful are given by the following facts:

- Modular forms occur naturally in connection with problems arising in many areas of mathematics and theoretical physics and the Fourier coefficients a_n often encode the arithmetically interesting information about a problem.
- The spaces $M_k(\Gamma)$ are finite dimensional and algorithmically computable.

One common theme is the following: Assume you have some sequence of numbers $a_n \in \mathbb{N}$ (or $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) which arise "naturally" (e.g. they count something) and you want to find an explicit formula for them. Then in a lot of applications, where modular forms appear, the following strategy works:

- ① Consider the generating series $G(\tau) = \sum_{n \geq 0} a_n q^n$.
- ② Try to find $k \in \mathbb{Z}$, $N \geq 1$ such that $G \in M_k(\Gamma_0(N))$. Often this can be done by showing the modular transformation property (1.1) for the generators of $\Gamma_0(N)$ using well-known tools from calculus (e.g. Poisson summation formula).
- ③ Determine $\dim M_k(\Gamma_0(N)) = d$. We will see that this can be done explicitly by using complex analysis (residue theorem, Riemann-Roch).
- ④ Construct a basis of $\dim M_k(\Gamma_0(N))$. Often one can construct d linearly independent elements by using, for example, Eisenstein series. The Fourier coefficients of these elements are given explicitly.
- ⑤ Write G in terms of this basis. For this one just needs to check the first few Fourier coefficients.

This strategy will then lead to an explicit formula for a_n . We will use this strategy now to prove two well-known theorems in classical number theory.

1.1 The four square theorem

We start by illustrating some applications coming from classical number theory. For this we start with the following well-known theorem:

Theorem 1.1 (Theorem of Lagrange (1770)). *Every positive integer is a sum of four¹ squares.*

For example $1 = 1^2 + 0^2 + 0^2 + 0^2$ or $30 = 1^2 + 2^2 + 3^2 + 4^2 = 0^2 + 1^2 + 2^2 + 5^2$ and

$$2023 = 1^2 + 2^2 + 13^2 + 43^2 = 3^2 + 3^2 + 18^2 + 41^2.$$

In particular, these examples show that the representation as a sum of four squares is not unique.

Question: *In how many ways can a natural number n be written as a sum of four squares?*

In other words, the question asks for an explicit formula for the function

$$r_4(n) = \# \{ (a, b, c, d) \in \mathbb{Z}^4 \mid n = a^2 + b^2 + c^2 + d^2 \}.$$

For example, $r_4(1) = 8$ since

$$1 = 1^2 + 0^2 + 0^2 + 0^2 = 0^2 + 1^2 + 0^2 + 0^2 = \dots = (-1)^2 + 0^2 + 0^2 + 0^2 = \dots$$

The question was answered by Jacobi who gave the following explicit formula for $r_4(n)$.

Theorem 1.2 (Jacobi's four-square theorem (1834)). *For all $n \in \mathbb{Z}_{\geq 1}$ we have*

$$r_4(n) = 8 \sum_{\substack{d|n \\ 4 \nmid d}} d.$$

Here the sum runs over all positive divisors d of n , which are not divisible by 4.

Example 1. *i) If p is prime, then there are $8(p+1)$ ways to write p as a sum of four squares.*

ii) The divisors of 2023 are 1, 7, 17, 119, 289, and 2023, which are all not divisible by 4 and therefore we have

$$r_4(2023) = 8(1 + 7 + 17 + 119 + 289 + 2023) = 19648$$

ways of writing 2023 as a sum of four squares.

¹Four is the smallest integer with this property, since 5 is not the sum of two squares and 7 is not the sum of three.

We will now use the strategy mentioned before to prove Theorem 1.2:

- ① We consider the generating series of $r_4(n)$, i.e. set

$$G(\tau) = \sum_{n \geq 0} r_4(n)q^n = 1 + 8q + 24q^2 + 32q^3 + 24q^4 + 48q^5 + 96q^6 + 64q^7 + 24q^8 + 104q^9 + \dots$$

- ② Now we will sketch how to show that $G \in M_2(\Gamma_0(4))$, i.e. we need to check the modular transformation property

$$G\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 G(\tau)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$. Since we just need to check this on the generators of $\Gamma_0(4)$ we first show (Homework 1) that $\Gamma_0(4)$ is generated by the matrices $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$. Therefore, we just need to check

$$G(\tau + 1) = G(\tau), \quad G\left(\frac{\tau}{4\tau + 1}\right) = (4\tau + 1)^2 G(\tau) \tag{1.3}$$

since (1.1) is trivial for the negative identity matrix. Since we defined G by the Fourier expansion we automatically get $G(\tau + 1) = G(\tau)$. To show the second equation we define the **theta-function** by

$$\Theta(\tau) = \sum_{n \in \mathbb{Z}} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \dots$$

For this function one can show the following.

Proposition 1.3. *The theta-function satisfies the two functional equations*

$$\Theta(\tau + 1) = \Theta(\tau), \quad \Theta\left(-\frac{1}{4\tau}\right) = \sqrt{\frac{2\tau}{i}} \Theta(\tau) \quad (\tau \in \mathbb{H}). \tag{1.4}$$

Proof. The first equation follows directly from definition and the second follows from the Poisson transformation formula. See [Z, Proposition 9] for details. \square

Now notice that we have $G(\tau) = \Theta(\tau)^4$. Using $\frac{\tau}{4\tau + 1} = -\frac{1}{4(\frac{1}{4\tau} - 1)}$ in Proposition 1.4 then implies $G\left(\frac{\tau}{4\tau + 1}\right) = (4\tau + 1)^2 G(\tau)$.

- ③ As we will see we have $\dim_{\mathbb{C}} M_2(\Gamma_0(4)) = 2$.

- ④ Now define the Eisenstein series of weight 2 by

$$E_2(\tau) = 1 - 24 \sum_{n \geq 1} \frac{nq^n}{1 - q^n} = 1 - 24 \sum_{n \geq 1} \sigma_1(n)q^n = 1 - 24q - 72q^2 - 96q^3 - 168q^4 + \dots,$$

where $\sigma_1(n) = \sum_{d|n} d$ is the sum of all divisors of n . Later we will see that E_2 almost transforms like a modular form of weight 2 as we will have

$$E_2\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 E_2(\tau) - \frac{6}{\pi} ic(c\tau + d). \tag{1.5}$$

Using this one then checks by direct calculation that $E_2(\tau) - 2E_2(2\tau)$ and $E_2(\tau) - 4E_2(4\tau)$ also satisfy (1.3). Moreover, comparing their first few Fourier coefficients show that they are linearly independent and therefore they form a basis of $M_2(\Gamma_0(4))$. (We ignored the growth condition here, but this one is easy to check for all appearing functions in this example.)

- ⑤ Finally we want to write G in terms of the basis we found. Comparing the first few Fourier coefficients (which is sufficient as we will see) we find

$$G(\tau) = -\frac{1}{3}(E_2(\tau) - 4E_2(4\tau)) = 8 \sum_{n \geq 1} \left(\sum_{d|n} d - \sum_{\substack{d|n \\ 4|d}} d \right) q^n,$$

which then gives exactly the formula in 1.2 for $r_4(n)$.

1.2 Sum of divisors and the Hurwitz identity

In this section, we will give another classical example for the application of modular forms. For this we will prove some identities of general divisor sums. For $l \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 1}$ the l -th **divisor sum** $\sigma_l(n)$ is defined by

$$\sigma_l(n) = \sum_{d|n} d^l,$$

where the sum runs over all positive divisors d of n . In particular $\sigma_0(n)$ counts the divisors of n and $\sigma_1(n)$ is the sum of all divisor of n . For example since the divisor of 6 are 1, 2, 3, 6, we have $\sigma_0(6) = 4$ and $\sigma_1(6) = 1 + 2 + 3 + 6 = 12$. A few more examples:

n	$\sigma_1(n)$	$\sigma_3(n)$	$\sigma_5(n)$	$\sigma_7(n)$	$\sigma_9(n)$	$\sigma_{11}(n)$
1	1	1	1	1	1	1
2	3	9	33	129	513	2049
3	4	28	244	2188	19684	177148
4	7	73	1057	16513	262657	4196353
5	6	126	3126	78126	1953126	48828126
6	12	252	8052	282252	10097892	362976252
7	8	344	16808	823544	40353608	1977326744
8	15	585	33825	2113665	134480385	8594130945
9	13	757	59293	4785157	387440173	31381236757

As a generalization of E_2 from the previous section, we define for an even $k \geq 2$ the (normalized) **Eisenstein series of weight k** by

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

where again $q = e^{2\pi i \tau}$ and B_k denotes the k -th **Bernoulli number** defined by the generating function

$$\sum_{k=0}^{\infty} \frac{B_k}{k!} X^k = \frac{X}{e^X - 1}. \tag{1.6}$$

A few example for the first Bernoulli numbers are given by the following table The Eisenstein

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
B_k	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$	0	$-\frac{691}{2730}$	0	$\frac{7}{6}$	0	$-\frac{3617}{510}$

series of weight 4,6 and 8 are given by the following q -series

$$\begin{aligned} E_4(\tau) &= 1 + 240 \sum_{n \geq 1} \sigma_3(n)q^n = 1 + 240q + 2160q^2 + 6720q^3 + 17520q^4 + \dots \\ E_6(\tau) &= 1 - 504 \sum_{n \geq 1} \sigma_5(n)q^n = 1 - 504q - 16632q^2 - 122976q^3 - 532728q^4 + \dots \\ E_8(\tau) &= 1 + 480 \sum_{n \geq 1} \sigma_7(n)q^n = 1 + 480q + 61920q^2 + 1050240q^3 + 7926240q^4 + \dots \end{aligned} \quad (1.7)$$

The goal of this section will be to give two different proofs of the following identity. One of these will again use the strategy used before (i.e. we use modular forms) and the other will be done by explicit calculation.

Theorem 1.4 (Hurwitz identity). *For all $n \in \mathbb{Z}_{\geq 1}$ we have*

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

For example for $n = 3$ we have $\sigma_7(3) = 1 + 3^7 = 2188$ and

$$\sigma_3(3) + 120 \sum_{j=1}^2 \sigma_3(j)\sigma_3(3-j) = 1 + 3^3 + 120(1 \cdot (1 + 2^3) + (1 + 2^3) \cdot 1) = 28 + 120 \cdot 18 = 2188.$$

🐱 ————— Until here in lecture 1 (14th April, 2023) ————— 🐱

Modular proof of Theorem 1.4. First notice that the identity in question equivalent to the equation

$$E_8(\tau) = E_4(\tau)^2.$$

We will see that for all even $k \geq 4$ we have $E_k \in M_k$ and that (Homework 1) we have $E_4^2 \in M_8$. Further we will show that $\dim M_8 = 1$ and therefore E_4^2 needs to be a multiple of E_8 . But this multiple is 1, since both have 1 as the constant term in their Fourier expansion. \square

Since we did not prove any of the claims in the above proof, we will also give a combinatorial/elementary proof. These kinds of proofs will also be generalized at a later stage, when we take about combinatorial modular forms.

Combinatorial proof of Theorem 1.4. We use the elements $F_n \in \mathbb{Z}[[q]] \cap \mathbb{Q}(q)$ defined by

$$F_n = \frac{q^n}{1 - q^n} = \sum_{m=1}^{\infty} q^{mn} \quad (n \in \mathbb{N}),$$

to write

$$\begin{aligned} \left(\sum_{n>0} \sigma_3(n)q^n \right)^2 &= \left(\sum_{u>0} u^3 F_u \right)^2 = \sum_{u,v>0} \frac{uv}{12} ((u+v)^4 + (u-v)^4 - 2u^4 - 2v^4) F_u F_v \\ &= \sum_{w>0} \frac{w^4}{12} \left\{ \sum_{u+v=w} uv F_u F_v + 2 \sum_{v-u=w} uv F_u F_v - 4w F_w \sum_{u>0} u F_u \right\}. \end{aligned}$$

Using the identity $F_a F_b = F_a F_{a+b} + F_b F_{a+b} + F_{a+b}$ we can rewrite the expression in curly brackets as

$$\begin{aligned} & \sum_{0 < u < w} u(w-u)F_w(2F_u+1) + 2 \sum_{u > 0} u(u+w)(F_u F_w - F_{u+w} F_w - F_{u+w}) - 4wF_w \sum_{u > 0} uF_u \\ &= 2F_w \left(\sum_{0 < n \leq w} + \sum_{n > w} - \sum_{n > 0} \right) n(w-n)F_n + \frac{1}{6}(w^3-w)F_w - 2 \sum_{u > w} u(u-w)F_u. \end{aligned}$$

The first term here vanishes identically since every positive $n > 0$ satisfies either $0 < n \leq w$ or $n > w$ but not both. It follows that

$$\begin{aligned} \left(\sum_{n > 0} \sigma_3(n)q^n \right)^2 &= \sum_{w > 0} \frac{w^7 - w^5}{72} - \sum_{u > 0} u \left(\sum_{0 < w < u} \frac{w^4(u-w)}{6} \right) F_u \\ &= \sum_{w > 0} \frac{w^7 - w^3}{120} F_w = \sum_{n > 0} \frac{\sigma_7(n) - \sigma_3(n)}{120} q^n. \end{aligned}$$

□

2 Modular forms for $\mathrm{SL}_2(\mathbb{Z})$

The modular forms mentioned in the previous section were given by q -series. But actually modular forms are functions from the upper half plane to the complex numbers. That they can be written as q -series will follow later as a simple implication of their definition. We will start by giving the definition of the upper half plane and the action of the modular group on this space. With this, we will define modular functions and modular forms, before giving (non-trivial) examples.

2.1 The modular group and fundamental domains

The **upper half plane**, denoted \mathbb{H} , is the set of all complex numbers with positive imaginary part:

$$\mathbb{H} = \{ \tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0 \} = \{ x + iy \in \mathbb{C} \mid x, y \in \mathbb{R}, y > 0 \}.$$

The **modular group** (or special linear group) $\mathrm{SL}_2(\mathbb{Z})$ is the group of 2×2 -matrices with integer entries and determinant one:

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathbb{C}$ we define the fractional linear transformation

$$\gamma(\tau) := \frac{a\tau + b}{c\tau + d}.$$

This gives a left action of $\mathrm{SL}_2(\mathbb{Z})$ on \mathbb{H} (Homework 1)

The group $\mathrm{SL}_2(\mathbb{Z})$ contains the following three matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which correspond to the identity and the fractional transformation $\tau \mapsto -\frac{1}{\tau}$ and $\tau \mapsto \tau + 1$. The latter two fractional transformation will play the major role in our studies, since we have following:

Proposition 2.1. *The matrices S and T generate $\mathrm{SL}_2(\mathbb{Z})$.*

Proof. Homework 1. □

Remark 2.2. Some authors denote by the modular group the group of transformations generated by $\gamma(\cdot)$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Since $(-I)(\tau) = \tau$ this group is isomorphic to $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$.

Definition 2.3. *Two points $\tau_1, \tau_2 \in \mathbb{H}$ are called $\mathrm{SL}_2(\mathbb{Z})$ -equivalent if there exists a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma(\tau_1) = \tau_2$. A **fundamental domain** \mathcal{F} for $\mathrm{SL}_2(\mathbb{Z})$ is a closed subset of \mathbb{H} , such that*

- i) every $\tau \in \mathbb{H}$ is $\mathrm{SL}_2(\mathbb{Z})$ -equivalent to a point in \mathcal{F} .*
- ii) no two points in the interior of \mathcal{F} are $\mathrm{SL}_2(\mathbb{Z})$ -equivalent.*

Proposition 2.4. *The following set is a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$*

$$\mathcal{F} = \left\{ \tau \in \mathbb{H} \mid |\tau| \geq 1 \text{ and } |\mathrm{Re}(\tau)| \leq \frac{1}{2} \right\}.$$

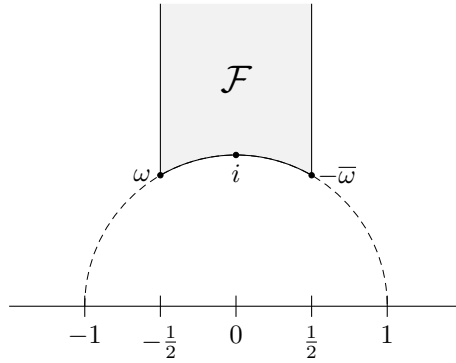


Figure 1: Fundamental domain \mathcal{F} and the points $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $-\bar{\omega} = S(\omega) = \frac{1}{2} + \frac{\sqrt{3}}{2}i$.

Proof. We first show that every element $\tau \in \mathbb{H}$ is equivalent to a point in \mathcal{F} : For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we have (see Homework 1)

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}. \quad (2.1)$$

Since c, d are integers, we can find a matrix $\gamma_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, such that $|c\tau + d|$ is minimal. In particular we get by (2.1) that

$$\mathrm{Im}(\gamma_0(\tau)) \geq \mathrm{Im}(\gamma(\tau)) \quad \text{for all } \gamma \in \mathrm{SL}_2(\mathbb{Z}). \quad (2.2)$$

Since the action of T corresponds to a horizontal translation, we can find a $j \in \mathbb{Z}$, such that $\gamma_1 = T^j \gamma_0$ satisfies $-\frac{1}{2} \leq \mathrm{Re}(\gamma_1(\tau)) \leq \frac{1}{2}$. We now already have $\gamma_1(\tau) \in \mathcal{F}$ because otherwise we would have $|\gamma_1(\tau)| < 1$ and therefore

$$\mathrm{Im}(S\gamma_1(\tau)) = \frac{\mathrm{Im}(\gamma_1(\tau))}{|\gamma_1(\tau)|^2} > \mathrm{Im}(\gamma_1(\tau)) = \mathrm{Im}(\gamma_0(\tau)),$$

which is not possible by (2.2).

We now prove that no two points in the interior of \mathcal{F} are $\mathrm{SL}_2(\mathbb{Z})$ -equivalent: Let $\tau \in \mathcal{F}$ and assume we have a $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that also $\gamma(\tau) \in \mathcal{F}$. Without loss of generality we can assume that $\mathrm{Im}(\gamma(\tau)) \geq \mathrm{Im}(\tau)$ (otherwise replace γ by γ^{-1}). By (2.1) we therefore have $|c\tau + d| \leq 1$. Since $c, d \in \mathbb{Z}$ and $\tau \in \mathcal{F}$ this can just be the case if $|c| \leq 1$, which leaves us with the following cases:

- i) $c = 0, d = \pm 1$: In this case we have $\gamma = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix}$ and therefore we either have $\gamma = I$ or $\mathrm{Re}(\tau) = \pm \frac{1}{2}$, i.e. τ is on one of the vertical boundary lines of \mathcal{F} .
- ii) $c = \pm 1, d = 0$ and $|\tau| = 1$: In this case we have $\gamma = \begin{pmatrix} a & \mp 1 \\ \pm 1 & 0 \end{pmatrix} = \pm T^a S$. This gives either $a = 0$ with τ and $\gamma(\tau)$ on the unit circle (and symmetrically located with respect to the imaginary axis), $a = -1$ with $\tau = \gamma(\tau) = \omega$ or $a = 1$ with $\tau = \gamma(\tau) = -\bar{\omega}$.
- iii) $c = d = \pm 1$ and $\tau = \omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$: In this case we have $\gamma = \begin{pmatrix} a & a \mp 1 \\ \pm 1 & \pm 1 \end{pmatrix} = \pm T^a ST$ which gives either $a = 0$ and $\gamma(\tau) = \omega$ or $a = 1$ and $\gamma(\tau) = -\bar{\omega}$.
- iv) $c = -d = \pm 1$ and $\tau = -\bar{\omega} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$: This case is similar to case iii).

In all cases we conclude that either $\gamma = I$ or τ and $\gamma(\tau)$ are on the boundary of \mathcal{F} . \square

Remark 2.5. The following diagram shows how the fundamental domain \mathcal{F} is translated by different matrices in $\mathrm{SL}_2(\mathbb{Z})$.

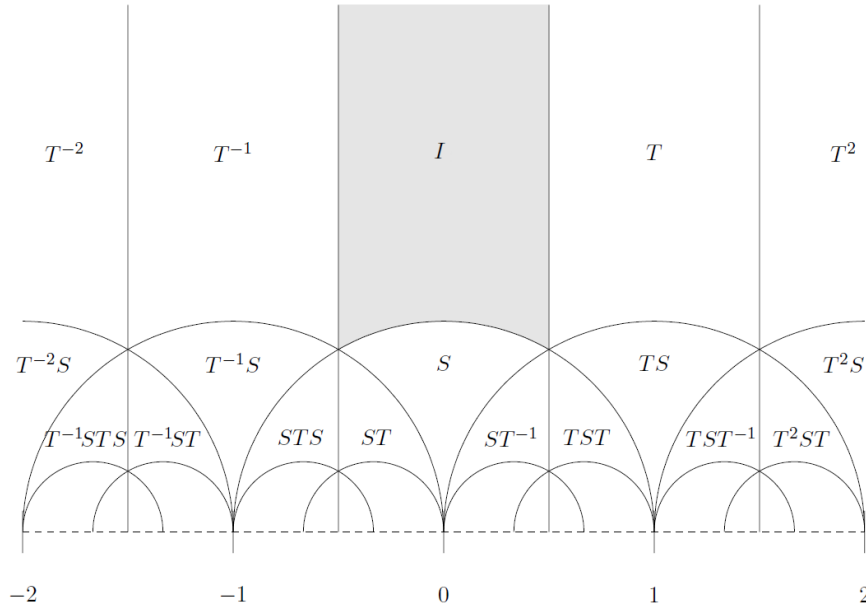


Figure 2: Translations of the fundamental domain \mathcal{F} .

2.2 Modular functions and modular forms

We will now recall some basic definitions from complex analysis. For details, we refer to [SS] and [FB].

Definition 2.6. Let $U \subset \mathbb{C}$ be an open subset of the complex numbers. A function $f : U \rightarrow \mathbb{C}$ is called **holomorphic** on U , if for all $z_0 \in U$ the limit

$$\lim_{h \rightarrow 0} \frac{f(z_0 + h) - f(z_0)}{h}$$

exists. If it exists, it is denoted by $f'(z_0)$. By $\mathcal{O}(U)$, we denote the set of all holomorphic functions on the open set U .

A basic fact from complex analysis is that holomorphic functions are also analytic. This means that if f is holomorphic on U , then for each $z_0 \in U$ there exists a $\epsilon > 0$, such that f can be written as a power series

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n,$$

for all $z \in U$ with $|z - z_0| < \epsilon$ and some $a_n \in \mathbb{C}$.

Definition 2.7. A function f is **meromorphic** on U , if there exists a discrete subset $P \subset U$ with

- i) f is holomorphic on $U \setminus P$.
- ii) f has poles at $p_j \in P$.

If f is meromorphic on U , then for each $p \in U$, there exists a unique integer $v_p(f) \in \mathbb{Z}$, a $\epsilon > 0$ and a non-vanishing holomorphic function g on the neighborhood $|z - p| < \epsilon$, such that

$$f(z) = (z - p)^{v_p(f)} g(z)$$

for all $0 < |z - p| < \epsilon$. The $v_p(f) \in \mathbb{Z}$ is called **the order of f at the point $p \in U$** and we have:

- i) If $v_p(f) < 0$ then f has a pole of order $|v_p(f)|$ at p .
- ii) If $v_p(f) = 0$ then f has no pole and no zero at p .
- iii) If $v_p(f) > 0$ then f has a zero of order $v_p(f)$ at p .

Equivalent to above condition is that f has a **Laurent expansion** in all $p \in U$ of the form

$$f(z) = \sum_{n=v_p(f)}^{\infty} a_n (z - p)^n,$$

for $0 < |z - p| < \epsilon$ and $a_n \in \mathbb{C}$ with $a_{v_p(f)} \neq 0$.

Example 2. i) The rational function $f(z) = \frac{z-2}{(z-1)(z+1)^2}$ is meromorphic on \mathbb{C} with $v_2(f) = 1$, $v_1(f) = -1$ and $v_{-1}(f) = -2$. Its Laurent expansion around $z = 1$ is given by

$$f(z) = -\frac{1}{4}(z-1)^{-1} + \frac{1}{2} - \frac{7}{16}(z-1) + \frac{5}{16}(z-1)^2 + \dots$$

ii) The function $e^{\frac{1}{z}}$ is holomorphic on $\mathbb{C} \setminus \{0\}$, but it is not meromorphic on \mathbb{C} , since it has an essential singularity at $z = 0$.

Definition 2.8. For a function $f : \mathbb{H} \rightarrow \mathbb{C}$ and a matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ we define the **slash operator of weight $k \in \mathbb{Z}$** by

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

This gives a right action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{O}(\mathbb{H})$ (Homework 1).

Definition 2.9. A meromorphic function $f : \mathbb{H} \rightarrow \mathbb{C}$ is called a **weakly modular function of weight** $k \in \mathbb{Z}$, if it satisfies

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau), \quad (2.3)$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and all $\tau \in \mathbb{H}$. In other words, if it is invariant under the slash operator, i.e., $f|_k \gamma = f$.

✂ ————— Until here in lecture 2 (21st April, 2023) ————— ✂

Remark 2.10. (i) Since $-I \in \mathrm{SL}_2(\mathbb{Z})$, a weakly modular function of weight k satisfies $f(\tau) = (-1)^k f(\tau)$. This shows that there are no non-trivial weakly modular functions of odd weight.

(ii) A weakly modular function f is uniquely determined by its values $f(\tau)$ for $\tau \in \mathcal{F}$.

If f is a weakly modular function of weight k , we have

$$\begin{aligned} f(\tau + 1) &= f(\tau), \\ f(-1/\tau) &= \tau^k f(\tau), \end{aligned} \quad (2.4)$$

by choosing the matrices T and S for (2.3). These two conditions are already sufficient for f to be a weakly modular function of weight k .

Proposition 2.11. A meromorphic function $f : \mathbb{H} \rightarrow \mathbb{C}$ which satisfies (2.4) is already a weakly modular function of weight k .

Proof. This is Homework 1, Exercise 2 (iv). □

Now consider the following holomorphic map from the upper half plane to the punctured unit disc

$$\begin{aligned} \mathbb{H} &\longrightarrow \mathbb{D}^* := \{z \in \mathbb{C} \mid 0 < |z| < 1\}, \\ \tau &\longmapsto q_\tau := e^{2\pi i \tau}. \end{aligned}$$

First notice that this is indeed a map from \mathbb{H} to \mathbb{D}^* , since if $\tau = x + iy$ then $q_\tau = e^{2\pi i \tau} = e^{-2\pi y} e^{2\pi x i}$, which lies in \mathbb{D}^* because of $y > 0$.

The equation $f(\tau + 1) = f(\tau)$ implies that f can be written in the form

$$f(\tau) = \tilde{f}(q_\tau),$$

where \tilde{f} is a meromorphic function on the punctured unit disc \mathbb{D}^* .

Definition 2.12. (i) A weakly modular function f is **meromorphic (resp. holomorphic) in ∞** , if the function \tilde{f} extends to a meromorphic (resp. holomorphic) function at 0.

(ii) The **order at ∞** of a meromorphic weakly modular function f is defined by $v_\infty(f) := v_0(\tilde{f})$.

Extending to a meromorphic (resp. holomorphic) function at 0, means that there exists a $N \in \mathbb{Z}$ (resp. $N \in \mathbb{Z}_{\geq 0}$) such that the Laurent expansion of \tilde{f} around 0 has the form

$$\tilde{f}(q) = \sum_{n=N}^{\infty} a_n q^n,$$

for some $a_n \in \mathbb{C}$. The smallest such N is given by $v_0(\tilde{f})$.

Definition 2.13. A weakly modular function (of weight k) f is called **modular function (of weight k)** if it is meromorphic at ∞ .

Definition 2.14. A holomorphic function $f : \mathbb{H} \rightarrow \mathbb{C}$ is called a **modular form of weight k** , if

- i) f is a modular function of weight k ,
- ii) f is holomorphic at ∞ .

By M_k , we denote the space of all modular forms of weight k .

In other words, modular forms of weight k are holomorphic functions $f : \mathbb{H} \rightarrow \mathbb{C}$, which satisfy (2.3) and which have a **Fourier expansion** of the form

$$f(\tau) = \sum_{n=0}^{\infty} a_n q_\tau^n$$

for some $a_n \in \mathbb{C}$, which are called the **Fourier coefficients** of f . By abuse of notation, we will, in the following, always write q instead of q_τ .

Definition 2.15. i) A modular form $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$ is called a **cusp form**, if $a_0 = 0$.

ii) By S_k we denote² the space of all cusp forms of weight k .

In other words, cusp forms are modular forms that vanish as $\tau \rightarrow i\infty$ or equivalently have order $v_\infty(f) > 0$ at infinity. We have the decomposition $M_k = \mathbb{C}E_k \oplus S_k$ (Homework 1, Exercise 3 (i)).

Example 3. i) For all $k \in \mathbb{Z}$ the function $f(\tau) = 0$ is a modular form of weight k .

ii) There are no non-trivial modular forms of odd weight.

iii) For all $c \in \mathbb{C}$ the constant function $f(\tau) = c$ is a modular form of weight 0.

Of course, other non-trivial examples of modular forms exist, as we will see in the next section.

2.3 Eisenstein series

In this section we will introduce Eisenstein series, which are one of the most important examples of modular forms. These already appeared in the first section as q -series. Here we will give their "correct" definition as a function in a complex variable $\tau \in \mathbb{H}$ and calculate their Fourier expansion. For this we will also need to recall the **Riemann zeta function**

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad (s \in \mathbb{C}, \operatorname{Re}(s) > 1)$$

which will give the constant term in the Fourier expansion of the Eisenstein series.

Proposition 2.16. For even $k \geq 4$ the **Eisenstein series of weight k** , defined by

$$G_k(\tau) = \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\tau + n)^k}, \quad (2.5)$$

is a modular form of weight k .

²"S" in S_k stands for the German word "Spitzenform" for cusp form.

Proof. First one can check that for $k > 2$ the above sum is absolutely convergent and uniformly convergent on compact subset (actually also on \mathcal{F}) of \mathbb{H} and therefore G_k is a holomorphic function on \mathbb{H} . For the proof of this fact we refer to the literature (see for example [Ki, Lemma 2.7] or [S, p. 82, Lemma 1]).

To check that G_k is holomorphic at infinity, we will show that $G_k(\tau)$ approaches an explicit finite limit as $\tau \rightarrow i\infty$. By the uniform convergence we can exchange summation and the limit and obtain

$$\lim_{\tau \rightarrow i\infty} G_k(\tau) = \frac{1}{2} \lim_{\tau \rightarrow i\infty} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\tau + n)^k} = \frac{1}{2} \sum_{0 \neq n \in \mathbb{Z}} \frac{1}{n^k} = \zeta(k).$$

Now we check the modularity conditions for G_k . For this it is important that the sum converges absolutely and therefore we are allowed to arrange the terms in any way. To show that $G_k(\tau+1) = G_k(\tau)$ we calculate

$$G_k(\tau+1) = \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m(\tau+1) + n)^k} = \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\tau + (m+n))^k}.$$

As (m, n) runs over $\mathbb{Z}^2 \setminus \{(0,0)\}$, so does $(m, m+n) = (m, n')$, so by the absolute convergence we get

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

Similarly, to show $G_k(-1/\tau) = \tau^k G_k(\tau)$ we derive

$$G_k(-1/\tau) = \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(-m/\tau + n)^k} = \tau^k \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(n\tau - m)^k} = \tau^k G_k(\tau),$$

since also $(n, -m)$ runs over $\mathbb{Z}^2 \setminus \{(0,0)\}$. □

We will now calculate the Fourier expansion of G_k for which we will need the following lemma.

Lemma 2.17. (*Lipschitz's formula*) For $k \geq 2$ and $\tau \in \mathbb{H}$ we have

$$\sum_{n \in \mathbb{Z}} \frac{1}{(\tau + n)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{d=1}^{\infty} d^{k-1} q^d. \quad (2.6)$$

Proof. (Sketch) This follows by differentiating the following two expression of the cotangent $k-1$ -times

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

See for example [Z, Proposition 5] for more details. □

Proposition 2.18 (Fourier expansion of G_k). For even $k \geq 4$ the Fourier expansion of G_k is given by

$$G_k(\tau) = \zeta(k) + \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \quad (2.7)$$

Proof. Again we use the absolute convergence which allows the following rearrangements

$$\begin{aligned} G_k(\tau) &= \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\tau + n)^k} \stackrel{k \text{ even}}{=} \frac{1}{2} \sum_{0 \neq n \in \mathbb{Z}} \frac{1}{n^k} + \sum_{m=1}^{\infty} \sum_{n \in \mathbb{Z}} \frac{1}{(m\tau + n)^k} \\ &\stackrel{(2.6)}{=} \zeta(k) + \frac{(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \sum_{d=1}^{\infty} d^{k-1} q^{md} = \zeta(k) + \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \end{aligned}$$

□

In the definition of G_k we needed $k > 2$ to assure absolute convergence. But the q -series in (2.7) also makes sense³ for $k = 2$ and also defines a holomorphic function in $\tau \in \mathbb{H}$. We therefore use this equation to define the **Eisenstein series of weight 2** by

$$G_2(\tau) := \zeta(2) + (2\pi i)^2 \sum_{n=1}^{\infty} \sigma_1(n) q^n. \quad (2.8)$$

This is not a modular form anymore, but plays an important role in the theory of modular forms. We have the following Proposition which gives the failure of G_2 to be a modular form.

Proposition 2.19 (Modular transformation of G_2). *For $\tau \in \mathbb{H}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we have*

$$G_2\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 G_2(\tau) - \pi ic(c\tau + d). \quad (2.9)$$

☞ ————— Until here in lecture 3 (28th April, 2023) ————— ☞

Proof. We will just sketch the idea of this proof. For details see for example [Z, Proposition 6] or [Ko, Chapter III, Proposition 7]. The sum (2.5) does not converge absolutely for $k = 2$, but it does for $k > 2$. We now use what is called Hecke's trick and consider for $\epsilon > 0$ the function

$$G_{2,\epsilon}(\tau) = \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m\tau + n)^2 |m\tau + n|^{2\epsilon}}. \quad (2.10)$$

This sum does converge absolutely and we can use the same argument as before to see that for $\epsilon > 0$

$$G_{2,\epsilon}\left(\frac{a\tau + b}{c\tau + d}\right) = (cz + d)^2 |cz + d|^{2\epsilon} G_{2,\epsilon}(\tau). \quad (2.11)$$

One then shows that the limit $\epsilon \rightarrow 0$ of $G_{2,\epsilon}$ exists and equals $G_2(\tau) - \frac{\pi}{2\mathrm{Im}(\tau)}$. Taking the limit $\epsilon \rightarrow 0$ in (2.11) then proves the statement. □

We will later see that (2.19) means that G_2 is a **quasimodular form**.

Proposition 2.20 (L. Euler (1735)). *For even $k \geq 2$ we have*

$$\zeta(k) = -\frac{B_k (2\pi i)^k}{2k (k-1)!},$$

where B_k denotes the k -th Bernoulli number defined in (1.6).

³The q -series (2.7) actually makes for any $k \geq 2$, but for odd k these are not modular forms.

Proof. See for example [FB, Proposition III.7.14]. □

We get the following values of $\zeta(k)$ for $k = 2, 4, 6, 8, 10, 12$:

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}, \quad \zeta(8) = \frac{\pi^8}{9450}, \quad \zeta(10) = \frac{\pi^{10}}{93555}, \quad \zeta(12) = \frac{691\pi^{12}}{638512875}.$$

Using Proposition 2.20 we define for even $k \geq 2$ the **normalized Eisenstein series** by

$$E_k(\tau) = \frac{1}{\zeta(k)} G_k(\tau) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \quad (2.12)$$

These are the q -series which also appeared in (1.7).

2.4 Cusp forms and the discriminant function Δ

In this section, we will consider cusp forms, which are modular forms vanishing at the "cusps". By cusps, one usually denotes the classes of $\mathbb{Q} \cap \{\infty\}$ modulo the action of a subgroup of $SL_2(\mathbb{Z})$. For the level one case, where we consider the whole group $SL_2(\mathbb{Z})$, we have $|SL_2(\mathbb{Z}) \backslash (\mathbb{Q} \cap \{\infty\})| = 1$, because every rational number can be sent to ∞ by a linear fractional transformation. This means there is just one cusp. A cusp form of level one is, therefore, a modular form which vanishes at ∞i or, equivalently, has a vanishing constant term in its Fourier expansion.

Definition 2.21. We define the **discriminant function** Δ by ($q = e^{2\pi i\tau}$)

$$\Delta(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}. \quad (2.13)$$

The function $\tau(n)$ defined by $\Delta(\tau) = \sum_{n=1}^{\infty} \tau(n) q^n$ is called **Ramanujan tau function**.

Expanding the product in the definition of Δ gives the following first values for $\tau(n)$

$$\Delta(\tau) = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + 84480q^8 - 113643q^9 + \dots \quad (2.14)$$

Remark 2.22. i) Ramanujan observed in 1915 that $\tau(n)$ is multiplicative, i.e. $\tau(m \cdot n) = \tau(m) \cdot \tau(n)$ for coprime $m, n \in \mathbb{Z}_{\geq 1}$. For example $\tau(6) = -6048 = -24 \cdot 252 = \tau(2) \cdot \tau(3)$. This was proved by Mordell the next year and later generalized by Hecke to the theory of **Hecke operators**, which we will discuss later. The function Δ is an example of a **Hecke eigenform** (meaning it is an eigenvector for all Hecke operators having 1 as the coefficient of q), which all satisfy the property that their Fourier coefficients are multiplicative. The divisor-sums $\sigma_{k-1}(n)$ are also multiplicative and the Eisenstein series, after some normalization, are also examples of Hecke eigenforms.

ii) Lehmer (1947) conjectured that $\tau(n) \neq 0$ for all $n \geq 1$, an assertion sometimes known as Lehmer's conjecture. This conjecture is still unproven but checked for all $1 \leq n \leq 816212624008487344127999$ (due to Derickx, van Hoeij, and Zeng in 2013).

Since $|e^{2\pi i\tau}| < 1$ for $\tau \in \mathbb{H}$, the terms of the infinite product (2.13) are all non-zero and tend exponentially rapidly to 1, so Δ gives a holomorphic and everywhere non-zero function on \mathbb{H} . It gives the first example of a non-trivial cusp form.

Proposition 2.23. The function $\Delta(\tau)$ is a cusp form of weight 12.

Proof. Since $\Delta(\tau) \neq 0$, we can consider its logarithmic derivative. We find

$$\frac{1}{2\pi i} \frac{d}{d\tau} \log \Delta(\tau) = \frac{1}{2\pi i} \frac{d}{d\tau} \log \left(q \prod_{n=1}^{\infty} (1 - q^n)^{24} \right) = \frac{1}{2\pi i} \frac{d}{d\tau} \left(\log(q) + 24 \sum_{n=1}^{\infty} \log(1 - q^n) \right).$$

Since $q = e^{2\pi i \tau}$ we have $\frac{1}{2\pi i} \frac{d}{d\tau} = q \frac{d}{dq}$ and therefore

$$\frac{1}{2\pi i} \frac{d}{d\tau} \log \Delta(\tau) = 1 - 24 \sum_{n=1}^{\infty} n \frac{q^n}{1 - q^n} = 1 - 24 \sum_{n=1}^{\infty} n \sum_{d=1}^{\infty} q^{dn} = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n = E_2(\tau). \quad (2.15)$$

By Proposition 2.19 and $E_2(\tau) = \frac{6}{\pi^2} G_2(\tau)$ we have

$$E_2 \left(\frac{a\tau + b}{c\tau + d} \right) = (c\tau + d)^2 E_2(\tau) - \frac{6}{\pi} ic(c\tau + d). \quad (2.16)$$

Combining (2.15), (2.16) and using

$$\frac{d}{d\tau} \left(\frac{a\tau + b}{c\tau + d} \right) = \frac{ad - bc}{(c\tau + d)^2} = \frac{1}{(c\tau + d)^2}$$

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

$$\frac{1}{2\pi i} \frac{d}{d\tau} \log \left(\frac{\Delta \left(\frac{a\tau + b}{c\tau + d} \right)}{(c\tau + d)^{12} \Delta(\tau)} \right) = \frac{1}{(c\tau + d)^2} E_2 \left(\frac{a\tau + b}{c\tau + d} \right) - \frac{12}{2\pi i} \frac{c}{c\tau + d} - E_2(\tau) = 0.$$

In other words, $(\Delta|_{12}\gamma)(\tau) = C(\gamma)\Delta(\tau)$ for all $\tau \in \mathbb{H}$ and all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, where $C(\gamma)$ is a non-zero complex number depending only on γ . We want to show that $C(\gamma) = 1$ for all γ .

The slash operator $|_k$ gives a right action of $\mathrm{SL}_2(\mathbb{Z})$ on \mathbb{H} , i.e. for γ_1, γ_2 we get

$$C(\gamma_1)C(\gamma_2)\Delta = C(\gamma_1)\Delta|_{12}\gamma_2 = \Delta|_{12}(\gamma_1)|_{12}\gamma_2 = \Delta|_{12}(\gamma_1\gamma_2) = C(\gamma_1\gamma_2)\Delta.$$

Therefore $C : \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathbb{C}$ is a homomorphism and we just need to prove $C(T) = C(S) = 1$. By definition we have $\Delta(T(\tau)) = \Delta(\tau)$, since it is defined by a q -series, which gives $C(T) = 1$. To show $C(S) = 1$, we set $\tau = i$ in $\tau^{-12}\Delta(-\frac{1}{\tau}) = (\Delta|_{12}S)(\tau) = C(S)\Delta(\tau)$. \square

Remark 2.24. Since E_4^3 and Δ are modular forms of weight 12 and $\Delta(\tau) \neq 0$ for $\tau \in \mathbb{H}$, the **modular invariant** (or j -invariant), defined by

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

is a holomorphic function in \mathbb{H} satisfying $j(\gamma(\tau)) = j(\tau)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Since Δ has a zero of order 1 at ∞ and E_4 does not vanish there, the function j has a pole of order 1 at ∞ . Therefore j is a modular function of weight 0, which is not a modular form. Its Fourier expansion, the Laurent expansion at $q = 0$ of \tilde{j} , starts with

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + \dots$$

These Fourier coefficients, for the positive exponents of q , are the dimensions of the graded part of an infinite-dimensional graded algebra representation of the so called monster group.

2.5 Structure of the space of modular forms

We now come to a very important technical result about modular forms. To state and prove this result, we will use some definitions and results from complex analysis that can be found again in [FB] or [SS]. Especially the notion of contour integration will be necessary, which can be found in [SS, Section 1.3] or [FB, Chapter 2].

Proposition 2.25 (Argument principle). *If f is a meromorphic function inside and on some closed contour \mathcal{C} with interior $D \subset \mathbb{C}$, and f has no zeros or poles on \mathcal{C} , then*

$$\frac{1}{2\pi i} \int_{\mathcal{C}} \frac{f'(z)}{f(z)} dz = \sum_{p \in D} v_p(f).$$

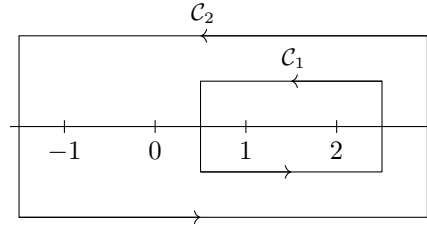
Proof. See for example [FB, Proposition III.7.4]. □

Example 4. *We again consider the rational function $f(z) = \frac{z-2}{(z-1)(z+1)^2}$, which is meromorphic on \mathbb{C} with $v_2(f) = 1, v_1(f) = -1, v_{-1}(f) = -2$ and $v_p(f) = 0$ for $p \in \mathbb{C} \setminus \{-1, 1, 2\}$.*

With the two contours \mathcal{C}_1 and \mathcal{C}_2 shown on the right, we get for example

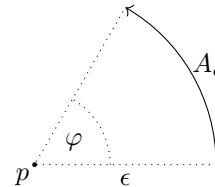
$$\frac{1}{2\pi i} \int_{\mathcal{C}_1} \frac{f'(z)}{f(z)} dz = v_1(f) + v_2(f) = 0,$$

$$\frac{1}{2\pi i} \int_{\mathcal{C}_2} \frac{f'(z)}{f(z)} dz = v_{-1}(f) + v_1(f) + v_2(f) = -2.$$



Lemma 2.26. (Integration over arcs) *Let f be a meromorphic function on some open set $U \subset \mathbb{C}$. For an arc $A_\epsilon \subset U$ of radius $\epsilon > 0$, center $p \in U$, angle φ not intersecting any zeros or poles of f , we have*

$$\lim_{\epsilon \rightarrow 0} \frac{1}{2\pi i} \int_{A_\epsilon} \frac{f'(z)}{f(z)} dz = \frac{\varphi}{2\pi} v_p(f).$$



Proof. See for example part (4) in the proof of [FB, Theorem VI.2.3]. □

Lemma 2.27. *Let f be a modular function of weight k with no zeros or poles on a (not necessarily closed) contour $\mathcal{C} \subset \mathbb{H}$. Then*

$$\int_{\mathcal{C}} \frac{f'(\tau)}{f(\tau)} d\tau - \int_{\gamma(\mathcal{C})} \frac{f'(\tau)}{f(\tau)} d\tau = -k \int_{\mathcal{C}} \frac{c}{c\tau + d} d\tau$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

Proof. Differentiating $f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$ gives

$$f'(\gamma(\tau)) \frac{d(\gamma(\tau))}{d\tau} = (c\tau + d)^k f'(\tau) + kc(c\tau + d)^{k-1} f(\tau).$$

Dividing the left-hand side by $f(\gamma(\tau))$ and the right-hand side by $(c\tau + d)^k f(\tau)$ leads to

$$\frac{f'(\gamma(\tau))}{f(\gamma(\tau))} d(\gamma(\tau)) = \frac{f'(\tau)}{f(\tau)} d\tau + k \frac{c}{c\tau + d} d\tau$$

and therefore

$$\int_C \left(\frac{f'(\tau)}{f(\tau)} d\tau - \frac{f'(\gamma(\tau))}{f(\gamma(\tau))} d(\gamma(\tau)) \right) = -k \int_C \frac{c}{c\tau + d} d\tau.$$

□

Example 5. For $\gamma = S$ Lemma 2.27 gives for a modular function f of weight k

$$\int_C \frac{f'(\tau)}{f(\tau)} d\tau - \int_{S(C)} \frac{f'(\tau)}{f(\tau)} d\tau = -k \int_C \frac{1}{\tau} d\tau. \tag{2.17}$$

Since the factor $(c\tau + d)^k$ does not vanish for $\tau \in \mathbb{H}$ and $c, d \in \mathbb{Z}$, we have $v_p(f) = v_{\gamma(p)}(f)$ for $\gamma \in SL_2(\mathbb{Z})$ and a modular function f . The following theorem gives a restriction on the orders of a modular functions, which will be crucial to describe the space M_k afterwards.

Theorem 2.28 (Valence formula). For a non-zero modular function f of weight k we have

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\omega(f) + \sum_{\substack{p \in SL_2(\mathbb{Z}) \backslash \mathbb{H} \\ p \neq i, \omega}} v_p(f) = \frac{k}{12}. \tag{2.18}$$

✂ ————— Until here in lecture 4 (12th May, 2023) ————— ✂

Proof. The idea of the proof is to count the (order) of the zeros and poles in $SL_2(\mathbb{Z}) \backslash \mathbb{H}$ by integrating the logarithmic derivative f'/f of f around the boundary of the fundamental domain \mathcal{F} and then applying the argument principle.

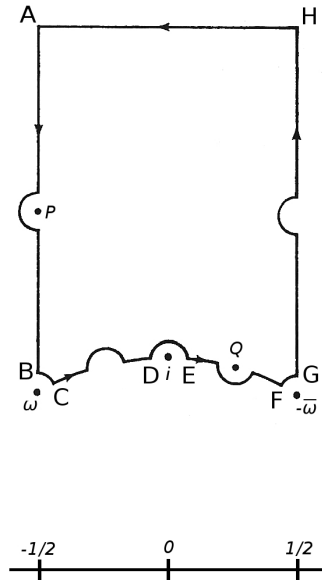


Figure 3: The contour \mathcal{C} .

More precisely, we need an approximation first and start with a curve as shown in Figure 3. The contour \mathcal{C} is chosen in such a way that it contains exactly one represent in $SL_2(\mathbb{Z}) \backslash \mathbb{H}$ of each pole and zero, except i, ω (and $-\bar{\omega} = S(\omega)$) which are kept outside.

Since f is a modular functions, it is meromorphic at ∞ . This means that for some $T \in \mathbb{R}$ the function f has no poles or zeros with imaginary part larger than T . Therefore we can choose the the top line from $H = \frac{1}{2} + iT$ to $A = -\frac{1}{2} + iT$ such that f does not have any poles or zeros on or on top of the line HA .

The rest of the contour follows the boundary of \mathcal{F} with a few exceptions: For each zero or pole $P \neq i, \omega$ on the boundary, we simply circle around it with a small enough radius and the other way round for the congruent point on the other side of the boundary (this way we will only count the point once). This procedure is illustrated for two such points P and Q in Figure 3.

So far we still followed the boundary of \mathcal{F} (modulo $SL_2(\mathbb{Z})$) but since we don't want to include i and ω we also have to circle around those points with a small enough radius ϵ (and the same way for $-\bar{\omega} = S(\omega)$).

By the argument principle (Proposition 2.25) we obtain

$$\frac{1}{2\pi i} \int_{\mathcal{C}} \frac{f'(\tau)}{f(\tau)} d\tau = \sum_{\substack{p \in SL_2(\mathbb{Z}) \backslash \mathbb{H} \\ p \neq i, \omega}} v_p(f). \quad (2.19)$$

On the other hand we can evaluate the contour integral over \mathcal{C} on the left-hand side section by section:

- i) AB and GH : The integral from A to B cancels the integral from G to H , because $f(\tau+1) = f(\tau)$, and the lines go in opposite direction, i.e.

$$\frac{1}{2\pi i} \left(\int_A^B + \int_G^H \right) \frac{f'(\tau)}{f(\tau)} d\tau = 0.$$

- ii) HA : By the map $q = e^{2\pi i \tau}$ the line from H to A gets send to a circle in the unit disc of radius $e^{-2\pi T}$ running clockwise around 0. Recall that $f(\tau) = \tilde{f}(q)$ and therefore we have $\frac{f'(\tau)}{f(\tau)} d\tau = \frac{\tilde{f}'(q)}{\tilde{f}(q)} dq$. By the argument principle we get

$$\frac{1}{2\pi i} \int_H^A \frac{f'(\tau)}{f(\tau)} d\tau = \frac{1}{2\pi i} \int_{|q|=e^{-2\pi T}} \frac{\tilde{f}'(q)}{\tilde{f}(q)} dq = -v_0(\tilde{f}) = -v_\infty(f).$$

Here the minus sign comes from the fact that the contour integral runs clockwise around 0.

- iii) BC , DE and FG : All these three sections are small arcs of a small radius ϵ which approach angles $\frac{\pi}{3}$, π and $\frac{\pi}{3}$ as $\epsilon \rightarrow 0$. Using Lemma 2.26 and noticing that all three arcs run clockwise (minus sign), we obtain

$$\begin{aligned} \lim_{\epsilon \rightarrow 0} \frac{1}{2\pi i} \left(\int_B^C + \int_D^E + \int_F^G \right) \frac{f'(\tau)}{f(\tau)} d\tau &= -\frac{1}{2\pi} \left(\frac{\pi}{3} v_\omega(f) + \pi v_i(f) + \frac{\pi}{3} v_{-\bar{\omega}}(f) \right) \\ &= -\frac{1}{2} v_i(f) - \frac{1}{3} v_\omega(f), \end{aligned}$$

where we used $v_{-\bar{\omega}}(f) = v_{S(\omega)}(f) = v_\omega(f)$ in the last equation.

- iv) CD and EF : First notice that the transformation $S(\tau) = -\frac{1}{\tau}$ sends the contour CD to the contour EF , but with directions reversed. By (2.17) we therefore have

$$\frac{1}{2\pi i} \left(\int_C^D \frac{f'(\tau)}{f(\tau)} d\tau + \int_E^F \frac{f'(\tau)}{f(\tau)} d\tau \right) = -\frac{k}{2\pi i} \int_C^D \frac{1}{\tau} d\tau.$$

Sending $\epsilon \rightarrow 0$, the integral on the right-hand side is just an integral over an arc from ω to i :

$$\lim_{\epsilon \rightarrow 0} -\frac{k}{2\pi i} \int_C \frac{1}{\tau} d\tau = -\frac{k}{2\pi i} \int_{\text{arc from } \omega \text{ to } i} \frac{1}{\tau} d\tau \stackrel{\tau = e^{\Theta i}}{=} -\frac{k}{2\pi} \int_{\frac{2\pi}{3}}^{\frac{\pi}{2}} d\Theta = \frac{k}{2\pi} \left(\frac{2\pi}{3} - \frac{\pi}{2} \right) = \frac{k}{12}$$

and therefore we obtain

$$\frac{1}{2\pi i} \left(\int_C^D + \int_E^F \right) \frac{f'(\tau)}{f(\tau)} d\tau = \frac{k}{12}.$$

Combining the parts i) - iv) and plugging them into the left-hand side of (2.19) finishes the proof. \square

Recall that the difference between a modular function and a modular form is, that a modular form is holomorphic on \mathbb{H} and at ∞ . This means that for $f \in M_k$ all the numbers in (2.18) are positive and therefore for a fixed k there are just finitely many solutions. This leads to the following proposition.

Proposition 2.29. *Let $k \in \mathbb{Z}$ be an integer. Then*

- i) $M_0 = \mathbb{C}$,
- ii) If $k = 2$, $k < 0$ or if k is odd then $M_k = 0$.
- iii) If $k \in \{4, 6, 8, 10, 14\}$, then $M_k = \mathbb{C}E_k$.
- iv) If $k < 12$ or $k = 14$ then $S_k = 0$.
- v) $S_{12} = \mathbb{C}\Delta$ and if $k > 12$ then $S_k = \Delta \cdot M_{k-12}$.
- vi) If $k \geq 4$ then $M_k = \mathbb{C}E_k \oplus S_k$.

Proof. i) We know that the constant functions are elements in M_0 and we want to show the reverse. Let $f \in M_0$ be an arbitrary modular form of weight 0 and let $c \in \mathbb{C}$ be any element in the image of f . Then $f(z) - c \in M_0$ has a zero in \mathbb{H} , i.e. one of the terms in (2.18) is strictly positive. Since the right-hand side is 0, this can only happen if $f(z) - c$ is the zero function, i.e. f is constant.

- ii) We already saw that $M_k = 0$ if k is odd. If $k = 2$ or $k < 0$ then the right-hand side of (2.18) is negative or $\frac{1}{6}$, which has no positive solutions on the left-hand side.
- iii) When $k \in \{4, 6, 8, 10, 14\}$, then there is only one possible way of choosing the $v_p(f)$, such that (2.18) holds:

$$k = 4 : v_\omega(f) = 1 \text{ and all other } v_p(f) = 0.$$

$$k = 6 : v_i(f) = 1 \text{ and all other } v_p(f) = 0.$$

$$k = 8 : v_\omega(f) = 2 \text{ and all other } v_p(f) = 0.$$

$$k = 10 : v_\omega(f) = v_i(f) = 1 \text{ and all other } v_p(f) = 0.$$

$$k = 14 : v_\omega(f) = 2, v_i(f) = 1 \text{ and all other } v_p(f) = 0.$$

For such k two arbitrary modular forms $f_1, f_2 \in M_k$ have the same order at all points, i.e. $\frac{f_1}{f_2}$ is a modular form of weight 0, which by i) must be constant. Therefore f_1 and f_2 are proportional and since $E_k \in M_k$ the statement follows.

- iv) If $f \in S_k$ we have $v_\infty(f) > 0$, which is not possible in (2.18) for $k < 12$ or $k = 14$.
- v) We know that $v_\infty(\Delta) = 1$ and by (2.18) this can be the only zero of Δ . Therefore for any $f \in S_k$ the function $\frac{f}{\Delta}$ is a modular form of weight $k - 12$.

vi) This was part of Homework 1. □

Theorem 2.30. (*Dimension formula*) For an even positive integer k we have

$$\dim_{\mathbb{C}} M_k = \begin{cases} \lfloor \frac{k}{12} \rfloor + 1 & , \quad k \not\equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor & , \quad k \equiv 2 \pmod{12} \end{cases} \quad (2.20)$$

Proof. This will now follow by induction on k from the results in Proposition 2.29. For $k < 12$ the above dimension formula is already proven. Combing the results of Proposition 2.29 we have

$$M_{k+12} = \mathbb{C}E_{k+12} \oplus \Delta \cdot M_k$$

and since $\lfloor \frac{k}{12} \rfloor + 1 = \lfloor \frac{k+12}{12} \rfloor$ the statement follows inductively. □

k	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36
$\dim_{\mathbb{C}} M_k$	1	0	1	1	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4

Figure 4: Dimension of M_k for even $0 \leq k \leq 36$.

Completion of the modular proof of Theorem 1.4. Both E_4^2 and E_8 are modular forms of weight 8. Since $\dim_{\mathbb{C}} M_8 = 1$ there must exist a $c \in \mathbb{C}$ with $E_4^2 = cE_8$. But since both have 1 as the constant term in their Fourier expansion we deduce $c = 1$. □

Both E_4^3 and E_6^2 are modular forms of weight 12 having 1 as the constant term in their Fourier expansion and therefore $E_4^3 - E_6^2 \in S_{12}$. By Proposition 2.29 v) this has to be a multiple of Δ and comparing the first few Fourier coefficients gives

$$\Delta(\tau) = \frac{E_4(\tau)^3 - E_6(\tau)^2}{1728}. \quad (2.21)$$

In general every modular form can be written (uniquely) as a polynomial in E_4 and E_6 :

Proposition 2.31. For $k \geq 0$, the set $\{E_4^a E_6^b \mid a, b \geq 0, 4a + 6b = k\}$ is a basis of the space M_k .

✎ ————— Until here in lecture 5 (19th May, 2023) ————— ✎

Proof. We first check that the mentioned set has the correct size. Let N_k be the number of solutions to $4a + 6b = k$ in nonnegative integers a and b . For $k \leq 12$ one can check directly that $N_k = \dim_{\mathbb{C}} M_k$ (given in (2.20)) and for $k \geq 12$ one can check that $N_k = N_{k-12} + 1$. Therefore we have $N_k = \dim_{\mathbb{C}} M_k$ for all k . It remains to show that the set is linearly independent. Suppose we have a relation of the form

$$\sum_{\substack{4a+6b=k \\ a,b \geq 0}} \lambda_{a,b} E_4(\tau)^a E_6(\tau)^b = 0$$

for all $\tau \in \mathbb{H}$. If there is a pure E_4 term, say $\lambda_{a,0} E_4(\tau)^a$, then setting $\tau = i$ shows $\lambda_{a,0} E_4(i)^a = 0$ since $E_6(i) = 0$ (Homework 1). Since $E_4(i) \neq 0$ (which follows from the valence formula (2.18)) we deduce $\lambda_{a,0} = 0$. Therefore all nonzero terms in the sum have $b \geq 1$. As E_6 is not identically 0, we can divide by it and get

$$\sum_{\substack{4a+6b=k \\ a,b \geq 0}} \lambda_{a,b} E_4(\tau)^a E_6(\tau)^{b-1} = 0,$$

which is a linear relation in weight $k - 6$. By induction we see that the remaining coefficients are 0. \square

Remark 2.32. Starting with a modular form $f = \sum_{n=0}^{\infty} a_n q^n \in M_k$ and choosing a and b with $4a + 6b = k$, we have $f - a_0 E_4^a E_6^b \in S_k$. By Proposition 2.29 v) we have $S_k = \Delta \cdot M_{k-12}$, i.e. we find a $g \in M_{k-12}$ with $f = a_0 E_4^a E_6^b + \Delta \cdot g$. With the explicit expression (2.21) of Δ , this gives a recursive algorithm (and in fact another way of proving Proposition 2.31) to write f as a polynomial in E_4 and E_6 .

Proposition 2.33. *Modular forms with different weights are linearly independent over \mathbb{C} .*

Proof. Suppose we have nonzero modular forms f_1, f_2, \dots, f_m with respective weights $k_1 < k_2 < \dots < k_m$, such that they admit a nontrivial linear relation

$$\alpha_1 f_1(\tau) + \alpha_2 f_2(\tau) + \dots + \alpha_m f_m(\tau) = 0 \quad (2.22)$$

for all $\tau \in \mathbb{H}$ and $\alpha_j \neq 0$ for $j = 1, \dots, m$. Replacing τ by $S(\tau)$ and using the modularity, i.e. $f_j(S(\tau)) = \tau^{k_j} f_j(\tau)$, we obtain

$$\alpha_1 \tau^{k_1} f_1(\tau) + \alpha_2 \tau^{k_2} f_2(\tau) + \dots + \alpha_m \tau^{k_m} f_m(\tau) = 0$$

for all $\tau \in \mathbb{H}$. With Fourier expansions $f_j(\tau) = \sum_{n=0}^{\infty} a_n^{(j)} q^n$ where $q = e^{2\pi i \tau}$, this is equivalent to

$$\sum_{n=0}^{\infty} \left(\alpha_1 \tau^{k_1} a_n^{(1)} + \alpha_2 \tau^{k_2} a_n^{(2)} + \dots + \alpha_m \tau^{k_m} a_n^{(m)} \right) e^{2\pi i n \tau} = 0.$$

Now consider the case of $\tau = iy$ ($y > 0$) being on the positive imaginary axis, then

$$\sum_{n=0}^{\infty} \left(\alpha_1 (iy)^{k_1} a_n^{(1)} + \alpha_2 (iy)^{k_2} a_n^{(2)} + \dots + \alpha_m (iy)^{k_m} a_n^{(m)} \right) e^{-2\pi n y} = 0. \quad (2.23)$$

For $n > 0$ and any $r \geq 0$ we have $\lim_{y \rightarrow \infty} y^r e^{-2\pi n y} = 0$. Now let N be the smallest integer, such that at least for one $1 \leq j \leq m$ we have $a_N^{(j)} \neq 0$. Dividing (2.23) by $e^{-2\pi N y}$ and taking the limit $y \rightarrow \infty$ we obtain

$$\lim_{y \rightarrow \infty} \alpha_1 (iy)^{k_1} a_N^{(1)} + \alpha_2 (iy)^{k_2} a_N^{(2)} + \dots + \alpha_m (iy)^{k_m} a_N^{(m)} = 0.$$

But the left-hand side of this equation is the limit $y \rightarrow \infty$ of a non-constant polynomial in y , which can not be zero and therefore a relation of the form (2.22) can not exist. \square

Proposition 2.34. *The modular forms E_4 and E_6 are algebraically independent over \mathbb{C} .*

Proof. Let $P \in \mathbb{C}[X, Y]$ be with $P(E_4(\tau), E_6(\tau)) = 0$ for all $\tau \in \mathbb{H}$. By Proposition 2.33 we can reduce this to the case where $P(E_4, E_6)$ is a sum of modular forms of the same weight k . But by Proposition 2.31 we know that $E_4^a E_6^b$ with $4a + 6b = k$ are linearly independent and therefore we conclude $P = 0$. \square

Summarizing all the results we get the following description of the space of modular forms.

Corollary 2.35. *Let M denote the space of all modular forms (of level 1), then we have*

$$M = \bigoplus_{k=0}^{\infty} M_k = \mathbb{C}[E_4, E_6] \cong \mathbb{C}[X, Y],$$

i.e. M is a graded \mathbb{C} -algebra, which is isomorphic to the polynomial ring in two variables.

Finally, we give another consequence of the valence formula (2.18). The following statement can be used to determine if two modular forms of a given weight k are the same if they have the same first $\frac{k}{12}$ Fourier coefficients.

Corollary 2.36 (Sturm bound). *Let $f, g \in M_k$ be two modular forms of weight k with Fourier expansions $f(\tau) = \sum_{n \geq 0} a_n q^n$ and $g(\tau) = \sum_{n \geq 0} b_n q^n$. If $a_n = b_n$ for $0 \leq n < \frac{k}{12} + 1$ then $f = g$.*

Proof. If we set $h = f - g$ then $h \in M_k$ and $v_\infty(h) > \frac{k}{12}$ since $h(\tau) = \sum_{n \geq \frac{k}{12} + 1} (a_n - b_n) q^n$. By the valence formula (2.18) this is just possible if h is the zero function and therefore $f = g$. \square

3 Modular forms for congruence subgroups

In this course, we just considered modular forms of level 1. We want to consider higher level modular forms or more precisely modular forms for congruence subgroups. A complete discussion of modular forms for higher level can be found for example in [DS]. So far we always required that a modular form (or (weakly-)modular function) satisfies $f|_k \gamma = f$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. This condition will be weakened now and we will just require it for $\gamma \in \Gamma$, where $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ are certain subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

3.1 Congruence subgroups

Definition 3.1. *i) For $N \in \mathbb{Z}_{\geq 1}$ we define the following subgroups of $\mathrm{SL}_2(\mathbb{Z})$*

$$\begin{aligned}\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}, \\ \Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid a \equiv d \equiv 1 \pmod{N} \right\}, \\ \Gamma(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) \mid b \equiv 0 \pmod{N} \right\}.\end{aligned}$$

By definition we have the inclusions

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

*ii) A subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is called **congruence subgroup** if there exists a N with $\Gamma(N) \subset \Gamma$. The smallest such N is called the **level of Γ** .*

We have $\Gamma(1) = \Gamma_1(1) = \Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$ and hence $\mathrm{SL}_2(\mathbb{Z})$ is the only congruence subgroup of level 1. The congruence subgroups all have finite index, which can be computed explicitly:

Proposition 3.2. *For $N \geq 1$ we have*

$$\begin{aligned}[\Gamma_1(N) : \Gamma(N)] &= N, \\ [\Gamma_0(N) : \Gamma_1(N)] &= N \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right), \\ [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] &= N \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right).\end{aligned}$$

Proof. The last formula is part of Homework 2. \square

For example we have $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(2)] = 2 \left(1 + \frac{1}{2}\right) = 3$. As before we can define weakly modular functions for Γ :

Modular forms and their combinatorial variants - Modular forms for congruence subgroups

Definition 3.3. Let Γ be a congruence subgroup. A meromorphic function $f : \mathbb{H} \rightarrow \mathbb{C}$ is a **weakly modular function** of weight $k \in \mathbb{Z}$ for Γ , if $f|_{\gamma} = f$ for all $\gamma \in \Gamma$.

Again we could give the definition for a fundamental domain for Γ , which is just the same as before by replacing $\mathrm{SL}_2(\mathbb{Z})$ by Γ . These are given by $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ -many translates of \mathcal{F} :

Proposition 3.4. Let Γ be a congruence subgroup written as a disjoint union of cosets as

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i=1}^n \alpha_i \Gamma.$$

Then $\mathcal{G} = \bigcup_{i=1}^n \alpha_i^{-1} \mathcal{F}$ is a fundamental domain for Γ .

Proof. We will just give the argument why any point $\tau \in \mathbb{H}$ is Γ -equivalent to a point in \mathcal{G} . Since \mathcal{F} is a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ we can find a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma.\tau \in \mathcal{F}$. By the above decomposition we also have $\gamma = \alpha_i \gamma'$ for some $1 \leq i \leq n$ and $\gamma' \in \Gamma$. Therefore we get that $\gamma'.\tau \in \alpha_i^{-1} \mathcal{F} \subset \mathcal{G}$. \square

For example, one can check that

$$\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(2) \cup S\Gamma_0(2) \cup (ST)^{-1}\Gamma_0(2),$$

which gives the following fundamental domain for $\Gamma_0(2)$:

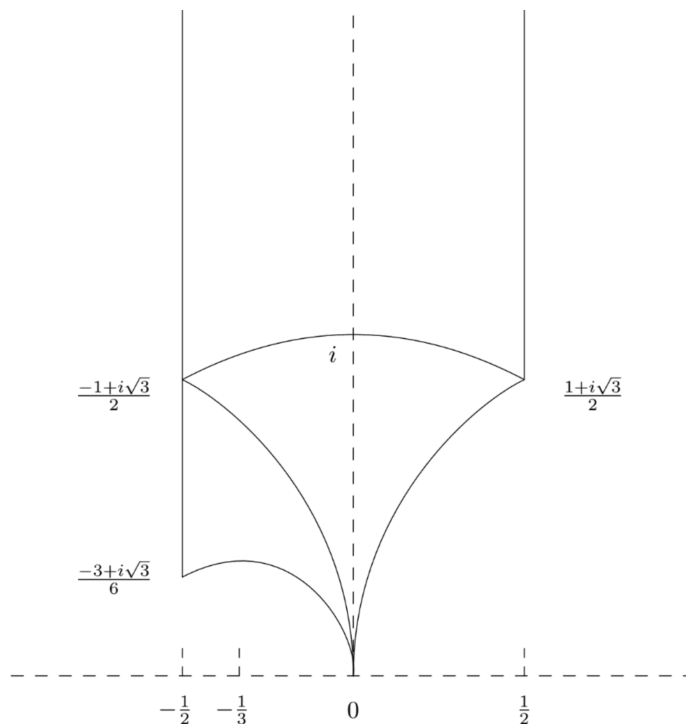


Figure 5: A fundamental domain of $\Gamma_0(2)$.

3.2 Modular forms for congruence subgroups

Definition 3.5. Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and let $k \in \mathbb{Z}$. A holomorphic function $f : \mathbb{H} \rightarrow \mathbb{C}$ is a **modular form of weight k for Γ** if

- i) $f|_k\gamma = f$ for all $\gamma \in \Gamma$,
- ii) $f|_k\gamma$ is holomorphic at ∞ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

By $M_k(\Gamma)$ we denote the space of modular forms of weight k for Γ , i.e. with the notation used before we have $M_k = M_k(\mathrm{SL}_2(\mathbb{Z}))$. We say f is a cusp form if $f|_k\gamma$ vanishes at ∞ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $S_k(\Gamma)$ denotes the space of all cusp forms.

 ————— Until here in lecture 6 (26th May, 2023) ————— 

References

- [CS] H. Cohen, F. Strömberg: *Modular Forms: A Classical Approach*, Graduate Studies in Mathematics, Volume: 179, American Mathematical Society, 2017.
- [DS] F. Diamond, J. Shurman: *A first course in modular forms*, Graduate Texts in Mathematics, No. 228. Springer-Verlag, New York, 2005.
- [FB] E. Freitag, R. Busam: *Complex analysis*, Second edition, Universitext, Springer-Verlag, Berlin, 2009.
- [Ki] L. J. P. Kilford: *Modular forms. A classical and computational introduction*, Imperial College Press, London, 2008.
- [Ko] N. Koblitz: *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, No. 97. Springer-Verlag, New York, 1993.
- [L] S. Lang: *Introduction to modular forms*, Grundlehren der mathematischen Wissenschaften, No. 222. Springer-Verlag, Berlin-New York, 1976.
- [S] J.-P. Serre: *A course in arithmetic*, Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. (Chapter VII)
- [SS] E. Stein, R. Shakarchi: *Complex analysis*, Princeton Lectures in Analysis, 2. Princeton University Press, Princeton, NJ, 2003
- [Z] D. Zagier: *Elliptic modular forms and their applications*, first part in "The 1-2-3 of modular forms", Universitext. Springer-Verlag, Berlin, 2008. (available at http://people.mpim-bonn.mpg.de/zagier/files/doi/10.1007/978-3-540-74119-0_1/fulltext.pdf)