Modular forms for congruence subgroups and the four-squares-theorem

Janine Roshardt and Annika Weidmann

8. May 2024

1 Modular forms for congruence subgroups

1.1 Congruence subgroups: Definition and basic facts

Definition. The *principle congruence group of level N* is the subgroup

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

Remark 1. $\Gamma(N)$ is simply the kernel of $\Gamma \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ because $M \in \Gamma(N) \Leftrightarrow M \equiv \mathrm{id}_2 \pmod{N}$.

Definition. A subgroup $\Lambda \leq \Gamma$ is called a *congruence subgroup of level N* if it contains the principle congruence group of level N:

$$\Gamma(N) \leq \Lambda \leq \Gamma$$

Example 1. Two important examples are

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

and

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}.$$

Observe that we have

$$\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N) \leq \Gamma.$$

Lemma 1.1. *A congruence subgroup $\Lambda \leq \Gamma$ has finite index in Γ.*

Proof. As we have $\Gamma(N) \leq \Lambda$ we have a sujection $\Gamma/\Gamma(N) \twoheadrightarrow \Gamma/\Lambda$. Hence, in particular

$$\begin{aligned} |\Gamma/\Lambda| \leq |\Gamma/\Gamma(N)| &= |\Gamma/\ker(\Gamma \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))| \\ &= |\mathrm{im}(\Gamma \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))| \\ &\leq |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))| \leq N^4 < \infty \end{aligned}$$

□

Remark 2. The question of whether every subgroup of finite index is in fact a congruence subgroup is one that has and still does attract a lot of attention. It is the so-called *congruence subgroup problem*. The answer of $\mathrm{SL}_2(\mathbb{Z})$ is actually negative. However, for higher dimensions and the rings of integers of other number fields the answer also can be positive.[1]

Example 2. One can explicitly calculate these finite indices. Some examples are

$$[\Gamma : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right),$$
$$[\Gamma : \Gamma_1(N)] = N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right),$$
$$[\Gamma : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

see also Exercise 1.2.3 on page 21 of [2].

1.2 Cusps

We again can let the matrices act on numbers – here we take the rationals and some symbol for infinite by Möbius transformations, i.e., for $\frac{\alpha}{\beta} \in \mathbb{Q} \cup \{\infty\}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ we set

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{\alpha}{\beta} = \frac{a\frac{\alpha}{\beta} + b}{c\frac{\alpha}{\beta} + d} = \frac{a\alpha + b\beta}{c\alpha + d\beta}$$

where we use the convention $\frac{\pm 1}{0} = \infty$.

Definition. For $\Lambda \leq \Gamma$ a congruence subgroup, we call the elements of $\mathbb{Q} \cup \{\infty\}/\sim_\Lambda$, i.e., the orbits of $\mathbb{Q} \cup \infty$ under Λ, the *cusps* of Λ.

Lemma 1.2. *For $\Lambda \leq \Gamma$ a congruence subgroup we have $\left|\mathbb{Q} \cup \{\infty\}/\sim_\Lambda\right| < \infty$, i.e., every congruence subgroup has only finitely many cusps.*

Proof. For every element $\frac{a}{c} \in \mathbb{Q} \cup \{\infty\}$ not both a and c can be zero. Thus, we can extend $\begin{pmatrix} a \\ c \end{pmatrix}$ to a matrix in $\mathrm{SL}(2, \mathbb{Z})$. Observe also that

$$\begin{pmatrix} a & u \\ c & w \end{pmatrix} \infty = \begin{pmatrix} a & u \\ c & w \end{pmatrix} \frac{1}{0} = \frac{a \cdot 1 + 0}{c \cdot 1 + 0} = \frac{a}{c}$$

Hence, every cusp can be written in the form $M\infty$ for some $M \in \Gamma$. Note moreover, that if $M_1 \sim_\Lambda M_2$, i.e., if $\exists G \in \Lambda : GM_1 = M_2$ then we also have that $\exists G \in \Lambda : GM_1\infty = M_2\infty \Leftrightarrow M_1\infty \sim_\Lambda M_2\infty$. But we already know by Lemma 1.1 that there are only finitely many cosets of Λ in Γ. Thus, there can also only be finitely many orbits under the action of Λ. □

[1] The interested reader may also consult `https://encyclopediaofmath.org/wiki/Congruence_subgroup_problem` or directly `https://doi.org/10.1007/BF02684586`.

In fact one even can explicitly find the number of cusps for given groups.

Example 3.

1. Γ has only one cusp. This is in fact equivalent to $\mathrm{SL}_2(\mathbb{Z})$ acting transitively on $\mathbb{Q} \cup \{\infty\}$. This is so due to Bézout's theorem.[2] **Caution:** $\mathrm{SL}_2(\mathbb{Z})$ does not act transitively on $\mathbb{H}$ but obviously $\mathbb{H}$ contains elements that $\mathbb{Q} \cup \{\infty\}$ does not so this is no contradiction.

2. $\Gamma_0(p)$ for p prime has exactly two cusps. One can see this by applying an element of $\left(\begin{smallmatrix} a & b \\ p\gamma & d \end{smallmatrix}\right) \in \Gamma_0(p)$, i.e., $p \nmid a, d$, to two easy points, e.g. 0 and ∞:

$$\begin{pmatrix} a & b \\ p\gamma & d \end{pmatrix} 0 = \frac{a0 + b}{p\gamma 0 + d} = \frac{b}{d}$$
$$\begin{pmatrix} a & b \\ p\gamma & d \end{pmatrix} \infty = \frac{a\infty + b}{p\gamma\infty + d} = \frac{a}{p\gamma}.$$

   We see that the orbit of 0 are all rationals whose denominator is not divisible by p (and so in particular can never be zero) and the orbit of ∞ is formed by all rationals whose denominator is divisible by p but not their numerator (and so it is in particular never zero). This clearly is a partition of the rationals and so we indeed have found two distinct orbits, which are the only orbits.

1.3 Modular forms for congruence subgroups

We want to enlarge the space of modular forms we are considering. Thus, we have to weaken the conditions for being a modular form. The first condition will stay the same, for the second we will simply replace the whole group by our favourite congruence subgroup Λ and adapt condition 3 to the special choice of subgroup we made.

Definition. Let Λ be a congruence subgroup of level N. A function $f : \mathbb{H} \to \mathbb{C}$ is called a *modular form of weight k for Λ* if

1. f is holomorphic on $\mathbb{H}$
2. $\forall L \in \Lambda : f|_k L = f$
3. For every $G \in \Gamma$ $f|_k G$ has a Fourier series expansion fo the form

$$(f|_k G)(\tau) = \sum_{n=0}^{\infty} a_{f,G}(n) q^{\frac{n}{N}}$$

   for some coefficients $a_{f,G} \in \mathbb{C}$.

If we have $a_{f,G}(0) = 0$ for all $G \in \Gamma$ we say that f is a *cusp form*.
For the vector space of all weight k modular forms for a congruence subgroup $\Lambda \leq \Gamma$ we write $M_k(\Lambda)$ and analogously for the space of cusp forms for Λ we write $S_k(\Lambda)$.

[2] For a spelled out discussion let me refer you to the second part of `https://math.stackexchange.com/a/3589564`

Remark 3. Two remarks to the third condition:

- Having such a Fourier expansion is equivalent to $f|_k G$ remaining bounded for $\mathrm{Im}(\tau) \to \infty$ for all $G \in \Gamma$.
- If we have $G_1 \sim_\Lambda G_2$ for $G_1, G_2 \in \Gamma$ then we also have $f|_k G_1 = f|_k G_2$ because as this is a well defined group action we have $(f|_k(LG_1))(z) = ((f|_k L)|_k G_1)(z)$ and by the second condition we have $f|_k L = f$ for $L \in \Lambda$. Hence, it also suffices to check the third condition for a system of representatives of ${}_\Lambda\backslash\Gamma$ – of which we already know that it is finite.

Definition. Given $\frac{a}{c} \in \mathbb{Q} \cup \{\infty\}$ we already saw in the proof of Lemma 1.2 that we can write $G\infty = \frac{a}{c}$ for some $G \in \Gamma$. We then call the Fourier expansion of $f|_k G$ the *expansion of f at the cusp $\frac{a}{c}$*.

Remark 4. This is not well-defined, i.e., there is no unique Fourier expansion associated to a cusp $\frac{a}{c}$: If we have $M \in \Gamma$ such that $M\infty = \frac{a}{c}$ then also $\pm M \left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right) \infty = \frac{a}{c}$ for $j \in \mathbb{Z}$. On the other hand, a quick calculation (it's really quick, I bet you nearly can do it in your head) shows that

$$\left(f|_k \left(G \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}\right)\right)(z) = (\pm 1)^k \left(f|_k G\right)(z + j).$$

So if $\left(f|_k G\right)(z) = \sum_{n=0}^{\infty} a_{f,G}(n) \left(e^{\frac{2\pi i z}{N}}\right)^n$ is a Fourier expansion of $f|_k M$, i.e., a Fourier expansion of f at the cusp $M\infty = \frac{a}{c}$, then $\forall j \in \mathbb{Z}$ also

$$\begin{aligned}
\left(f|_k \left(\pm G \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}\right)\right)(z) &= (\pm 1)^k \sum_{n=0}^{\infty} a_{f,G}(n) \left(e^{\frac{2\pi i (z+j)}{N}}\right)^n \\
&= \sum_{n=0}^{\infty} (\pm 1)^k a_{f,G}(n) e^{\frac{2\pi i}{N} jn} \left(e^{\frac{2\pi i z}{N}}\right)^n \\
&= \sum_{n=0}^{\infty} \tilde{a}_{f,G}(n) \left(e^{\frac{2\pi i z}{N}}\right)^n
\end{aligned}$$

is a just as valid expansion of f at the cusp $M \left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right) \infty = \frac{a}{c}$. (Compare also with [2] page 17 et seq.)

Lemma 1.3. *For every $f \in M_k(\Gamma)$ and every $N \in \mathbb{N}$ we have $f(Nz) \in M_k(\Gamma_0(N))$.*

Proof. That $f(Nz)$ is still holomorphic and has no negative Fourier coefficients is rather obvious. Hence, we only have to test whether $f(Nz)$ transforms correctly under the weight k action of elements in $\Gamma_0(N)$ namely not at all. Denote $M_N : z \mapsto Nz$ and let $L = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ be arbitrary then $\exists \gamma \in \mathbb{Z} : c = N\gamma$ and so

$$\begin{aligned}
\left((f \circ M_N)|_k L\right)(z) &= (cz + d)^{-k} (f \circ M_N) \left(\frac{az + b}{cz + d}\right) \\
&= (\gamma(Nz) + d)^{-k} f \left(\frac{a(Nz) + Nb}{\gamma(Nz) + d}\right) \\
&= \left(f|_k \begin{pmatrix} a & Nb \\ \gamma & d \end{pmatrix}\right)(Nz)
\end{aligned}$$

Now since $ad - \gamma Nb = ad - bc = 1$ we have $\left(\begin{smallmatrix} a & Nb \\ \gamma & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and so because $f \in M_k$ we get

$$\left(f|_k \begin{pmatrix} a & Nb \\ \gamma & d \end{pmatrix}\right)(Nz) = f(Nz) = (f \circ M_N)(z).$$

□

Example 4.

1. For $N \in \mathbb{N}$ and $4 \leq k \in \mathbb{Z}$ an example of a modular form of weight k for $\Gamma_0(N)$ is the Eisensteinreihe

$$E_{k,\Gamma_0(N)}(z) := \sum_{[M] \in \Gamma_\infty \backslash \Gamma_0(N)} (1|_k M)(z)$$

for Γ_∞ the subgroup generated by the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, i.e., $\Gamma_\infty := \{\pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n : n \in \mathbb{Z}\}$. Compare this also with the usual normalized Eisenstein series. We actually already proved in a previous talk a very analogous representation for those (see also [1], Bemerkung 2.3.7.).

2. What about weight 2? As we defined the above very analogous to how we defined the usual Eisenstein series and for them we had a fuss with the weight 2 case, one would suspect that this case also now demands a special treatment. Remember that we had two types of normalized Eisenstein series of weight 2: One, we called it $E_2^*(z)$, was a modular form of weight 2 but not holomorphic and the other one, we called it $E_2(z)$ was holomorphic but not a modular form. Maybe we can make us of some of the work we already have put in. For example by the proof of the above lemma 1.3 we would have $E_2^*(Nz)$ transforms correctly under the weight 2 action of $\Gamma_0(N)$. However, it of course still would not be holomorphic. But we have by the definition of E_2^*:

$$E_2^*(Nz) = E_2(Nz) - \frac{3}{\pi \mathrm{Im}(Nz)} = E_2(Nz) - \frac{3}{N\pi \mathrm{Im}(z)}.$$

So maybe $NE_2^*(Nz) + \frac{3}{\pi \mathrm{Im}(z)}$ could work? But no, that does not transform correctly anymore. How about

$$\begin{aligned} E_2^*(z) - NE_2^*(Nz) &= E_2(z) - \frac{3}{\pi \mathrm{Im}(z)} - NE_2(Nz) + N\frac{3}{N\pi \mathrm{Im}(z)} \\ &= E_2(z) - NE_2(Nz) \ ? \end{aligned}$$

This is transforms correctly under the weight 2 action of $\Gamma_0(N)$ as it is a linear combination of E_2^* and it is holomorphic with the right Fourier expansion as it is a linear combination of E_2. Hence, we define

$$E_{2,\Gamma_0(N)}(z) := E_2(z) - NE_2(Nz) \in M_2(\Gamma_0(N)).$$

3. We want to add as a little side remark, that in fact modular forms to $\Gamma_0(N)$ can be written as a product of powers of the Dedekind eta function. For example $S_2(\Gamma_0(11)) = \langle \eta^2(z)\eta^2(11z) \rangle$. But unfortunately, we do not have time nor space to follow this interesting path further down.

1.4 Lifting modular forms for congruence subgroups to modular forms for all of $\mathrm{SL}_2(\mathbb{Z})$

The goal of this section is just as the title says: Given a modular form to a congruence subgroup we want to associated a modular for for all of $\mathrm{SL}_2(\mathbb{Z})$ to it.

Definition. For a congruence subgroup $\Lambda \leq \mathrm{SL}_2(\mathbb{Z})$ we define for $f \in M_k(\Lambda)$

$$\mathrm{tr}(f) := \sum_{[M] \in \Lambda\backslash\Gamma} f|_k M \tag{1}$$

and

$$\pi(f) := \prod_{[M] \in \Lambda\backslash\Gamma} f|_k M.$$

Eq. 1 is also called the *trace of f*.

Remark 5. Observe that the sum and product are actually just taken over a system of representatives of $\Lambda\backslash\Gamma$. As we already have show that such as system is always finite (because Λ has finite index), we sort of can think of the above sum and product as being finite ones.

Proposition 1.4. *Let $\Lambda \leq \Gamma$ be a congruence subgroup with index $\ell := [\Gamma : \Lambda]$. Then we have $\forall f \in M|_k(\Lambda)$:*

$$\mathrm{tr}(f) \in M|_k \qquad\qquad \pi(f) \in M|_{k\ell}$$

Proof. As discussed the sum and the product are basically finite and thus, being holomorphic and having such a Fourier series expansion are preserved. So it is only left to show the invariance under the weight k action of Λ. So let $\mathcal{R}$ be a set of representatives for $\Lambda\backslash\Gamma$ then $\forall G \in \Gamma$ also $\mathcal{R}' := \{MG : M \in \mathcal{R}\}$ is a system of representatives for $\Lambda\backslash\Gamma$ and so we have $\forall G \in \Gamma$ using the group action property and the linearity of the action

$$\begin{aligned}
\mathrm{tr}(f)|_k G &= \left(\sum_{[M] \in \Lambda\backslash\Gamma} f|_k M \right) \Bigg|_k G \\
&= \sum_{[M] \in \Lambda\backslash\Gamma} (f|_k M)|_k G \\
&= \sum_{[M] \in \Lambda\backslash\Gamma} f|_k (MG) \\
&= \sum_{[M] \in \mathcal{R}} f|_k (MG) \\
&= \sum_{[N] \in \mathcal{R}'} f|_k N = \mathrm{tr}(f).
\end{aligned}$$

And similarly for $\pi(f)$

$$\begin{aligned}\pi(f)|_{k\ell}G &= \left(\prod_{[M]\ \in\ \Lambda\backslash\Gamma} f|_k M\right)\Bigg|_{k\ell} G \\ &= \prod_{[M]\ \in\mathcal{R}} (f|_k M)|_k G \\ &= \prod_{[M]\ \in\mathcal{R}} f|_k (MG) \\ &= \prod_{[N]\ \in\mathcal{R}'} f|_k N = \mathrm{tr}(f).\end{aligned}$$

□

Example 5.

- For $k \geq 4$ we have $\mathrm{tr}(E_{k,\Gamma_0(N)}) = E_k$. The difference in the definition of these to series was that once we took a system of representatives for ${\Gamma_\infty}\backslash\Gamma_0(N)$ and once for ${\Gamma_\infty}\backslash\Gamma$. But for the trace we exactly sum over a system of representatives for ${\Gamma_0(N)}\backslash\Gamma$, hence, we get the above identity.
- For $k = 2$ we get $\mathrm{tr}(E_{2,\Gamma_0(N)}) = 0$ as by the above proposition 1.4 we have $\mathrm{tr}(E_{2,\Gamma_0(N)}) \in M_2 = \{0\}$.

1.5 Sturm's bound on the dimension of spaces of modular forms

In this section we will estimate the dimension of $M_k(\Lambda)$. Recall that we already determined the dimension of M_k (Thm 2.5.6 in [1])

$$\dim(M_k) = \begin{cases} 0 & \text{if } k < 0 \text{ or } k \text{ odd}, \\ 1 & \text{if } k = 0, \\ \lfloor \frac{k}{12} \rfloor & \text{if } k \equiv 2 \pmod{12}, \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{if } k \not\equiv 2 \pmod{12}. \end{cases}$$

We will show the following: If $\Lambda \subseteq \Gamma$ is a congruence subgroup of level N and index $\ell := [\Gamma : \Lambda]$. Then for $k \geq 0$ it holds that

$$\dim(M_k(\Lambda)) \leq \lfloor \frac{klN}{12} \rfloor + 1.$$

This is called the Sturm's bound. Note that if $\Lambda = \Gamma$ then $N = \ell = 1$ and the inequality holds by Thm 2.5.6 in [1].

The main result needed to prove Sturm's bound is the following:

Proposition 1.5. *Let Λ be a congruence group of level N of index $l = [\Gamma : \Lambda]$ and $k \geq 0$. Let $L \in \Gamma$ and $f \in M_k(\Lambda)$ with fourier series*

$$f|_k L = \sum_{n=0}^{\infty} a_{f,L}(n) q^{n/N}.$$

From

$$a_{f,L}(n) = 0 \text{ for } 0 \leq n \leq \frac{k\ell N}{12}$$

it follows that $f = 0$

Proof. For $g = \pi(f) \in M_{k\ell}$ it holds that $a_g(n) = 0$ for $0 \leq n \leq \frac{k\ell}{12}$. Hence, $ord_\infty(g) > \frac{k\ell}{12}$. Recall that if $g \neq 0$,

$$\text{ord}_\infty(g) + \frac{1}{2}\text{ord}_i(g) + \frac{1}{3}\text{ord}_\rho(g) + \sum_{\substack{\tau \in \Gamma\backslash\mathbb{H} \\ \tau \neq i,\rho \mod \Gamma}} \text{ord}_\tau(g) = \frac{k\ell}{12}$$

where $\rho = e^{\pi i/3}$ by Thm. 2.3.1 in [1]. Since all the terms in this equation are nonnegative, we arrive at a contradiction. Hence,

$$\pi(f) = \prod_{M \in \Lambda\backslash\Gamma} f|_k M = 0.$$

The identity theorem tells us that for an $M \in \Lambda\backslash\Gamma$, $f|_k M = 0$. And therefore,

$$f = f|_k M M^{-1} = (f|_k M)|_k M^{-1} = 0.$$

□

Corollary 1.6 (Sturm's bound)**.** *Using the notation from last theorem it holds that*

$$dim M_k(\Lambda) \leq \left\lfloor \frac{k\ell N}{12} \right\rfloor + 1$$

Proof. Let $f_1, \ldots, f_r \in M_k(\Lambda)$ with $r > \lfloor \frac{k\ell N}{12} \rfloor + 1$. By choosing coefficients $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$, not all zero, appropriately, we can achieve that in $\sum_{i=1}^r \alpha_i f_i$ all fourier coefficients of index $0 \leq n \leq \frac{k\ell N}{12}$ vanish. It follows that $\sum_{i=1}^r \alpha_i f_i = 0$ which means that f_i are linearly dependent. □

Example 6. Let $\Lambda = \Gamma_0(2)$. The index of $\Gamma_0(2)$ in Γ is $\ell = [\Gamma : \Gamma_0(2)] = 3$ and the level is $N = 2$. According to corollary 1.6,

$$\dim M_2(\Gamma_0(2)) \leq \lfloor \frac{2 \cdot 3 \cdot 2}{12} \rfloor + 1 = 2$$

Moreover, $\dim S_2(\Gamma_0(2)) = 0$ because if $f \in S_2(\Lambda)$ we get that $\pi(f) \in S_6 \Rightarrow f = 0$. One can show that $\dim M_2(\Gamma_0(2)) = 1$

For $k \geq 2$ there are explicit formulas for the dimension of $M_k(\Lambda)$ and of $S_k(\Lambda)$. The proof uses the Riemann-Roch theorem.

Proposition 1.7. *Let* Λ *be a congruence subgroup of level* N*. The following holds:*

1. *If* $k < 0$, $M_k(\Lambda) = \{0\}$
2. $M_0(\Lambda) = \mathbb{C}$

Proof. Let $f \in M_k(\Lambda)$ and $\ell = [\Gamma : \Lambda]$. It holds that $\pi(f) \in M_{kl}$. From talk 5 about the modular group and modular forms (Thm 5.7) we know that for $k < 0$ it holds that $M_{kl} = 0$. Hence, $g = 0$ and by the same reasoning as in proposition 1.5 $f = 0$. If $k = 0$ Sturm's bound tells us that $\dim(M_0(\Lambda)) \leq 1$. All constant functions are modular forms of weight 0 for Γ and so $\mathbb{C} \subseteq M_0(\Lambda)$ and so, $M_0(\Lambda) = \mathbb{C}$. □

2 Jacobi theta function

In this section we discuss the properties of the Jacobi theta function and we will show that $\vartheta^4 \in M_2(\Gamma_0(4))$.

Definition. The series

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

is called the *Jacobi theta function*. Here we use $q = e^{2\pi i \tau}$ for brevity.

Claim. *The Jacobi theta function is holomorphic on* $\mathbb{H}$.

Proof. Note that on $\{\tau \in \mathbb{H} \mid \mathrm{Im}(\tau) \geq c\}$ for some fixed $c > 0$, $\sum_{n \in \mathbb{Z}} |q^{n^2}| = \sum_{n \in \mathbb{Z}} e^{-2\pi \Im(\tau) n^2} \leq \sum_{n \in \mathbb{Z}} e^{-2\pi c n^2}$. So on $\{\tau \in \mathbb{H} \mid \mathrm{Im}(\tau) \geq c\}$ ϑ converges absolutely uniformly. This shows that ϑ is holomorphic on $\mathbb{H}$. □

Claim. *Moreover,* ϑ *satisfies the transformation properties*

$$\vartheta(\tau + 1) = \vartheta(\tau) \tag{2}$$

$$\vartheta(\tau) + \vartheta(\tau + \frac{1}{2}) = 2\vartheta(4\tau). \tag{3}$$

Proof. Equation (2) is a consequence of $q = e^{2\pi i \tau} = e^{2\pi i(\tau+1)}$.

For equation (3) note that

$$\begin{aligned}
\vartheta(\tau + \frac{1}{2}) &= \sum_{n \in \mathbb{Z}} (e^{2\pi i(\tau + \frac{1}{2})})^{n^2} \\
&= \sum_{n \in \mathbb{Z}} (-q)^{n^2} \text{ where } q = e^{2\pi i \tau} \\
\Rightarrow \vartheta(\tau) + \vartheta(\tau + \frac{1}{2}) &= \sum_{n \in \mathbb{Z}} q^{n^2} + (-q)^{n^2} \\
&= 2 \sum_{n \in \mathbb{Z}} q^{(2n)^2} \\
&= 2\vartheta(4\tau).
\end{aligned}$$

□

Actually, we would hope that there might be a $k \in \mathbb{N}$ such that ϑ even is a modular form of weight k. For that we have to check if

1. ϑ is holomorphic on $\mathbb{H}$

2. $\vartheta(\tau+1)=\vartheta(\tau)$
3. $\vartheta(-\frac{1}{\tau})=\tau^k\vartheta(\tau)$
4. ϑ can be written as a Fourier series of the form $\vartheta(\tau)=\sum_{n=0}^{\infty}a_\vartheta(n)q^n$ with $q=e^{2\pi i\tau}$.

1, 2 and 4 are clearly satisfied. Let's check 3:

Proposition 2.1. *For all $\tau\in\mathbb{H}$ it holds that*

$$\vartheta(-\frac{1}{\tau})=\sqrt{-i\tau/2}\vartheta(\tau/4).$$

Equivalently,

$$\vartheta(-\frac{1}{4\tau})=\sqrt{-2i\tau}\vartheta(\tau) \tag{4}$$

for all $\tau\in\mathbb{H}$.

So the answer to whether ϑ is a modular form, will unfortunately be negative. For the proof of this Proposition we use the Poisson summation formula that might be familiar to you from analysis 4. We will not give a proof here.

Lemma 2.2 (Poisson summation formula)**.** *Take a function $f\in\mathcal{S}(\mathbb{R})$ in the Schwartz space. It holds that*

$$\sum_{n\in\mathbb{Z}}f(n)=\sum_{k\in\mathbb{Z}}\hat{f}(k).$$

Recall that a Schwartz function is a smooth function $f:\mathbb{R}\to\mathbb{C}$ such that

$$\sup\left|x^\alpha\frac{d^\beta}{dx^\beta}f(x)\right|<\infty$$

for all $\alpha,\beta\in\mathbb{N}_0$, i.e., f and all it's derivatives decay faster than the inverse of any polynomial.

Example 7. One can check that $e^{-\pi x^2}$ is an example of a Schwartz function and the fourier transform is given by $\widehat{e^{-\pi x^2}}=e^{-\pi x^2}$.

Proof of proposition 2.1. By the identity theorem it's enough to show 2.1 in the case that $\tau=it/2$ for $t>0$. (This set possesses an accumulation point in $\mathbb{H}$). We need to show

$$\sum_{n\in\mathbb{Z}}e^{-\pi n^2/t}=\vartheta(\frac{i}{2t})\overset{!}{=}\sqrt{-2i\frac{it}{2}}\vartheta(\frac{it}{2})=\sqrt{t}\sum_{n\in\mathbb{Z}}e^{-\pi n^2t}$$

for $t>0$. We will apply the Poisson summation formula for $f_t(x)=e^{-\pi x^2/t}$. A

calculation shows that $\hat{f}_t(n) = \sqrt{t} f_{1/t}(n)$.

$$\begin{aligned}
\hat{f}_t(n) &= \int_{\mathbb{R}} e^{-\pi x^2/t} e^{-2\pi i n x} dx \\
&= \sqrt{t} \int_{\mathbb{R}} e^{-\pi x^2} e^{-2\pi i n \sqrt{t} x} dx \\
&= \sqrt{t} \int_{\mathbb{R}} e^{-\pi x^2} e^{-2\pi i n \sqrt{t} x} dx \text{ by substituting } x \text{ by } x/\sqrt{t} \\
&= \sqrt{t} \widehat{e^{-\pi x^2}}(\sqrt{t} n) \\
&= \sqrt{t} e^{-\pi n^2 t} \text{ (because } \widehat{e^{-\pi x^2}} = e^{-\pi x^2}) \\
&= \sqrt{t} f_{1/t}(n).
\end{aligned}$$

Thus, by the Poisson summation formula we get that

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2/t} = \sum_{n\in\mathbb{Z}} f_t(n) = \sum_{n\in\mathbb{Z}} \widehat{f}_t(n) = \sum_{n\in\mathbb{Z}} \sqrt{t} f_{1/t}(n) = \sqrt{t} \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t}.$$

This is what we wanted to show. □

Proposition 2.1 shows that $\vartheta(-\frac{1}{\tau}) \neq \tau^k \vartheta(\tau)$ and $\vartheta \notin M_k$. However, the following proposition holds:

Proposition 2.3. *It holds that $\vartheta^4 \in M_2(\Gamma_0(4))$.*

Proof. We need to check that

1. ϑ^4 is holomorphic on $\mathbb{H}$,
2. $\vartheta^4|_2 M = \vartheta^4$ for all $M \in \Gamma_0(4)$,
3. For each $L \in \Gamma$, the Fourier expansion of $\vartheta^4|_2 L$ is of the form

$$(\vartheta^4|_2 L)(\tau) = \sum_{n=0}^{\infty} a_L(n) q^{n/N}.$$

Ad item 1: We already know that ϑ is holomorphic on $\mathbb{H}$. Ad item 2: One can show that $\Gamma_0(4)$ is generated by the matrices

$$-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, U = \begin{pmatrix} -1 & 0 \\ 4 & -1 \end{pmatrix}.$$

We already showed that $\vartheta(\tau + 1) = \vartheta(\tau)$ and so ϑ transforms correctly under T. We can also check that ϑ^4 transforms correctly under $-I$:

$$\vartheta|_2(-I) = (-1)^2 \vartheta\left(\frac{-\tau}{-1}\right) = \vartheta(\tau).$$

For U we use the Jacobi transformation formula:

$$\begin{aligned}\vartheta^4(U\tau) &= \vartheta^4\left(-\frac{\tau}{4\tau-1}\right) = \vartheta^4\left(-\frac{1}{4(1-\frac{1}{4\tau})}\right)\\ &= \left(\sqrt{-2i(1-\frac{1}{4\tau})}\right)^4 \vartheta^4\left(1-\frac{1}{4\tau}\right)\\ &= \left(\sqrt{-2i(1-\frac{1}{4\tau})}\right)^4 \vartheta^4\left(-\frac{1}{4\tau}\right)\\ &= \left(\sqrt{-2i(1-\frac{1}{4\tau})}\right)^4 (\sqrt{-2i\tau})^4\vartheta^4(\tau)\\ &= (-4\tau+1)^2\vartheta^4(\tau) = j(U,\tau)^2\vartheta^4(\tau).\end{aligned}$$

Ad item 3: It is enough to show that f is holomorphic at the cusps of $\Gamma_0(4)$. $\Gamma_0(4)$ has the three cusps $0, \frac{1}{2}, \infty$. By definition, ϑ^4 is holomorphic at ∞. For the other cusps note that

$$S\infty = 0, L\infty = \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}\infty = 1/2.$$

We apply the Jacobi transformation to get that

$$\vartheta^4|_2 S = \tau^{-2}\vartheta^4\left(-\frac{1}{4\frac{\tau}{4}}\right) = \tau^{-2}\left(\sqrt{-2i\frac{\tau}{4}}\right)^4\vartheta^4\left(\frac{\tau}{4}\right) = -\frac{1}{4}\vartheta^4\left(\frac{\tau}{4}\right).$$

and

$$\begin{aligned}\vartheta^4|_2 L &= (2\tau+1)^{-2}\vartheta^4\left(\frac{\tau}{2\tau+1}\right) = (2\tau+1)^{-2}\vartheta^4\left(-\frac{1}{4(-\frac{1}{2}-\frac{1}{4\tau})}\right)\\ &= (2\tau+1)^{-2}\left(\sqrt{2i(\frac{1}{2}+\frac{1}{4\tau})}\right)\vartheta^4\left(-\frac{1}{2}-\frac{1}{4\tau}\right) = -\frac{1}{4\tau^2}\vartheta^4\left(-\frac{1}{2}-\frac{1}{4\tau}\right).\end{aligned}$$

From the Jacobi transformation and equation (3) we get that

$$\vartheta\left(-\frac{1}{2}-\frac{1}{4\tau}\right) = \sqrt{-2i\tau}\sum_{n\in\mathbb{Z}} e^{2\pi i(n+1/2)^2\tau}.$$

□

3 Four squares theorem

In this section we want to demonstrate how effortlessly a cute theorem – that was proven by Lagrange in the 18th century – can be proven, using the theory we have developed so far.

Theorem 3.1. *Let $n \in \mathbb{N}$ be arbitrary. Then there exist $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ such that*

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2\ ,$$

i.e., every natural number can be written as the sum of four square.

Proof. For $n \in N$ define the representation number $r_4(n) := |\{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 : n = x_1^2 + x_2^2 + x_3^2 + x_4^2\}|$, where r stands for **r**epresentation and 4 for the number of squares. Now if we can prove that $r_4(n)$ is positive for every $n \in \mathbb{N}$ then we have proven the first part (i.e., the existence part) of the theorem. As we took all this time to study the theta function we now also would like to put it to use. Indeed we can, as we have

$$\vartheta^4(\tau) = \left(\sum_{n\in\mathbb{Z}} q^{n^2}\right)^4 = \sum_{x_1,x_2,x_3,x_4\in\mathbb{Z}} q^{x_1^2+x_2^2+x_3^2+x_4^2} = \sum_{n=0}^{\infty} r_4(n) q^n.$$

So if we were to know the Fourier coefficients for every $n \in \mathbb{N}$ then we would be done. Then what do we know about ϑ^4? Well, by calculating a huge product $(1 + 2q + 2q^4 + 2q^9 + \dots)^4$ we could find the coefficient for every n. But how do we use this to show that all of them are non-zero, without calculating infinitely many of them? Well, we also have see in proposition 2.3 that $\vartheta^4 \in M_2(\Gamma_0(4))$ – and actually that is all we need to find an explicit formula for the Fourier coefficients of ϑ^4: One can show that $E_2(z) - 2E_2(2z)$ and $E_2(z) - 4E_2(4z)$ form a basis for $M_2(\Gamma_0(4))$, see [3]. Hence, also ϑ^4 is a linear combination of these two functions – and we know the Fourier expansion of those two functions as we already have seen that $E_2(z) = 1 - 24\sum_{n=1}^{\infty}\left(\sum_{d|n} d\right) q^n$.
So all that is left to do, is to find the linear combination of these two functions which is equal to ϑ^4. To cut a long story (or search) short we will prove the following claim:

Claim. $\vartheta^4(\tau) = \frac{1}{3}\left(4E_2(4\tau) - E_2(\tau)\right)$

Proof of Claim. To prove this claim we can compare the Fourier coefficients of both sides. Luckily, proposition 1.5 allows us to reduce this to only comparing the the first few initial coefficients. More precisely, we instantiate proposition 1.5 with $\Lambda = \Gamma_0(4), L = I_2, k = 2, N = 4$ and as we can calculate using the formula in example 2: $\ell = [\Gamma : \Gamma_0(4)] = 6$. Hence, we only need to check the first $\frac{2\cdot 6\cdot 4}{12} = 4$ coefficients. This can be done explicitly by hand (the first four Fourier coefficients are 1, 8, 24 and 32). $\square_{\text{Claim.}}$

The n-th Fourier coefficient of $\frac{1}{3}\left(4E_2(4\tau) - E_2(\tau)\right)$ is $8\sum_{\{d|n,\ 4\nmid d\}} d$ as a direct calculation shows, hence in particular it is always positive (as 1 always is part of the sum). So, while proving the existence, on the way we also have proved a formula for the amount of ways a natural number can be written in such a way. $\square$

Corollary 3.2. *As a corollary of the proof we even obtain a formula for the number of ways in which a given natural number can be written as sums of four squares:*

$$|\{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 : n = x_1^2 + x_2^2 + x_3^2 + x_4^2\}| = 8\sum_{\substack{d|n\\ 4\nmid d}} d\ .$$

We can conclude not only that every natural number *has* an expansion as the sum of four squares but in fact it even *has at least eight* such expansions – which is also what one should have suspected, because if we know that n has

an expansion $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and all the x_i are nonzero, then for every i we can replace x_i with $-x_i$. This will give us in total eight ways of writing n as a sum of four squares.

References

[1] Schwagenscheidt, Modulformen, lecture notes, Section 2.9, 2.10

[2] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics, vol 228, Springer, New York, NY (2005) https://doi.org/10.1007/978-0-387-27226-9_1

[3] S. Sridhar *Modular Forms and Jacobi's Four Square Theorem*, lecture notes, 2017, `https://web.math.princeton.edu/~ssridhar/resources/Papers/4squareNotes.pdf`