Modular forms and applications
Exercise Sheet 2

For this exercise sheet we define the following congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, where $N \in \mathbb{Z}_{\geq 1}$:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} | a,b,c,d \in \mathbb{Z}, ad - Nbc = 1 \right\},$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} | a,b,c,d \in \mathbb{Z}, ad - Nbc = 1,\ d \equiv 1 \,(\mathrm{mod}\, N) \right\}.$$

Exercise 1. Let $\mathbb{P}^1(\mathbb{C})$ denote the projective line. The action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$ can be realized as restriction of the natural action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{P}^1(\mathbb{C})$. Here we embed $\mathbb{C} \ni z \mapsto [z:1] \in \mathbb{P}^1(\mathbb{C})$ and $\infty = [1:0] \in \mathbb{P}^1(\mathbb{C})$. Prove the following assertions about $\gamma \in \mathrm{SL}_2(\mathbb{R}) \smallsetminus \{\pm I_2\}$:

(a) $|\mathrm{tr}\,\gamma| < 2$ if and only if γ fixes exactly one point in $\mathbb{H}$ and one in $\overline{\mathbb{H}} = \{x + iy |\ x \in \mathbb{R},\ y < 0\}$.

Definition: such a matrix is called elliptic.

(b) $|\mathrm{tr}\,\gamma| > 2$ if and only if γ fixes two points, both contained in $\mathbb{R} \sqcup \{\infty\}$ (where we see $\mathbb{R} \subset \mathbb{C} \subset \mathbb{P}^1(\mathbb{C})$ by the above map), and none in $\mathbb{H}$.

Definition: such a matrix is called hyperbolic.

(c) $|\mathrm{tr}\,\gamma| = 2$ if and only if γ fixes only one point on $\mathbb{R} \sqcup \{\infty\}$ and none otherwise.

Definition: such a matrix is called parabolic.

Let $\Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. Denote $\overline{\Gamma} = \Gamma/\{\pm I_2\}$. We call $z \in \mathbb{H}$ an elliptic point for Γ if $\mathrm{Stab}_{\overline{\Gamma}}(z)$ is not trivial. We identify two Γ-elliptic points $z_1 \sim z_2$ if there exist $\gamma \in \Gamma$ such that $\gamma z_1 = z_2$.

(d) Show that $\mathrm{SL}_2(\mathbb{Z})$ has two equivalence classes of elliptic points.

(e) Show that an elliptic matrix in $\mathrm{SL}_2(\mathbb{Z})$ has finite order.

(f) Show that $\Gamma(N)$ for any $N \geq 2$ and $\Gamma_1(N)$ for any $N \geq 4$, do not have elliptic points.

(g) Does $\Gamma_1(3)$ have an elliptic point?

Solution. Let $\gamma \in \mathrm{SL}_2(\mathbb{R}) \smallsetminus \{\pm I_2\}$.

(a) Consider the characteristic polynomial

$$X^2 - \mathrm{Tr}(\gamma)X + 1 \in \mathbb{R}[X]$$

of γ. This can have $0, 1$ or 2 roots depending on $\mathrm{Tr}(\gamma)$. If $|\mathrm{Tr}(\gamma)| < 2$ then this polynomial has two non-real roots, i.e. γ has two non-real eigenvalues, say λ and $\overline{\lambda}$. Let $\binom{z_1}{z_2}$ be an eigenvector to the eigenvalue λ. Then $z_2 \neq 0$, otherwise $az_1 = \lambda z_1$ which is not possibile since $\lambda \notin \mathbb{R}$ (similarly $z_1 \neq 0$).

After dividing we may assume $z_2 = 1$. Since λ is not real then so cannot be z_1. Now both $\binom{z_1}{1}$ and $\binom{\overline{z_1}}{1}$ are eigenvector of γ and in particular the modular action of γ fixes both z_1 and $\overline{z_1}$ one of them lying in $\mathbb{H}$, the other in $\overline{\mathbb{H}}$.

Conversely if the modular action of γ fixes $z_1 \in \mathbb{H}$. Then $\binom{z_1}{1}$ is an eigenvector of γ. Since γ is real and $z_1 \in \mathbb{H}$ the eigenvalue (which is equal to $j(\gamma)(z_1)$, see Exercise sheet 1 for the j-function) cannot be real. Hence $|\mathrm{Tr}(\gamma)| < 2$.

(b) If $|\mathrm{Tr}(\gamma)| > 2$, then γ has two real eigenvalues. It is therefore diagonalizable with eigenvalues, say $\lambda, \lambda^{-1} \in \mathbb{R}$. Let $\binom{z_1}{z_2}$ be a λ-eigenvector. Then the modular action of γ fixes $z_1/z_2 \in \mathbb{R} \sqcup \{\infty\}$ (where we set eventually $z_1/0 = \infty$). Any eigenvector for λ^{-1} will give another fixed point for the modular action of γ.

Conversely suppose that γ fixes two points as described. Then γ has two real eigenvector and so two real eigenvalues. Say $\lambda \neq \lambda^{-1}$. Hence $|\mathrm{Tr}(\gamma)| > 2$.

(c) Now suppose $\mathrm{Tr}(\gamma) = \pm 2$. Then γ has exactly one eigenvalue, i.e. $\frac{\mathrm{Tr}(\gamma)}{2} = \pm 1$. Since γ is not $\pm$ the identity it is not diagonalizable and in particular it has only one, up to scalar, eigenvector, which is also real (it could be $(1, 0)$ which is saying the γ fixes infinity), this will be a fixed point for the modular action. Conversely if γ fixes only one point in $\mathbb{R} \cup \{\infty\}$, then γ has only one eigenvector and hence also only one eigenvalue, which is then forced to be ± 1.

(d) Suppose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ fixes a point in $\mathbb{H}$. Then we have $-2 < \mathrm{Tr}(\gamma) < 2$. In particular, since $\mathrm{Tr}(\gamma)$ is an integer it can be either -1, or 0 or 1.

Let $z \in \mathbb{H}$ be an elliptic point for $\mathrm{SL}_2(\mathbb{Z})$. After translating by an element of $\mathrm{SL}_2(\mathbb{Z})$ we may assume that $|z| \geq 1$ and $-1/2 \leq \mathrm{Re}(z) \leq 1/2$. Suppose $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ fixes z. Then we have

$$z = \frac{(a-d) \pm i\sqrt{4-(a+d)^2}}{2c},$$

in particular the imaginary part of z is either $\frac{1}{c}$ or $\frac{\sqrt{3}}{2c}$ depending upon the trace. The constraint $|\mathrm{Re}(z)| \leq 1/2$ and $|z| \geq 1$ implies $\mathrm{Im}(z) \geq \frac{\sqrt{3}}{2}$ and so in either cases we infer that $c = \pm 1$. We then infer that

$$-1 \leq a - d \leq 1$$

and together with $-1 \leq a + d \leq 1$ we deduce $-2 \leq 2a, 2d \leq 2$ and so $a, d \in \{0, \pm 1\}$. We insert the above condition in z (keeping in mind det to be 1) and we actually obtain that z can be one of the following three: i, ρ or $\rho + 1 = T \cdot \rho$.

(e) From the above computations one sees that the stabilizers in $\mathrm{SL}_2(\mathbb{Z})$ of i and ρ are finite cyclic group of order 4 and 6 respectively. By the previous point any elliptic matrix in $\mathrm{SL}_2(\mathbb{Z})$ is conjugate to a matrix in $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(i)$ or $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\rho)$ and hence it is of oder a divisor of 4 or 6 respectively.

(f) Suppose $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$ is elliptic. Then as we have already seen $\mathrm{Tr}(\gamma) = a + d \in \{0, \pm 1\}$. On the other hand $d \equiv 1 \mod (N)$ and by the determinant condition we deduce $a \equiv ad - bc \equiv 1 \mod (N)$. Hence $a + d \equiv 2 \mod (N)$. Hence for $N > 3$ we deduce that $\Gamma_1(N)$ does not contain any elliptic matrix. In particular $\Gamma(N) \leqslant \Gamma_1(N)$ do not have elliptic points. For $\Gamma(2)$ the proof is similar: suppose $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(2)$ is elliptic. Then $|a + d| < 2$. But a and d are both odd numbers. In particular we must have $a = -d$. The determinant condition gives us

$$-a^2 - bc = 1,$$

in particular since both b and c are event it would imply that $3 = -1 = a^2 \mod (4)$. But 3 is not a square modulo 4 as it is easy to check. We deduce that $\Gamma(2)$ does not contain elliptic matrices.

(g) For $N = 3$ the case $a + d = -1 \equiv 2 \mod (3)$ can (and indeed does) happen. So we have at least one elliptic matrix (and so point). For example

$$\begin{pmatrix} 16 & -7 \\ 39 & -17 \end{pmatrix}$$

fixes $\frac{17+\rho}{39}$.

Exercise 2 (Fourier expansions at the cusps of modular functions)**.** Let $k \in \mathbb{Z}$. Recall the slash k action of $\mathrm{SL}_2(\mathbb{R})$ from Exercise sheet 1: for a function $f \colon \mathbb{H} \to \mathbb{C}$ and a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ we defined the function

$$f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = j(c,d)(z)^{-k} f(\frac{az+b}{cz+d}) = (cz+d)^{-k} f(\frac{az+b}{cz+d})$$

(a) Let $f : \mathbb{H} \to \mathbb{C}$ be an holomorphic function and let $h > 0$ be a positive real number. Suppose that $f|_k \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} = f$. Show that there are complex numbers $(c_n(f))_n$ such that for all $z \in \mathbb{H}$ we have

$$f(z) = \sum_{n \in \mathbb{Z}} c_n(f) e^{2\pi i n z/h}.$$

Express $c_n(f)$ in terms of f and $n \in \mathbb{Z}$.

(b) Let $\Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup, $k \in \mathbb{Z}$ and $f \colon \mathbb{H} \to \mathbb{C}$ an holomorphic function. Suppose that for all $\gamma \in \Gamma$ we have

$$f|_k \gamma = f.$$

Let $\delta \in \mathrm{SL}_2(\mathbb{Z})$. Show that there exists an $h \in \mathbb{Z}_{\geq 1}, (a_{n,\delta}(f)) \subset \mathbb{C}$, so that

$$f|_k \delta(z) = \sum_{n \in \mathbb{Z}} a_{n,\delta}(f) e^{2\pi i n \frac{z}{h}}.$$

Let f now be a weight k modular form for $\mathrm{SL}_2(\mathbb{Z})$. Then we can write

$$f(z) = \sum_{n=0}^{\infty} a_n(f) e^{2\pi i n z}.$$

Define $\mathrm{ord}_\infty(f) = \min\{n \in \mathbb{Z}_{\geq 0},\ a_n(f) \neq 0\}$.

(c) Show that there exists $y_0 > 0$ so that f has neither a zero nor a pole in the region $\{x + it,\ x \in \mathbb{R},\ t \geq y_0\}$.

(d) For $t \geq y_0$ set $\gamma_{\infty,t} = \{x + it,\ |\mathrm{Re}(x)| \leq 1/2\}$. Show that

$$\frac{1}{2\pi i} \int_{\gamma_{\infty,t}} \frac{f'}{f}(z) \, \mathrm{d}z = -\,\mathrm{ord}_\infty(f),$$

where we integrate from right to left.

Let $\Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. Every element of the form $\delta \cdot \infty$, $\delta \in \mathrm{SL}_2(\mathbb{Z})$, is called a cusp point. For Γ a congruence subgroup we identify two cusp points α_0, α_1 if there exists $\gamma \in \Gamma$ so that $\gamma\alpha_0 = \alpha_1$. We call any equivalence class of cusp points *a cusp of* Γ.

(e) Show that $\Gamma_0(p)$ has two cusps for any prime number p.

(f) Denote $\pm\Gamma = \langle -I_2, \Gamma\rangle$. Let $\delta \in \mathrm{SL}_2(\mathbb{Z})$ and $\alpha = \delta \cdot \infty$. Show that there exists $h \in \mathbb{Z}_{\geq 1}$ so that

$$\mathrm{Stab}_{\delta^{-1}\pm\Gamma\delta}(\infty) = \langle -I_2, \begin{pmatrix} 1 & h \\ & 1 \end{pmatrix}\rangle.$$

(g) Show the h above satisfies $h = [\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\alpha) : \mathrm{Stab}_{\pm\Gamma}(\alpha)]$. In particular, it is independent of δ.

(h) For a modular form f of Γ of weight k we can write

$$f|_k\delta(z) = \sum_{n=0}^{\infty} a_{n,\delta}(f) e^{2\pi i n z/h},$$

with h as above. We define $\mathrm{ord}_\alpha(f) = \mathrm{ord}_\infty(f|_k\delta) \coloneqq \min\{n,\ a_{n,\delta}(f) = 0\}$. Show that this is independent of δ.

Solution. (a) We propose two solutions (up to you choose how different they are):

- Consider the map

$$\phi\colon \mathbb{H} \to \mathbb{D} \smallsetminus \{0\}; z \mapsto e^{2\pi i z/h},$$

where $\mathbb{D}$ denotes the open unit disk. If we restrict the map to $\mathbb{H}_{-h/2,h/2} \coloneqq \{z \in \mathbb{H}, -h/2 < \mathrm{Re}(z) \leq h/2\}$ this map is bijective and biholomorphic if we restrict the domain further to $\mathrm{Re}(z) < h/2$ with holomorphic inverse $\psi\colon \mathbb{D} \smallsetminus (-1, 0] \to \mathbb{H}_{-h/2,h/2};\ re^{i\theta} \mapsto \frac{h}{2\pi i}(\log|q| + i\theta)$, for $\theta \in (-\pi, \pi)$. We can extend ψ to $\mathbb{D} \smallsetminus \{0\}$ by chosing an argument, for the sake of concreteness $(-1, 0) \ni x \mapsto \frac{h}{2\pi i}(\log|x| + i\pi)$. This map is *not continuous* at any point in $(-1, 0)$.
Consider the map

$$\tilde{f}\colon \mathbb{D} \smallsetminus \{0\} \to \mathbb{C}; q \mapsto f(\psi(q)).$$

We claim, thanks to the periodicity of f, that this map is indeed holomorphic. This would imply that $\tilde{f}$ has a Laurent series with positive convergence radius around 0, i.e. that

$$\tilde{f}(q) = \sum_{n\in\mathbb{Z}} c_n(f) q^n,$$

i.e. with $z = \psi(q)$

$$f(z) = \sum_{n\in\mathbb{Z}} c_n(f) e^{2\pi i n z/h}.$$

We now argue why $\tilde{f}$ is holomorphic. The picture is clear, but the computations is a bit messy and you can avoid to read it if do not really want to go into the details. We show indeed that $\tilde{f}$ is complex differentiable at any $q_0 \in (-1, 0)$. Let $(q_n)_n \subset \mathbb{D} \smallsetminus \{0\}$ be any sequence so that $q_n = r_n e^{i\theta_n} \to q_0$ as $n \to \infty$. We want to show that the limit

$$\frac{\tilde{f}(q_n) - \tilde{f}(q_0)}{q_n - q_0}$$

exists (and it is independent of the sequence). We may assume that $\theta_n \in (-\pi, \pi]$ for all n. The sequence (θ_n) can be partitioned into two sequences (one of them possibly empty) $(\theta_{n_j})_j, (\theta_{n_k})_k$ so that $\theta_{n_j} \to -\pi$ and $\theta_{n_k} \to \pi$. Notice that $\psi(q_{n_j}) \to \psi(q_0) - h$.

$$\begin{aligned}\frac{\tilde{f}(q_{n_j}) - \tilde{f}(q_0)}{q_{n_j} - q_0} &= \frac{f(\psi(q_{n_j})) - f(\psi(q_0))}{\psi(q_{n_j}) + h - \psi(q_0)} \frac{\psi(q_{n_j}) + h - \psi(q_0)}{q_{n_j} - q_0} \\ &= \frac{f(\psi(q_{n_j}) + h) - f(\psi(q_0))}{\psi(q_{n_j}) + h - \psi(q_0)} \frac{\psi(q_{n_j}) + h - \psi(q_0)}{e^{2\pi i(\psi(q_{n_j})+h)/h} - e^{2\pi i(\psi(q_0)/h}},\end{aligned}$$

letting $j \to \infty$ this becomes $f'(\psi(q_0))\frac{h}{2\pi i q_0}$. Similarly (without the need of translation by h) one computes the limit for the sequence (q_{n_k}) and see that it is as well $f'(\psi_(q_0))\frac{h}{2\pi i q_0}$. In particular $\tilde{f}$ is complex differentiable at q_0.

- The alternative (probably cleaner) proposed solution is the following. For fixed $y > 0$ consider the h-periodic function
$$\mathbb{R} \ni x \mapsto f_y(x) = f(x + iy + z).$$
By Fourier analysis there exist Fourier coefficients $c_n(f_y) = c_n(f, y) \in \mathbb{C}$ so that
$$f_y(x) = \sum_{n\in\mathbb{Z}} c_n(f, y)e^{2\pi ix/h}.$$
We now want to understand the y-dependency of the coefficients
$$c_n(f, y) = \frac{1}{h}\int_0^h f(x + iy)e^{-2\pi inx/h}\mathrm{d}x.$$
Since f is holomorphic it satisfies Cauchy-Riemann equations we can use these to gain information on the y derivatives of $c_n(f, y)$, concretely:
$$\begin{aligned}\partial_y c_n(f, y) &= \frac{1}{h}\int_0^h (\partial_y f)(x + iy)e^{-2\pi inx/h}\ \mathrm{d}x \\ &= \frac{i}{h}\int_0^h (\partial_x f)(x + iy)e^{-2\pi inx/h}\ \mathrm{d}x \\ &= \frac{-2\pi n}{h}\frac{1}{h}\int_0^h f(x + iy)e^{-2\pi inx/h}\ \mathrm{d}x = -\frac{2\pi n}{h}c_n(f, y).\end{aligned}$$
The solutions of this functional equation are of the form $c_n(f, y) = c_n(f)e^{-2\pi ny/h}$.

(b) By definition there exists $h \in \mathbb{Z}_{\geq 1}$ so that $\Gamma(h) \leqslant \Gamma$. Recall that $\Gamma(h) \lhd \mathrm{SL}_2(\mathbb{Z})$. The function $f|_k\delta$ transforms like a modular form for the congruence subgroup $\delta^{-1}\Gamma\delta$, which contains $\Gamma(h)$. In particular $\left(\begin{smallmatrix}1 & h\\ & 1\end{smallmatrix}\right) \in \delta^{-1}\Gamma\delta$, and so
$$(f|_k\delta)|_k\begin{pmatrix}1 & h\\ & 1\end{pmatrix} = f|_k\delta,$$
and so we can use the previous subexercise.

(c) This is better viewed using the meromorphic function $\tilde{f}\colon \mathbb{D} \smallsetminus \{0\} \to \mathbb{C}$ so that for any $z \in \mathbb{C}$ we have $\tilde{f}(e^{2\pi iz}) = f(z)$. See the correction of the first bullet for details.

Since zero and poles of a meromorphic function are discrete, there exists a $r \in (0, 1)$ so that $\tilde{f}$ does not have any pole or zero in the disk $\{0 < |z| < r\}$.[1] Hence, f does not have any pole or zero in the region $\mathrm{Im}(z) > \frac{1}{2\pi}\log(1/r)$.

(d) Let $\tilde{f}\colon \mathbb{D} \smallsetminus \{0\} \to \mathbb{C}$ the meromorphic function so that $\tilde{f}(e^{2\pi iz}) = f(z)$ for all $z \in \mathbb{H}$. For any $r \in (0, 1)$ we have, by known results of complex analysis
$$\int_{\partial B_r(0)} \frac{\tilde{f}'(q)}{\tilde{f}(q)}\ \mathrm{d}q = 2\pi i \sum_{q\in B_r(0)} \mathrm{ord}_q(f). \tag{0.1}$$
The integration being anti-clockwise. In particular, if we choose r small enough we have
$$\int_{\partial B_r(0)} \frac{\tilde{f}'(q)}{\tilde{f}(q)}\ \mathrm{d}q = 2\pi i\,\mathrm{ord}_0(\tilde{f}) = 2\pi i\,\mathrm{ord}_\infty(f),$$

[1] Here we are assuming indeed that $\tilde{f}$ has a removable singularity at 0, everything works fine if we only assume that $\tilde{f}$ has at most a pole at 0

where the last equality follows by definition. From the equality $\tilde{f}(e^{2\pi iz}) = f(z)$, we deduce that $\tilde{f}'(e^{2\pi iz}) = \frac{1}{2\pi i}e^{-2\pi iz}f'(z)$

$$\begin{aligned}\int_{\partial B_r(0)} \frac{\tilde{f}'}{f}(q)\,\mathrm{d}q &= \int_0^1 (2\pi ire^{2\pi ix})\frac{\tilde{f}'}{\tilde{f}}(re^{2\pi ix})\,\mathrm{d}x \\ &= \int_0^1 2\pi ie^{2\pi i(x-\frac{i}{2\pi}\log r)}\frac{\tilde{f}'}{f}(e^{2\pi i(x-\frac{i}{2\pi}\log r)})\,\mathrm{d}x \\ &= \int_{-1/2}^{1/2} \frac{f'}{f}(x+i\frac{\log(1/r)}{2\pi})\,\mathrm{d}x.\end{aligned}$$

Hence the desired equality for r (respectively $\frac{1}{r}$) small (resp. $\frac{1}{r}$ big) enough.

(e) Let $\frac{a}{pc} \in \mathbb{Q}$, with $(a, pc) = 1$. Then there exists $b, d \in \mathbb{Z}$ so that $ad - pcb = 1$ and we see that

$$\left(\begin{smallmatrix} a & b \\ pc & d \end{smallmatrix}\right) \cdot \infty = \frac{a}{pc}.$$

Let now $\frac{a}{c} \in \mathbb{Q}$ so that $(ap, c) = 1$. Then there exists $b, d \in \mathbb{Z}$ so that $-apd + bc = 1$ and we have

$$\left(\begin{smallmatrix} b & a \\ pd & c \end{smallmatrix}\right) \cdot 0 = \frac{a}{c}.$$

We proved that $\Gamma_0(p)$ has two cusps and they are represented by ∞ and 0 respectively.

(f) First notice that

$$\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) = \left\{ \begin{pmatrix} \pm 1 & b \\ & \pm 1 \end{pmatrix}, b \in \mathbb{Z} \right\} \simeq \mathbb{Z}/2 \times \mathbb{Z}$$

where the last isomorphism is *as abstract group*. In particular $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)/\{\pm 1\} \simeq \mathbb{Z}$ and each of its subgroups is cyclic. In particular there exists $h \in \mathbb{Z}_{\geq 1}$ so that

$$\langle \begin{pmatrix} 1 & h \\ & 1 \end{pmatrix} \rangle / \{\pm I_2\} = \mathrm{Stab}_{\delta^{-1}\Gamma\delta}(\infty)/\{\pm I_2\} \leqslant \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)/\{\pm I_2\},$$

and so the claim.

(g) Clearly $h = [\mathrm{Stab}_{\mathrm{PSL}_2(\mathbb{Z})}(\infty) : \mathrm{Stab}_{\delta^{-1}\overline{\Gamma}\delta}(\infty)] = [\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) : \mathrm{Stab}_{\delta^{-1}\pm\Gamma\delta}(\infty)]$, where $\overline{\Gamma} = \Gamma/\{\pm I_2\}$. Notice that $\mathrm{Stab}_{\delta^{-1}\pm\Gamma\delta}(\infty) = \delta^{-1}\,\mathrm{Stab}_{\pm\Gamma}(\alpha)\delta$ and $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) = \delta^{-1}\,\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\alpha)\delta$. and so

$$[\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty) : \mathrm{Stab}_{\delta^{-1}\Gamma\delta}(\infty)] = [\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\alpha) : \mathrm{Stab}_{\pm\Gamma}(\alpha)].$$

(h) Suppose $\delta_1 \cdot \infty = \alpha = \delta_2 \cdot \infty$. In particular $\delta_1^{-1}\delta_2 \in \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)$, and so there exists $m \in \mathbb{Z}$ so that $\delta_1^{-1}\delta_2 = \left(\begin{smallmatrix} 1 & m \\ & 1 \end{smallmatrix}\right)$ and so

$$\begin{aligned}\sum_{n=0}^{\infty} a_{n,\delta_1}(f)e^{\frac{2\pi inz}{h}} &= f|_k\delta_1(z) \\ &= f|_k\delta_2(z+m) = \sum_{n=0}^{\infty} a_{n,\delta_2}(f)e^{\frac{2\pi im}{h}}e^{\frac{2\pi inz}{h}}.\end{aligned}$$

It follows that $a_{n,\delta_1}(f) = a_{n,\delta_2}(f)e^{\frac{2\pi im}{h}}$ and so the claim.

Exercise 3. Recall that we defined the principal congruence subgroup $\Gamma(N)$ for any integer $N \geq 1$ as the Kernel of the following group homomorphism

$$\pi_N \colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}); \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a \,(\mathrm{mod}\, N) & b \,(\mathrm{mod}\, N) \\ c \,(\mathrm{mod}\, N) & d \,(\mathrm{mod}\, N) \end{pmatrix}$$

(a) Show that π_N is surjective.

Possible strategy: You may first want to show that for integers $c, d \in \mathbb{Z}$ so that $(c, d, N) = 1$ (that is, there is no prime dividing c, d and N simultaneously), we can find $c', d' \in \mathbb{Z}$ so that $c' \equiv c \,(\mathrm{mod}\, N)$, $d' \equiv d \mod N$ and $(c', d') = 1$.

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

(c) Find isomorphisms of groups

$$\Gamma_1(N)/\Gamma(N) \to \mathbb{Z}/N\mathbb{Z}, \qquad \Gamma_0(N)/\Gamma_1(N) \to (\mathbb{Z}/N\mathbb{Z})^\times.$$

(d) Use the above to compute $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N}(1+\frac{1}{p})$ and $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] = N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$.

Solution. (a) Consider a matrix

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z})$$

so that $ad - bc \equiv 1 \mod (N)$. We want to find a matrix

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

so that $g' \mod (N) \equiv g \mod (N)$.

First we notice that $(a, c, N) = 1$, i.e. there is no prime dividing all the three. Indeed if there would exist a prime $p|a, c, N$, then $p|ad - bc = 1 + kN$ (for some $k \in \mathbb{Z}$) and simultaneously $p|N$, which would imply $p|1$.

We try to find coprime integers a', c' so that $a' \equiv a \mod (N)$ and $c' \equiv c \mod (N)$. For this purpose choose $a' = a$ if $a \neq 0$ otherwise choose $a' = N$. and write $c' = c + k_1 N$ for some k_1 to be chosen. If $p|a'$ we have three possible cases:

- (C1): p divides c but not N,
- (C2): p divides N but not c,
- (C3): p divides neither c nor N.

In particular choose $k_1 \in \mathbb{Z}$ so that if $p|a'$ and p obeys (C1) or (C2), then $k_1 \equiv 1 \mod p$ and otherwise if $p|a'$ and p obeys (C3) then choose k_1 so that $k_1 \equiv 0 \mod p$. This is possible because a' has finitely many prime divisors and because of the Chinese Remainder Theorem.

By construction we have that for any $p|a'$ we have $p \nmid c'$. In particular $(a', c') = 1$.

At this point let $b_0, d_0 \in \mathbb{Z}$ so that $a'd_0 - b_0c' = 1$. Choose

$$b' = b + b_0(1 - (a'd - bc')) \equiv b \mod (N), \qquad d' = d + d_0(1 - (a'd - bc')) \equiv d \mod (N),$$

then

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

has determinant

$$a'd' - b'c' = (a'd - c'b)(1 - (a'd_0 - c'b_0)) + (a'd_0 - c'b_0) = 1$$

and $g' \equiv g \mod (N)$.

We have so

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|.$$

We compute the latter, first by the Chinese remainder Thoerem we notice that

$$\mathrm{SL}_2(\mathbb{Z}/N) \simeq \prod_{p|N} \mathrm{SL}_2(\mathbb{Z}/p^{\mathrm{ord}_p(N)}),$$

in particular it is sufficient to compute the cardinality of $\mathrm{SL}_2(\mathbb{Z}/p^k)$, when p is prime. To do that we count the number of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

such that $ad - bc \in (\mathbb{Z}/p^k)^\times$ and we divide by $\varphi(p^k)$. The entry a can be chosen among p^k numbers. Suppose $p|a$, then we can freely choose d, but both $b, c \in (\mathbb{Z}/p^k)^\times$ (and every choice is fine). If $p \nmid a$, then we have two cases: if $p|d$, this forces $b, c \in (\mathbb{Z}/p)^\times$ (and every choice is fine), if $p \nmid d$ then we have two additional cases: if p divides c, then any choice of b is fine and if $p \nmid c$, then

$$ad - bc \notin (\mathbb{Z}/p^k)^\times \Leftrightarrow b \equiv adc^{-1} \mod p,$$

which happens, once fixed a, c, d, for p^{k-1} b's. so in total we have

$$\begin{aligned}
|\mathrm{SL}_2(\mathbb{Z}/p^k)| &= \frac{1}{\varphi(p^k)} \left(p^{k-1}p^k\varphi(p^k)^2 + \varphi(p^k)(p^{k-1}\varphi(p^k)^2 + \varphi(p^k)(p^{k-1}p^k + \varphi(p^k)(p^k - p^{k-1})))\right) \\
&= \frac{1}{\varphi(p^k)} \left(p^k p^{k-1}\varphi(p^k)^2 + p^{k-1}\varphi(p^k)^3 + p^k p^{k-1}\varphi(p^k)^2 + \varphi(p^k)^4\right) \\
&= \frac{1}{\varphi(p^k)} \left(2p^k p^{k-1}\varphi(p^k)^2 + p^k\varphi(p^k)^3\right) \\
&= p^k\varphi(p^k)(2p^{k-1} + \varphi(p^k)) \\
&= p^{3k}(1 - 1/p)(1 + 1/p) = p^{3k}(1 - 1/p^2).
\end{aligned}$$

In particular we infer

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

(b) Consider the map

$$\Gamma_1(N) \to \mathbb{Z}/N; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b,$$

it is a group homomorphism since for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$ we have $a \equiv d \equiv 1 \mod (N)$. The kernel is easily seen to be $\Gamma(N)$.

Also the group homomorphism

$$\Gamma_0(N) \to (\mathbb{Z}/N)^\times; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d$$

induces an isomorphism $\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$

(c) We have

$$[\Gamma_1(N) : \Gamma(N)] = N.$$

And $[\Gamma_0(N) : \Gamma_1(N)] = \varphi(N)$. Hence

$$[\Gamma_0(N) : \Gamma(N)] = \varphi(N)N$$

Exercise 4 (graded). (a) Prove that $\mathrm{SL}_2(\mathbb{Z})$ is generated by $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$

(b) Consider the fundamental domain $\mathrm{SL}_2(\mathbb{Z})$ seen in class

$$\mathcal{F} = \{z \in \mathbb{H},\ -1/2 < \mathrm{Re}(z) \leq 1/2,\ |z| > 1 \text{ if } \mathrm{Re}(z) < 0, |z| \geq 1 \text{ if } \mathrm{Re}(z) \geq 0\}.$$

Draw $T \cdot \mathcal{F}$, $S \cdot \mathcal{F}$, and $ST^2S \cdot \mathcal{F}$.

(c) Find representatives for $\Gamma_0(3) \setminus \mathrm{SL}_2(\mathbb{Z})$. You may want to use Exercise 3d.

(d) Draw a fundamental region[2] for $\Gamma_0(3)$.

Solution. (a) Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. If $c = 0$, then we have $a = d = \pm 1$. After multiplying by $S^2 = -I_2$ if necessary we may assume that $a = d = 1$, i.e. $\gamma = \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} = T^b$. Suppose now that $c \neq 0$. Then there exist $q, r \in \mathbb{Z}$, $0 \leq r < |c|$, with $a = qc + r$. Hence,

$$ST^{-q}\gamma = \begin{pmatrix} -c & -d \\ r & b - qd \end{pmatrix}.$$

If $r = 0$, then we are in the first case we considered. Otherwise, there exist $q_2, r_2 \in \mathbb{Z}$, $0 \leq r_2 < r$ so that

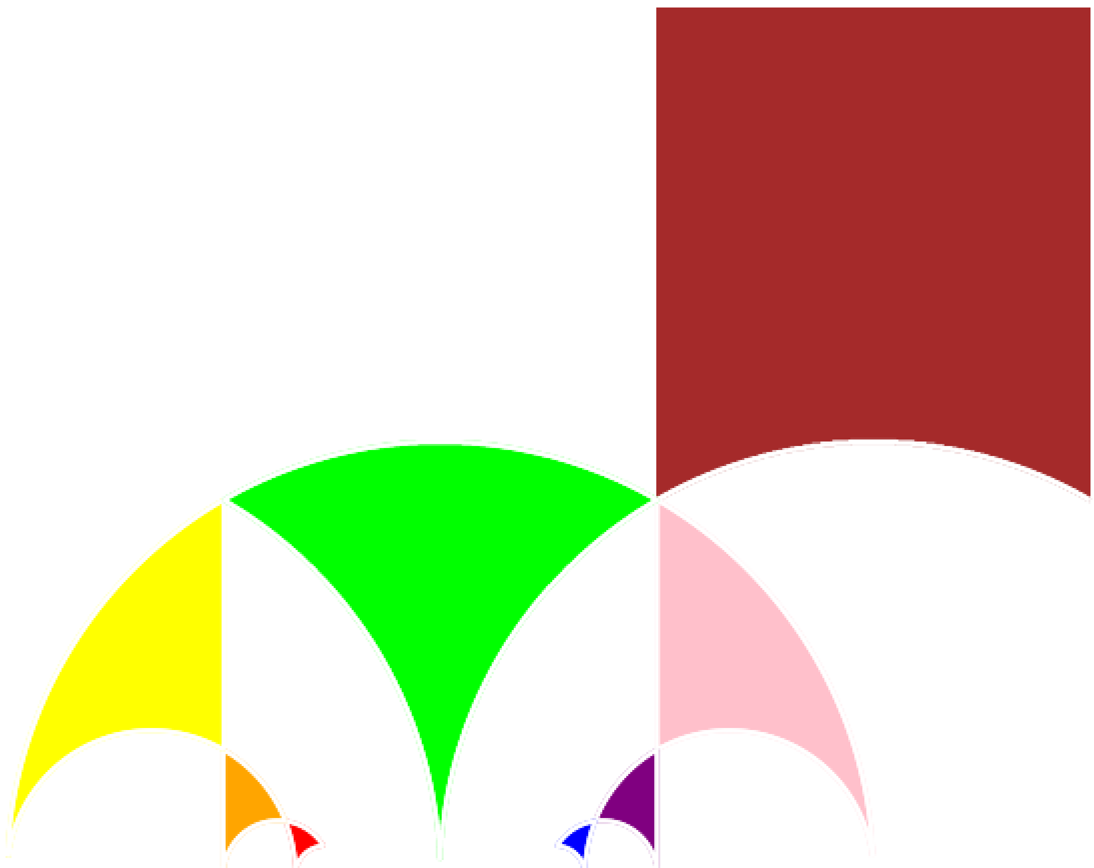
$$ST^{-q_2}ST^{-q_1}\gamma = \begin{pmatrix} -r & b' \\ r_2 & d' \end{pmatrix},$$

for some $b', d' \in \mathbb{Z}$. This algorithm takes at most $|c|$ steps to obtain a remainder $r_m = 0$ and it shows that there exists $q_1, \ldots, q_m \in \mathbb{Z}$ so that

$$\gamma = \pm ST^{q_m} \cdots ST^{q_1}.$$

(b) See the following picture. I avoided the axes for aesthetic reasons. In brown you can see $T\mathcal{F}$, in lime you can see $S\mathcal{F}$, in yellow, orange and red you can see $ST^{-1}S\mathcal{F}, ST^{-2}S\mathcal{F}, ST^{-3}S\mathcal{F}$ respectively. In pink, purple and blue you can see $STS\mathcal{F}, ST^2S\mathcal{F}$ and $ST^3S\mathcal{F}$. I produced the images with the Sage online editor and apparently the legend is not working for the regionplot function.

[2]By region I mean that it has not to be connected. A connected fundamental region is usually called fundamental domain.



(c) By Exercise 3d we need to find 4 matrices in $\mathrm{SL}_2(\mathbb{Z})$ that are $\Gamma_0(3)$-inequivalent. One sees that $\gamma_j = \left(\begin{smallmatrix} 1 & \\ j & 1 \end{smallmatrix}\right)$, $j = -1, 0, 1$, are pairwise inequivalent. In fact for $j \neq k \in \{-1, 0, 1\}$ we have

$$\begin{pmatrix} 1 & \\ j & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ -k & 1 \end{pmatrix} = \begin{pmatrix} 1 & \\ j-k & 1 \end{pmatrix} \notin \Gamma_0(3).$$

We have for $j \in \{-1, 0, 1\}$ that

$$\begin{pmatrix} 1 & \\ j & 1 \end{pmatrix} S^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & j \end{pmatrix} \notin \Gamma_0(3).$$

In particular we see that

$$\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(3) \sqcup \Gamma_0(3)\gamma_{-1} \sqcup \Gamma_0(3)\gamma_1 \sqcup \Gamma_0(3)S.$$

(d) First we prove the following: Let $\Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$ be a finite index subgroup and suppose $-I_2 \in \Gamma$ and $\Gamma \setminus \mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_i' \Gamma\gamma_i$, where the dash is there to indicate a finite union. Then

$$\mathcal{G} = \bigcup_i{}' \gamma_i \mathcal{F}$$

is (almost) a fundamental domain for the action of Γ on $\mathbb{H}$. One may need to pay extra attention to the elliptic points if one really want a fundamental domain (or region). Strictly speaking, if $z' \in \mathcal{F}$ is an elliptic point (i.e. either i or $e^{\pi i/3}$), then it might be that there exists γ_j, γ_i representatives and $\delta \in \Gamma$ so that $\delta\gamma_i z' = \gamma_j z'$, that is $\delta \in \gamma_j \operatorname{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(z')\gamma_i^{-1}$, or at least I can not see a reason to exclude this. Anyway, this is not so important as it suffices to eventually remove finitely many points and the quality of the picture does not change.

For the following picture (which gives in fact a connected fundamental domain) I used the following representatives: $I_2, ST = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right), ST^{-1} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right), S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. This is a set of representatives, since $TST = \left(\begin{smallmatrix} 1 & \\ 1 & 1 \end{smallmatrix}\right)$, $T \in \Gamma_0(3)$, $-T^{-1}ST^{-1} = \left(\begin{smallmatrix} 1 & \\ -1 & 1 \end{smallmatrix}\right)$, $-T^{-1} \in \Gamma_0(3)$.