MODULAR FORMS EXAMPLE SHEET 4

1a. Show that the group $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ (p prime) has order $p(p^2-1)$.

The rows of an element of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ are a pair of linearly independent vectors v_1, v_2 in $(\mathbb{Z}/p\mathbb{Z})^2$. There are p^2-1 choices for v_1, and for any fixed v_1, p vectors v_2 that are scalar multiples of v_2. Thus there are p^2-p vectors v_2 such that v_1, v_2 is linearly independent. The matrix with rows v_1 and v_2 is then invertible, so its determinant is a unit in $\mathbb{Z}/p\mathbb{Z}$. Rescaling v_2 so that the determinant is 1 reduces the number of choices for v_2 from p^2-p to p. Thus there are $p(p^2-1)$ choices for v_1 and v_2 together.

1b. Show by induction on e that $\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ has order $p^{3e}(1-\frac{1}{p^2})$.

It suffices to show that the kernel of $\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^{e-1}\mathbb{Z})$ has order p^3. An element of this kernel has the form $\begin{pmatrix} 1+p^{e-1}a & p^{e-1}b \\ p^{e-1}c & 1+p^{e-1}d \end{pmatrix}$, with a, b, c, d well-defined modulo p. The determinant is 1 mod p^e iff $a+d$ is zero mod p. There are thus p^3 choices for a, b, c, and these choices determine d uniquely as an element of $\mathbb{Z}/p\mathbb{Z}$.

1c. Show that $\Gamma(N)$ has index $N^3\prod_{p|N}(1-\frac{1}{p^2})$ in $\mathrm{SL}_2(\mathbb{Z})$, where the product is over all prime divisors p of N.

It is equvialent to show that this is the order of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. This follows easily from 1b and the Chinese Remainder Theorem.

1d. Show that $\Gamma_1(N)$ has index $N^2\prod_{p|N}(1-\frac{1}{p^2})$ in $\mathrm{SL}_2(\mathbb{Z})$.

The quotient $\Gamma_1(N)/\Gamma(N)$ is isomorphic to the strictly upper triangular matrices with entries in $\mathbb{Z}/N/\mathbb{Z}$; this is a cyclic group of order N. The result thus follows from 1c.

1e. Show that $\Gamma_0(N)$ has index $N\prod_{p|N}(1+\frac{1}{p})$ in $\mathrm{SL}_2(\mathbb{Z})$.

The quotient $\Gamma_0(N)/\Gamma_1(N)$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$; this has order $N\prod_{p|N}(1-\frac{1}{p})$. The result thus follows from 1d.

2. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, containing $\pm I$. Let $x \in \mathbb{Q}\cup\{\infty\}$. Let Z_x denote the stabilizer of x in $\mathrm{SL}_2(\mathbb{Z})$, and let $\Gamma_x = Z_x \cap \Gamma$. The *width* of the cusp x (relative to the congruence subgroup Γ) is the index $[Z_x : \Gamma_x]$, and is denoted $R_\Gamma(x)$.

2a. Show that for $\gamma \in \Gamma$, one has $R_\Gamma(\gamma x) = R_\Gamma(x)$.

We have $Z_{\gamma x} = \gamma Z_x \gamma^{-1}$, so $\Gamma_{\gamma x} = \gamma\Gamma_x\gamma^{-1}$. Now $R_{\gamma x} = [Z_{\gamma x} : \Gamma_{\gamma x}] = [\gamma Z_x\gamma^{-1} : \gamma\Gamma_x\gamma^{-1}] = R_x$.

2b. For x, y in $\mathbb{Q} \cup \{\infty\}$, let $Z_{x,y}$ denote the set $\{\delta \in \mathrm{SL}_2(\mathbb{Z}) : \delta x \in \Gamma \cdot y\}$. Show that for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma x = y$, $Z_{x,y}$ is equal to the "double coset" $\Gamma\gamma Z_x$ of elements of $\mathrm{SL}_2(\mathbb{Z})$ of the form $\gamma'\gamma z$ for $\gamma' \in \Gamma$, and $z \in Z_x$.

It is clear that any element of $\Gamma\gamma Z_x$ takes x to an element of the Γ-orbit of y. To show the other inclusion, let $\delta \in Z_{x,y}$. Then there exists γ' in Γ that takes y to δx. Then $(\gamma)^{-1}(\gamma')^{-1}\delta x = x$, so $(\gamma)^{-1}(\gamma')^{-1}\delta$ is an element z of Z_x. But then $\delta = \gamma'\gamma z$ lies in $\Gamma\gamma Z_x$.

2b. For x, y in $\mathbb{Q} \cup \{\infty\}$, let $Z_{x,y}$ denote the set $\{\delta \in \mathrm{SL}_2(\mathbb{Z}) : \delta x \in \Gamma \cdot y\}$. Show that for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma x = y$, $Z_{x,y}$ is equal to the "double coset" $\Gamma\gamma Z_x$ of elements of $\mathrm{SL}_2(\mathbb{Z})$ of the form $\gamma'\gamma z$ for $\gamma' \in \Gamma$, and $z \in Z_x$.

By definition, the set HgK is the (non-disjoint) union of the cosets Hgk for $k \in K$. For k, k' in K, Hgk intersects Hgk' if and only if they are equal. This occurs if, and only if, there exists h in H such that $gk = hgk'$, or, equivalently, if there exists h in H such that $gk(k')^{-1}g^{-1} = h$. The latter holds if, and only if, $k(k')^{-1}$ lies in $g^{-1}Hg$ (and hence in $K \cap g^{-1}Hg$.) In particular, $Hgk = Hgk'$ if, and only if the cosets $(K \cap g^{-1}Hg)k$ and $(K \cap g^{-1}Hg)k'$ coincide. This gives a bijection betweeen the cosets of H in HgK and the cosets of $K \cap g^{-1}Hg$ in K. Conjugating by g gives a bijection between these cosets and the cosets of $gKg^{-1} \cap H$ in gKg^{-1}.

2d. Show that the sum of $R_\Gamma(x)$, as x runs over a set of representatives for the Γ-orbits in $\mathbb{Q} \cup \infty$, is equal to the index of Γ in $\mathrm{SL}_2(\mathbb{Z})$. [HINT: write $\mathrm{SL}_2(\mathbb{Z})$ as a disjoint union of cosets $\Gamma\gamma_i$, and for each Γ-orbit Γx in $\mathbb{Q} \cup \infty$, count the number of such cosets that take ∞ to a point in Γx.]

Write $\mathrm{SL}_2(\mathbb{Z})$ as a disjoint union of cosets $\Gamma\gamma_i$ for $\gamma_1, \ldots, \gamma_r \in \mathrm{SL}_2(\mathbb{Z})$. Let $\{x_j\}$ represent the set of Γ-orbits on $\mathbb{Q} \cup \{\infty\}$. Since $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{Q} \cup \{\infty\}$, every element of $\mathbb{Q} \cup \{\infty\}$ is in the Γ-orbit of $\gamma_i x_1$ for some i. For each j, fix a δ_j from the set $\{\gamma_1, \ldots, \gamma_r\}$ such that $\delta_j x_1$ is in the Γ-orbit of x_j. Then for each j, the set Z_{x_1,x_j} is the double coset $\Gamma\delta_j Z_{x_1}$. We have shown that Z_{x_1,x_j} is the union of n_j right cosets of Γ, where n_j is the index of $\delta_j Z_{x_1}\delta_j^{-1} \cap \Gamma$ in $\delta_j Z_{x_1}\delta_j^{-1}$. Since $\delta_j Z_{x_j}\delta_j^{-1} = Z_{x_j}$, we have $n_j = R_\Gamma(x_j)$.

Now $\mathrm{SL}_2(\mathbb{Z})$ is the disjoint union of Z_{x_1,x_j} over all j. Since each of these is the disjoint untion of $R_\Gamma(x_j)$ cosets of Γ, the sum of the $R_\Gamma(x_j)$ is equal to the index of Γ in $\mathrm{SL}_2(\mathbb{Z})$.

3a. Find a set of representatives for the set of cusps of the congruence subgroups $\Gamma_0(4), \Gamma_0(6)$, and $\Gamma_1(5)$, and find their widths.

$\Gamma_0(4)$: Note that there are two $\Gamma_0(2)$-orbits (those of 0 and ∞) on $\mathbb{Q} \cup \{\infty\}$. Since $\Gamma_0(4)$ has index 2 in $\Gamma_0(2)$, each of these orbits breaks up into at most two orbits for $\Gamma_0(4)$. It is easy to see that the orbit of 0 under both $\Gamma_0(2)$ and $\Gamma_0(4)$ consists of all fractions of the form $\frac{b}{d}$ with d odd. By contrast, The $\Gamma_0(4)$-orbit of ∞ consists of ∞ together with all fractions of the form $\frac{a}{c}$ with $4|c$, a odd. Note that $\frac{1}{2}$ is therefore not in the $\Gamma_0(4)$-orbit of ∞,

but is in the $\Gamma_0(2)$-orbit. Thus the $\Gamma_0(2)$-orbit of ∞ breaks up into two $\Gamma_0(4)$-orbits: those of ∞ and $\frac{1}{2}$.

The stabilizer of ∞ in $\mathrm{SL}_2(\mathbb{Z})$ is the group of matrices of the form $\pm T^n$; all of these lie in $\Gamma_0(4)$, so the width of ∞ is 1. The stabilizer of 0 is matrices of the form $\pm \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$, and such a matrix lies in $\Gamma_0(4)$ if, and only if, n is divisibly by 4, so the width of 0 is 4. The widths sum to the index of $\Gamma_0(4)$ in $\mathrm{SL}_2(\mathbb{Z})$, which is 6, so the remaining cusp $\frac{1}{2}$ must have width 1.

$\Gamma_0(6)$: Note that $\Gamma_0(6)$ is the intersection of $\Gamma_0(2)$ (which has index 3 in $\mathrm{SL}_2(\mathbb{Z})$) with $\Gamma_0(3)$ (which has index 4 in $\mathrm{SL}_2(\mathbb{Z})$.) So $\Gamma_0(6)$ has index 12 in $\mathrm{SL}_2(\mathbb{Z})$. Moreover, every intersection of a $\Gamma_0(2)$-orbit with a $\Gamma_0(3)$-orbit is stable under $\Gamma_0(6)$, and is thus a union of $\Gamma_0(6)$-orbits.

There are two $\Gamma_0(2)$-orbits: those of zero and ∞, and likewise two $\Gamma_0(3)$-orbits (also represented by zero and ∞). We have:

- 0 is in the orbit of 0 under both $\Gamma_0(2)$ and $\Gamma_0(3)$: it has width six for $\Gamma_0(6)$ by the same argument as for $\Gamma_0(4)$.
- ∞ is in the orbit of ∞ under both $\Gamma_0(2)$ and $\Gamma_0(3)$; it has width one.
- $\frac{1}{2}$ is in the orbit of ∞ for $\Gamma_0(2)$ and of 0 for $\Gamma_0(3)$.
- $\frac{1}{3}$ is in the orbit of 0 for $\Gamma_0(2)$ and of ∞ for $\Gamma_0(3)$.

The widths sum to 12, so the widths of $\frac{1}{2}$ and $\frac{1}{3}$ sum to at most 5, with equality if, and only if, they are the only cusps other than 0 and ∞. On the other hand, the width of $\frac{1}{2}$ for $\Gamma_0(6)$ is divisible by its width for $\Gamma_0(3)$, by definition, and this latter width is 3. Similarly 2 divides the width of $\frac{1}{3}$. These widths must therefore be 3 and 2, respectively, and the list above must be a complete list of cusps for $\Gamma_0(6)$.

$\Gamma_1(5)$: We replace $\Gamma_1(5)$ with $\pm\Gamma_1(5)$, so we can use the theory of widths developed in the last question. The group $\pm\Gamma_1(5)$ has index 2 in $\Gamma_0(5)$, and hence index 12 in $\mathrm{SL}_2(\mathbb{Z})$.

There are two orbits of $\Gamma_0(5)$ on $\mathbb{Q} \cup \{\infty\}$: those of 0 and ∞. We have $\Gamma_1(5) \subset \pm\Gamma_1(5) \subset \Gamma_0(5)$, each with index 2, and (since -1 acts trivially), the orbits of $\Gamma_1(5)$ and $\pm\Gamma_1(5)$ on $\mathbb{Q} \cup \{\infty\}$ are the same. Thus the orbits of 0 and ∞ under $\Gamma_0(5)$ each decompose into at most two orbits under $\Gamma_1(5)$.

The orbit of ∞ under $\Gamma_0(5)$ consists of all $\frac{a}{c}$ with 5 dividing c but not a. Under $\Gamma_1(5)$, the orbit of ∞ consists of all $\frac{a}{c}$ with 5 dividing c and $a \equiv 1 \pmod 5$. In particular $\frac{2}{5}$ is in the $\Gamma_0(5)$-orbit of ∞ but not the $\Gamma_1(5)$-orbit. Thus the $\Gamma_0(5)$-orbit of ∞ is the union of the $\Gamma_1(5)$-orbits of ∞ and $\frac{2}{5}$.

Similarly, the $\Gamma_0(5)$-orbit of 0 is the union of the $\Gamma_1(5)$-orbits of 0 and $\frac{1}{2}$. The width of each of these cusps is divisible by the width of 0 for $\Gamma_0(5)$; that is, by 5.

We thus have four cusps, two of which have width divisible by 5, whose widths (for $\pm\Gamma_1(5)$ sum to 12. The two cusps with width divisible by 5 must thus have width exactly 5, and the remaining two cusps must have width 1.

4a. Show that the group $\Gamma_0(4)$ is generated by the matrices $\pm\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and $\pm\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}$.

Let T denote the matrix $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, and let U denote the matrix $\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}$. Left multiplication by T adds the bottom row of a matrix to the top; right multiplication by T adds the left column of a matrix to its right column. Similarly, left multiplication by U adds 4 times the top row to the bottom row, and right multiplication by U adds 4 times the right column to the left column. We must show we can reduce any matrix in $\Gamma_0(4)$ to ± 1 by these operations.

Given $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, with c nonzero, we can multiply by T (or its inverse) on the right a number of times to get a new matrix $\begin{pmatrix}a & b'\\ c & d'\end{pmatrix}$ with $|d'| < \frac{|c|}{2}$. (We won't get equality because c and d are relatively prime). Multiplying by a power of U on the right, we can get a new matrix $\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}$ with $|c'| < 2|d'| < |c|$. Iterating, we eventually obtain $c = 0$. If $c = 0$ the matrix is $\pm T^n$ for some n, and we are done.

4b. Show that for $n > 6$, the matrices $\pm\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and $\pm\begin{pmatrix}1 & 0\\ n & 1\end{pmatrix}$ do *not* generate $\Gamma_0(n)$.

Under the isomorphism $\Gamma_0(n)/\Gamma_1(n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, the above matrices all have image ± 1.