18.785 Analytic Number Theory Problem Set #3

Holden Lee

2/21/11

Problem 1 *(Invariant measure)*

(A) Bruhat decomposition

Since $S \in \mathrm{SL}_2(\mathbb{R})$, $B \cup BSB \subseteq \mathrm{SL}_2(\mathbb{R})$.

Now we show that for $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{R})$, $M \in B$ iff $c = 0$ and $M \in BSB$ iff $c \neq 0$. The first is obvious. For the second, note that the matrices in BSB are in the form

$$\begin{bmatrix} e & f \\ 0 & e^{-1} \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} g & h \\ 0 & g^{-1} \end{bmatrix} = \begin{bmatrix} fg & fh - eg^{-1} \\ e^{-1}g & e^{-1}h \end{bmatrix}, \quad e, g \neq 0.$$

The lower left entry is hence nonzero. Conversely, if $c = 0$, then M can be written in the above form by letting

$$\begin{aligned} e &= c^{-1} \\ f &= a \\ g &= 1 \\ h &= dc^{-1}. \end{aligned}$$

(Note this gives $b = \frac{ad-1}{c}$ which is true since $\det(M) = 1$.) Hence $M \in BSB$. This shows $\mathrm{SL}_2(\mathbb{R}) = B \sqcup BSB$.

(B)

1. $|y|^{-2}dxdy$ is invariant under diagonal matrices: The matrix $\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \in \mathrm{SL}_2(\mathbb{R})$ corresponds to the transformation $z \mapsto cz$ or $x + yi \mapsto cx + cyi$, where $c = a^2$. Then $|y|^{-2}dxdy$ becomes
$$|cy|^{-2}d(cx)d(cy) = |y|^{-2}dxdy.$$

2. $|y|^{-2}dxdy$ is invariant under unipotent matrices: The matrix $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ corresponds to the transformation $z \mapsto z + a$, or $x + yi \mapsto (x + a) + yi$. Then $|y|^{-2}dxdy$ becomes
$$|y|^{-2}d(x + a)dy = |y|^{-2}dxdy.$$

3. $|y|^{-2}dxdy$ is invariant under S: S corresponds to the transformation $z \mapsto -\frac{1}{z}$, or $r \operatorname{cis}\theta \mapsto -\frac{1}{r}\operatorname{cis}(-\theta)$. Noting that the Jacobian from rectangular to polar coordinates is r,

$$|y|^{-2}dxdy = \frac{r}{|r\sin\theta|^2}drd\theta.$$

Under S, this gets sent to

$$\frac{\frac{1}{r}}{\left|\frac{1}{r^2}\sin\theta\right|^2}d\left(-\frac{1}{r}\right)d(-\theta) = \frac{-r^3}{|r\sin\theta|^2}\cdot\frac{dr}{r^2}\cdot(-d\theta) = \frac{r}{|r\sin\theta|^2}drd\theta,$$

which is the same as the original expression.

Now note that $B = DU$, where D is the subgroup of diagonal matrices in $\mathrm{SL}_2(\mathbb{R})$ and U is the subgroup of unipotent matrices, as

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}\begin{bmatrix} 1 & ba^{-1} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix}.$$

Since $|y|^{-2}$ is invariant under D, U, and S, it is invariant under B and BSB. Hence by the Bruhat decomposition it is invariant under $\mathrm{SL}_2(\mathbb{R})$.

Problem 2 *(Genus)*

(A)

By the Riemann-Hurwitz formula, for $f : \mathcal{R} \to \mathcal{R}'$ a holomorphic map of compact Riemann surfaces that is m-to-1 at finitely many points,

$$2g(\mathcal{R}) - 2 = m(2g(\mathcal{R}') - 2) + \sum_{p\in\mathcal{R}}(e_p - 1), \tag{1}$$

where e_p is the ramification index of p. We also have the following: For $p' \in \mathcal{R}'$,

$$m = \sum_{p\in\mathcal{R}, f(p)=p'} e_p. \tag{2}$$

Let $\Gamma' = \mathrm{SL}_2(\mathbb{Z})$. For a group $G \subseteq \mathrm{SL}_2(\mathbb{Z})$, let $\overline{G}$ denote its image in $\mathrm{PSL}_2(\mathbb{Z})$. Putting in $\mathcal{R}' = \Gamma'\backslash\mathcal{H}^*$ and $\mathcal{R} = \Gamma\backslash\mathcal{H}^*$, and noting that $g(\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}^*) = 0$, $m = \mu = [\Gamma' : \Gamma]$, (1) becomes

$$g(\Gamma\backslash\mathcal{H}^*) = 1 - \mu + \frac{1}{2}\sum_{p\in\Gamma\backslash\mathcal{H}^*}(e_p - 1).$$

Now the only nonequivalent cusp of Γ' is ∞ and the only nonequivalent elliptic points of Γ' are i and $\omega = e^{\frac{2\pi i}{3}}$, by Proposition 3.5.3. Thus the stabilizer of any elliptic point z of $\overline{\Gamma'}$ is a subgroup $\overline{\Gamma'}_z$ conjugate to one of the following subgroups.

$$\overline{\Gamma'}_\omega = \left\{\pm I, \pm\left[\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right], \pm\left[\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right]\right\} \tag{3}$$

$$\overline{\Gamma'}_i = \left\{\pm I, \pm\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\right\} \tag{4}$$

These groups have order 2 and 3 in $\mathrm{PSL}_2(\mathbb{Z})$, respectively. If $z \in \mathcal{H}^*$ elliptic in $\Gamma' = \mathrm{SL}_2(\mathbb{Z})$ remains elliptic under Γ, we must have $\Gamma'_z \subseteq \Gamma$; in this case $e_z = [\overline{\Gamma'}_z : \overline{\Gamma}_z] = 1$. Otherwise, $e_z = [\overline{\Gamma'}_z : \overline{\Gamma}_z] = |\overline{\Gamma'}_z|$.

First consider the points of $\Gamma\backslash\mathcal{H}^*$ lying over i. Note ν_2 is the number of such points with $e_z = 1$. Let a be the number of points with $e_z = 2$. By (2),

$$\mu = 2a + \nu_2,$$

so $a = \frac{\mu-\nu_2}{2}$. Hence

$$\sum_{p\in\Gamma\backslash\mathcal{H}^*,\, f(p)=i} (e_p - 1) = a = \frac{\mu - \nu_2}{2}. \tag{5}$$

Next consider the points of $\Gamma\backslash\mathcal{H}^*$ lying over ω. Note ν_3 is the number of points with $e_z = 1$. Let b be the number of points with $e_z = 3$. By (2),

$$\mu = 3a + \nu_3,$$

so $a = \frac{\mu-\nu_3}{3}$. Hence

$$\sum_{p\in\Gamma\backslash\mathcal{H}^*,\, f(p)=\omega} (e_p - 1) = a = \frac{2(\mu - \nu_3)}{3}. \tag{6}$$

Finally consider the cusps of $\overline{\Gamma}$. We claim that if p is a cusp of Γ', then it is a cusp of Γ. Indeed, if γ is a parabolic element of Γ' fixing p, then since Γ has finite index in Γ', some nonzero power γ^m is contained in Γ; it fixes p. (Note $\gamma^m \neq I$ since γ has infinite order.) Hence using (2),

$$\sum_{p\in\Gamma\backslash\mathcal{H}^*,\, f(p)=\infty} (e_p - 1) = \left(\sum_{p\in\Gamma\backslash\mathcal{H}^*,\, f(p)=\infty} e_p\right) - \nu_\infty = \mu - \nu_\infty. \tag{7}$$

We've accounted for all elliptic points and cusps of Γ. Putting (5), (6), and (7) into (1) gives

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}. \tag{8}$$

(B)

Below, p will always represent a prime.

Lemma 2.1:

$$[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma_0(N)}] = N \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

Proof. Let G be the group

$$\{(a, y) | a \in (\mathbb{Z}/N\mathbb{Z})^\times, y \in \mathbb{Z}/N\mathbb{Z}\}/\{\pm(1, 0)\}$$

with the operation

$$(a, y)(a', y') = (aa', ay' + a'^{-1}y).$$

The fact that G is a group can be shown directly, or by noting that the group structure on G is the "pushforward" of the group structure on $\Gamma_0(N)$ by π below. We claim that

$$1 \to \overline{\Gamma(N)} \to \overline{\Gamma_0(N)} \xrightarrow{\pi} G \to 1$$

is a short exact sequence, where

$$\pi\left(\begin{bmatrix} a & b \\ Nc & d \end{bmatrix}\right) = (a, b) \bmod N.$$

We verify:

1. π is surjective: Given $(\overline{a}, \overline{b}) \in G$, we can choose b so that $a \equiv \overline{a} \pmod N, b \equiv \overline{b} \pmod N$ so that $\gcd(a, b) = 1$. Let d be an integer such that $ad \equiv 1 \pmod N$. By Bézout's Theorem we can find k, l so that $ak - lb = \frac{1-ad}{N}$. Then $a(d + kN) - Nlb = 1$, and the following matrix is in $\mathrm{SL}_2(\mathbb{Z})$.

$$\pi\left(\begin{bmatrix} a & b \\ Nl & d + kN \end{bmatrix}\right) = (a, b).$$

2. $\ker(\pi) = \overline{\Gamma(N)}$: The inclusion $\overline{\Gamma(N)} \subseteq \ker(\pi)$ is clear. Conversely, if $A = \begin{bmatrix} a & b \\ Nc & d \end{bmatrix} \in \Gamma_0(N)$, $\pi(A) = (1, 0)$, then $a \equiv 1 \pmod N$ and $b \equiv 0 \pmod N$; moreover $ad - (Nc)d = 1$ and $a \equiv 1 \pmod N$ imply $b \equiv 1 \pmod N$.

First suppose $N \neq 2$. Then $|G| = \frac{1}{2}\varphi(N)N$, so

$$[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma_0(N)}] = \frac{[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma(N)}]}{|G|} = \frac{\frac{N^3}{2}\prod_{p|N}\left(1 - \frac{1}{p^2}\right)}{N\prod_{p|N}\left(1 - \frac{1}{p}\right)} = N\prod_{p|N}\left(1 + \frac{1}{p}\right).$$

For $N = 2$, $[\mathrm{PSL}_2(\mathbb{Z}), \overline{\Gamma(N)}] = 6$ and $|G| = 2$, so $[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma_0(N)}] = 3$ (and the above formula works as well). □

Lemma 2.2: The equivalence classes of elliptic points of order 2 in $\Gamma_0(N)$ are in bijection with the solutions to $a^2 + 1 \equiv 0 \pmod N$, and the elliptic points of order 3 in $\Gamma_0(N)$ are in bijection with the solutions to $a^2 + a + 1 \equiv 0 \pmod N$.

Proof. Let z be an elliptic point of order 2 in $\Gamma_0(N)$. Its stabilizer subgroup in $\mathrm{PSL}_2(\mathbb{Z})$ is conjugate to (4), and must be the same as the stabilizer subgroup in $\overline{\Gamma_0(N)}$. Let $\gamma z = z$ with $\gamma \neq \pm 1$. Then γ is conjugate to $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and has characteristic polynomial $x^2 + 1$. It must have trace 0 and be in $\overline{\Gamma_0(N)}$. Hence modulo N it is in the form

$$\begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix}, \quad a + a^{-1} \equiv 0 \pmod N. \tag{9}$$

This gives a so that $a^2 + 1 \equiv 0 \pmod N$. Note that the map $z \mapsto a$ is well-defined because equivalent z get sent to the same a: If z_1 and z_2 are elliptic points with $\gamma_j z_j = z_j, \gamma_j \neq \pm I$

and $\tau z_1 = z_2, \tau \in \overline{\Gamma_0(N)}$, then $\tau\gamma_1\tau^{-1}z_2 = z_2$ so $\tau\gamma_1\tau^{-1} = \gamma_2$. Working modulo N, we write $\gamma_1 = \left[\begin{smallmatrix} a & b \\ 0 & a^{-1} \end{smallmatrix}\right]$, $\tau = \left[\begin{smallmatrix} c & d \\ 0 & c^{-1} \end{smallmatrix}\right]$ and hence

$$\gamma_2 = \tau\gamma_1\tau^{-1} = \begin{bmatrix} a & -ad + c^2b + ca^{-1}d \\ 0 & a^{-1} \end{bmatrix}$$

which has the same upper-left-hand entry.

Let m be the number of solutions to $a^2 + 1 \equiv 0 \pmod{N}$. Note for every such solution, $\left[\begin{smallmatrix} a & 1 \\ -a^2-1 & -a \end{smallmatrix}\right]$ is an elliptic matrix with upper lefr corner a, so there are at least m $\Gamma_0(N)$-inequivalent elliptic points of order 2. It suffices to show there are at most m distinct elliptic points of order 2.

Lemma 2.3: For each

$$(z, t) \in P := \frac{(\mathbb{Z}/N\mathbb{Z})^2 - \{(0, 0)\}}{(\mathbb{Z}/N\mathbb{Z})^\times}$$

take an integer matrix of the form $\left[\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right]$. These matrices form a set of right coset representatives for $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ (or of $\overline{\Gamma_0(N)}$ in $\mathrm{PSL}_2(\mathbb{Z})$).

Proof. First note that coset representatives for $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ correspond to coset representatives for $\Gamma_0(N)/\Gamma(N)$ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Thus we work modulo N. We show that the map (of sets)

$$\begin{aligned} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \backslash (\Gamma_0(N)/\Gamma(N)) &\to P \\ \begin{bmatrix} x & y \\ z & t \end{bmatrix} &\mapsto (z, t) \end{aligned}$$

is well-defined and bijective. For each $(z, t) \in P$ we can find a matrix of the above form by Bézout, so this map is surjective.

First, it is well-defined: If $\left[\begin{smallmatrix} a^{-1} & b \\ 0 & a \end{smallmatrix}\right] \in \Gamma(N)$, then

$$\begin{bmatrix} a^{-1} & b \\ 0 & a \end{bmatrix} \begin{bmatrix} x & y \\ z & t \end{bmatrix} = \begin{bmatrix} a^{-1}x + bz & a^{-1}y + bt \\ az & at \end{bmatrix}. \tag{10}$$

whose bottom row is just the original multiplied by a.

It remains to show that the map is injective, i.e. every matrix in the form $\left[\begin{smallmatrix} x' & y' \\ az & at \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ with $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ is in the same coset. Suppose $\left[\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is the coset representative. Assume $z \neq 0$ (if $z = 0$, work with t instead of z; the argument is similar). Then given $\left[\begin{smallmatrix} x' & y' \\ az & at \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$, we have $ax't - ay'z = 1$ so $x't - y'z = a^{-1}$. Taking this modulo $\gcd(z, N)$ gives $x't \equiv a^{-1} \pmod{\gcd(z, N)}$, which has a unique solution for x' modulo $\gcd(z, N)$. Hence there are $\frac{N}{\gcd(z,N)}$ possible values of x' modulo N. The value of x' uniquely determines y', so there are $\frac{N}{\gcd(z,N)}$ matrices with bottom row az, at. Fixing a and letting b range over the residues modulo N in (10), $a^{-1}x + bz$ can take $\frac{N}{\gcd(z,N)}$ values. Hence all the matrices with bottom row az, at are in the coset $\Gamma_0(N) \begin{bmatrix} x & y \\ z & t \end{bmatrix}$, as needed. □

Let $\gamma_1, \gamma_2 \neq \pm I$ be stabilizers for elliptic points p_1, p_2 in $\Gamma_0(N)$, and suppose p_1, p_2 are $\Gamma_0(N)$-inequivalent. By Proposition 3.5.3, we can write $\gamma_j = M_j S M_j^{-1}$, where $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $M_j \in \mathrm{PSL}_2(\mathbb{Z})$. Write $M_j = A_j R_j$ where R_j is one of the coset representatives above and $A_j \in \overline{\Gamma_0(N)}$. Then

$$\gamma_1 = A_1 R_1 S R_1^{-1} A_1^{-1}$$
$$\gamma_2 = A_2 R_2 S R_2^{-1} A_2^{-1}$$

Let $R = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$ be a coset representative chosen above. Then

$$RSR^{-1} = \begin{bmatrix} yt + xz & -x^2 - y^2 \\ t^2 + z^2 & -yt - zx \end{bmatrix}.$$

In order for this to be in $\Gamma_0(N)$, we must have

$$t^2 + z^2 \equiv 0 \pmod{N}. \tag{11}$$

We count the number of $(t, z) \in P$ that make this equation true. Note that $\gcd(t, z) = 1$. Let $g = \gcd(t, N)$. If (11) holds then $g|z$ giving $g = 1$. Thus we can divide the equation above by z^2 and let $x = \frac{t}{z}$ to get $x^2 + 1 \equiv 0 \pmod{N}$. Each solution (t, z) corresponds to a solution x. Thus there are m coset representatives R such that $RSR^{-1} \in \overline{\Gamma_0(N)}$.

Now if $R_1 = R_2$, then $\gamma_2 = A_2 A_1^{-1} \gamma_1 A_1 A_2^{-1}$ so γ_1, γ_2 are conjugate in $\overline{\Gamma_0(N)}$ and p_1, p_2 are $\Gamma_0(N)$-equivalent. The number of $\Gamma_0(N)$-inequivalent elliptic points is hence at most the number of distinct coset representatives R such that $RSR^{-1} \in \Gamma_0(N)$, which equals m. But we've already shown there are at least m distinct elliptic points, so the number must equal exactly m.

For the case that z is an elliptic point of order 3, we have $\gamma z = z$ for some γ conjugate to $T = \left[\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right]$ instead. The proof is the same with minor changes.

1. The trace is 1 so we have $a^2 + a + 1 \equiv 0 \pmod{N}$ in (9) instead.

2. The map $z \mapsto a$ is sujective because the elliptic point corresponding to $\left[\begin{smallmatrix} a & 1 \\ -a^2-a-1 & -1-a \end{smallmatrix}\right]$ maps to a.

3. Keeping the same notation, the bottom-left entry in RTR^{-1} is $z^2 + tz + t^2$ instead of $t^2 + z^2$.

□

It remains to count the number of solutions to $a^2 + 1 \equiv 0 \pmod{N}$. Let $p|N, p \neq 2$. The number of solutions to $a^2 \equiv -1 \pmod{p}$ is 2 if -1 is a square modulo p and 0 otherwise. By Hensel's Lemma solutions lift uniquely to modulo $p^{v_p(n)}$. The number of solutions to $a^2 \equiv -1 \pmod{2^\alpha}$ is 1 if $\alpha = 1$ and 0 if $\alpha > 1$. Hence by the Chinese Remainder Theorem the total number of solutions is

$$\nu_2 = \begin{cases} \prod_{p|N, p\neq 2} \left(1 + \left(\frac{-1}{p}\right)\right), & 4 \nmid N \\ 0, & 4|N. \end{cases} \tag{12}$$

Now $a^2+a+1 \equiv 0 \pmod{N}$ has no solutions if $2|N$. If $2 \nmid N$, then rewrite as $(2a+1)^2 \equiv -3 \pmod{N}$. For $p \neq 2, 3$, this equation has 2 solutions if -3 is a square mod p and 0 otherwise; solutions mod p lift to solutions mod $p^{v_p(n)}$. For $p = 3$, we see that there is 1 solution mod 3 but none mod 9. Hence

$$\nu_3 = \begin{cases} \prod_{p|N,\, p\neq 2,3} \left(1 + \left(\frac{-3}{p}\right)\right), & 2 \nmid N,\, 9 \nmid N \\ 0, & \text{else.} \end{cases} \tag{13}$$

Finally, we count the cusps.

Lemma 2.4: Suppose $z \in \mathcal{H}$, Γ' is a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$, $\Gamma \subseteq \Gamma'$ is a subgroup of finite index, and $\sigma_1, \ldots, \sigma_k \in \Gamma'$ are such that $\sigma_j(z)$ are all the Γ-inequivalent points. Then

$$\Gamma' = \bigsqcup_{j=1}^{k} \Gamma \sigma_j \Gamma'_z.$$

Proof. Given $\gamma \in \Gamma'$, there exists σ_j such that $\gamma(z)$ is Γ-equivalent to $\sigma_j(z)$. This means there exists $A \in \Gamma$ such that $\gamma(z) = A\sigma_j(z)$. Then $\sigma_j^{-1}A^{-1}\gamma(z) = z$ so there exists $\tau \in \Gamma'_z$ such that $\sigma_j^{-1}A^{-1}\gamma = \tau$. Rearranging gives

$$\gamma = A\sigma_j\tau \in \Gamma\sigma_j\Gamma'_z.$$

These double cosets are disjoint because if $\gamma \in \Gamma\sigma_j\Gamma'_z$, then $\gamma(z)$ is Γ-equivalent to $\sigma_j(z)$, and by assumption different $\sigma_j(z)$ are Γ-inequivalent. □

Take $\Gamma' = \mathrm{SL}_2(\mathbb{Z})$, $\Gamma = \Gamma_0(\mathbb{Z})$, and $z = 0 = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\infty$; then $\sigma_1(z), \ldots, \sigma_k(z)$ are all the cusps, and ν_∞ is the number of double cosets $\Gamma_0(N)\backslash\Gamma'/\Gamma'_z$. Considering our coset representatives $\left[\begin{smallmatrix} * & * \\ z & t \end{smallmatrix}\right]$, two of them are in the same double coset if they are related on the right by an element of $\Gamma'_z = \{\left[\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right]\}$. Now

$$\begin{bmatrix} * & * \\ z & t \end{bmatrix} \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} = \begin{bmatrix} * & * \\ nt+z & t \end{bmatrix}.$$

Thus the number of double cosets is the number of pairs (z, t) under the equivalence relation $(z, t) \sim (z', t')$ if $z' = nt + z, t = t'$ for some n. Fixing t, there are $\varphi(\gcd(n/t, t))$ inequivalent choices for z. Hence

$$\nu_\infty = \sum_{d|N} \varphi(\gcd(n, n/d)). \tag{14}$$

Now we can put (12), (13), and (14) into (8) to get $g(X_0(N))$.

Problem 3 *(Picard's Little Theorem)*

Suppose f is an entire function omitting two values y_1, y_2.

Note $\mu_2 = 6$ so

$$g(X(2)) = 1 + \mu_N \cdot \frac{N-6}{12N}\bigg|_{N=2} = 0.$$

The number of cusps is

$$\frac{\mu_N}{N} = 3.$$

There is one cusp at ∞ and two inequivalent cusps on $\mathbb{R}$. Note that $\Gamma(2)\backslash\mathcal{H}$ is analytically isomorphic to $\mathbb{C} - \{y_1, y_2\}$ (say, via φ) since they both have genus 0 and two finite points omitted.(From [?], any compact Riemann surface of genus 0 and no cusps is analytically isomorphic to the Riemann sphere.)

Thus f induces a holomorphic map $g : \mathbb{C} \to \Gamma(2)\backslash\mathcal{H}$. Now $\mathcal{H}$ is a covering space of $\Gamma(2)\backslash\mathcal{H}$ so g induces a analytic map h so that the following diagram commutes. (Here π is the projection map.)

$$\begin{tikzcd}
& \mathcal{H} \arrow[d, "\pi"] \\
\mathbb{C} \arrow[ur, "h"] \arrow[r, "g"] \arrow[dr, "f"'] & \Gamma(2)\backslash\mathcal{H} \arrow[d, "\cong"', "\varphi"] \\
& \mathbb{C} - \{y_1, y_2\}.
\end{tikzcd}$$

Now $u(z) = e^{iz}$ is an analytic map from $\mathcal{H}$ to $D - \{0\}$ (D being the unit disc centered at 0). Hence $u(h(z))$ is an entire function with image contained in D. Then $u(h(z))$ is bounded so constant by Liouville's Theorem. But the inverse image of any point under u is discrete, so this means that $h(z)$ is constant, and $f(z) = \varphi(\pi(h(z))$ is constant.

Problem 4 *(An automorphic form)*

For $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$,

$$\begin{aligned} \gamma(z) &= \frac{az+b}{cz+d} \\ \gamma'(z) &= \frac{\cancelto{1}{ad-bc}}{(cz+d)^2} \end{aligned} \tag{15}$$

We differentiate the equation

$$f|[\gamma]_k(x) = f(\gamma(x))(cx+d)^{-k} = f(x) \tag{16}$$

and use (15) and (16) to obtain

$$\begin{aligned} f'(x) &= f'(\gamma(x))\gamma'(x)(cx+d)^{-k} - kf(\gamma(x))(cx+d)^{-k-1} \\ &= f'(\gamma(x))(cx+d)^{-2-k} - kf(x)(cx+d)^{-1} && (17) \\ f'(\gamma(x)) &= (cx+d)^{k+1}(f'(x)(cx+d) + kf(x)). && (18) \end{aligned}$$

Now differentiate $f'(x)$ again and use (15), (16), and (18) to obtain

$$\begin{aligned} f''(x) &= f''(\gamma(x))\gamma'(x)(cx+d)^{-2-k} - f'(\gamma(x))(k+2)(cx+d)^{-3-k} \\ &\quad - kf'(x)(cx+d)^{-1} + kf(x)(cx+d)^{-2} \\ &= f''(\gamma(x))(cx+d)^{-4-k} - (2+k)(cx+d)^{-2}(f'(x)(cx+d)+kf(x)) \\ &\quad - kf'(x)(cx+d)^{-1} + kf(x)(cx+d)^{-2} \\ f''(\gamma(x)) &= f''(x)(cx+d)^{k+4} + (k+2)(cx+d)^{k+2}(f'(x)(cx+d)+kf(x)) \\ &\quad + kf'(x)(cx+d)^{k+3} - kf(x)(cx+d)^{k+2}. \end{aligned} \tag{19}$$

Use (16), (18), and (19) to write

$$\begin{aligned} g(\gamma(x)) &= (k+1)f'(\gamma(x))^2 - kf(\gamma(x))f''(\gamma(x)) \\ &= (k+1)(cx+d)^{2k+2}\left[f'(x)^2(cx+d)^2 + 2kf(x)f'(x)(cx+d) + k^2f(x)^2\right] \\ &\quad - kf(x)(cx+d)^k[f''(x)(cx+d)^{k+4} + (k+2)(cx+d)^{k+2}(f'(x)(cx+d)+kf(x)) \\ &\quad + kf'(x)(cx+d)^{k+3} - kf(x)(cx+d)^{k+2}] \\ &= (cx+d)^{2k+4}\left[(k+1)f'(x)^2 - kf''(x)\right] \\ &\quad + (cx+d)^{2k+3}\left[2k(k+1)f(x)f'(x) - k(k+2)f(x)f'(x) - k^2f(x)f'(x)\right] \\ &\quad + (cx+d)^{2k+2}\left[k^2(k+1)f(x)^2 - k^2(k+2)f(x)^2 + k^2f(x)^2\right] \\ &= (cx+d)^{2k+4}[(k+1)f'(x)^2 - kf''(x)] \\ &= (cx+d)^{2k+4}g(x) \end{aligned}$$

Hence $g|[\gamma]_{2k+4} = g$, and g is a weight $(2k+4)$-modular form. (Note that since f is holomorphic, so are its derivatives, and so g is holomorphic.)

If f is a modular form, then translating a cusp to ∞ we can write the Fourier expansion as

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

Note $f'(z) = \sum_{n\geq 1} 2\pi i n a_n e^{2\pi i n z}$ has no constant term, and neither does $f''(z)$. Hence $g(z) = (k+1)f'(z)^2 - kf(z)f''(z)$ has no constant term, and is a cusp form.