18.786 Number Theory II **Spring 2024**
Problem Set #3 **Due: 3/13/2024**

Description

These problems are related to the material covered in Lectures 4-8. Your solutions should be written up in latex and submitted as a pdf-file on Gradescope before midnight on the date due. Collaboration is permitted/encouraged, but you must identify your collaborators or the name of your group on pset partners, and any references you consulted. If there are none write "**Sources consulted: none**" at the top of your solution.

Problem 1. Automorphic forms in an adelic setting (50 points)

Let $\mathbb{A}_{\mathbb{Q}}$ denote the adele ring of $\mathbb{Q}$, which we recall contains $\mathbb{Q}$ embedded diagonally as the subring of principal adeles. Let $\mathbb{A}_{\mathbb{Q}}^{\infty} := \{a \in \mathbb{A}_{\mathbb{Q}} : \|a\|_{\infty} = 0\}$ denote the finite adeles, and embed each completion of $\mathbb{Q}$ in $\mathbb{A}_{\mathbb{Q}}$ via $(x \mapsto (0, \ldots, 0, x, 0, \ldots 0))$.[1]

Note that under these embeddings the finite adeles $\mathbb{A}_{\mathbb{Q}}^{\infty} \subseteq \mathbb{A}_{\mathbb{Q}}$ and the $\mathbb{Q}$-completions $\mathbb{Q}_p, \mathbb{R} \subseteq \mathbb{A}_{\mathbb{Q}}$ are $\mathbb{A}_{\mathbb{Q}}$-ideals that are rings, but they are not subrings of $\mathbb{A}_{\mathbb{Q}}$ (because they do not contain $1 \in \mathbb{A}_{\mathbb{Q}}$), whereas $\mathbb{Q} \subseteq \mathbb{A}_{\mathbb{Q}}$ is a subring but not an $\mathbb{A}_{\mathbb{Q}}$-ideal.

(a) Show that one can embed $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^{\infty})$ and $\mathrm{GL}_2(\mathbb{R})$ in $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ so that we have isomorphisms of topological groups

$$\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}) \simeq \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^{\infty}) \times \mathrm{GL}_2(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^{\infty})\mathrm{GL}_2(\mathbb{R}) = \mathrm{GL}_2(\mathbb{R})\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^{\infty}),$$

and thus may view any subgroup of $\mathrm{GL}_2(\mathbb{R})$ or $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^{\infty})$ as a subgroup of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$.

Let $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p \simeq \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ denote the profinite completion of $\mathbb{Z}$, which we view as a subring of $\mathbb{A}_{\mathbb{Q}}^{\infty}$ (via the embeddings of $\mathbb{Z}_p \subseteq \mathbb{Q}_p$). For each positive integer N we define

$$K_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) : c \equiv 0 \bmod N\} \subseteq \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}^{\infty}),$$
$$\Gamma_0(N) := K_0(N) \cap \mathrm{GL}_2^{+}(\mathbb{Z}) \subseteq \mathrm{SL}_2(\mathbb{Z}).$$

(b) Show that

$$\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Q})\mathrm{GL}_2^{+}(\mathbb{R})K_0(N),$$

thus we can write any $a \in \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ as $g = \gamma\sigma\kappa$ with $\gamma \in \mathrm{GL}_2(\mathbb{Q})$, $\sigma \in \mathrm{GL}_2^{+}(\mathbb{R})$, and $\kappa \in K_0(N)$, not necessarily uniquely.

(c) Show that there is a natural isomorphism of topological coset/double-coset spaces

$$\Gamma_0(N)\backslash\mathrm{GL}_2^{+}(\mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})/K_0(N).$$

(d) Let $K_{\infty}^{+} = \mathrm{SO}_2(\mathbb{R})$ and let Z_{∞}^{+} denote the subgroup of scalar matrices in $\mathrm{GL}_2^{+}(\mathbb{R})$. Show that we have a natural isomorphism of topological spaces

$$\Gamma_0(N)\backslash\mathbf{H} \simeq \mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})/K_0(N)K_{\infty}^{+}Z_{\infty}^{+}$$

and that $\Gamma_0(N)$ is an arithmetic lattice in $\mathrm{SL}_2(\mathbb{R})$. Let $X_0(N) := X_{\Gamma_0(N)}$ denote the corresponding compact Riemann surface.

[1] See the 18.785 Lecture notes for more about the ring $\mathbb{A}_{\mathbb{Q}}$.

Let $k \in \mathbb{Z}_{>0}$ be even. For any cusp form $f \in S_k(\Gamma_0(N))$, we define the function $\varphi_f\colon \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}) \to \mathbb{C}$ by writing $g \in \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ in the form $g = \gamma\sigma\kappa$ as in **(b)** and putting

$$\varphi_f(g) := (f|_k\sigma)(i),$$

where $(f|_k\sigma)(z) := \det(\sigma)^{k/2} j(\sigma,z)^{-k} f(\sigma z)$ is the slash operator and $j\big(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z\big) := cz+d$ is the automorphy factor.

(e) Show that φ_f is well defined, in other words, for all $\gamma, \gamma' \in \mathrm{GL}_2(\mathbb{Q})$, $\sigma, \sigma' \in \mathrm{GL}_2^+(\mathbb{R})$, $\kappa, \kappa' \in K_0(N)$ such that $\gamma\sigma\kappa = \gamma'\sigma'\kappa'$, we have $(f|_k\sigma)(i) = (f|_k\sigma')(i)$.

Define $\xi\colon K_\infty^+ \to \mathbb{C}$ by $\xi(r_\theta) := e^{ik\theta}$ for $r_\theta = \left(\begin{smallmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{smallmatrix}\right) \in K_\infty^+ = \mathrm{SO}_2(\mathbb{R})$.

(f) Let $K := K_0(N)K_\infty^+$. Show that $\varphi := \varphi_f$ satisfies the following:

- (i) **automorphy**: $\varphi(\gamma g) = \varphi(g)$ for all $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ and $g \in \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$.
- (ii) K**-finite**: $\varphi(g r_\theta \kappa) = \xi(r_\theta)\varphi(g)$ for all $g \in \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$, $r_\theta \in K_\infty^+$, $\kappa \in K_0(N)$, so the $\mathbb{C}$-vector space spanned by $\{\varphi(gh) : h \in K\}$ has finite dimension.
- (iii) **central action**: $\varphi(\lambda g) = \varphi(g)$ for all scalar $\lambda \in \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ and $g \in \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$.
- (iv) Z**-finite**: For every $g \in \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}^\infty)$ the map $\mathbf{H} \to \mathbb{C}$ given by

  $$z \mapsto \varphi(g\sigma) j(\sigma, i)^k \det(\sigma)^{-k/2},$$

  where $\sigma \in \mathrm{GL}_2^+(\mathbb{R})$ satisfies $\sigma i = z$, is well-defined and holomorphic.
- (v) **moderate growth**: There exist $c, r \in \mathbb{R}_{>0}$ such that for all $g \in \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}^\infty)$ the function ϕ_g on $\mathrm{GL}_2^+(\mathbb{R})$ defined by $\sigma \mapsto \varphi(g\sigma)$ satisfies the bound

  $$|\phi_g(\sigma)| \le c\|\sigma\|^r,$$

  with $\|\sigma\| := a^2 + b^2 + c^2 + d^2 + \det(\sigma)^{-2}$ for $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.
- (vi) **cuspidal**: Show that the function ϕ_g defined in (v) is bounded on $\mathrm{GL}_2^+(\mathbb{R})$.

(g) Show that any smooth function $\varphi\colon \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}) \to \mathbb{C}$ satisfying conditions (i)-(vi) above arises as φ_f for some $f \in S_k(\Gamma_0(N))$. Such functions are cuspidal automorphic forms on $\mathbb{A}_\mathbb{Q}$ for $K_0(N)$.

Remark. Our definition of K-finiteness depends not only on K, but also on the choice of the function ξ (a fundamental idempotent). Our definition of Z-finiteness is specific to the GL_2 setting, where holomorphicity is equivalent to being an eigenfunction for the Casimir element Δ, which together with 1 generates the center $Z(\mathfrak{g})$ of the universal enveloping algebra for the complexified Lie algebra $\mathfrak{g} := \mathfrak{gl}_2 \otimes_\mathbb{R} \mathbb{C}$; in general one specifies a finite index ideal of $Z(\mathfrak{g})$ that annihilates φ. An automorphic form on $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ is cuspidal if for all $g \in \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ we have

$$\int_{\mathbb{Q}\backslash\mathbb{A}_\mathbb{Q}} \varphi(\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) g)\, dx = 0.$$

See [1, Cor. 12.4] for a proof that this is implied by the cuspidal condition above.

Remark. The $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ automorphic forms for $K_0(N)$ described in this problem admit many generalizations, including: (1) replace $\mathbb{Q}$ with a number field F and $\widehat{\mathbb{Z}}$ with $\widehat{\mathcal{O}}_F$, (2) replace GL_2 with a connected linear algebraic group G and $\Gamma_0(N)$ with any arithmetic subgroup of $G(F)$ (and adjust $K_0(N)$ and $\mathrm{GL}_2^+(\mathbb{R})$ accordingly), (3) allow a character χ (and adjust the fundamental idempotent and the central action condition accordingly).

Problem 2. Subgroups of the modular group (50 points)

In this problem we consider subgroups of the modular group $\Gamma(1) := \mathrm{SL}_2(\mathbb{Z})$. We use $\Gamma(N)$ to denote the subgroup of $\Gamma(1)$ congruent to the identity modulo a positive integer N. For any subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ we use $\overline{\Gamma}$ to denote $\Gamma/Z(\Gamma) \subseteq \mathrm{PSL}_2(\mathbb{Z})$.

(a) Show that $X(1) := X_{\Gamma(1)}$ has hyperbolic volume $\pi/3$ and is therefore compact.

(b) Show that every elliptic element of $\Gamma(1)$ is conjugate to a power of $R := \left(\begin{smallmatrix}1 & -1\\ 1 & 0\end{smallmatrix}\right)$ or $S := \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$, every parabolic element is conjugate to a power of $T := \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, and that $\overline{\Gamma}(1)$ admits the presentation $\langle r, s \,|\, r^3 = s^2 = 1\rangle$.

(c) Show that the commutator subgroup $\overline{\Gamma}(1)' := \langle \alpha\beta\alpha^{-1}\beta^{-1} : \alpha, \beta \in \overline{\Gamma}(1)\rangle \le \overline{\Gamma}(1)$ is a normal subgroup of index 6 is isomorphic to the free group on two letters.

(d) Show that $\overline{\Gamma}(2) \le \overline{\Gamma}(1)$ is also a normal subgroup of index 6 isomorphic to the free group on two letters.

(e) Are the isomorphic normal subgroups $\overline{\Gamma}(1)', \overline{\Gamma}(2) \le \overline{\Gamma}(1)$ equal? If not, describe their intersection and determine the least integer N (if any) for which $\overline{\Gamma}(N) \subseteq \overline{\Gamma}(1)'$.

For a subgroup Γ of $\Gamma(1)$ let $e_n(\Gamma)$ count the Γ-inequivalent elliptic points of order n, and let $e_\infty(\Gamma)$ count the Γ-inequivalent cusps.

(f) Prove that for any finite index subgroup Γ of $\Gamma(1)$ the following formula holds

$$g(\Gamma) := g(X_\Gamma) = 1 + \frac{[\overline{\Gamma}(1) : \overline{\Gamma}]}{12} - \frac{e_2(\Gamma)}{4} - \frac{e_3(\Gamma)}{3} - \frac{e_\infty(\Gamma)}{2}.$$

Your proof should rely only on material covered in the first two chapters of [2].

(g) Compute an explicit (and reasonably sharp) lower bound on $g(\Gamma(N))$ as a function of N and determine its asymptotic growth. Use this to explicitly determine the sets of integers $\{N : g(\Gamma(N)) = g\}$ for $g \le 10$ (you are welcome to use a computer algebra system to help, but you must prove your list is complete).

(h) Let $\Gamma := \Gamma(1)'$ be the commutator subgroup of $\Gamma(1)$. Compute $g(\Gamma)$ using your formula, then compute $\dim S_k(\Gamma)$ for $2 \le k \le 6$.

Definition. A congruence subgroup Γ is a subgroup of $\mathrm{SL}(2,\mathbb{Z})$ that contains $\Gamma(N)$ for some positive integer N. The least such N is the level of Γ.

Definition. The width of a cusp x of a finite index $\Gamma \le \mathrm{SL}(2,\mathbb{Z})$ is the least integer $h \ge 1$ for which $\pm\sigma\Gamma_x\sigma_{-1} = \pm\langle\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right)\rangle$, where $\sigma \in \mathrm{SL}_2(\mathbb{R})$ satisfies $\sigma x = \infty$.

(i) Prove that for all $N \ge 1$, the group $\Gamma(1)/\Gamma(N) \simeq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ contains a subgroup of index 7 only when $7|N$, in which case it projects on to an index 7 subgroup of $\mathrm{SL}(2,\mathbb{Z}/7\mathbb{Z})$. Conclude that every congruence subgroup of index 7 has level 7.

(j) Consider the subgroup $\Gamma := \left\langle \left(\begin{smallmatrix}1 & 5\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right), \left(\begin{smallmatrix}2 & 3\\ 1 & 2\end{smallmatrix}\right)\right\rangle$ of $\mathrm{SL}(2,\mathbb{Z})$ found in [3], which evidently has a cusp of width 5. Prove that if Γ contains $\Gamma(N)$ then the width of every cusp of Γ divides N. Then show that Γ has index 7 in $\mathrm{SL}(2,\mathbb{Z})$ and is therefore not a congruence subgroup, and compute $g(\Gamma)$ using your formula.

Problem 3. Survey

Complete the following survey by rating each problem you attempted on a scale of 1 to 10 according to how interesting you found it (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found it (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			

Please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material to you (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
2/26	Meromorphic differentials				
2/28	Dimension formulas				

Please feel free to record any additional comments you have on the problem sets and the lectures, in particular, ways in which they might be improved.

References

[1] A. Knightly and C. Li, *Traces of Hecke operators*, American Mathematical Society, 2006.

[2] T. Miyake, *Modular forms*, Springer, 2006.

[3] A.J. Scholl, *On the Hecke algebra of a noncongruence subgroup*, Bull. London Math. Soc. **29** (1997), 395–399.