18.786 Number Theory II **Spring 2024**
Problem Set #7 **Due: 5/14/2024**

Description

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. Pick any combination of problems that sum to 100 points, then complete the survey problem.

Problem 1. Commutator subgroups and adelic images of $E/\mathbb{Q}$ (50 points)

Let $E/\mathbb{Q}$ be an elliptic curve without potential complex multiplication, let

$$\rho_E\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

be its adelic Galois representation, and let $G_E := \rho_E(\mathrm{Gal}_{\mathbb{Q}})$ denote its image.

Serre's open image theorem implies that G_E is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and in particular, has finite index. The goal of this problem is to prove another result of Serre, which states that the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E]$ is divisible by 2, and we thus never have $G_E = \mathrm{GL}_2(\widehat{\mathbb{Z}})$; the proof also gives an explicit non-obvious constraint on the open subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that can arise as Galois images of elliptic curves $E/\mathbb{Q}$ that allows us to rule out some otherwise plausible looking candidates.

Recall that every group G has a commutator subgroup

$$[G : G] := \{ghg^{-1}h^{-1} : g, h \in G\},$$

a normal subgroup of G that determines the maximal abelian quotient $G^{\mathrm{ab}} := G/[G : G]$. For any $G \le \mathrm{GL}_2(\widehat{\mathbb{Z}})$ the commutator subgroup $[G, G]$ lies in the intersection $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$. Indeed, $G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$ is a normal subgroup contained in the kernel of the determinant map $\det\colon G \to \widehat{\mathbb{Z}}^\times$, and we have an abelian quotient $G/(G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})) \subseteq \widehat{\mathbb{Z}}^\times = \mathrm{GL}_2(\widehat{\mathbb{Z}})/\mathrm{SL}_2(\widehat{\mathbb{Z}})$.

One might naïvely guess that $[G, G] = G \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$, but this is not always true. Indeed, it fails for $G = \mathrm{GL}_2(\widehat{\mathbb{Z}})$, but it always holds for G_E (as you will prove). This depends crucially on the fact that E is defined over $\mathbb{Q}$ rather than an extension of $\mathbb{Q}$; for elliptic curves E over number fields K that do not contain any roots of unity other than ± 1 we will have $\rho_E(G_K) = \mathrm{GL}_2(\widehat{\mathbb{Z}})$ for most E/K, except when $K = \mathbb{Q}$.

For an open $H \le \mathrm{SL}_2(\mathbb{Z}_\ell)$ the level of H is the least ℓ^n for which $H = \pi_{\ell^n}^{-1}(\pi_{\ell^n}(H))$, where $\pi_{\ell^n}\colon \mathrm{SL}_2(\mathbb{Z}_\ell) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is the reduction-modulo-ℓ^n map.

Let $\chi_{\mathrm{cyc}}\colon \mathrm{Gal}_{\mathbb{Q}} \to \widehat{\mathbb{Z}}^\times$ be the cyclotomic character defined by $\sigma(\zeta_n) = \zeta_n^{\chi_{\mathrm{cyc}}(\sigma) \bmod n}$.

(a) Show that for every $m \in \mathbb{Z}_{\ge 1}$ the reduction-modulo-m map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ is surjective.

(b) Show that $\#\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}} | 12$ and $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})^{\mathrm{ab}}$, $\mathrm{SL}_2(Z/3\mathbb{Z})^{\mathrm{ab}}$, $\mathrm{SL}_2(Z/4\mathbb{Z})^{\mathrm{ab}}$ are cyclic of order $2, 3, 4$, respectively.

(c) Show that $\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}} \simeq \mathbb{Z}/12\mathbb{Z}$ and reduction modulo 12 induces an isomorphism $\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}} \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}/12\mathbb{Z})^{\mathrm{ab}}$. Then show that for any positive integer m the group $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{\mathrm{ab}}$ is cyclic of order $\gcd(m, 12)$.

(d) Show that $\mathrm{SL}_2(\mathbb{Z}_2)^{\mathrm{ab}}$ is cyclic of order 4, $\mathrm{SL}_2(\mathbb{Z}_3)^{\mathrm{ab}}$ is cyclic of order 3, and $\mathrm{SL}_2(\mathbb{Z}_\ell)^{\mathrm{ab}}$ is trivial for every prime $\ell \geq 5$, and that the commutator subgroup of $\mathrm{SL}_2(\mathbb{Z}_2)$ has level 4 in $\mathrm{SL}_2(\mathbb{Z}_2)$, while the commutator subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$ has level 3 in $\mathrm{SL}_2(\mathbb{Z}_3)$.

(e) Show that the commutator subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is $\mathrm{SL}_2(\mathbb{Z}_\ell)$ for all $\ell \geq 3$.

(f) Show that the commutator subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ has level 2 and index 2 in $\mathrm{SL}_2(\mathbb{Z}_2)$ and conclude that the commutator subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ of level 2 and index 2, and in particular, is not equal to $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

(g) Show that if G is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ or $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ then $[G,G]$ is an open subgroup of $\mathrm{SL}_2(\widehat{\mathbb{Z}})$.

(h) Show that $\det \circ \rho_E = \chi_{\mathrm{cyc}}^{-1}$, and conclude that $\det(G_E) = \widehat{\mathbb{Z}}^\times$.

Recall the Kronecker-Weber theorem: the cyclotomic field $\mathbb{Q}^{\mathrm{cyc}} = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_n)$ is the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$.

(h) Show that $G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}) = [G_E, G_E]$. Deduce that $G_E \neq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, and moreover, that 2 divides the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E]$.

Problem 2. Quadratic twists and refinements (50 points)

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$ with $A, B \in \mathbb{Z}$, let d denote a nonsquare squarefree integer, and let $E_d\colon dy^2 = x^3 + Ax + B$ denote the quadratic twist of E by $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Let $\chi_{\mathrm{cyc}}\colon \mathrm{Gal}_{\mathbb{Q}} \to \widehat{\mathbb{Z}}$ denote the cyclotomic character defined in Problem 1, and let $\chi_d\colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ be the unique homomorphism that factors through the isomorphism $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})) \xrightarrow{\sim} \{\pm 1\}$.

We write $H \sim K$ when H and K are conjugate subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ or $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. When H is a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ or $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that contains -1, we call the index-2 subgroups of H that do not contain -1 refinements of H.

(a) Show there is a unique homomorphism $\psi\colon \widehat{\mathbb{Z}} \to \{\pm 1\}$ for which $\chi_d = \psi \circ \chi_{\mathrm{cyc}}^{-1}$ and let $H_d := \{\psi(\det g)g : g \in G_E\}$. Prove $H_d \sim \rho_{E_d}(\mathrm{Gal}_{\mathbb{Q}})$ and $\pm\rho_E(\mathrm{Gal}_{\mathbb{Q}}) \sim \pm\rho_{E_d}(\mathrm{Gal}_{\mathbb{Q}})$.

(b) Let H' be an index-2 subgroup of $\pm\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ that does not contain -1. Show that there is a unique d for which $\rho_{E_d}(\mathrm{Gal}_{\mathbb{Q}}) \sim H_d \sim H'$. Conclude that every refinement of $\pm\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ can be realized as $\rho_{E'}(\mathrm{Gal}_{\mathbb{Q}})$ for some quadratic twist $E'/\mathbb{Q}$ of E that is unique up to $\mathbb{Q}$-isomorphism.

(c) For each $N \leq \mathbb{Z}_{\geq 1}$ show that all $\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}}) \sim \rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}})$ for all but finitely many d, and that every refinement of $\pm\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$ arises as $\rho_{E_d,N}(\mathrm{Gal}_{\mathbb{Q}})$ for a unique d that divides $\mathrm{disc}(\mathbb{Q}(E[N])$.

Let H be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level N that contains -1. For each $M \in \mathbb{Z}_{\geq 1}$ let $\pi_M\colon \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ denote the reduction-modulo-m map.

(d) Let $N|M \in \mathbb{Z}_{\geq 1}$. Show that H has a refinement of level dividing M if and only if $\pi_M(H)$ has a refinement, and the level of every refinement of H is a multiple of N.

(e) Show by example that H may admit a refinement of level $2N$ even when it has no refinements of level N.

(f) Show that H has a refinement whose level divides $2N$ if and only -1 is not a square in $\pi_{2N}(H)^{\mathrm{ab}}$, the maximal abelian quotient of $\pi_{2n}(H)$.

(g) Show that if H has any refinements then it has infinitely many.

(h) Let $p \perp M \in \mathbb{Z}_{\geq 1}$ be an odd prime. Show that if H has a refinement of level NMp^e for some $e > 0$ then H has a refinement of level NM (hint: use Goursat's lemma). Conclude that if H has a refinement then it has one of level $N2^e$ for some $e \geq 0$.

(i) Show that if H has a refinement of level $N2^e$ for some $e \geq 1$ then H has a refinement of level $2N$, and if N is odd then H has a refinement of level N.

Conclude that either H has no refinements or it has infinitely many, including one of level N or $2N$, depending on whether $-1 \in \pi_{2N}(H)^{\mathrm{ab}}$ is a square or not.

Problem 3. Complex conjugation and curves of genus zero (50 points)

Recall that the categories of elliptic curves $E/\mathbb{C}$ (up to isomorphism) and complex tori $\mathbb{C}/L$ (up to homethety) are equivalent. Here $L \subseteq \mathbb{C}$ is a free $\mathbb{Z}$-module of rank 2 and thus has a $\mathbb{Z}$-module basis $[\omega_1, \omega_2]$ for some $\mathbb{R}$-linearly independent $\omega_1, \omega_2 \in \mathbb{C}^\times$. After applying the homethety $\pm\omega_2/\omega_1$ we can assume $L = [1, \tau]$ with $\tau \in \mathbf{H}$, in which case the corresponding elliptic curve E_L is defined by

$$E_L\colon y^2 = 4x^3 - g_2(\tau)x - g_3(\tau),$$

where $g_2(\tau) = 60\sum' \frac{1}{(m+n\tau)^4}$ and $g_3(\tau) = 140\sum' \frac{1}{(m+n\tau)^6}$, with the sums Σ' taken over the nonzero lattice points $m + n\tau \in L$. The map $\Phi\colon \mathbb{C}/L \to E_L(\mathbb{C})$ that sends L to the identity element of $E_L(\mathbb{C})$ and $z + L$ to the point $(\wp(z), \wp'(z))$ is then an isomorphism of topological groups that is also an isomorphism of compact Riemann surfaces, where

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega \in L - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Every elliptic curve $E/\mathbb{C}$ is isomorphic an elliptic curve defined by an equation of the form above, and this includes the base change to $\mathbb{C}$ of any elliptic curve defined over $\mathbb{Q}$. Moreover, if $E\colon y^2 = x^3 + Ax + B$ is an elliptic curve over $\mathbb{Q}$, there is a $\tau \in \mathbf{H}$ for which $g_2(\tau) = -4A$ and $g_3(\tau) = -4B$, and for $L = [t, \tau]$ the corresponding curve E_L will have rational coefficients.

(a) Show that if $g_2(L), g_3(L) \in \mathbb{R}$ (so E_L is defined over $\mathbb{R}$ not just $\mathbb{C}$), then L is stable under complex conjugation, in which case $\Phi(\mathbb{R}) \subseteq E_L(\mathbb{R})$ but $\Phi(\mathbb{C}) \not\subseteq E_L(\mathbb{R})$.

Now let E be an elliptic curve over $\mathbb{Q}$, let $\rho_E\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be its adelic Galois representation, fix an embedding $\overline{\mathbb{Q}} \subseteq \mathbb{C}$, and let $c \in \mathrm{Gal}_{\mathbb{Q}}$ denote the automorphism corresponding to the action of complex conjugation on $\overline{\mathbb{Q}} \subseteq \mathbb{C}$.

(b) Show that $E(\mathbb{R})$ has a subgroup isomorphic to $\mathbb{R}/\mathbb{Z}$, and we can choose a compatible system of bases for $E[N]$ so that $\rho_E(c)$ is upper triangular with a 1 in the upper left. Then show that $\det(\rho_E(c)) = -1$ and $\mathrm{tr}(\rho_E(c)) = 0$. Conclude that for $N > 2$ we cannot have $E[N] \subseteq E(\mathbb{Q})$.

(c) Show that for odd N we can chose a basis for $E[N]$ so that $\rho_E(c) = \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$, but this is not necessarily true for $N = 4$. Then show that for every N we can choose a basis for $E[N]$ so that $\rho_E(c)$ is either $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right)$.

(d) Let $H \le \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup of level N. Show that if the reduction of H to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ contains no element conjugate to $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right)$ then $X_H(\mathbb{R}) = \emptyset$, and in particular, $X_H(\mathbb{Q}) = \emptyset$.

Let X be a nice (smooth, projective, geometrically integral) curve over $\mathbb{Q}$ of genus 0. Then X can be defined by a quadratic form $ax^2 + by^2 + cz^2 = 0$ with $a, b, c \in \mathbb{Z}$ and $abc \neq 0$. Recall that if X has a rational point P, then $X \simeq \mathbb{P}^1_{\mathbb{Q}}$ (the isomorphism identifies $Q \in X(\mathbb{Q})$ with the slope of the line $\overline{PQ}$) and X has infinitely many rational points. The Hasse-Minkowski theorem implies that X has a rational point if and only if it has a rational point over every completion of $\mathbb{Q}$. It follows from Hilbert reciprocity that the number of places $p \le \infty$ of $\mathbb{Q}$ for which $X(\mathbb{Q}_p) = \emptyset$ is finite and even.

(f) Show that if p is an odd prime that does not divide abc then $X(\mathbb{Q}_p) \neq \emptyset$.

Let $H \le \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup of level N with $\det(H) = \mathbb{Z}^\times$. Then X_H is a nice curve over $\mathbb{Q}$ that has good reduction modulo every prime $p \nmid N$ (this means that the reduction of X_H to $\mathbb{F}_p$ is also a nice curve). If X_H has genus zero this means that we can choose an integral model $ax^2 + by^2 + cz^2$ for X_H with $p \nmid abc$.

(g) Suppose N is a prime power and X_H has genus zero. Show that $X_H(\mathbb{Q}) = \emptyset$ if and only if the image of H to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ contains no conjugate of $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right)$.

(h) By applying the genus formula for X_H with $H = \{\pm 1\} \le \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (see the notes for Lecture 21), derive a formula for $g(X(N))$ as a function of N and list the positive integers N for which $g(X(N)) = 0$; your list should include $N \le 3$. Conclude that for the N in your list, for every H of level N we have $g(X_H) = 0$.

(i) Up to conjugation there are 6 subgroups of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ with $\det(H) = (\mathbb{Z}/3\mathbb{Z})^\times$ that contain -1; their indexes are 1, 3, 4, 6, 6, 12. Use **(g)** to determine which of the corresponding modular curves X_H have rational points.

(j) Up to conjugation there are 3 subgroups of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ with $\det(H) = (\mathbb{Z}/3\mathbb{Z})^\times$ that do not contain -1; there indexes are 8, 8, 24. Determine which of the corresponding modular curves X_H have rational points.

Problem 4. 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			
Problem 3			

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
5/6	Modular curves X_H				
5/8	Counting points on X_H				

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.