Elliptic Curves with Surjective Adelic Galois Representations

Aaron Greicius

CONTENTS

Let K be a number field. The $\mathrm{Gal}(\overline{K}/K)$-action on the torsion of an elliptic curve E/K gives rise to an adelic representation $\rho_E\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\hat{\mathbb{Z}})$. From an analysis of maximal closed subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ we derive useful necessary and sufficient conditions for ρ_E to be surjective. Using these conditions, we compute an example of a number field K and an elliptic curve E/K that admits a surjective adelic Galois representation.

1. INTRODUCTION

Let E/K be an elliptic curve, with K a number field. Fix an algebraic closure $\overline{K}$ of K and define $G_K := \mathrm{Gal}(\overline{K}/K)$. For each positive integer $m \geq 1$ and each prime number $\ell \geq 1$, the action of G_K on the various torsion subgroups of $E(\overline{K})$ gives rise to continuous representations

$$\rho_{E,m}\colon G_K \to \mathrm{Aut}(E(\overline{K})[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

and

$$\rho_{E,\ell^\infty}\colon G_K \to \mathrm{Aut}(E(\overline{K})[\ell^\infty]) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell).$$

These representations are neatly packaged into the single representation

$$\rho_E\colon G_K \to \mathrm{Aut}(E(\overline{K})_{\mathrm{tor}}) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}})$$

describing the action of G_K on the full torsion subgroup of $E(\overline{K})$. Here $\hat{\mathbb{Z}} := \varprojlim \mathbb{Z}/m\mathbb{Z} \simeq \prod_{\ell \text{ prime}} \mathbb{Z}_\ell$ is the profinite completion of $\mathbb{Z}$. We refer to ρ_{E,ℓ^∞} and ρ_E respectively as the *ℓ-adic* and *adelic* representations associated to E/K. It is proved in [Serre 72] that if E does not have complex multiplication (non-CM), then the adelic image of Galois, $\rho_E(G_K)$, is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Equivalently, since the adelic image is always a closed subgroup, Serre's result asserts that $\rho_E(G_K)$ is of finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ when E/K is non-CM. The question naturally

2000 AMS Subject Classification: Primary 11G05; Secondary 11F80, 11N36

Keywords: Elliptic curves, Galois representations, ℓ-adic, adelic, torsion, maximal subgroups, profinite

1058-6458/2010 $ 0.50 per page

arises, then, whether this index is ever 1. In other words, are there elliptic curves E/K for which ρ_E is surjective?

When $K = \mathbb{Q}$ the answer is no, as Serre himself proves in the same paper [Serre 72, Section 4.4]. As we show below, the obstacle in this situation is essentially the fact that $\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$, leaving open the possibility of ρ_E being surjective for other number fields K. Indeed, we provide simple necessary and sufficient conditions for the adelic representation to be surjective and give an example of a (non-Galois) cubic extension $K/\mathbb{Q}$ and an elliptic curve E/K for which ρ_E is surjective.

1.1 Statement of Results

When is ρ_E surjective? That is, when do we have $\rho_E(G_K) = \mathrm{GL}_2(\hat{\mathbb{Z}})$? We may put aside the arithmogeometric component of this question for the time being and ask more generally, when is a closed subgroup $H \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ in fact all of $\mathrm{GL}_2(\hat{\mathbb{Z}})$?

The group $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is both a profinite and a product group, as articulated by the two isomorphisms

$$\varprojlim \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}}) \simeq \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell). \qquad (1\text{–}1)$$

Consider the projection maps $\pi_\ell \colon \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ that arise from the product group description of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. An obvious necessary condition for a closed subgroup H to be all of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is that the restrictions $\pi_\ell \colon H \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ must all be surjective. It turns out that this condition is not so far from being sufficient; one need only further stipulate that the restriction of the abelianization map to H be surjective. As we will show, the abelianization of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is isomorphic to $\{\pm 1\} \times \hat{\mathbb{Z}}^*$, and we may describe the abelianization map as $(\mathrm{sgn}, \det) \colon \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \{\pm 1\} \times \hat{\mathbb{Z}}^*$, where det is the determinant map, and $\mathrm{sgn} \colon \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \{\pm 1\}$ is a certain "sign" map on $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Taken together this yields the following theorem.

Theorem 1.1. *Let $H \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be a closed subgroup. Then $H = \mathrm{GL}_2(\hat{\mathbb{Z}})$ if and only if*

(i) $\pi_\ell : H \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ *is surjective for all primes ℓ and*

(ii) $(\mathrm{sgn}, \det) : H \to \{\pm 1\} \times \hat{\mathbb{Z}}^*$ *is surjective.*

Returning to our representation ρ_E, we can easily rephrase Theorem 1.1 to derive simple necessary and sufficient conditions for surjectivity.

Theorem 1.2. *Let E/K be an elliptic curve defined over a number field K. Let $\Delta \in K^\times$ be the discriminant of any Weierstrass model of E/K. Then ρ_E is surjective if and only if*

(i) *the ℓ-adic representation $\rho_{\ell^\infty} \colon G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective for all ℓ,*

(ii) $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$, *and*

(iii) $\sqrt{\Delta} \notin K^{\mathrm{cyc}}$.

Remark 1.3. Suppose Δ and Δ' are the discriminants of two Weierstrass models of E/K. Then $\Delta' = u^{12}\Delta$ for some $u \in K$. Thus $\Delta \notin K^{\mathrm{cyc}}$ if and only if $\Delta' \notin K^{\mathrm{cyc}}$. In other words, condition (iii) is well defined.

Remark 1.4. Condition (i) is clearly equivalent to the surjectivity of the restrictions of the projection maps π_ℓ to $\rho_E(G_K)$. As will be explained below, conditions (ii) and (iii) are equivalent to the surjectivity of the restriction of the abelianization map to $\rho_E(G_K)$.

This theorem suggests that when on the hunt for an elliptic curve with surjective adelic Galois representation, we should first find a "suitable" extension $K/\mathbb{Q}$ that satisfies condition (ii) and that could possibly satisfy condition (iii) for some E/K. Note first that for $K = \mathbb{Q}$, condition (iii) will never be satisfied, since $\sqrt{\Delta} \in \mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}^{\mathrm{cyc}}$. Thus there are no elliptic curves $E/\mathbb{Q}$ with surjective ρ_E. Likewise, condition (ii) will not be satisfied by any quadratic extension of $\mathbb{Q}$. With an eye toward finding a candidate number field of minimal degree, we should then cast our net among the non-Galois cubic extensions of $\mathbb{Q}$. A candidate number field K having been fixed, the more difficult task is finding an elliptic curve E/K satisfying condition (i). In our example we work over the field $\mathbb{Q}(\alpha)$, where α is the real root of $f(x) = x^3 + x + 1$. Thanks to similarities between the fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}$, we are able to extend to elliptic curves $E/\mathbb{Q}(\alpha)$ the techniques used in [Serre 72] to compute the ℓ-adic images of elliptic curves $E/\mathbb{Q}$. This allows us to easily find examples of elliptic curves over $\mathbb{Q}(\alpha)$ with surjective adelic Galois representations. We record one example here as a theorem.

Theorem 1.5. *Let $K = \mathbb{Q}(\alpha)$, where α is the real root of $f(x) = x^3 + x + 1$. Let E/K be the elliptic curve defined by the Weierstrass equation $y^2 + 2xy + \alpha y = x^3 - x^2$. The associated adelic representation $\rho_E \colon G_K \to \mathrm{GL}_2(\hat{\mathbb{Z}})$ is surjective.*

1.2 Related Results

The results of this paper first appeared in my doctoral thesis [Greicius 07], wherein I also asked, in the spirit of [Duke 97] and [Jones 06], whether in fact for any suitable K "most" elliptic curves have surjective adelic Galois representations. David Zywina has since answered this question in the affirmative.

In more detail, given a number field K with ring of integers $\mathcal{O}_K$, fix a norm $\|\cdot\|$ on $\mathbb{R} \otimes_{\mathbb{Z}} \mathcal{O}_K^2 \simeq \mathbb{R}^{2[K:\mathbb{Q}]}$. Given $x > 0$, define $B_K(x)$ to be the set of pairs $(a, b) \in \mathcal{O}_K^2$ having norm no greater than x for which the associated curve $E(a, b)$ given by $y^2 = x^3 + ax + b$ is an elliptic curve. Now define $S_K(x)$ to be the subset of $B_K(x)$ consisting of pairs (a, b) whose associated elliptic curves have surjective adelic Galois representations. In [Zywina 08] the following theorem is proved using sieve methods.

Theorem 1.6. (Zywina.) *Suppose $K \neq \mathbb{Q}$ satisfies $K \cap \mathbb{Q}^{\text{cyc}} = \mathbb{Q}$. Then*

$$\lim_{x \to \infty} \frac{|S_K(x)|}{|B_K(x)|} = 1.$$

In other words, most elliptic curves over K have surjective adelic Galois representation.

Remark 1.7. In fact, Zywina considers more generally the situation in which $K \cap \mathbb{Q}^{\text{cyc}}$ is not required to be $\mathbb{Q}$. As we recall below, in terms of arithmetic this means simply that the inclusion $\det(\rho_E(G_K)) \subseteq \hat{\mathbb{Z}}^*$ is not necessarily an equality. He proves [Zywina 08, Theorem 1.3] the expected generalization to this setting; namely, if $K \neq \mathbb{Q}$, then for "most" elliptic curves E/K we have $\rho_E(G_K) = \{A \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : \det A \in \det(\rho_E(G_K))\}$.

1.3 Notation and Conventions

Let G be a topological group, and let $H \subseteq G$ be a closed subgroup. The *commutator of H*, denoted by H', is the closure of the usual commutator subgroup $[H, H]$. By a quotient of G we shall always mean a continuous quotient. The *abelianization* of G is the quotient $G^{\text{ab}} := G/G'$.

The two isomorphisms of (1–1) give rise to reduction maps $r_m : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and projection maps $\pi_\ell : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$, respectively. Following [Lang and Trotter 76], we associate with these maps the following notation:

(i) Let $P \subset \mathbb{Z}$ be the set of prime numbers. Given any $S \subseteq P$ let π_S be the projection $\pi_S : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \prod_{\ell \in S} \mathrm{GL}_2(\mathbb{Z}_\ell)$. Furthermore, for any $X \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ we define $X_S := \pi_S(X)$. If $S = \{\ell\}$, we write X_ℓ instead of $X_{\{\ell\}}$. Thus, if we let $G = \mathrm{GL}_2(\hat{\mathbb{Z}})$, then under our notation we have $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ and $G_S = \prod_{\ell \in S} \mathrm{GL}_2(\mathbb{Z}_\ell)$.

(ii) Similarly, given any nonnegative integer m and any subset $X \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we define $X(m) = r_m(X) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

As a slight abuse, we will use the same notation when working with subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ or $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Let K be a number field with algebraic closure $\overline{K}$. We set $G_K := \mathrm{Gal}(\overline{K}/K)$. The set of finite places of K will be denoted by Σ_K. For a rational prime ℓ, let S_ℓ be the set of places of Σ_K lying above ℓ. Next, define $\Sigma_{\overline{K}}$ to be the inverse limit of the sets $\Sigma_{K'}$, where K' runs over the finite subextensions of $\overline{K}/K$. Fix a place $v \in \Sigma_K$. The completion at v is denoted by K_v, the residue field at v by k_v, and the cardinality of the residue field by N_v. We define $S_v := \{w \in \Sigma_{\overline{K}} : w \mid v\}$. Given $w \in S_v$, the *decomposition group* of w is defined as $D_w := \{\sigma \in G_K : \sigma(w) = w\}$. There is a surjection $D_w \twoheadrightarrow \mathrm{Gal}(\overline{k_v}/k_v)$. The kernel of this map is the *inertia group* of w, denoted by I_w. The Frobenius element Frob_w is the coset of D_w/I_w mapping to the Frobenius element of $\mathrm{Gal}(\overline{k_v}/k_v)$. A Galois representation ρ is *unramified at v* if $I_w \subseteq \ker \rho$ for some (and hence all) $w \in S_v$.

Lastly, if E/K is an elliptic curve, we define S_E to be the set of places in Σ_K where E has bad reduction.

2. SOME (PROFINITE) GROUP THEORY

In this section we set about proving Theorem 1.1. As we shall see, every proper closed subgroup H of a profinite group G is contained in a maximal closed subgroup, from which it follows that $H = G$ if and only if H is not contained in any maximal closed subgroup. The necessary and sufficient conditions described in Theorem 1.1 are then a consequence of Proposition 2.5 below, which describes the maximal closed subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ in terms of the quotient maps to $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\mathrm{GL}_2(\hat{\mathbb{Z}})^{\text{ab}}$.

2.1 Maximal Closed Subgroups

Definition 2.1. Let G be a topological group. A *maximal closed subgroup* of G is a closed subgroup $H \subsetneq G$ such that if K is closed and $H \subseteq K \subsetneq G$, then $H = K$.

Lemma 2.2. *Let G be a profinite group. Any closed subgroup $H \subsetneq G$ is contained in a maximal closed subgroup. All maximal closed subgroups of G are open.*

Proof. Let H be any proper closed subgroup of G. Since G is profinite, we have $H = \overline{H} = \bigcap\{HN | N \lhd_o G\}$ (see [Wilson 98, 0.3.3]). Here $N \lhd_o G$ signifies that N is a normal open subgroup of G. If $HN = G$ for all $N \lhd_o G$, then $H = G$, a contradiction. Thus there is an $N \lhd_o G$ such that $H \subseteq HN \subsetneq G$. Now consider the quotient map $\pi\colon G \to G/N$. Since N is open, the quotient group G/N is finite. Since $HN/N \subsetneq G/N$, there is a maximal subgroup $K \subsetneq G/N$ containing HN/N. Then $L = \pi^{-1}(K)$ is a maximal closed subgroup of G containing HN, and hence H. In fact L is open, since $[G : L]$ is finite. Thus we have proved that every proper closed subgroup is contained in an *open* maximal closed subgroup. It follows that maximal closed subgroups are themselves open. □

Consider now a product of profinite groups $G = \prod_{\alpha\in\Lambda} G_\alpha$. Since the projections π_α are all surjective, we get many maximal closed subgroups of G of the form $\pi_\alpha^{-1}(K_\alpha)$, where $K_\alpha \subsetneq G_\alpha$ is a maximal closed subgroup of G_α. Similarly, there are maximal closed subgroups of G arising from the abelianization $G^{\mathrm{ab}} = G/G'$ via the abelianization map $G \to G/G'$. We show below that under certain technical conditions all maximal closed subgroups of G are accounted for in this way. We will make use of the following notion.

Definition 2.3. Given a profinite group G, let $\mathrm{Quo}(G)$ be the set of isomorphism classes of finite, nonabelian, simple quotients of G.

Remark 2.4. In [Serre 98, IV-25], $\mathrm{Occ}(G)$ is similarly defined to be the set of (isomorphism classes of) finite nonabelian simple groups H that "occur" in G, in the sense that there exist closed subgroups $K_1 \subseteq K_2 \subseteq G$ with $K_1 \lhd K_2$ and $K_2/K_1 \simeq H$. We have $\mathrm{Quo}(G) \subseteq \mathrm{Occ}(G)$. As with Serre's Occ, the operation Quo behaves well with respect to inverse limits. Namely, If $G = \varprojlim G_\alpha$ is an inverse limit of profinite groups, and the maps $G \to G_\alpha$ are all surjective, then $\mathrm{Quo}(G) = \bigcup_{\alpha\in\Lambda} \mathrm{Quo}(G_\alpha)$. In particular, $\mathrm{Quo}(\prod_\alpha G_\alpha) = \bigcup \mathrm{Quo}(G_\alpha)$.

Proposition 2.5. *Let $\{G_\alpha\}_{\alpha\in\Lambda}$ be a family of profinite groups such that $Quo(G_\alpha) \cap Quo(G_{\alpha'}) = \varnothing$ for all $\alpha \neq \alpha'$. Let $G = \prod_{\alpha\in\Lambda} G_\alpha$ and suppose $H \subsetneq G$ is a maximal closed subgroup. Then either*

(i) *$H_\alpha = \pi_\alpha(H)$ is a maximal closed subgroup of G_α for some α, in which case $H = H_\alpha \times \prod_{\alpha'\neq\alpha} G_\alpha$,*

or

(ii) *$H_\alpha = G_\alpha$ for all α, in which case H contains G' and the image of H in $G^{\mathrm{ab}} = G/G'$ is maximal.*

In other words, all maximal closed subgroups of G arise either from a maximal closed subgroup of G_α for some $\alpha \in \Lambda$ or from a maximal closed subgroup of $G^{\mathrm{ab}} = G/G'$.

The proof of Proposition 2.5 will rely on the following variant of Goursat's lemma.

Lemma 2.6. (Topological Goursat's lemma.) *Let G_1, G_2 be profinite groups, and let H be a maximal closed subgroup of $G_1 \times G_2$ such that $\pi_i(H) = G_i$ for the two projections π_1 and π_2. Identifying the G_i with their canonical injections in $G_1 \times G_2$, let $N_i = H \cap G_i$. Then the N_i are open normal subgroups of the G_i, the quotients G_i/N_i are simple groups, and there is an isomorphism $\phi : G_1/N_1 \simeq G_2/N_2$, whose graph is induced by H.*

Proof. The proof that the N_i are open and normal is straightforward. The isomorphism ϕ then arises from the chain of isomorphisms $G_1/N_1 \simeq H/N_1N_2 \simeq G_2/N_2$.

It remains only to show that the G_i/N_i are simple. The isomorphism ϕ implies that $N_1 = G_1$ if and only if $N_2 = G_2$ if and only if $H = G_1 \times G_2$. Since H is maximal, we see that $N_1 \neq G_1$. Now suppose we had $N_1 \subsetneq N \subsetneq G_1$ for some normal subgroup $N \lhd G_1$. Since N is closed and normal in G_1, it is also closed and normal considered as a subgroup of $G_1 \times G_2$, in which case HN is closed and $H \subsetneq HN$. Furthermore, $HN \subsetneq G_1 \times G_2$, since $HN \cap G_1 = (H \cap G_1)N = N_1N = N \neq G_1$. This contradicts the fact that H is maximal. Thus there can be no such N. This proves that G_1/N_1 (and hence G_2/N_2) is simple. □

Proof of Proposition 2.5. If $H_\alpha \subsetneq G_\alpha$ for some α, then H_α is maximal in G_α. Furthermore, since $H \subseteq H_\alpha \times \prod_{\alpha'\neq\alpha} G_\alpha \subsetneq G$, we must have $H = H_\alpha \times \prod_{\alpha'\neq\alpha} G_\alpha$.

Assume now that $H_\alpha = G_\alpha$ for all $\alpha \in \Lambda$. Since $H \subsetneq G$ is open, there is a finite nonempty set $S \subseteq \Lambda$ such that $\ker \pi_S \subseteq H$. Since H is maximal, the projection H_S is a maximal closed subgroup of G_S and $H = H_S \times \prod_{\alpha'\notin S} G_{\alpha'}$. Since $G' = \prod_{\alpha\in\Lambda} G'_\alpha$, it suffices to prove the corresponding statement for H_S. In other words, we need only prove that given any finite set $S \subseteq \Lambda$ and any maximal closed subgroup $H \subseteq G_S$, if $H_\alpha = G_\alpha$ for all $\alpha \in S$, then $G'_S \subseteq H$. We do so using induction on $|S|$, the case $|S| = 1$ being trivial.

Assume $|S| > 1$. Take any $\alpha \in S$ and set $S' = S - \{\alpha\}$.

Suppose $H_{S'} \neq G_{S'}$. Then $H_{S'}$ is maximal and we have $H = H_{S'} \times G_\alpha$. By induction, $H_{S'}$ contains $G'_{S'}$, and thus H contains G'_S.

Suppose $H_{S'} = G_{S'}$. Let $N_{S'} = H \cap G_{S'}$ and let $N_\alpha = H \cap G_\alpha$, where we identify G_α with $\ker \pi_{S'}$ and $G_{S'}$ with $\ker \pi_\alpha$. By the topological Goursat's lemma, these subgroups are normal in G_S and there is an isomorphism of simple groups $G_{S'}/N_{S'} \simeq G_\alpha/N_\alpha$. But

$$\begin{aligned}\mathrm{Quo}(G_{S'}) \cap \mathrm{Quo}(G_\alpha) &= \mathrm{Quo}(\prod_{\alpha' \in S'} (G_{\alpha'})) \cap \mathrm{Quo}(G_\alpha)\\ &= \bigcup_{\alpha' \in S'} \mathrm{Quo}(G_{\alpha'}) \cap \mathrm{Quo}(G_\alpha)\\ &= \varnothing.\end{aligned}$$

Thus the simple groups $G_{S'}/N_{S'}$ and G_α/N_α are abelian, in which case $G'_{S'} \subseteq N_{S'}$ and $G'_\alpha \subseteq N_\alpha$. It follows that $G'_S \subseteq H$. □

Corollary 2.7. *Let H be a maximal closed subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}}) = \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell)$. Then either*

(i) *$H_\ell = \pi_\ell(H)$ is a maximal closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for some prime ℓ*

or

(ii) *$H_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all ℓ, in which case $G' \subseteq H$.*

Proof. We need only show that the groups $\mathrm{GL}_2(\mathbb{Z}_\ell)$ satisfy the technical condition of the proposition. We have

$$\begin{aligned}\mathrm{Quo}(\mathrm{GL}_2(\mathbb{Z}_\ell)) &= \mathrm{Quo}(\varprojlim \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}))\\ &= \bigcup \mathrm{Quo}(\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})).\end{aligned}$$

Now any element of $\mathrm{Quo}(\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}))$ must appear as one of the factor groups in a Jordan–Hölder series of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. However, as is well known, the only (potentially) simple factor group that appears in a Jordan–Hölder series of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is $\mathrm{PSL}_2(\mathbb{F}_\ell)$ (see [Serre 98, IV-25], for example). Then $\mathrm{Quo}(\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})) \subseteq \{[\mathrm{PSL}_2(\mathbb{F}_\ell)]\}$, where the brackets denote isomorphism class. Since $\mathrm{PSL}_2(\mathbb{F}_\ell) \not\simeq \mathrm{PSL}_2(\mathbb{F}_{\ell'})$ for $\ell \neq \ell'$, we have $\mathrm{Quo}(\mathrm{GL}_2(\mathbb{Z}_\ell)) \cap \mathrm{Quo}(\mathrm{GL}_2(\mathbb{Z}_{\ell'})) = \varnothing$. □

2.2 The Abelianization of $\mathrm{GL}_2(\hat{\mathbb{Z}})$

Theorem 1.1 follows easily from Corollary 2.7 once we have identified $\mathrm{GL}_2(\hat{\mathbb{Z}})^{\mathrm{ab}} = \mathrm{GL}_2(\hat{\mathbb{Z}})/(\mathrm{GL}_2(\hat{\mathbb{Z}}))'$. From the product description $\mathrm{GL}_2(\hat{\mathbb{Z}}) = \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell)$, we see immediately that $\mathrm{GL}_2(\hat{\mathbb{Z}})' = \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell)'$. So our task is reduced to determining $\mathrm{GL}_2(\mathbb{Z}_\ell)'$ for each prime ℓ.

Lemma 2.8. *Let $\ell \neq 2$ be prime. Then $\mathrm{GL}_2(\mathbb{Z}_\ell)' = \mathrm{SL}_2(\mathbb{Z}_\ell) = \ker(\mathrm{GL}_2(\mathbb{Z}_\ell) \xrightarrow{\det} \mathbb{Z}_\ell^*)$.*

Proof. See [Lang and Trotter 76, Part II, Section 3, Lemma 1, and Part III, Section 4]. □

The $\ell = 2$ case is slightly subtler. Recall first that we may identify $\mathrm{GL}_2(\mathbb{F}_2)$ with the permutation group $\mathfrak{S}_3$ by considering the matrices as permutations of the three nonzero vectors of $\mathbb{F}_2 \times \mathbb{F}_2$. This allows us to define a sign map $\mathrm{sgn}\colon \mathrm{GL}_2(\mathbb{F}_2) \to \{\pm 1\}$. By composing with reduction maps, we get sign maps from $\mathrm{GL}_2(\mathbb{Z}_2)$ and $\mathrm{GL}_2(\hat{\mathbb{Z}})$. By abuse of notation we will denote all of these maps by sgn.

Lemma 2.9. *The map $(\mathrm{sgn}, \det)\colon \mathrm{GL}_2(\mathbb{Z}_2) \to \{\pm 1\} \times \mathbb{Z}_2^*$ is surjective. We have*

$$\begin{aligned}\mathrm{GL}_2(\mathbb{Z}_2)' = (\ker \mathrm{sgn}) \cap \mathrm{SL}_2(\mathbb{Z}_2) = \ker \mathrm{GL}_2(\mathbb{Z}_2)\\ \xrightarrow{(\mathrm{sgn}, \det)} \{\pm 1\} \times \mathbb{Z}_2^*.\end{aligned}$$

Proof. See [Lang and Trotter 76, Part III, Section 2]. □

Combining the two lemmas yields the following result.

Proposition 2.10. *The map $(\mathrm{sgn}, \det)\colon \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \{\pm 1\} \times \hat{\mathbb{Z}}^*$ is surjective. The commutator subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is $\mathrm{GL}_2(\hat{\mathbb{Z}})' = \ker(\mathrm{sgn}, \det)$. We may identify the abelianization $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\hat{\mathbb{Z}})^{\mathrm{ab}}$ with*

$$\mathrm{GL}_2(\hat{\mathbb{Z}}) \xrightarrow{(\mathrm{sgn}, \det)} \{\pm 1\} \times \hat{\mathbb{Z}}^*.$$

We can now prove our first theorem.

Proof of Theorem 1.1. If $H = \mathrm{GL}_2(\hat{\mathbb{Z}})$, then conditions (i) and (ii) obviously hold. Suppose $H \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$ and $\pi_\ell(H) = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all primes ℓ. Then there is a maximal closed subgroup K with $H \subseteq K \subsetneq G$. Clearly K also satisfies $\pi_\ell(K) = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all primes ℓ. Then K contains the commutator subgroup $\mathrm{GL}_2(\hat{\mathbb{Z}})' = \ker(\mathrm{sgn}, \det)$, by Proposition 2.5. Since $K \neq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we have $(\mathrm{sgn}, \det)(K) \neq \{\pm 1\} \times \hat{\mathbb{Z}}^*$. Since $H \subseteq K$, we also have $(\mathrm{sgn}, \det)(H) \neq \{\pm 1\} \times \hat{\mathbb{Z}}^*$. □

2.3 Maximal Closed Subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$

It will be useful in what follows to have a more detailed picture of the maximal closed subgroup structure of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. According to Propositions 2.5 and 2.10, we may proceed by examining the maximal closed subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\mathrm{GL}_2(\hat{\mathbb{Z}})^{\mathrm{ab}} \simeq \{\pm 1\} \times \hat{\mathbb{Z}}^*$.

For the most part we will be concerned with maximal closed subgroups $H \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$ for which the determinant map is surjective. Of course, maximal closed subgroups with $\det(H) \neq \hat{\mathbb{Z}}^*$ correspond to maximal closed subgroups of $\hat{\mathbb{Z}}^*$. These in turn are neatly described by class field theory via the isomorphism $\hat{\mathbb{Z}}^* \simeq \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$.

2.3.1 Maximal Closed Subgroups Arising from $\{\pm 1\} \times \hat{\mathbb{Z}}^*$.

Let $H \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be a maximal closed subgroup such that $H_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all ℓ and $\det(H) = \hat{\mathbb{Z}}^*$. By Corollary 2.7 and the definition of $(\mathrm{sgn}, \det)$, this H corresponds to a maximal subgroup $\{\pm 1\} \times \hat{\mathbb{Z}}^*$ that surjects onto the two factors $\{\pm 1\}$ and $\hat{\mathbb{Z}}^*$. It follows easily that the corresponding subgroup is the kernel of a character $\{\pm 1\} \times \hat{\mathbb{Z}}^* \to \{\pm 1\}$ of the form (id, χ), for some nontrivial character $\chi \colon \hat{\mathbb{Z}}^* \colon \to \{\pm 1\}$. In other words, our original $H \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is the kernel of a character of the form $\mathrm{sgn} \cdot (\chi \circ \det)$ for some nontrivial character $\chi \colon \hat{\mathbb{Z}}^* \to \{\pm 1\}$; that is, $H = H_\chi := \{g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : \mathrm{sgn}(g) = \chi(\det(g))\}$. We call H_χ the *Serre subgroup of* $\mathrm{GL}_2(\hat{\mathbb{Z}})$ *with character* χ.

2.3.2 Maximal Closed Subgroups Arising from $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

Suppose now that our maximal closed subgroup corresponds to a subgroup $H \subsetneq \mathrm{GL}_2(\mathbb{Z}_\ell)$. Set $M := \mathrm{M}_2(\mathbb{Z}_\ell)$. The open normal subgroups $V_{\ell^n} := I + \ell^n M$ constitute a fundamental basis of open neighborhoods of the identity in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. For $n \geq 1$ the quotient $V_{\ell^n}/V_{\ell^{n+1}}$ is isomorphic to $\mathrm{M}_2(\mathbb{F}_\ell)$, and comes equipped with a $\mathrm{GL}_2(\mathbb{F}_\ell)$-module structure; multiplication by $g \in \mathrm{GL}_2(\mathbb{F}_\ell)$ is defined as $g \cdot (I + \ell^n A) := I + \ell^n GAG^{-1}$, where G is any lift of g to $\mathrm{GL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$. Now since H is open, it must contain V_{ℓ^n} for some n, in which case H corresponds to the maximal subgroup $H(\ell^n) \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. How big must n be before we can see this correspondence? This question is answered by the following lemmas and corollaries.

Lemma 2.11. [Lang and Trotter 76, Part I, Section 6, Lemmas 2 and 3] *Let* $U \subseteq V_\ell = I + \ell\,\mathrm{M}_2(\mathbb{Z}_\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$.

(i) *If* ℓ *is odd and* $U \twoheadrightarrow V_\ell/V_{\ell^2}$, *then* $U = V_\ell$.

(ii) *If* $\ell = 2$ *and* $U \cap V_4 \twoheadrightarrow V_4/V_8$, *then* $U \cap V_4 = V_4$. *If in addition* $U \twoheadrightarrow V_2/V_8$, *then* $U = V_2$.

Lemma 2.12. [Serre 98, IV-23] *Let* $\ell \geq 5$. *Suppose* $H \subseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ *is a closed subgroup such that* $H \twoheadrightarrow \mathrm{SL}_2(\mathbb{F}_\ell)$. *Then* $H = \mathrm{SL}_2(\mathbb{Z}_\ell)$.

Corollary 2.13. *Let* $H \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$ *be a closed subgroup.*

(i) *If* $\ell = 2$ *and* $H \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$, *then* $H = \mathrm{GL}_2(\mathbb{Z}_\ell)$.

(ii) *If* ℓ *is odd and* $H \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z})$, *then* $H = \mathrm{GL}_2(\mathbb{Z}_\ell)$.

(iii) *If* $\ell \geq 5$, $H \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$ *and* $\det(H) = \mathbb{Z}_\ell^*$, *then* $H = \mathrm{GL}_2(\mathbb{Z}_\ell)$.

Proof. The first two statements are simple consequences of Lemma 2.11 and the observation that if $H \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)/V_{\ell^n}$, then $(H \cap V_{\ell^r}) \twoheadrightarrow V_{\ell^r}/V_{\ell^n}$ for any $r < n$.

To prove the third statement, we need only show that $\mathrm{SL}_2(\mathbb{Z}_\ell) \subseteq H$. Since $H \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$, we also have $H' \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)' = \mathrm{SL}_2(\mathbb{F}_\ell)$. Then $H' \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)' = \mathrm{SL}_2(\mathbb{Z}_\ell)$ is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ that surjects onto $\mathrm{SL}_2(\mathbb{F}_\ell)$. Thus $H' = \mathrm{SL}_2(\mathbb{Z}_\ell)$, by Lemma 2.12, and we see that $\mathrm{SL}_2(\mathbb{Z}_\ell) \subseteq H$, as desired. □

Corollary 2.14. *The maximal closed subgroups of* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *are in one-to-one correspondence with*

(i) *the maximal subgroups of* $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ *if* $\ell = 2$;

(ii) *the maximal subgroups of* $\mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z})$ *if* ℓ *is odd.*

For $\ell \geq 5$ *the maximal closed subgroups of* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *with surjective determinant are in one-to-one correspondence with the maximal subgroups of* $\mathrm{GL}_2(\mathbb{F}_\ell)$ *with surjective determinant.*

The maximal subgroup structure of $\mathrm{GL}_2(\mathbb{F}_\ell)$ for ℓ prime is well known (see [Serre 72, Section 2.6] or [Mazur 77, p. 36], for example). According to Corollary 2.14, for $\ell \geq 5$ these account for all maximal closed subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with surjective determinant. For the primes 2 and 3, we get a few extra closed subgroups coming from $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, respectively. We conclude this section with a slightly closer look at the subgroup structure of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$.

Lemma 2.15. *Let* H *be a subgroup of* $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ *such that* $H \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. *Then* $[G : H] \leq 2$.

Proof. Set $M := \mathrm{M}_2(\mathbb{Z}/8\mathbb{Z})$. Since $H(I + 4M) = \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$, and since $\#(I + 4M) = 2^4$, we need only show that $\#(H \cap (I + 4M)) \geq 2^3$. For this it suffices to show that

$$H \cap (I + 4M) \supseteq \{I + 4A : \operatorname{tr} A \equiv 0 \pmod 2\}.$$

As above, $I + 4M$ is a $\mathrm{GL}_2(\mathbb{F}_2)$-module, where the action is defined by conjugation. Since $H \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_2)$, the subgroup $H \cap (I+4M) \subseteq I+4M$ is in fact a $\mathrm{GL}_2(\mathbb{F}_2)$-submodule of $I+4M$. Furthermore, $\{I+4A : \operatorname{tr} A \equiv 0 \pmod 2\}$ is generated as a $\mathrm{GL}_2(\mathbb{F}_2)$-module by $I+4\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$. Thus we need only show that $I+4\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right) \in H$. Since $H \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, it follows that H contains an element of the form

$$B = \left(I + 2\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\right)(I+4A).$$

Then H also contains $B^2 = I+4\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$. □

Corollary 2.16. *Let $H \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ be a closed subgroup such that $H \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ and $(\mathrm{sgn}, \det)(H) = \{\pm 1\} \times \mathbb{Z}_2^*$. Then $H = \mathrm{GL}_2(\mathbb{Z}_2)$.*

Proof. We need only prove that the mod-8 image $H(8)$ is all of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$. By the previous lemma, $H(8)$ is of index at most 2. Then $H(8)$ contains $\ker(\mathrm{sgn}, \det)$, the commutator of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$, and corresponds via $(\mathrm{sgn}, \det)$ to a subgroup of $\{\pm 1\} \times (\mathbb{Z}/8\mathbb{Z})^*$. But by hypothesis, $(\mathrm{sgn}, \det)(H(8)) = \{\pm 1\} \times (\mathbb{Z}/8\mathbb{Z})^*$. Thus $H(8) = \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ and $H = \mathrm{GL}_2(\mathbb{Z}_2)$. □

Remark 2.17. In fact, there are exactly seven index-2 subgroups of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$, corresponding to the seven nontrivial characters of $\{\pm 1\} \times \mathbb{Z}/8\mathbb{Z}^*$. Let us denote the three nontrivial characters of $(\mathbb{Z}/8\mathbb{Z})^*$ by χ_3, χ_5, and χ_7; here χ_i is the unique character whose kernel is generated by i in $(\mathbb{Z}/8\mathbb{Z})^*$. Then the index-2 subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$ are the kernels of the characters sgn, $\chi_i \circ \det$, and $\mathrm{sgn} \cdot (\chi_i \circ \det)$, where $i \in \{3, 5, 7\}$.

Suppose H is one of these index-2 subgroups. Then the image of H in $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ is either all of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ or of index 2. Furthermore, the image is of index 2 if and only if $(I+4M) \subseteq H$. The only subgroups above for which this is true are $\ker(\mathrm{sgn})$, $\ker(\chi_5 \circ \det)$, and $\ker(\mathrm{sgn} \cdot (\chi_5 \circ \det))$. Their corresponding images modulo 4 are the three subgroups of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ of index 2, namely $\ker(\mathrm{sgn})$, $\ker(\det) = \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$, and $\ker(\mathrm{sgn} \cdot \det)$.

3. SOME ARITHMETIC

3.1 The Adelic Representation

We return to the situation of an elliptic curve E/K with K a number field and consider its ℓ-adic representations $\rho_{E,\ell^\infty} \colon G_K \to \mathrm{GL}_2(\hat{\mathbb{Z}})$ and adelic representation $\rho_E \colon G_K \to \mathrm{GL}_2(\hat{\mathbb{Z}})$. Deriving necessary and sufficient conditions for ρ_E to be surjective is now simply an exercise in translating the statements of Theorem 1.1 into statements about our Galois representations.

Theorem 3.1. *Let E/K be an elliptic curve defined over a number field K. Let $\Delta \in K^\times$ be the discriminant of any Weierstrass model of E/K. Then ρ_E is surjective if and only if*

(i) *the ℓ-adic representation $\rho_{\ell^\infty} \colon G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective for all ℓ,*

(ii) *$K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$, and*

(iii) *$\sqrt{\Delta} \notin K^{\mathrm{cyc}}$.*

Proof. Set $H = \rho_E(G_K)$. According to Theorem 1.1, we have $H = \mathrm{GL}_2(\hat{\mathbb{Z}})$ if and only if $\pi_\ell(H) = \mathrm{GL}_2(\hat{\mathbb{Z}})$ for all ℓ and $(\mathrm{sgn}, \det)(H) = \{\pm 1\} \times \hat{\mathbb{Z}}^*$.

Since $\rho_{E,\ell^\infty} = \pi_\ell \circ \rho_E$, the first statement is clearly equivalent to condition (i) above. It remains to show that the surjectivity of $(\mathrm{sgn}, \det)|_H$ is equivalent to conditions (ii) and (iii). To do so, we must understand how sgn and det arise from the arithmetic of our elliptic curve.

The det map is easy to identify. From properties of the Weil pairing, it follows that it is essentially the cyclotomic character; i.e., we have a commutative diagram

$$\begin{tikzcd}
G_K \arrow[r, "\rho_E"] \arrow[dr, "\mathrm{res}"] & \mathrm{GL}_2(\hat{\mathbb{Z}}) \arrow[d, "\det"] \\
 & \mathrm{Gal}(K^{\mathrm{cyc}}/K) \simeq \hat{\mathbb{Z}}^*.
\end{tikzcd}$$

The sgn map, on the other hand, was defined as the composition

$$\mathrm{GL}_2(\hat{\mathbb{Z}}) \xrightarrow{r_2} \mathrm{GL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3 \xrightarrow{\mathrm{sgn}} \{\pm 1\}.$$

Since $r_2 \circ \rho_E = \rho_{E,2}$, if we start with some $\sigma \in G_K$, we see that $\mathrm{sgn}(\rho(\sigma))$ is ± 1 depending on whether σ is an even or odd permutation of the three nontrivial points of $E[2](\overline{K})$. If we choose a Weierstrass model for E/K and write e_i for the x-coordinates of the three nontrivial 2-torsion points, we have $\sqrt{\Delta} = \pm 4 \prod_{i>j}(e_i - e_j)$ (see [Serre 72, Section 5.3]). Thus σ is even if and only if $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$. In other words, $\mathrm{sgn} \circ \rho_E = \chi_\Delta$, where $\chi_\Delta \colon G_K \to \{\pm 1\}$ is the (possibly trivial) character defined by $K(\sqrt{\Delta})$.

Now consider the tower of fields

$$\begin{tikzcd}
 & & \overline{K} \arrow[dl, dash] \arrow[dd, dash, "G_K"] \arrow[dr, dash] & \\
 & K^{\mathrm{cyc}} \arrow[dl, dash] \arrow[dr, dash, "N_2"] & & K(\sqrt{\Delta}) \arrow[dl, dash, "N_1"'] \\
\mathbb{Q}^{\mathrm{cyc}} \arrow[dr, dash, "N_2"] \arrow[ddr, dash, "\hat{\mathbb{Z}}^*"'] & & K \arrow[dl, dash] & \\
 & K \cap \mathbb{Q}^{\mathrm{cyc}} \arrow[d, dash] & & \\
 & \mathbb{Q} & &
\end{tikzcd}$$

Here various Galois extensions have been labeled with their corresponding Galois group. Namely, we have (taking some liberties with identifications) $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}) = \hat{\mathbb{Z}}^*$, $\mathrm{Gal}(K(\sqrt{\Delta})/K) = N_1 \subseteq \{\pm 1\}$ and $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/K \cap \mathbb{Q}^{\mathrm{cyc}}) = \mathrm{Gal}(K^{\mathrm{cyc}}/K) = N_2 \subseteq \hat{\mathbb{Z}}^*$.

We have just seen that the map $(\mathrm{sgn}, \det) \circ \rho_E \colon G_K \to \{\pm 1\} \times \hat{\mathbb{Z}}^*$ is just the product of the restriction maps

$$\begin{aligned} G_K &\xrightarrow{\mathrm{res}\times\mathrm{res}} N_1 \times N_2, \\ \sigma &\longmapsto (\sigma|_{K(\sqrt{\Delta})}, \sigma|_{K^{\mathrm{cyc}}}), \end{aligned}$$

and in general we have $(\mathrm{sgn}, \det)(H) \subseteq N_1 \times N_2 \subseteq \{\pm 1\} \times \hat{\mathbb{Z}}^*$. Thus $(\mathrm{sgn}, \det)(H) = \{\pm 1\} \times \hat{\mathbb{Z}}^*$ if and only if both set inequalities in this chain are in fact equalities. By Galois theory, the first inequality is an equality if and only if $\sqrt{\Delta} \notin K^{\mathrm{cyc}}$, and the second inequality is an equality if and only if $\sqrt{\Delta} \notin K$ and $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$. Combining these, we conclude that $(\mathrm{sgn}, \det)(H) = \{\pm 1\} \times \hat{\mathbb{Z}}^*$ if and only if $\sqrt{\Delta} \notin K^{\mathrm{cyc}}$ and $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$. □

Remark 3.2. Conditions (ii) and (iii) are equivalent to the single statement

(ii)′ $K(\sqrt{\Delta}) \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$.

Though this has the advantage of brevity, we prefer the stated form of the theorem, since it more clearly points the way to finding elliptic curves with surjective adelic representations.

Remark 3.3. The theorem and its proof elucidate what happens when $K = \mathbb{Q}$. Since $\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$, we have $\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}^{\mathrm{cyc}}$. Tracing through the various maps, we see that for any $\sigma \in G_{\mathbb{Q}}$,

$$\begin{aligned} \mathrm{sgn}(\rho_E(\sigma)) = \sigma|_{\mathbb{Q}(\sqrt{\Delta})} &= (\sigma|_{\mathbb{Q}^{\mathrm{cyc}}})|_{\mathbb{Q}(\sqrt{\Delta})} \\ &= \chi_\Delta(\det(\rho_E(\sigma))), \end{aligned}$$

where as before, $\chi_\Delta \colon \hat{\mathbb{Z}}^* \to \{\pm 1\}$ is the (possibly trivial) character arising from the extension $\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}$. Then $\rho_E(G_{\mathbb{Q}})$ is contained in the Serre subgroup $H_{\chi_\Delta} = \{g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : \mathrm{sgn}\, g = \chi_\Delta(\det g)\}$. Thus $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] \geq [\mathrm{GL}_2(\hat{\mathbb{Z}}) : H_{\chi_\Delta}] = 2$. In particular, $\rho_{E/\mathbb{Q}}(G_{\mathbb{Q}}) \neq \mathrm{GL}_2(\hat{\mathbb{Z}})$.

3.2 Semistable Elliptic Curves

Guided now by Theorem 3.1, we would like to find elliptic curves E/K for which ρ_{E,ℓ^∞} is surjective for all ℓ. Recall that when E/K is non-CM, the adelic image is open, which implies that $\rho_{E,\ell^\infty}(G_K) = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all but finitely many primes. Accordingly, we will call the primes ℓ for which ρ_{E,ℓ^∞} is not surjective the *exceptional primes of* E/K. Ideally, we would like to be able to determine the set of exceptional primes for any given non-CM elliptic curve. For $\ell \geq 5$, Corollary 2.13 and the surjectivity of $\det : \rho_{E,\ell^\infty}(G_K) \to \mathbb{Z}_\ell^*$ imply that ρ_{E,ℓ^∞} is surjective if and only if $\rho_{E,\ell}$ is surjective. For $\ell = 2, 3$ we have to do a little more work.

In either case, an important first step is to determine the mod-ℓ image $\rho_{E,\ell}(G_K)$ for all ℓ. It turns out that we can learn much about $\rho_{E,\ell}(G_K)$ simply by studying the image of inertia $\rho_{E,\ell}(I_w)$ for various inertia subgroups $I_w \subseteq \mathrm{Gal}(\overline{K}/K)$. (See Section 1.3 for notation and definitions related to inertia groups.) Serre studies inertia representations extensively in [Serre 72]. When the non-CM elliptic curve E is semistable, the results are particularly nice, yielding techniques for computing the exceptional primes of E. Modulo some group theory, everything follows from the picture of the inertia representations given by the lemma below, which is essentially a synthesis of various facts scattered throughout [Serre 72]—more specifically, the corollary to Proposition 13 in Section 1.12 and some properties of semistable curves discussed in Section 5.4.

Lemma 3.4. *Let K be a number field, ℓ a rational prime unramified in K, and E/K a semistable elliptic curve with j-invariant j_E. Fix $v \in \Sigma_K$ and $w \in \Sigma_{\overline{K}}$ with $w \mid v$. Recall that S_E is the set of bad places of E/K, and that S_ℓ is the set of places $v \in \Sigma_K$ such that $v \mid l$. Then we have the following:*

(i) *If $v \in \Sigma_K - S_E - S_\ell$, then $\rho_{E,\ell}(I_w)$ is trivial.*

(ii) *If $v \in S_E - S_\ell$, then $\rho_{E,\ell}(I_w)$ is either trivial or cyclic of order ℓ.*

(iii) *If $v \in S_E$ and $\ell \nmid v(j_E)$, then $\rho_{E,\ell}(I_w)$ contains an element of order ℓ.*

(iv) *If $v \mid l$, then*

$$\rho_{E,\ell}(I_w) = \left\{ \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix} : s \in \mathbb{F}_\ell^* \right\}$$

when E has (good) ordinary reduction at v,

$$\rho_{E,\ell}(I_w) = \left\{ \begin{pmatrix} s & t \\ 0 & 1 \end{pmatrix} : s \in \mathbb{F}_\ell^*, t \in \mathbb{F}_\ell \right\}$$

when E has bad (multiplicative) reduction at v, and $\rho_{E,\ell}(I_w)$ is a nonsplit Cartan subgroup when E has (good) supersingular reduction at v.

Amazingly enough, this simple description of the inertia representations imposes strict restrictions on nonsurjective mod-ℓ representations arising from a semistable E/K. The propositions and corollaries that follow are for the most part straightforward generalizations of the results in [Serre 72, Section 5.4]. We formulate them for a number field K satisfying the following properties:

(i) There is a real embedding $K \hookrightarrow \mathbb{R}$. This gives rise to a complex conjugation map $\sigma \in G_K$ satisfying $\sigma^2 = 1$ and $\det(\rho_{E,\ell}(\sigma)) = -1$ for all $\ell \geq 3$. It follows that $\rho_{E,\ell}(\sigma)$ is diagonalizable in $\mathrm{GL}_2(\mathbb{F}_\ell)$ for all $\ell \geq 3$, with eigenvalues 1 and -1.

(ii) The narrow class group $\mathcal{C}_K^\infty$ is trivial. Recall that $\mathcal{C}_K^\infty$ is the group of fractional ideals of K modulo the subgroup of totally real principal fractional ideals. This assumption has as a consequence that any abelian extension of K unramified at all finite primes is trivial.

(iii) We have $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$. This property ensures that $\det\colon \rho_E(G_K) \to \hat{\mathbb{Z}}^*$ is surjective.

Proposition 3.5. *Let K be a number field with a real embedding and a trivial narrow class group and satisfying $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$. Let E/K be a semistable elliptic curve with j-invariant j_E. Suppose ℓ is a prime unramified in K. If $\ell = 2, 3, 5$, suppose further that $\ell \nmid v(j_E)$ for some $v \in S_E$. If $\rho_{E,\ell}(G_K) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$, then $\rho_{E,\ell}(G_K)$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

Proof. The proposition is nearly identical to [Serre 72, Proposition 21]. As such we are content to sketch a proof, mainly just to illustrate Lemma 3.4 at work.

If $v \in S_E$ and $\ell \nmid v(j_E)$, then according to Lemma 3.4, the mod-ℓ image contains an element of order ℓ. From group theory it follows that the mod-ℓ image either contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ or is contained in a Borel subgroup. The former is impossible, since the determinant map is surjective (since $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$), and we assume that the mod-ℓ representation is not surjective.

Now assume that ℓ is unramified in K and $\ell \geq 7$. Lemma 3.4 implies that the mod-ℓ image contains a split semi-Cartan subgroup or a nonsplit Cartan subgroup. Again it follows from group theory that the mod-ℓ image is contained in either a Borel subgroup or a Cartan subgroup, or else it is contained in the normalizer of a Cartan subgroup, but not the Cartan subgroup itself. The last case would give rise to a (nontrivial) unramified character $\chi\colon G_L \to \{\pm 1\}$, contradicting the fact that K has trivial narrow class group. If the mod-ℓ image is contained in a Cartan subgroup, it must be a split Cartan subgroup, thanks to the complex conjugation $\sigma \in G_K$, which is diagonalizable modulo ℓ. Since split Cartan subgroups are contained in a Borel subgroup, we are done. □

As we mentioned in the introduction, Theorem 3.1 leads the hunter of elliptic curves with surjective adelic representations naturally to non-Galois cubic extensions of $\mathbb{Q}$. With this in mind we include the following corollaries, which specialize to number fields K with $[K : \mathbb{Q}] = 3$. Note that in this case the existence of a real embedding is automatic.

Corollary 3.6. *Let E, K, and ℓ be as in Proposition 3.5 and suppose that $\rho_{E,\ell}(G_K) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$. Assume further that $[K : \mathbb{Q}] = 3$ and that $(U_K^+ - 1) \cap U_K \neq \varnothing$. There is a basis of $E[l](\overline{K})$ in terms of which $\rho_{E,\ell}$ is of the form $\left(\begin{smallmatrix} \chi_1 & * \\ 0 & \chi_2 \end{smallmatrix}\right)$ for characters $\chi_i : G_K \to \mathbb{F}_\ell^*$. Furthermore, one of the characters is trivial and the other is $\det \circ \rho_{E,\ell}$.*

Remark 3.7. Recall that U_K (respectively U_K^+) is the group of units (respectively totally positive units) of K.

Proof. Since $\rho_{E,\ell}(G_K) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$, Proposition 3.5 implies that $\rho_{E,\ell}(G_K)$ is contained in a Borel subgroup. The first statement now follows easily.

Assume that we have picked a basis such that $\rho_{E,\ell}$ is of the form $\left(\begin{smallmatrix} \chi_1 & * \\ 0 & \chi_2 \end{smallmatrix}\right)$. Since $\chi_1 \cdot \chi_2 = \det \circ \rho_{E,\ell}$, we need only show that one of the characters is trivial. A character $\chi\colon G_K \to \mathbb{F}_\ell^*$ is trivial if and only if it is unramified for all $v \in \Sigma_K$—a consequence of K having trivial narrow class group. Thus we need only show that one of the two characters is unramified everywhere.

First observe that both characters are unramified for all $v \nmid l$. Indeed, if $v \notin S_E$ and $v \nmid l$, then $\rho_{E,\ell}$ is itself unramified. Likewise, if $v \in S_E$ and $v \nmid l$, then by Lemma 3.4, for any $w \mid v$ the image of I_w in $\mathrm{GL}_2(\mathbb{F}_\ell)$ is either trivial or cyclic of order ℓ. In either case, we see that

$$\rho_{E,\ell}(I_w) \subseteq \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} : t \in \mathbb{F}_\ell \right\},$$

whence both χ_i are unramified. So it remains only to show that there is one character that is also unramified at each place $v \mid l$. The argument now divides into cases depending on the splitting behavior of ℓ.

Case 1: ℓ is inert. Take the unique $v \mid l$ and an inertia group I_w for some $w \mid v$. The image of inertia $\rho_{E,\ell}(I_w)$ cannot be a nonsplit Cartan subgroup, since it is contained in a Borel subgroup. But then by Lemma 3.4, $\rho_{E,\ell}(I_w)$ must be of the form $\left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$. Then one of the χ_i, call it χ_{i_0}, is trivial when restricted to I_w. This shows that χ_{i_0} is unramified at v, and hence everywhere, as desired.

Case 2: ℓ is totally split. Suppose $(\ell) = \mathfrak{pqr}$. As in the inert case, at each $v \mid l$, exactly one of the characters is unramified. Since there are three places above ℓ, by the pigeonhole principle one of the characters, call it χ_{i_0}, is unramified at at least two of the places.

Suppose χ_{i_0} is ramified at exactly one place. Assume that this place is $v = \mathfrak{p}$. In terms of Galois theory, χ_{i_0} corresponds to an abelian extension L/K with $\mathrm{Gal}(L/K) \simeq \mathbb{F}_\ell^*$ such that only $\mathfrak{p}$ and possibly ∞ ramify in L. According to class field theory, there is a modulus of the form $\mathfrak{m} = \infty \cdot \mathfrak{p}^n$ such that L is contained in the ray class field $K_\mathfrak{m}$. We then have a surjection $\mathcal{C}_K^\mathfrak{m} \simeq \mathrm{Gal}(K_\mathfrak{m}/K) \twoheadrightarrow \mathrm{Gal}(L/K) \simeq \mathbb{F}_\ell^*$, where $\mathcal{C}_K^\mathfrak{m}$ is the group of fractional ideals of K relatively prime to $\mathfrak{p}$ modulo the group of principal ideals of the form (a), where $a \equiv 1 \pmod{\mathfrak{p}^n}$ and a is totally positive. Furthermore, there is an exact sequence [Neukirch 99, Section VI.1]

$$1 \to U_K^+/U_{\mathfrak{m},1} \to (\mathcal{O}_K/\mathfrak{p}^n)^* \to \mathcal{C}_K^\mathfrak{m} \to \mathcal{C}_K^\infty \to 1,$$

where $U_{\mathfrak{m},1}$ is the subgroup of totally positive units that are congruent to 1 modulo $\mathfrak{p}^n$. Since $\mathcal{C}_K^\infty = 1$ in our case, we get a composition of surjections

$$(\mathcal{O}_K/\mathfrak{p}^n)^* \twoheadrightarrow \mathcal{C}_K^\mathfrak{m} \twoheadrightarrow \mathbb{F}_\ell^*,$$

whose kernel contains $U_K^+/U_{\mathfrak{m},1}$. Since $\ell \nmid (\ell - 1)$, the composition must factor as

$$\begin{tikzcd}
(\mathcal{O}_K/\mathfrak{p}^n)^* \arrow[rr, two heads] \arrow[dr, two heads] & & \mathbb{F}_\ell^* \, . \\
& (\mathcal{O}_K/\mathfrak{p})^* \arrow[ur, two heads] &
\end{tikzcd}$$

Since $(\mathcal{O}_K/\mathfrak{p})^* \simeq \mathbb{F}_\ell^*$, the surjection $(\mathcal{O}_K/\mathfrak{p})^* \twoheadrightarrow \mathbb{F}_\ell^*$ is in fact an isomorphism.

Now take any $u \in (U_K^+ - 1) \cap U_K$. Then u is a unit and $u + 1 \in U_K^+$. Since the image of $u + 1$ in $(\mathcal{O}_K/\mathfrak{p})^*$ is in the kernel of the isomorphism $(\mathcal{O}_K/\mathfrak{p})^* \to \mathbb{F}_\ell^*$, we must have $u + 1 \equiv 1 \pmod{\mathfrak{p}}$. But then $u \equiv 0 \pmod{\mathfrak{p}}$, a contradiction because u is a unit. Thus χ_{i_0} must be ramified at all places in S_ℓ, and hence at all places in Σ_K. It follows that χ_{i_0} is trivial.

Case 3: $(\ell) = \mathfrak{pq}$. Lastly, suppose $(\ell) = \mathfrak{pq}$, with $f(\mathfrak{p}) := [\mathcal{O}_K/\mathfrak{p}\mathcal{O} : \mathbb{F}_\ell] = 2$. Assume that each character is ramified at exactly one of the primes lying above ℓ. Suppose χ_{i_0} is ramified at $\mathfrak{q}$ and χ_{1-i_0} is ramified at $\mathfrak{p}$. Then, using χ_{i_0}, we may argue exactly as in the totally split case to show that $\alpha \in \mathfrak{q}$, a contradiction. Thus one of the characters is unramified at both primes lying above ℓ, making it trivial. □

Corollary 3.8. *Let E, K, and ℓ be as in Corollary 3.6 and $\rho_{E,\ell}(G_K) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$. Given $v \in \Sigma_K - S_E$, let $\phi_v \in \mathrm{End}(\tilde{E_v})$ be the Frobenius endomorphism and let t_v be its trace. Then $t_v \equiv 1 + N_v \pmod{l}$.*

Remark 3.9. Since $\#\tilde{E}_v(k_v) = 1 - t_v + N_v$, the condition $t_v \equiv 1 + N_v \pmod{l}$ is equivalent to $\ell \mid \#\tilde{E}_v(k_v)$.

Proof. Suppose first that $v \in \Sigma_K - S_E - S_\ell$. The representation ρ_{ℓ^∞} is unramified at v, and the ℓ-adic Tate modules of E/K and its reduction $\tilde{E}_v/k_v$ are isomorphic as D_w/I_w-modules for any $w \in S_v$. Then $\mathrm{tr}(\phi_v) = \mathrm{tr}(\rho_\ell(\mathrm{Frob}_w)) \pmod{l}$ and $N_v = \det(\phi_v) = \det(\rho_\ell(\mathrm{Frob}_w)) \pmod{l}$ for any $w \in S_v$. (Observe that although strictly speaking Frob_w is a coset in D_w/I_w, the value $\rho_\ell(\mathrm{Frob}_w)$ is well defined, since ρ_ℓ is unramified at v.)

Now by Corollary 3.6,

$$\begin{aligned} t_v \equiv \mathrm{tr}(\rho_\ell(\mathrm{Frob}_w)) &\equiv \chi_1(\mathrm{Frob}_w) + \chi_2(\mathrm{Frob}_w) \\ &\equiv 1 + \det(\rho_{E,\ell}(\mathrm{Frob}_w)) \\ &\equiv 1 + \det(\rho_\ell(\mathrm{Frob}_w)) \\ &\equiv 1 + N_v \pmod{l}, \end{aligned}$$

and the claim is proved in this case.

Now suppose $v \notin S_E$ but $v \in S_\ell$. Since $\rho_{E,\ell}(G_K)$ is contained in a Borel subgroup, it cannot contain a nonsplit Cartan subgroup. It follows from Lemma 3.4 that E has ordinary reduction at v.

First consider $\ell = 2$. Let v be a place of K lying over 2. Since E has good ordinary reduction at v, the reduction $\tilde{E}_v$ has exactly one point, P, of order 2. Then P is fixed by $\mathrm{Gal}(\overline{k_v}/k_v)$, and hence is k_v-rational. But then 2 divides $\#\tilde{E}_v(k_v) = 1 - t_v + N_v$, in which case $t_v \equiv 1 + N_v \pmod 2$.

Now consider $\ell \geq 3$. Pick a basis $\{P_1, P_2\}$ of $E[\ell][\overline{K}]$ such that $\rho = \left(\begin{smallmatrix}\chi_1 & * \\ 0 & \chi_2\end{smallmatrix}\right)$, as in Corollary 3.6. We know that one of the χ_i is trivial.

Suppose $\chi_1 = 1$. Then E has a K-rational point P of order ℓ. If $\langle P\rangle$ is in the kernel of the reduction map, we have an exact sequence

$$0 \to \langle P\rangle \to E[l](\overline{K}) \to \tilde{E}_v[l](\overline{k_v}) \to 0.$$

But then the representation of I_w for any $w \mid v$ looks like $\left(\begin{smallmatrix}1 & * \\ 0 & 1\end{smallmatrix}\right)$, contradicting Lemma 3.4. Thus the reduction map sends P to a nontrivial k_v-rational point of $\tilde{E}_v[l](k_v)$. It follows that ℓ divides $\#\tilde{E}_v(k_v)$, whence $t_v \equiv 1 + N_v \pmod l$.

Suppose $\chi_2 = 1$. Let C be the G_K-invariant cyclic subgroup defined by P_1. Consider the quotient $E' = E/C$. Since E' is isogenous to E, it has the same reduction type at all places of Σ_K, and furthermore $\rho_{E'} \sim \rho_E$. In particular, it follows that $t'_v = t_v$ and $\#\tilde{E}'_v(k_v) = \#\tilde{E}_v(k_v)$ for our place v. Now since χ_2 is trivial, $E'[l]$ has a nontrivial K-rational point, and we may argue as in the $\chi_1 = 1$ case to prove $t_v \equiv 1 + N_v \pmod l$. □

Suppose K satisfies the conditions of the previous corollaries. We now have the necessary means for determining the set of primes ℓ for which $\rho_{E,\ell}$ is surjective for a given semistable elliptic curve E/K. First compute $\#\tilde{E}_v(k_v)$ for some $v \notin S_E$. Let R be the set of prime divisors of $\#\tilde{E}_v(k_v)$ and let T be the set of primes in $\mathbb{Z}$ that ramify in K. According to Corollary 3.8, the set of primes ℓ for which $\rho_{E,\ell}$ is not surjective is contained in $\{2,3,5\} \cup R \cup T$. For this finite set of primes we can then use the following criterion for checking whether $\rho_{E,\ell}(G_K) = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Proposition 3.10. *Let $\ell \geq 5$, and suppose $H \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ is a subgroup satisfying*

(i) *H contains elements s_1, s_2 such that $\left(\frac{\operatorname{tr}(s_i)^2 - 4\det(s_i)}{l}\right) = (-1)^i$ and $\operatorname{tr}(s_i) \neq 0$.*

(ii) *H contains an element t such that $u = \operatorname{tr}(t)^2/\det(t) \neq 0, 1, 2, 4$ and $u^2 - 3u + 1 \neq 0$.*

Then H contains $\mathrm{SL}(\mathbb{F}_\ell)$. In particular, if $\det : H \to \mathbb{F}_\ell^*$ is surjective, then $H = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Proof. See [Serre 72, Propostion 19]. □

3.3 A Suitable Cubic Extension

Let us fix a suitable number field. For the remainder of the paper we will let K be the cubic extension $\mathbb{Q}(\alpha)$, where α is the real root of $f(x) = x^3 + x + 1$.

We easily see that K satisfies the conditions of Corollaries 3.6 and 3.8. The root α defines the sole real embedding $K \hookrightarrow \mathbb{R}$. The discriminant of f is -31. This implies that K is non-Galois, and hence that $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$. It also follows that the ring of integers $\mathcal{O}_K$ is $\mathbb{Z}[\alpha]$, and that 31 is the only rational prime that ramifies in $\mathcal{O}_K$. Further computation then reveals that the ideal and narrow class groups of K are trivial. Lastly we show that α is an element of $(U_K^+ - 1) \cap U_K$. Since $\alpha(\alpha^2 + 1) = -1$, we have $\alpha \in U_K$. (In fact, one can show that α generates U_K.) But then $\alpha + 1 = -\alpha^3$ is also a unit. It is also not difficult to see that $\alpha + 1$ is positive, and hence totally positive. Thus we have $\alpha + 1 \in U_K^+$ and $\alpha \in (U_K^+ - 1)$.

As described in Section 3.2, with the help of Corollaries 3.6 and 3.8 we can now easily find elliptic curves $E/\mathbb{Q}(\alpha)$ with surjective adelic representations.

3.4 An Example

Let $K = \mathbb{Q}(\alpha)$ and let E/K be the elliptic curve $y^2 + 2xy + \alpha y = x^3 - x^2$. We compute $(\Delta_E) = P_{131}Q_{2207}$, where the rational primes 131 and 2207 factor as $(131) = P_{131}Q_{131}R_{131}$ and $(2207) = P_{2207}Q_{2207}$, with $f(P_{2207}) = 2$. Furthermore, $(j_E) = (2)^{12}(3)^3/Q_{131}Q_{2207}$. Since the conductor of an elliptic curve divides the discriminant [Silverman 94, IV.11.2], we see that E is semistable with conductor $N = P_{131}Q_{2207}$.

Set $H = \rho(G_K) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$. From the splitting behavior of 131 and 2207 we may deduce that $\sqrt{\Delta} \notin K^{\mathrm{cyc}}$. Since in addition $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$, it follows that the abelianization map $(\mathrm{sgn}, \det)\colon H \to \{\pm 1\} \times \hat{\mathbb{Z}}^*$ is surjective. By Theorem 3.1 we need only show that E/K has no exceptional primes, i.e., that $H_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all primes ℓ.

Recall that for a good place $v \in S_E$, we denote by t_v the trace of the Frobenius element $\phi_v \in \mathrm{End}(\tilde{E}_v)$. Using Magma, we now reduce at various places to obtain Table 1.

Since $v(j_E) = -1$ for all $v \in S_E$, it follows from Corollary 3.8 that for all $\ell \neq 31$, if $H(\ell) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$, then $\ell \mid 16$ and $\ell \mid 15$ (the values of $\#\tilde{E}_v(k_v)$ in rows 2 and 3 of our table). There is no such ℓ. Thus $H(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$ for all $\ell \neq 31$. Since $\det_H$ is surjective, Corollary 2.13 implies $H_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all $\ell \neq 2, 3, 31$. It remains only to show that these three primes are not exceptional.

v	$\#\tilde{E}_v(k_v)$	N_v	t_v	
(7)	324	343	20	$(t_v^2 - 4N_v^2) \equiv 20 \pmod{31}$
Q_{11}	16	11	-4	$(t_v^2 - 4N_v^2) \equiv 3 \pmod{31}$
Q_{23}	15	23	9	
Q_{29}	24	29	6	

TABLE 1. Traces of Frobenius elements.

Case $\ell = 31$. The values (modulo 31) of $t_v^2 - 4N_v^2$ for $v = (7)$ and $v = Q_{11}$ are 20 and 3 respectively. The first is a square modulo 31; the second is not. Furthermore, for $v = (7)$ we have $u = t_v^2/N_v \equiv 10 \not\equiv 0, 1, 2, 4 \pmod{31}$ and $u^2 - 3u + 1 \not\equiv 0 \pmod{31}$. Thus setting s_1 and t equal to $\rho_{E,31}(\mathrm{Frob}_w)$ for any $w \mid (7)$, and setting s_2 equal to $\rho_{E,31}(\mathrm{Frob}_{w'})$ for any $w' \mid Q_{11}$, we see that $H(31) \subseteq \mathrm{GL}_2(\mathbb{F}_{31})$ satisfies the conditions of Proposition 3.10. Thus $H(31)$ contains $\mathrm{SL}_2(\mathbb{F}_{31})$. Since $\det : H(31) \to \mathbb{F}_{31}^*$ is surjective, we have $H(31) = \mathrm{GL}_2(\mathbb{F}_{31})$, and hence $H_{31} = \mathrm{GL}_2(\mathbb{Z}_{31})$.

Case $\ell = 3$. Let $M := \mathrm{M}_2(\mathbb{Z}_3)$. Since $H(3) = \mathrm{GL}_2(\mathbb{F}_3)$, we need only show that $H \supseteq I + 3M$. By Lemma 2.11, it suffices to show that $H(9) \supseteq (I + 3M)/(I + 9M)$. Let $v = Q_{29}$, and let $\pi \in H_3$ be $\rho(\mathrm{Frob}_w)$ for any $w \in S_v$. From our table, the characteristic polynomial of π is $t^2 - 6t + 29$. Modulo 9 this factors as $(t - 7)(t - 8)$. Since $7 \not\equiv 8 \pmod{3}$, π is diagonalizable in $\mathrm{GL}_2(\mathbb{Z}_3)$. After a change of basis, we may assume that $\pi \equiv \left(\begin{smallmatrix} -2 & 0 \\ 0 & -1 \end{smallmatrix}\right) \pmod{9}$, in which case

$$\pi^2 \equiv \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \equiv I + 3 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \pmod{9}.$$

But $(I + 3M)/(I + 9M)$ is a $\mathrm{GL}_2(\mathbb{F}_3)$-module, and since $H(9) \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_3)$, it follows that $H(9) \cap (I + 3M)/(I + 9M)$ is a $\mathrm{GL}_2(\mathbb{F}_3)$-submodule. (See Section 2.3.2.) Furthermore, it is easily seen that $I + 3 \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ generates $(I + 3M)/(I + 9M)$ as a $\mathrm{GL}_2(\mathbb{F}_3)$-module. Thus $H(9) \supseteq (I + 3M)/(I + 9M)$, and hence $H_3 = \mathrm{GL}_2(\mathbb{Z}_3)$.

Case $\ell = 2$. Let $M := \mathrm{M}_2(\mathbb{Z}_2)$. First we will show that $H(4) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. Since $H \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_2)$, it suffices to show that $H(4) \supseteq (I + 2M)/(I + 4M)$.

Let $\pi = \rho_{2^\infty}(\sigma) \in H_2$ be the image of a complex conjugation automorphism $\sigma \in G_K$. A calculation shows that Δ_E is positive (thinking of $K = \mathbb{Q}(\alpha)$ as a subfield of $\mathbb{R}$). Thus $\sqrt{\Delta_E}$ is fixed by complex conjugation. This means that $\pi \in \ker(H_2 \xrightarrow{\mathrm{sgn}} \{\pm 1\}) = N(2^\infty)$; i.e., the image $r_2(\pi)$ is contained in the normal subgroup

$$\left\{ I, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{F}_2).$$

But from the remarks in Section 3.3, we have $\operatorname{tr} \pi = 1 + (-1) = 0$. Thus $\pi \equiv I \pmod{2}$; i.e., we have $\pi = I + 2A \in I + 2M$. Since the characteristic polynomial of π is $t^2 - 1$, it follows that the characteristic polynomial of A is $t^2 + t$. Since this has distinct roots modulo 2, it follows that A, and hence π, is diagonalizable in $\mathrm{GL}_2(\mathbb{Z}_2)$. After a suitable change of basis we may assume that

$$\pi = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = I + 2 \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} =: I + 2A.$$

As with the $\ell = 3$ case, since $H(2) = \mathrm{GL}_2(\mathbb{F}_2)$, the subgroup $H(4) \cap (I + 2M)/(I + 4M)$ is in fact a $\mathrm{GL}_2(\mathbb{F}_2)$-submodule of $(I + 2M)/(I + 4M)$. Again it is easily seen that $I + 2A$ generates $(I + 2M)/(I + 4M)$ as a $\mathrm{GL}_2(\mathbb{F}_2)$-module. Thus

$$H(4) \supseteq (I + 2M)/(I + 4M)$$

and

$$H(4) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}).$$

Since $(\mathrm{sgn}, \det)(H) = \{\pm 1\} \times \mathbb{Z}_2^*$ and $H(4) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, it now follows from Corollary 2.16 that $H = \mathrm{GL}_2(\mathbb{Z}_2)$.

Having shown that $H_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all ℓ and that $(\mathrm{sgn}, \det)(H) = \{\pm 1\} \times \hat{\mathbb{Z}}^*$, we conclude that $H = \mathrm{GL}_2(\hat{\mathbb{Z}})$. In other words, the adelic representation ρ_E is surjective in this example.

ACKNOWLEDGMENTS

Thanks are due to Bjorn Poonen for suggesting this problem to me, to David Zywina for useful discussions, and to the referee, who suggested phrasing Proposition 3.5 and its corollaries in their present, more general, form. This work was partially supported by German Research Foundation (DFG) grant GR 3448/2-1.

REFERENCES

[Duke 97] William Duke. "Elliptic Curves with No Exceptional Primes." *C. R. Acad. Sci. Paris Sér. I Math.* 325:8 (1997), 813–818.

[Greicius 07] Aaron Greicius. "Elliptic Curves with Surjective Global Galois Representation." PhD thesis, University of California, Berkeley, 2007.

[Jones 06] Nathan Jones. "Almost All Elliptic Curves Are Serre Curves." arXiv:math/0611096v1 [math.NT].

[Lang and Trotter 76] Serge Lang and Hale Trotter. *Frobenius Distributions in* GL_2*-Extensions*, Lecture Notes in Mathematics 504. Berlin: Springer, 1976.

[Mazur 77] B. Mazur. "Modular Curves and the Eisenstein Ideal." *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), 33–186.

[Neukirch 99] Jürgen Neukirch. *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] 322. Berlin: Springer-Verlag, 1999.

[Serre 72] Jean-Pierre Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques." *Invent. Math.* 15:4 (1972), 259–331.

[Serre 98] Jean-Pierre Serre. *Abelian l-adic Representations and Elliptic Curves*, Research Notes in Mathematics 7. Wellesley, MA: A K Peters Ltd., 1998.

[Silverman 94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151. New York: Springer, 1994.

[Wilson 98] John S. Wilson. *Profinite Groups*, London Mathematical Society Monographs, New Series, 19. New York: Oxford University Press, 1998.

[Zywina 08] David Zywina. "Elliptic Curves with Maximal Galois Action on Their Torsion Points." arXiv:0809.3482v1 [math.NT].

Aaron Greicius, Institut für Mathematik, Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin, Germany (greicius@math.hu-berlin.de)

Received July 17, 2009; accepted November 11, 2009.