

*Pacific
Journal of
Mathematics*

**A BOUND FOR THE CONDUCTOR OF AN OPEN SUBGROUP
OF GL_2 ASSOCIATED TO AN ELLIPTIC CURVE**

NATHAN JONES

A BOUND FOR THE CONDUCTOR OF AN OPEN SUBGROUP OF GL_2 ASSOCIATED TO AN ELLIPTIC CURVE

NATHAN JONES

Given an elliptic curve E without complex multiplication defined over a number field K , consider the image of the Galois representation defined by letting Galois act on the torsion of E . Serre's open image theorem implies that there is a positive integer m for which the Galois image is completely determined by its reduction modulo m . We prove a bound on the smallest such m in terms of standard invariants associated with E . The bound is sharp and improves upon previous results.

1. Introduction

Let K be a number field, let E/K be an elliptic curve and let E_{tors} denote its torsion subgroup. Denote by $G_K := \mathrm{Gal}(\bar{K}/K)$ the absolute Galois group of K and consider the Galois representation

$$\rho_{E,K} : G_K \rightarrow \mathrm{Aut}(E_{\mathrm{tors}}) \simeq \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

defined by letting G_K act on the torsion of E and choosing compatible bases thereof. A celebrated theorem of J.-P. Serre [1972] states that, if E has no complex multiplication, then the image of $\rho_{E,K}$ is open inside $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, or equivalently that

$$(1) \quad [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E,K}(G_K)] < \infty.$$

Consequently, one may find a positive integer m with the property that

$$\ker(\mathrm{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})) \subseteq \rho_{E,K}(G_K).$$

Definition 1.1. Given an open subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we define the positive integer m_G by

$$m_G := \min\{m \in \mathbb{N} : \ker(\mathrm{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})) \subseteq G\}$$

and call it the *conductor* of G . In case $G = \rho_{E,K}(G_K)$ for an elliptic curve E defined over a number field K and without complex multiplication, we denote the conductor of G by $m_{E,K}$.

MSC2010: 11F80, 11G05.

Keywords: elliptic curves, Galois representations.

The purpose of this note is to prove the following upper bound for $m_{E,K}$. In its statement, Δ_K denotes the absolute discriminant of the number field K , Δ_E denotes the minimal discriminant ideal attached to the elliptic curve E , $N_{K/\mathbb{Q}} : K^\times \rightarrow \mathbb{Q}^\times$ denotes the usual norm map and

$$\text{rad}(m) := \prod_{\substack{\ell|m \\ \ell \text{ prime}}} \ell$$

denotes the radical of the positive integer m . Given a nonzero ideal $I \subseteq \mathcal{O}_K$, we identify the ideal $N_{K/\mathbb{Q}}(I) \subseteq \mathbb{Z}$ with the (unique) positive integer that generates it, and thus we may regard $N_{K/\mathbb{Q}}(\Delta_E) \in \mathbb{N}$.

Theorem 1.2. *Let K be a number field, let E be an elliptic curve over K without complex multiplication, and let $m_{E,K} \in \mathbb{N}$ be as in Definition 1.1. Then one has*

$$m_{E,K} \leq 2 \cdot [\text{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E,K}(G_K)] \cdot \text{rad}(|\Delta_K N_{K/\mathbb{Q}}(\Delta_E)|).$$

Remark 1.3. The bound in Theorem 1.2 both improves upon and generalizes a bound appearing in [Jones 2009] (see Corollary 1.5 below). Furthermore, using results in [Daniels 2015], we may see that there are infinitely many¹ elliptic curves E over \mathbb{Q} satisfying

$$(2) \quad m_{E,\mathbb{Q}} = 2 \cdot [\text{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E,\mathbb{Q}}(G_{\mathbb{Q}})] \cdot \text{rad}(|\Delta_E|).$$

Thus, our bound for $m_{E,K}$ is sharp when $K = \mathbb{Q}$.

Remark 1.4. Let

$$\rho_{E,m} : G_K \rightarrow \text{GL}_2(\mathbb{Z}/m\mathbb{Z}), \quad \rho_{E,\ell^\infty} : G_K \rightarrow \text{GL}_2(\mathbb{Z}_\ell)$$

denote the Galois representations defined by letting G_K act on $E[m]$ and on $E[\ell^\infty] := \bigcup_{n \geq 1} E[\ell^n]$ respectively, and let $K(E[m]) = \overline{K}^{\ker \rho_{E,m}(G_K)}$ denote the m -th division field of E . The conductor $m_{E,K}$ that we are considering should not be confused with ‘‘Serre’s constant,’’ defined for an elliptic curve E over \mathbb{Q} in [Daniels and González-Jiménez 2018] (see also [Cojocaru 2005]) by

$$A(E) := \prod_{\substack{\ell^n \text{ a prime power} \\ \rho_{E,\ell^n}(G_{\mathbb{Q}}) \neq \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \\ \forall k < n, \rho_{E,\ell^k}(G_{\mathbb{Q}}) = \text{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})}} \ell^n.$$

It is evident that $A(E)$ divides $m_{E,\mathbb{Q}}$, but $m_{E,\mathbb{Q}}$ is in general larger than $A(E)$. The main differences between these two constants are as follows:

¹Specifically, (2) holds for any Serre curve E with the property that Δ_E is square-free and $\Delta_E \not\equiv 1 \pmod 4$.

- (1) A prime power ℓ^n divides $m_{E,\mathbb{Q}}$ whenever $\ker(\mathrm{GL}_2(\mathbb{Z}_\ell) \rightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z})) \not\subseteq \rho_{E,\ell^\infty}(G_\mathbb{Q})$, whereas $A(E)$ is square-free, except possibly at the primes 2 and 3. In other words, for each prime ℓ , $m_{E,\mathbb{Q}}$ encodes the action of $G_\mathbb{Q}$ on the entire ℓ -adic Tate module, whereas, for $\ell \geq 5$, $A(E)$ only encodes the action of $G_\mathbb{Q}$ on the ℓ -torsion of E .
- (2) It may happen that there is a nontrivial intersection $\mathbb{Q} \neq \mathbb{Q}(E[m_1]) \cap \mathbb{Q}(E[m_2])$ for some $m_1, m_2 \in \mathbb{N}$ with $\mathrm{gcd}(m_1, m_2) = 1$. The constant $m_{E,\mathbb{Q}}$ encodes such “entanglements,” whereas $A(E)$ does not.

The general phenomenon of entanglements has come up in various recent papers; see for instance [Brau and Jones 2016], which studies elliptic curves E over \mathbb{Q} satisfying $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$ and $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$, and also [Bourdon et al. 2019], in which potential entanglements come up in an analysis of sporadic points on the modular curve $X_1(N)$.

Given an elliptic curve E defined over a number field K , computing the positive integer $m_{E,K}$ is a step toward understanding the image $\rho_{E,K}(G_K) \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. Following Serre’s open image result, there has been much interest in the nature of $\rho_{E,K}(G_K)$, for instance regarding its mod ℓ reductions (see [Mazur 1978; Merel 1996; Bilu and Parent 2011; Bilu et al. 2013; Lozano-Robledo 2013; Zywna 2015a]) and also more recently its reductions at composite levels (see [Dokchitser and Dokchitser 2012; Sutherland and Zywna 2017; Daniels and González-Jiménez 2018; Morrow 2019]). In addition to this connection, Theorem 1.2 also has analytic relevance; for instance in [Bell et al. 2020] it is applied to the study averages of constants appearing in various elliptic curve conjectures.

Serre’s open image result (1) implies that, for any E/K without complex multiplication (CM), there exists a bound $C_{E,K} > 0$ so that, for each prime $\ell > C_{E,K}$, we have $\rho_{E,\ell}(G_K) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Serre asked whether the constant $C_{E,K}$ may be chosen uniformly in E , i.e., whether

- (3) there exists $C_K > 0$ so that, for all E/K without CM and all prime $\ell > C_K$,

$$\rho_{E,\ell}(G_K) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

This question is still open, even in the case $K = \mathbb{Q}$. An affirmative answer to it would imply that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_K)] \ll_K 1,$$

although the implied constant is ineffective, because of an appeal to Faltings’ theorem (see [Zywna 2015b], which details this in the case $K = \mathbb{Q}$). Theorem 1.2 thus has the following corollary.

Corollary 1.5. *Assume that (3) holds. We then have*

$$m_{E,K} \ll_K \mathrm{rad}(N_{K/\mathbb{Q}}(\Delta_E)).$$

Theorem 1.2 is proved via the following two propositions, the first of which deals generally with open subgroups $G \subseteq \text{GL}_2(\widehat{\mathbb{Z}})$. Because of group-theoretical differences² present for the prime 2, it will be convenient to introduce the following modified radical:

$$(4) \quad \text{rad}'(m) := \begin{cases} \text{rad}(m) & \text{if } 4 \nmid m \\ 2 \text{rad}(m) & \text{if } 4 \mid m. \end{cases}$$

We will also distinguish the following case involving the prime 3, in whose statement G_3 (resp. $G(3)$) denotes the image of G under the projection map $\text{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \text{GL}_2(\mathbb{Z}_3)$ (resp. under $\text{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \text{GL}_2(\mathbb{Z}/3\mathbb{Z})$). The analysis proceeds a bit differently according to whether or not the condition

$$(5) \quad 9 \mid m_G, \quad \text{SL}_2(\mathbb{Z}_3) \not\subseteq G_3 \quad \text{and} \quad G(3) = \text{GL}_2(\mathbb{Z}/3\mathbb{Z})$$

holds.

Proposition 1.6. *Let $G \subseteq \text{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup and let m_G be as in Definition 1.1. We then have*

$$\frac{m_G}{\text{rad}'(m_G)} \text{ divides } [\pi^{-1}(G(\text{rad}'(m_G))) : G(m_G)],$$

where $\text{rad}'(\cdot)$ is defined as in (4) and $\pi : \text{GL}_2(\mathbb{Z}/m_G\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/\text{rad}'(m_G)\mathbb{Z})$ denotes the canonical projection map. Assuming that (5) holds, we have

$$\frac{9m_G}{\text{rad}'(m_G)} \text{ divides } [\pi^{-1}(G(\text{rad}'(m_G))) : G(m_G)].$$

In contrast with Proposition 1.6, our second proposition is specific to the situation where $G = \rho_{E,K}(G_K)$, making use of facts about the Weil pairing on an elliptic curve, together with the Nerón–Ogg–Shafarevich criterion for ramification in division fields.

Proposition 1.7. *Let K be a number field and let E be an elliptic curve defined over K without complex multiplication. Let $G := \rho_{E,K}(G_K)$ be the image of the Galois representation associated to E and let m_G be as in Definition 1.1. Assuming that (5) does not hold, we have*

$$\text{rad}'(m_G) \leq 2[\text{GL}_2(\mathbb{Z}/\text{rad}'(m_G)\mathbb{Z}) : G(\text{rad}'(m_G))] \text{rad}(|\Delta_K N_{K/\mathbb{Q}}(\Delta_E)|).$$

If (5) does hold, then

$$\frac{\text{rad}'(m_G)}{3} \leq 2[\text{GL}_2(\mathbb{Z}/\text{rad}'(m_G)\mathbb{Z}) : G(\text{rad}'(m_G))] \text{rad}(|\Delta_K N_{K/\mathbb{Q}}(\Delta_E)|).$$

²See [Dokchitser and Dokchitser 2012] (resp. [Elkies 2006]), which concerns the Galois representation on the 2-adic (resp. on the 3-adic) Tate module, illustrating these differences.

Since the index of a subgroup is preserved under taking the full preimage, we have that

$$[GL_2(\mathbb{Z}/\text{rad}'(m_G)\mathbb{Z}) : G(\text{rad}'(m_G))] = [GL_2(\mathbb{Z}/m_G\mathbb{Z}) : \pi^{-1}(G(\text{rad}'(m_G)))],$$

where $\pi : GL_2(\mathbb{Z}/m_G\mathbb{Z}) \rightarrow GL_2(\mathbb{Z}/\text{rad}'(m_G)\mathbb{Z})$ is the canonical projection map. Thus, [Theorem 1.2](#) follows from [Propositions 1.6](#) and [1.7](#).

Many of the ingredients that enter into the proof of [Theorem 1.2](#) may be verified for algebraic groups other than GL_2 . For instance, using these same techniques, one should be able to obtain a similar bound for the analogous integer $m_{A,K}$ associated to an abelian variety A defined over a number field K whose Galois representation has open image inside $GSp_{2g}(\widehat{\mathbb{Z}})$.

2. Notation and preliminaries

Throughout the paper, p and ℓ will always denote prime numbers. As usual, \mathbb{N} denotes the set of natural numbers (excluding zero) and \mathbb{Z} denotes the set of integers. We will occasionally use the abbreviations

$$\begin{aligned} \mathbb{N}_{\geq \alpha} &:= \{n \in \mathbb{N} : n \geq \alpha\}, \\ \mathbb{Z}_{\geq \alpha} &:= \{n \in \mathbb{Z} : n \geq \alpha\}. \end{aligned}$$

We recall that

$$\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/m\mathbb{Z}$$

is the inverse limit of the rings $\mathbb{Z}/m\mathbb{Z}$ with respect to the canonical projection maps $\mathbb{Z}/nm\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$. Under the isomorphism of the Chinese remainder theorem, we have that

$$(6) \quad \widehat{\mathbb{Z}} \simeq \prod_{\ell} \mathbb{Z}_{\ell},$$

where \mathbb{Z}_{ℓ} as usual denotes the ring of ℓ -adic integers. More generally, for any $m \in \mathbb{N}_{\geq 2}$ we define \mathbb{Z}_m and $\mathbb{Z}_{(m)}$ to be the quotients of $\widehat{\mathbb{Z}}$ corresponding under [\(6\)](#) to the following rings:

$$\mathbb{Z}_m \simeq \prod_{\ell|m} \mathbb{Z}_{\ell}, \quad \mathbb{Z}_{(m)} \simeq \prod_{\ell \nmid m} \mathbb{Z}_{\ell}.$$

For any $m \in \mathbb{N}_{\geq 2}$ we have an isomorphism

$$\widehat{\mathbb{Z}} \simeq \mathbb{Z}_m \times \mathbb{Z}_{(m)},$$

and projection maps

$$\widehat{\mathbb{Z}} \rightarrow \mathbb{Z}_m, \quad \widehat{\mathbb{Z}} \rightarrow \mathbb{Z}_{(m)}.$$

We note that these observations may also be applied to points in an algebraic group; in particular we have

$$\mathrm{GL}_2(\widehat{\mathbb{Z}}) \simeq \mathrm{GL}_2(\mathbb{Z}_m) \times \mathrm{GL}_2(\mathbb{Z}_{(m)}) \simeq \prod_{\ell} \mathrm{GL}_2(\mathbb{Z}_{\ell})$$

and we have projection maps

$$(7) \quad \pi_m : \mathrm{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \mathrm{GL}_2(\mathbb{Z}_m), \quad \pi_{(m)} : \mathrm{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \mathrm{GL}_2(\mathbb{Z}_{(m)}).$$

In most cases we will denote any projection map simply by π , but on some occasions we will decorate it with subscripts, such as in (7) or

$$\pi_{m^\infty, m} : \mathrm{GL}_2(\mathbb{Z}_m) \rightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}), \quad \pi_{nm, n} : \mathrm{GL}_2(\mathbb{Z}/nm\mathbb{Z}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

The ring $\widehat{\mathbb{Z}}$ is a topological ring under the profinite topology, and the group $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ inherits the structure of a profinite group. We recall that any open subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is a closed subgroup but not conversely. In general, given any closed subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we denote by $G_m \subseteq \mathrm{GL}_2(\mathbb{Z}_m)$ (resp. by $G_{(m)} \subseteq \mathrm{GL}_2(\mathbb{Z}_{(m)})$) its image under π_m (resp. under $\pi_{(m)}$) as in (7). We denote by $G(m)$ the image of G under the canonical projection

$$\mathrm{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

For any $m \in \mathbb{N}$ and any d dividing m , we denote the prime-to- d part of m by

$$m_{(d)} := \frac{m}{\prod_{\ell|d} \ell^{\mathrm{ord}_{\ell}(m)}}.$$

Finally, we let

$$\mathrm{id}_m : \mathrm{GL}_2(\mathbb{Z}_m) \rightarrow \mathrm{GL}_2(\mathbb{Z}_m), \quad \mathrm{id}_{(m)} : \mathrm{GL}_2(\mathbb{Z}_{(m)}) \rightarrow \mathrm{GL}_2(\mathbb{Z}_{(m)})$$

denote the identity maps, and we let 1_m (resp. $1_{(m)}$) denote the identity element of $\mathrm{GL}_2(\mathbb{Z}_m)$ (resp. of $\mathrm{GL}_2(\mathbb{Z}_{(m)})$). We may also at times denote by 1_m the identity element of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

For an abelian group A and a positive integer n we as usual denote by $A[n]$ the n -torsion subgroup of A . For a prime number ℓ we define

$$A[\ell^\infty] := \bigcup_{n=0}^{\infty} A[\ell^n], \quad A_{\mathrm{tors}} := \bigcup_{n=1}^{\infty} A[n], \quad A_{\mathrm{tors}, (\ell)} := \bigcup_{\substack{n=1 \\ \ell \nmid n}}^{\infty} A[n].$$

Note that, if $A[n]$ is finite for each $n \in \mathbb{N}$, we have

$$A_{\mathrm{tors}} \simeq A[\ell^\infty] \times A_{\mathrm{tors}, (\ell)}.$$

For a number field K , we denote by \mathcal{O}_K its ring of integers, by Δ_K its absolute discriminant and by

$$N_{K/\mathbb{Q}} : K \rightarrow \mathbb{Q}$$

the norm map. A critical issue that arises in the proof of [Proposition 1.7](#) is that of *entanglement* of division fields, i.e., the possibility that the field extension $K \subseteq K(E[m_1]) \cap K(E[m_2])$ is a nontrivial extension, where m_1 and m_2 are relatively prime positive integers. Putting $F := K(E[m_1]) \cap K(E[m_2])$, we have by Galois theory that

$$\begin{aligned} &\text{Gal}(K(E[m_1 m_2])/K) \\ &\simeq \{(\sigma_1, \sigma_2) \in \text{Gal}(K(E[m_1])/K) \times \text{Gal}(K(E[m_2])/K) : \sigma_1|_F = \sigma_2|_F\}. \end{aligned}$$

More generally, if G_1, G_2 and H are groups and $\psi_1 : G_1 \rightarrow H, \psi_2 : G_2 \rightarrow H$ are surjective group homomorphisms, we introduce the following notation for the fibered product:

$$G_1 \times_{\psi} G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\}$$

(here ψ is an abbreviation for the ordered pair (ψ_1, ψ_2)). Evidently,

$$K \neq K(E[m_1]) \cap K(E[m_2])$$

if and only if the fibered product

$$\text{Gal}(K(E[m_1])/K) \times_{\text{res}} \text{Gal}(K(E[m_2])/K)$$

is a fibered product over a nontrivial group, where

$$\text{res}_i : \text{Gal}(K(E[m_i])/K) \rightarrow \text{Gal}(K(E[m_1]) \cap K(E[m_2])/K)$$

denotes the restriction map.

3. Proof of [Proposition 1.6](#)

In this section we prove [Proposition 1.6](#), bounding $m_G / \text{rad}'(m_G)$ in terms of the index of $G(m_G)$ in $\pi^{-1}(G(\text{rad}'(m_G)))$, where $G \subseteq GL_2(\widehat{\mathbb{Z}})$ is any open subgroup. We recall that, in the profinite topology, any open subgroup of $GL_2(\widehat{\mathbb{Z}})$ is necessarily closed; we will establish some lemmas regarding closed subgroups of $GL_2(\widehat{\mathbb{Z}})$ which thus apply to the open subgroup G .

We begin by giving a more precise description of the local exponents $\beta_\ell \geq 0$ occurring in

$$(8) \quad m_G =: \prod_{\ell} \ell^{\beta_\ell}.$$

In what follows we use the maps

$$\begin{aligned}\pi_{\ell^{\beta+1}, \ell^\beta} \times \text{id}_{(\ell)} &: \text{GL}_2(\mathbb{Z}/\ell^{\beta+1}\mathbb{Z}) \times \text{GL}_2(\mathbb{Z}_{(\ell)}) \rightarrow \text{GL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z}) \times \text{GL}_2(\mathbb{Z}_{(\ell)}), \\ \pi_{\ell^\infty, \ell^{\beta+1}} \times \text{id}_{(\ell)} &: \text{GL}_2(\mathbb{Z}_\ell) \times \text{GL}_2(\mathbb{Z}_{(\ell)}) \rightarrow \text{GL}_2(\mathbb{Z}/\ell^{\beta+1}\mathbb{Z}) \times \text{GL}_2(\mathbb{Z}_{(\ell)})\end{aligned}$$

defined by the obvious projection in the first factor and the identity map in the second factor. For any prime ℓ , we define

$$(9) \quad \alpha_\ell := \begin{cases} 2 & \text{if } \ell = 2, \\ 1 & \text{if } \ell \geq 3. \end{cases}$$

The next lemma follows from ideas in [Serre 1968, Lemma 3, IV-23]. In its statement and henceforth, we will interpret $\text{GL}_2(\mathbb{Z}/\ell^0\mathbb{Z}) := \{1\}$ as the trivial group, so that $\ker \pi_{\ell,1} = \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Lemma 3.1. *Let $G \subseteq \text{GL}_2(\widehat{\mathbb{Z}})$ be a closed subgroup, let ℓ be a prime number, and let $\beta \in \mathbb{Z}_{\geq 0}$. Assume that*

$$\forall \gamma \in [\beta, \max\{\beta, \alpha_\ell\}] \cap \mathbb{Z}, \quad \ker(\pi_{\ell^{\gamma+1}, \ell^\gamma}) \times \{1_{(\ell)}\} \subseteq (\pi_{\ell^\infty, \ell^{\gamma+1}} \times \text{id}_{(\ell)})(G),$$

where α_ℓ is as in (9). We then have

$$\ker(\pi_{\ell^\infty, \ell^\beta}) \times \{1_{(\ell)}\} \subseteq G.$$

Proof. Since $G \subseteq \text{GL}_2(\widehat{\mathbb{Z}})$ is closed, it suffices to prove that, for each $n \in \mathbb{Z}_{\geq \max\{\beta, \alpha_\ell\}}$,

$$(10) \quad \ker(\pi_{\ell^{n+1}, \ell^n}) \times \{1_{(\ell)}\} \subseteq (\pi_{\ell^\infty, \ell^{n+1}} \times \text{id}_{(\ell)})(G).$$

We prove this by induction on n as follows (the base case $n = \max\{\beta, \alpha_\ell\}$ is true by hypothesis). First note that, for $n \geq 1$, we have

$$(11) \quad \ker(\pi_{\ell^{n+1}, \ell^n}) = \{I + \ell^n \tilde{X} \pmod{\ell^{n+1}} : \tilde{X} \in M_{2 \times 2}(\mathbb{Z}_\ell)\}.$$

Thus, (10) may be reformulated as saying

$$(12) \quad \begin{aligned} &\text{for all } X \in M_{2 \times 2}(\mathbb{F}_\ell), \text{ there exists } \tilde{X} \in M_{2 \times 2}(\mathbb{Z}_\ell) \\ &\text{such that } \tilde{X} \equiv X \pmod{\ell} \text{ and } g := (I + \ell^n \tilde{X}, 1_{(\ell)}) \in G. \end{aligned}$$

Our goal is to deduce that (12) continues to hold when n is replaced by $n+1$. Since G is a group, $g^\ell \in G$, and one sees by considering the binomial expansion

$$(13) \quad (I + \ell^n \tilde{X})^\ell = I + \binom{\ell}{1} \ell^n \tilde{X} + \binom{\ell}{2} \ell^{2n} \tilde{X}^2 + \cdots + \binom{\ell}{\ell-1} \ell^{(\ell-1)n} \tilde{X}^{\ell-1} + \ell^{\ell n} \tilde{X}^\ell$$

that

$$(\pi_{\ell^\infty, \ell^{n+2}} \times \text{id}_{(\ell)})(g^\ell) = (I + \ell^{n+1} \tilde{X} \pmod{\ell^{n+2}}, 1_{(\ell)}).$$

Since X in (12) was arbitrary, it follows by (11) that

$$\ker(\pi_{\ell^{n+2}, \ell^{n+1}}) \times \{1_{(\ell)}\} \subseteq (\pi_{\ell^\infty, \ell^{n+2}} \times \text{id}_{(\ell)})(G),$$

completing the induction and proving the lemma. \square

Remark 3.2. The “purely ℓ -adic version” of [Lemma 3.1](#) also follows by the same proof (without the $\mathrm{GL}_2(\mathbb{Z}_{(\ell)})$ factor). Precisely, for any prime ℓ and closed subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$, and any $\beta \in \mathbb{Z}_{\geq 0}$, one has

$$(14) \quad \forall \gamma \in [\beta, \max\{\beta, \alpha_\ell\}] \cap \mathbb{Z}, \quad \ker(\mathrm{GL}_2(\mathbb{Z}/\ell^{\gamma+1}\mathbb{Z}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^\gamma\mathbb{Z})) \subseteq G(\ell^{\gamma+1}) \\ \Rightarrow \ker(\mathrm{GL}_2(\mathbb{Z}_\ell) \rightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z})) \subseteq G,$$

where α_ℓ is as in [\(9\)](#).

Remark 3.3. The fact that the exponent α_ℓ in [\(14\)](#) is different for $\ell = 2$ and otherwise uniform for $\ell \geq 3$ stands in contrast with [\[Serre 1968, Lemma 3, IV-23\]](#), which breaks into cases according to whether $\ell \leq 3$ or $\ell \geq 5$. The underlying reason is that we are seeking to conclude that $\ker(\mathrm{GL}_2(\mathbb{Z}_\ell) \rightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z})) \subseteq G$, rather than the weaker conclusion $\ker(\mathrm{SL}_2(\mathbb{Z}_\ell) \rightarrow \mathrm{SL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z})) \subseteq G \cap \mathrm{SL}_2(\mathbb{Z}_\ell)$, the latter breaking into cases according to the condition $[\mathrm{SL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z}), \mathrm{SL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z})] = \mathrm{SL}_2(\mathbb{Z}/\ell^\beta\mathbb{Z})$, which happens if and only if $\ell \geq 5$; see [Lemma 3.6](#) below.

Definition 3.4. We define the exponents $\beta'_\ell = \beta'_\ell(G)$ by

$$\beta'_\ell := \min \left\{ \beta \in \mathbb{Z}_{\geq 0} : \forall \gamma \in [\beta, \max\{\beta, \alpha_\ell\}] \cap \mathbb{Z}, \right. \\ \left. \ker(\pi_{\ell^{\gamma+1}, \ell^\gamma}) \times \{1_{(\ell)}\} \subseteq (\pi_{\ell^\infty, \ell^{\gamma+1}} \times \mathrm{id}_{(\ell)})(G) \right\},$$

where α_ℓ is as in [\(9\)](#).

Corollary 3.5. We have $\beta_\ell = \beta'_\ell$, where β_ℓ is as in [\(8\)](#).

Proof. By [Lemma 3.1](#), for each prime ℓ we have

$$\ker(\pi_{\ell^\infty, \ell^{\beta'_\ell}}) \times \{1_{(\ell)}\} \subseteq G.$$

Since $\ker(\mathrm{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/\prod_\ell \ell^{\beta'_\ell}\mathbb{Z}))$ is equal to the subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ generated by $\ker(\pi_{\ell^\infty, \ell^{\beta'_\ell}}) \times \{1_{(\ell)}\}$ as ℓ varies over all primes, we then have

$$\ker\left(\mathrm{GL}_2(\widehat{\mathbb{Z}}) \rightarrow \mathrm{GL}_2\left(\mathbb{Z}/\prod_\ell \ell^{\beta'_\ell}\mathbb{Z}\right)\right) \subseteq G.$$

Thus, by [\(8\)](#) and [Definition 1.1](#), we see that $\beta_\ell \leq \beta'_\ell$.

Conversely, suppose for the sake of contradiction that $\beta_\ell < \beta'_\ell$. By definition of β_ℓ , we would then have

$$(15) \quad \ker(\pi_{\ell^\infty, \ell^{\beta'_\ell-1}}) \times \{1_{(\ell)}\} \subseteq \ker(\pi_{\ell^\infty, \ell^{\beta_\ell}}) \times \{1_{(\ell)}\} \subseteq G.$$

Furthermore, since $\pi_{\ell^\infty, \ell^{\beta'_\ell}}(\ker(\pi_{\ell^\infty, \ell^{\beta'_\ell-1}})) = \ker(\pi_{\ell^{\beta'_\ell}, \ell^{\beta'_\ell-1}})$, we then see that [\(15\)](#) would then imply

$$\forall \gamma \in [\beta'_\ell - 1, \max\{\beta'_\ell - 1, \alpha_\ell\}] \cap \mathbb{Z}, \quad \ker(\pi_{\ell^{\gamma+1}, \ell^\gamma}) \times \{1_{(\ell)}\} \subseteq (\pi_{\ell^\infty, \ell^{\gamma+1}} \times \mathrm{id}_{(\ell)})(G),$$

contradicting [Definition 3.4](#). Thus, $\beta'_\ell \leq \beta_\ell$. \square

We will find it useful to have sufficient conditions to conclude that $\mathrm{SL}_2(\mathbb{Z}_\ell) \subseteq G$, where $G \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$ is an arbitrary closed subgroup. The next lemma does so for ℓ odd, and gives us sufficient information to allow us to deal separately with the prime $\ell = 2$. As with [Lemma 3.1](#), it can be largely deduced from arguments found in the proof of [\[Serre 1968, Lemma 3, IV-23\]](#); we include the details here for the sake of completeness.

Lemma 3.6. *Let ℓ be a prime number and let $G \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$ be a closed subgroup. If $\ell \geq 5$, then we have*

$$\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G(\ell) \Rightarrow \mathrm{SL}_2(\mathbb{Z}_\ell) \subseteq G.$$

If $\ell = 3$, we have

$$G(3) = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \text{ and } \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}) \subseteq G(9) \Rightarrow \mathrm{SL}_2(\mathbb{Z}_3) \subseteq G.$$

Finally, if $\ell = 2$, we have

$$G(4) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \Rightarrow G = \mathrm{GL}_2(\mathbb{Z}_2) \text{ or } [\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : G(8)] = 2.$$

Proof. We first assume ℓ is odd. Under the stated hypotheses, we will show that $\mathrm{SL}_2(\mathbb{Z}_\ell) \subseteq G$ by establishing that

$$(16) \quad \mathrm{SL}_2(\mathbb{Z}_\ell) = [G, G],$$

where $[G, G]$ denotes the *closure* of the commutator subgroup of G . This amounts to showing that $\mathrm{SL}_2(\mathbb{Z}_\ell) \subseteq [G, G]$, since the reverse inclusion follows from the fact that every commutator has determinant 1. We begin by first showing, by induction on n , that

$$(17) \quad \ker(\mathrm{SL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})) \subseteq G(\ell^{n+1}) \quad \left(\begin{array}{l} \ell \geq 5 \text{ and } n \geq 0, \text{ or} \\ \ell = 3 \text{ and } n \geq 1 \end{array} \right).$$

The binomial expansion argument (13) of [Lemma 3.1](#) shows this, except for the case $\ell \geq 5$ and $n = 0$. To establish this final case, we first observe that

$$\det(I + \ell^n \tilde{X}) \equiv 1 + \ell^n \mathrm{tr} \tilde{X} \pmod{\ell^{n+1}} \quad (n \geq 1).$$

Thus, for $n \geq 1$, we have

$$(18) \quad \ker(\mathrm{SL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})) = \{I + \ell^n \tilde{X} \pmod{\ell^{n+1}} : \tilde{X} \in M_{2 \times 2}^{\mathrm{tr}=0}(\mathbb{Z}_\ell)\},$$

where

$$M_{2 \times 2}^{\mathrm{tr}=0}(\mathbb{Z}_\ell) := \{\tilde{X} \in M_{2 \times 2}(\mathbb{Z}_\ell) : \mathrm{tr} \tilde{X} \equiv 0 \pmod{\ell}\}.$$

In particular, $\ker(\mathrm{SL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z}))$ is a 3-dimensional subspace of the 4-dimensional $\mathbb{Z}/\ell\mathbb{Z}$ -vector space $\ker(\pi_{\ell^{n+1}, \ell^n})$. It follows from this, together

with the fact that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ reduced modulo ℓ generate $SL_2(\mathbb{Z}/\ell\mathbb{Z})$, that the set

$$\mathcal{K} := \left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \right\} \subseteq M_{2 \times 2}(\mathbb{Z})$$

satisfies

$$(19) \quad \langle I + \ell^n \mathcal{K} \pmod{\ell^{n+1}} \rangle = \ker(SL_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}/\ell^n\mathbb{Z})) \quad (n \geq 0).$$

Fix $X \in \mathcal{K}$. Note that $I + \ell^0 X \pmod{\ell} \in SL_2(\mathbb{Z}/\ell\mathbb{Z})$, which by hypothesis is contained in $G(\ell)$. Fix a lift $\tilde{X} \in M_{2 \times 2}(\mathbb{Z}_\ell)$ for which $I + \ell^0 \tilde{X} \in G$, and note that $\tilde{X}^2 \equiv \mathbf{0} \pmod{\ell}$, so $\tilde{X}^4 \equiv \mathbf{0} \pmod{\ell^2}$. Thus, since $\ell \geq 5$, we have

$$(I + \ell^0 \tilde{X})^\ell = I + \binom{\ell}{1} \tilde{X} + \binom{\ell}{2} \tilde{X}^2 + \dots + \binom{\ell}{\ell-1} \tilde{X}^{\ell-1} + \tilde{X}^\ell \equiv I + \ell \tilde{X} \pmod{\ell^2},$$

and more generally,

$$(I + \ell^n \tilde{X})^\ell \equiv I + \ell^{n+1} \tilde{X} \pmod{\ell^{n+2}} \quad (\ell \geq 5 \text{ and } n \geq 0, \text{ or } \ell = 3 \text{ and } n \geq 1).$$

Therefore (17) is established by induction on n .

We now proceed to verify (16) for ℓ an odd prime. When $\ell \geq 5$, the group $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ is a nonabelian simple group (see, e.g., [Huppert 1967, Chapter II, Hauptsatz 6.13]), and the exact sequence

$$1 \rightarrow \{\pm I\} \rightarrow SL_2(\mathbb{Z}/\ell\mathbb{Z}) \rightarrow PSL_2(\mathbb{Z}/\ell\mathbb{Z}) \rightarrow 1$$

does not split (see, e.g., [Zywina 2010, Lemma 2.3]). From this and a computer calculation³ for the prime $\ell = 3$, we then find that

$$\begin{aligned} \ell \geq 5 &\Rightarrow [SL_2(\mathbb{Z}/\ell\mathbb{Z}), SL_2(\mathbb{Z}/\ell\mathbb{Z})] = SL_2(\mathbb{Z}/\ell\mathbb{Z}), \\ \ell = 3 &\Rightarrow [GL_2(\mathbb{Z}/3\mathbb{Z}), GL_2(\mathbb{Z}/3\mathbb{Z})] = SL_2(\mathbb{Z}/3\mathbb{Z}), \end{aligned}$$

and so by the hypotheses of our lemma in this case, we have $[G(\ell), G(\ell)] = SL_2(\mathbb{Z}/\ell\mathbb{Z})$. Note further that the commutator subgroup $[G, G] \subseteq G$ projects modulo ℓ onto the commutator subgroup $[G(\ell), G(\ell)]$. We will prove by induction on $n \in \mathbb{N}$ that

$$(20) \quad [G(\ell^n), G(\ell^n)] = SL_2(\mathbb{Z}/\ell^n\mathbb{Z}) \quad (n \geq 1),$$

having just established the base case. Fix $n \geq 1$ and assume that (20) holds. Pick any $g \in G(\ell^{n+1})$ and $\tilde{X} \in M_{2 \times 2}^{\text{tr} \equiv 0}(\mathbb{Z}_\ell)$, so that, by (17) and (18), we have $I + \ell^n \tilde{X} \pmod{\ell^{n+1}} \in G(\ell^{n+1})$. We then compute the commutator

$$(21) \quad \begin{aligned} g(I + \ell^n \tilde{X})g^{-1}(I + \ell^n \tilde{X})^{-1} &\equiv g(I + \ell^n \tilde{X})g^{-1}(I - \ell^n \tilde{X}) \\ &\equiv I + \ell^n (g \tilde{X} g^{-1} - \tilde{X}) \pmod{\ell^{n+1}}. \end{aligned}$$

³For readers wishing to reproduce this or any other computer calculation mentioned in this paper, please find the appropriate Magma scripts listed in an appendix of the arXiv version [Jones 2019].

Consider the following computations in $M_{2 \times 2}(\mathbb{Z}/\ell\mathbb{Z})$:

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix}, \\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}, \\ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

It follows that, inside the additive 3-dimensional $\mathbb{Z}/\ell\mathbb{Z}$ -vector space

$$M_{2 \times 2}^{\text{tr}=0}(\mathbb{Z}/\ell\mathbb{Z}) := \{X \in M_{2 \times 2}(\mathbb{Z}/\ell\mathbb{Z}) : \text{tr } X = 0\},$$

we have

$$\ell \geq 3 \Rightarrow \langle \{gXg^{-1} - X : g \in \text{SL}_2(\mathbb{Z}/\ell\mathbb{Z}), X \in M_{2 \times 2}^{\text{tr}=0}(\mathbb{Z}/\ell\mathbb{Z})\} \rangle = M_{2 \times 2}^{\text{tr}=0}(\mathbb{Z}/\ell\mathbb{Z}).$$

Thus, varying g and \tilde{X} in (21), we see that

$$\ker(\text{SL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})) \subseteq [G(\ell^{n+1}), G(\ell^{n+1})],$$

verifying that (20) holds with n replaced by $n + 1$, thus completing the induction step. Since $[G, G] \subseteq \text{SL}_2(\mathbb{Z}/\ell)$ is a closed subgroup, we have therefore verified (16), proving Lemma 3.6 in case ℓ is odd.

Now assume $\ell = 2$ and note that (19) is still valid. By the hypothesis that $G(4) = \text{GL}_2(\mathbb{Z}/4\mathbb{Z})$, for each $X \in \mathcal{K}$ we may find a lift $\tilde{X} \in M_{2 \times 2}(\mathbb{Z}_2)$ for which $\tilde{X} \equiv X \pmod 2$ and $I + 2\tilde{X} \in G$. Again computing

$$(I + 2\tilde{X})^2 = I + 4\tilde{X} + 4\tilde{X}^2 \equiv I + 4\tilde{X} \pmod 8,$$

we see that $\ker(\text{SL}_2(\mathbb{Z}/8\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/4\mathbb{Z})) \subseteq G(8)$. Hence $[\text{GL}_2(\mathbb{Z}/8\mathbb{Z}) : G(8)] \leq 2$. Finally, if $G(8) = \text{GL}_2(\mathbb{Z}/8\mathbb{Z})$, then (14) with $\beta = 0$ implies that $G = \text{GL}_2(\mathbb{Z}_2)$. \square

Next we will employ the following group theoretical lemma.

Lemma 3.7. *Let G_1 and G_2 be finite groups and let $\pi : G_1 \rightarrow G_2$ be a surjective group homomorphism. Let $H_1 \subseteq G_1$ and $H_2 \subseteq G_2$ be subgroups satisfying $\pi(H_1) = H_2$ and let $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$ be normal subgroups satisfying $\pi(N_1) = N_2$. Assume that*

$$(22) \quad \gcd(\#N_1, \#\ker \pi) = 1 \quad \text{and} \quad [N_1, \ker \pi] = \{1\}.$$

We then have

$$N_1 \subseteq H_1 \iff N_2 \subseteq H_2.$$

Proof. The implication \Rightarrow is immediate and does not require (22). For the converse, suppose that $N_2 \subseteq H_2$ and let $n_1 \in N_1$. Since $\pi(N_1) = N_2 \subseteq H_2 = \pi(H_1)$, we see that there exists $h_1 \in H_1$ satisfying $\pi(n_1) = \pi(h_1)$, and we may thus find $k \in \ker \pi$ so that $n_1 k \in H_1$. Now by (22), we see that

$$(n_1 k)^{\#\ker \pi} = n_1^{\#\ker \pi} \in H_1,$$

which again by (22) implies that $n_1 \in H_1$. Thus, $N_1 \subseteq H_1$, proving the lemma. \square

Applying Lemma 3.7 in a special case, we obtain

Lemma 3.8. *Let $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be an open subgroup, let m_G be as in Definition 1.1 and let $\mathrm{rad}'(m_G)$ be defined by (4). For any prime ℓ and $d \in \mathbb{N}$, one has*

$$\mathrm{rad}'(m_G) \mid d \mid d\ell \mid m_G \Rightarrow \ell \text{ divides } [\pi_{\ell d, d}^{-1}(G(d)) : G(d\ell)].$$

Proof. We write $m := m_G$ and

$$d =: \ell^{\delta_\ell} \cdot d_{(\ell)}, \quad m =: \ell^{\beta_\ell} \cdot m_{(\ell)}$$

(where $\ell \nmid d_{(\ell)} m_{(\ell)}$), and note that, by hypothesis, $\alpha_\ell \leq \delta_\ell < \beta_\ell$. Further observe that, since $\beta_\ell = \beta'_\ell$, by Definitions 1.1 and 3.4, we have

$$\ker(\pi_{\ell^{\delta_\ell+1}, \ell^{\delta_\ell}}) \times \{1_{m_{(\ell)}}\} \not\subseteq G(\ell^{\delta_\ell+1} m_{(\ell)}).$$

We now apply Lemma 3.7 with

$$\begin{aligned} G_1 &:= \mathrm{GL}_2(\mathbb{Z}/\ell^{\delta_\ell+1} m_{(\ell)}\mathbb{Z}), & H_1 &:= G(\ell^{\delta_\ell+1} m_{(\ell)}), & N_1 &:= \ker(\pi_{\ell^{\delta_\ell+1}, \ell^{\delta_\ell}}) \times \{1_{m_{(\ell)}}\}, \\ G_2 &:= \mathrm{GL}_2(\mathbb{Z}/\ell^{\delta_\ell+1} d_{(\ell)}\mathbb{Z}), & H_2 &:= G(\ell^{\delta_\ell+1} d_{(\ell)}), & N_2 &:= \ker(\pi_{\ell^{\delta_\ell+1}, \ell^{\delta_\ell}}) \times \{1_{d_{(\ell)}}\}, \end{aligned}$$

and $\pi : \mathrm{GL}_2(\mathbb{Z}/\ell^{\delta_\ell+1} m_{(\ell)}\mathbb{Z}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^{\delta_\ell+1} d_{(\ell)}\mathbb{Z})$ the canonical projection map. The conclusion is that

$$\ker(\pi_{\ell^{\delta_\ell+1}, \ell^{\delta_\ell}}) \times \{1_{d_{(\ell)}}\} \not\subseteq G(\ell^{\delta_\ell+1} d_{(\ell)}).$$

Since $\ker(\pi_{\ell^{\delta_\ell+1}, \ell^{\delta_\ell}}) \times \{1_{d_{(\ell)}}\} \simeq \ker(\pi_{\ell d, d})$ is an ℓ -group, this proves the lemma. \square

Applying Lemma 3.8 prime by prime, for each prime ℓ dividing $m_G / \mathrm{rad}'(m_G)$, we obtain

$$\frac{m_G}{\mathrm{rad}'(m_G)} \text{ divides } [\pi^{-1}(G(\mathrm{rad}'(m_G))) : G(m_G)],$$

proving Proposition 1.6 in the case that (5) does not hold. In case (5) does hold, we have $G(3) = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and, by Lemma 3.6, we must also have $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}) \not\subseteq G(9)$. A computer search reveals that, up to conjugation in $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, there are two subgroups $G_1, G_2 \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ meeting these two criteria,⁴ and $G_1 \subseteq$

⁴The (genus zero) modular curve associated with G_2 has been considered by N. Elkies [2006], who exhibited an explicit map from it to the j -line.

G_2 . Furthermore, $[\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) : G_2] = 27$. From this it follows that 27 divides $[\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) : G(9)]$, and so

$$9 \cdot 3 \text{ divides } [\pi^{-1}(G(\mathrm{rad}'(m_G))) : G(3 \mathrm{rad}'(m_G))].$$

Now starting here and applying [Lemma 3.8](#), prime by prime, we conclude the proof of [Proposition 1.6](#) in the case that (5) holds.

4. Proof of [Proposition 1.7](#)

We now prove [Proposition 1.7](#). The proof will rely, in part, on the following corollary to the Néron–Ogg–Shafarevich criterion (see for instance [\[Ogg 1967\]](#) or [\[Silverman 1986, Chapter VII, Theorem 7.1\]](#)).

Theorem 4.1. *Let K be a number field, let E be an elliptic curve over K and let $\mathcal{L} \subseteq \mathcal{O}_K$ be a prime ideal of K , lying over the rational prime ℓ of \mathbb{Z} . The following are equivalent:*

- (a) E has good reduction at \mathcal{L} .
- (b) For each positive integer m that is not divisible by ℓ , the prime \mathcal{L} is unramified in $K(E[m])$.
- (c) The prime \mathcal{L} is unramified in $K(E_{\mathrm{tors},(\ell)})$.

We presently reduce the proof of [Proposition 1.7](#) to the following four lemmas. The first lemma follows immediately from the classification subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Lemma 4.2. *Let ℓ be a prime number and let $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ be any subgroup. We have*

$$\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \not\subseteq G(\ell) \Rightarrow \ell \leq [\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : G(\ell)].$$

The second lemma is a consequence of the Weil pairing on an elliptic curve.

Lemma 4.3. *Let E be an elliptic curve defined over a number field K , let $G := \rho_{E,K}(G_K) \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, and let ℓ be a prime number. For any positive integer n , we have*

$$\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \subseteq G(\ell^n) \neq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \Rightarrow \ell \mid \Delta_K.$$

Consequently,

$$\mathrm{SL}_2(\mathbb{Z}_\ell) \subseteq G_\ell \neq \mathrm{GL}_2(\mathbb{Z}_\ell) \Rightarrow \ell \mid \Delta_K.$$

Our third lemma utilizes the Néron–Ogg–Shafarevich criterion in the form of [Theorem 4.1](#).

Lemma 4.4. *Let E be an elliptic curve defined over a number field K , let $G := \rho_{E,K}(G_K) \subseteq GL_2(\widehat{\mathbb{Z}})$, let m_G be as in Definition 1.1 and let ℓ be an odd prime number dividing m_G . We then have*

$$G_\ell = GL_2(\mathbb{Z}_\ell) \Rightarrow \ell \mid \Delta_K N_{K/\mathbb{Q}}(\Delta_E).$$

For the prime $\ell = 2$ we must make a finer analysis, in the form of the next (and final) lemma. Let us make the abbreviation

$$r' := \text{rad}'(m_G).$$

Lemma 4.5. *Let E be an elliptic curve defined over a number field K , let $G := \rho_{E,K}(G_K) \subseteq GL_2(\widehat{\mathbb{Z}})$, let m_G be as in Definition 1.1 and assume that 4 divides m_G . We then have*

$$GL_2(\mathbb{Z}/4\mathbb{Z}) \times \{1_{r'_2}\} \not\subseteq G(r') \Rightarrow 4 \leq 2[\pi^{-1}(G(r'_2)) : G(r')]$$

and

$$GL_2(\mathbb{Z}/4\mathbb{Z}) \times \{1_{r'_2}\} \subseteq G(r') \Rightarrow 2 \mid \Delta_K N_{K/\mathbb{Q}}(\Delta_E).$$

Let us now deduce Proposition 1.7 from Lemmas 4.2–4.5, postponing the proofs of those lemmas until later. First, combining Lemma 3.6 with Lemmas 4.2–4.4, one concludes the following implications, for any prime $\ell \geq 5$ that divides m_G :

$$\begin{aligned} SL_2(\mathbb{Z}/\ell\mathbb{Z}) \not\subseteq G(\ell) &\Rightarrow \ell \leq [GL_2(\mathbb{Z}/\ell\mathbb{Z}) : G(\ell)], \\ SL_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G(\ell) &\Rightarrow \ell \mid \Delta_K N_{K/\mathbb{Q}}(\Delta_E). \end{aligned}$$

This implies that

$$\begin{aligned} (23) \quad r'_{(6)} &\leq \prod_{\substack{\ell \geq 5, \ell \mid r' \\ SL_2(\mathbb{Z}/\ell\mathbb{Z}) \not\subseteq G(\ell)}} [GL_2(\mathbb{Z}/\ell\mathbb{Z}) : G(\ell)] \prod_{\substack{\ell \geq 5 \\ \ell \mid \Delta_K N_{K/\mathbb{Q}}(\Delta_E) \\ SL_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G(\ell)}} \ell \\ &\leq [GL_2(\mathbb{Z}/r'_{(6)}\mathbb{Z}) : G(r'_{(6)})] \text{rad}(|\Delta_K N_{K/\mathbb{Q}}(\Delta_E)|)_{(6)}. \end{aligned}$$

If the prime $\ell = 3$ divides m_G then either condition (5) holds or it does not hold. Let us first assume that (5) does not hold, i.e., we assume that it is *not* the case that 9 divides m_G , $G(3) = GL_2(\mathbb{Z}/3\mathbb{Z})$ and $SL_2(\mathbb{Z}_3) \not\subseteq G_3$. We then use Lemmas 4.2–4.4, together with Lemma 3.6, to deduce the following implications:

$$\begin{aligned} SL_2(\mathbb{Z}/3\mathbb{Z}) \not\subseteq G(3) &\Rightarrow 3 \leq [GL_2(\mathbb{Z}/3\mathbb{Z}) : G(3)], \\ SL_2(\mathbb{Z}/3\mathbb{Z}) \subseteq G(3) \neq GL_2(\mathbb{Z}/3\mathbb{Z}) &\Rightarrow 3 \mid \Delta_K, \\ G(3) = GL_2(\mathbb{Z}/3\mathbb{Z}) \text{ and } SL_2(\mathbb{Z}_3) \subseteq G_3 \neq GL_2(\mathbb{Z}_3) &\Rightarrow 3 \mid \Delta_K, \\ G(3) = GL_2(\mathbb{Z}/3\mathbb{Z}) \text{ and } G_3 = GL_2(\mathbb{Z}_3) &\Rightarrow 3 \mid \Delta_K N_{K/\mathbb{Q}}(\Delta_E). \end{aligned}$$

Inserting this information into (23), we find that

$$(24) \quad r'_{(2)} \leq [\mathrm{GL}_2(\mathbb{Z}/r'_{(2)}\mathbb{Z}) : G(r'_{(2)})] \mathrm{rad}(|\Delta_K N_{K/\mathbb{Q}}(\Delta_E)|)_{(2)}.$$

On the other hand, in case (5) *does* hold, then we obviously have

$$(25) \quad \begin{aligned} \frac{r'_{(2)}}{3} = r'_{(6)} &\leq [\mathrm{GL}_2(\mathbb{Z}/r'_{(6)}\mathbb{Z}) : G(r'_{(6)})] \mathrm{rad}(|\Delta_K N_{K/\mathbb{Q}}(\Delta_E)|)_{(6)} \\ &\leq [\mathrm{GL}_2(\mathbb{Z}/r'_{(2)}\mathbb{Z}) : G(r'_{(2)})] \mathrm{rad}(|\Delta_K N_{K/\mathbb{Q}}(\Delta_E)|)_{(2)}. \end{aligned}$$

If $\ell = 2$ divides m_G , then either 4 divides m_G or does not. If $4 \nmid m_G$, then multiplying both sides of (24) and (25) by 2, we obtain the bounds of Proposition 1.7. Now assume that $4 \mid m_G$. In this case, when (5) does not hold, we insert the result of Lemma 4.5 into (24), concluding that

$$r' = 4r'_{(2)} \leq 2[\mathrm{GL}_2(\mathbb{Z}/r'\mathbb{Z}) : G(r')] \mathrm{rad}(|\Delta_K N_{K/\mathbb{Q}}(\Delta_E)|).$$

Likewise, in case condition (5) *does* hold, we insert these results into (25) and obtain

$$\frac{r'}{3} = \frac{4r'_{(2)}}{3} \leq 2[\mathrm{GL}_2(\mathbb{Z}/r'\mathbb{Z}) : G(r')] \mathrm{rad}(|\Delta_K N_{K/\mathbb{Q}}(\Delta_E)|).$$

Thus we see that Lemmas 4.2–4.5 indeed imply Proposition 1.7.

We now prove each of these lemmas. First we state an auxiliary lemma that is used throughout and may be found in [Ribet 1976, Lemma (5.2.1)].

Lemma 4.6 (Goursat’s lemma). *Let G_1, G_2 be groups and for $i \in \{1, 2\}$ denote by $\mathrm{pr}_i : G_1 \times G_2 \rightarrow G_i$ the projection map onto the i -th factor. Let $G \subseteq G_1 \times G_2$ be a subgroup and assume that*

$$\mathrm{pr}_1(G) = G_1, \quad \mathrm{pr}_2(G) = G_2.$$

Then there exists a group Γ together with a pair of surjective homomorphisms

$$\psi_1 : G_1 \rightarrow \Gamma, \quad \psi_2 : G_2 \rightarrow \Gamma$$

so that

$$G = G_1 \times_{\psi} G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\}.$$

Proof of Lemma 4.2. To prove Lemma 4.2, we will use the following classification of certain proper subgroups of GL_2 .

Definition 4.7. Let ℓ be any prime number.

- (i) A subgroup $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is called a *Borel subgroup* if it is conjugate in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ to the subgroup

$$(26) \quad \mathcal{B}(\ell) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : b \in \mathbb{Z}/\ell\mathbb{Z}, a, d \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\}.$$

(ii) A subgroup $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is called a *normalizer of a split Cartan subgroup* if it is conjugate in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ to the subgroup

$$(27) \quad \mathcal{N}_s(\ell) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\} \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} : b, c \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\}.$$

If ℓ is odd, then $G(\ell)$ is called a *normalizer of a nonsplit Cartan subgroup* if it is conjugate in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ to the subgroup

$$(28) \quad \mathcal{N}_{\mathrm{ns}}(\ell) := \left\{ \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} : x, y \in \mathbb{Z}/\ell\mathbb{Z}, x^2 - \varepsilon y^2 \neq 0 \right\} \cup \left\{ \begin{pmatrix} x & -\varepsilon y \\ y & -x \end{pmatrix} : x, y \in \mathbb{Z}/\ell\mathbb{Z}, x^2 - \varepsilon y^2 \neq 0 \right\},$$

where ε is any fixed nonsquare in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. If $\ell = 2$, then $G(2)$ is called a normalizer of a nonsplit Cartan subgroup if $G(2) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

(iii) A subgroup $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is called an *exceptional group* if its image in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is isomorphic to one of the groups A_4 , S_4 or A_5 (the symmetric or alternating groups).

The following lemma may be deduced from Propositions 15, 16 and Section 2.6 of [Serre 1972].

Lemma 4.8. *Let $G(\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ be a subgroup. Then one of the following must hold:*

- (1) $G(\ell)$ is contained in a Borel subgroup.
- (2) $G(\ell)$ is contained in the normalizer of a split Cartan subgroup.
- (3) $G(\ell)$ is contained in the normalizer of a nonsplit Cartan subgroup.
- (4) $G(\ell)$ is an exceptional group.
- (5) $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G(\ell)$.

We include the following table of indices $[\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : G(\ell)]$, for each of the proper subgroups $G(\ell)$ given in Lemma 4.8. In addition to the definitions (26), (27), and (28), we make the following abbreviations. For a prime ℓ for which $A_4 \subseteq \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we define the exceptional subgroup $\mathcal{E}_{A_4}(\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ by

$$\mathcal{E}_{A_4}(\ell) := \{g \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \varpi(g) \in A_4\},$$

where $\varpi : \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \rightarrow \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ denotes the usual projection. The exceptional subgroups $\mathcal{E}_{S_4}(\ell)$ and $\mathcal{E}_{A_5}(\ell)$ are defined similarly.

$G(\ell)$	$\mathcal{B}(\ell)$	$\mathcal{N}_s(\ell)$	$\mathcal{N}_{\mathrm{ns}}(\ell)$	$\mathcal{E}_{A_4}(\ell)$	$\mathcal{E}_{S_4}(\ell)$	$\mathcal{E}_{A_5}(\ell)$
$[\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : G(\ell)]$	$\ell + 1$	$\frac{\ell(\ell+1)}{2}$	$\frac{\ell(\ell-1)}{2}$	$\frac{\ell(\ell^2-1)}{12}$	$\frac{\ell(\ell^2-1)}{24}$	$\frac{\ell(\ell^2-1)}{60}$

We note that $\mathcal{N}_{\text{ns}}(2) = \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$, and also that each exceptional group only occurs for certain primes ℓ . In particular, if the expression given in the table is not a whole number, then the associated exceptional group does not occur as a subgroup of $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for that prime ℓ . The conclusion of [Lemma 4.2](#) follows immediately from this table. \square

Proof of Lemma 4.3. We will make use of the following commutative diagram, where

$$\text{res} : \text{Gal}(K(E_{\text{tors}})/K) \rightarrow \text{Gal}(K(\mu_\infty)/K), \quad \text{cyc} : \text{Gal}(K(\mu_\infty)/K) \rightarrow \widehat{\mathbb{Z}}^\times$$

denote respectively the restriction map and the cyclotomic character (the containment $K(\mu_\infty) \subseteq K(E_{\text{tors}})$ follows from the Weil pairing [[1940](#)], see also [[Silverman 1986](#), Chapter III, §8]).

$$(29) \quad \begin{array}{ccc} \text{Gal}(K(E[\ell^n])/K) & \xrightarrow{\rho_{E,K}} & \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \\ \text{res} \downarrow & & \det \downarrow \\ \text{Gal}(K(\mu_{\ell^n})/K) & \xrightarrow{\text{cyc}} & (\mathbb{Z}/\ell^n\mathbb{Z})^\times \end{array}$$

By considering the commutative diagram (29) and Galois theory, we see that $\text{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \subseteq G(\ell^n) \neq \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \Rightarrow \det(G(\ell^n)) \neq (\mathbb{Z}/\ell^n\mathbb{Z})^\times \Rightarrow \mathbb{Q} \neq \mathbb{Q}(\mu_{\ell^n}) \cap K$. Since $\mathbb{Q}(\mu_{\ell^n})$ is totally ramified at ℓ , it follows that ℓ is then ramified in $\mathbb{Q}(\mu_{\ell^n}) \cap K$, so ℓ is ramified in K , and thus ℓ divides Δ_K . \square

Proof of Lemma 4.4. In order to prove [Lemma 4.4](#), we will make use of the following definition and lemma, which allow us to understand in more detail the nature of the fibered products that may be present in G .

Definition 4.9. Let G be a profinite group and Σ a finite simple group. We say that Σ *occurs in* G if and only if there are closed subgroups G_1 and N_1 of G with $N_1 \subseteq G_1 \subseteq G$, N_1 normal in G_1 and $G_1/N_1 \simeq \Sigma$. We further define

$$\begin{aligned} \text{Occ}(G) &:= \{\text{finite simple nonabelian groups } \Sigma : \Sigma \text{ occurs in } G\}, \\ \text{Occ}_{\text{JH}}(G) &:= \{\text{finite simple nonabelian groups } \Sigma : \Sigma \text{ is a Jordan–H\"older factor of } G\}. \end{aligned}$$

Note that any simple Jordan–H\"older factor of G occurs in G (but generally not vice versa), i.e., we have $\text{Occ}_{\text{JH}}(G) \subseteq \text{Occ}(G)$. Also note that, if

$$1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$$

is an exact sequence of profinite groups, then

$$(30) \quad \text{Occ}(G) = \text{Occ}(G') \cup \text{Occ}(G''), \quad \text{Occ}_{\text{JH}}(G) = \text{Occ}_{\text{JH}}(G') \cup \text{Occ}_{\text{JH}}(G'').$$

Finally, as observed in [Serre 1968, IV-25], one has that

$$\text{Occ}(GL_2(\mathbb{Z}_\ell)) = \begin{cases} \emptyset & \text{if } \ell \in \{2, 3\}, \\ \{\text{PSL}_2(\mathbb{Z}/5\mathbb{Z})\} = \{A_5\} & \text{if } \ell = 5, \\ \{\text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})\} & \text{if } \ell > 5, \ell \equiv \pm 2 \pmod{5}, \\ \{\text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}), A_5\} & \text{if } \ell > 5, \ell \equiv \pm 1 \pmod{5}. \end{cases}$$

Thus, by (30) we have

$$(31) \quad \text{Occ}(GL_2(\mathbb{Z}(\ell))) = \{A_5\} \cup \{\text{PSL}_2(\mathbb{Z}/p\mathbb{Z})\}_{p \neq \ell, p \geq 5}.$$

Lemma 4.10. *Let $\ell \geq 5$ be a prime and let $G \subseteq GL_2(\mathbb{Z}_\ell)$ be a closed subgroup satisfying $SL_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G(\ell)$. Suppose further that $\psi : G \rightarrow H$ is a surjective group homomorphism onto a finite group H . Then either*

- (1) $\text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) \in \text{Occ}_{\text{JH}}(H)$, or
- (2) H is abelian and $SL_2(\mathbb{Z}_\ell) \subseteq \ker \psi$.

Proof. As observed earlier, since $\ell \geq 5$, the group $\text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is a simple nonabelian group, and we obviously have $\{\text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})\} \subseteq \text{Occ}_{\text{JH}}(SL_2(\mathbb{Z}/\ell\mathbb{Z}))$. Furthermore, by the hypothesis $SL(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G(\ell)$ together with (30), we see that $\{\text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})\} \subseteq \text{Occ}_{\text{JH}}(G(\ell))$. Thus, again by (30), we have

$$(32) \quad \{\text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})\} \subseteq \text{Occ}_{\text{JH}}(G).$$

Furthermore, we have that

$$(33) \quad \frac{\pm(\ker \psi)(\ell) \cap SL_2(\mathbb{Z}/\ell\mathbb{Z})}{\{\pm I\}} = \begin{cases} \{1\} & \text{or} \\ \text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}). \end{cases}$$

If the left side of (33) is trivial, then $\ker \psi$ is prosolvable (so that $\text{Occ}_{\text{JH}}(\ker \psi) = \emptyset$), and considering the exact sequence

$$1 \rightarrow \ker \psi \rightarrow G \rightarrow H \rightarrow 1,$$

we see by (30) and (32) that $\text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) \in \text{Occ}_{\text{JH}}(H)$. If, on the other hand, we have $\text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ in (33), then $SL_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq (\ker \psi)(\ell)$, which by Lemma 3.6 applied to $G = \ker \psi$ implies that $SL_2(\mathbb{Z}_\ell) \subseteq \ker \psi$. Thus H is abelian and ψ factors through the determinant map, as asserted. \square

We now proceed with the proof of Lemma 4.4. By Lemma 4.6, the hypothesis that $G_\ell = GL_2(\mathbb{Z}_\ell)$ and that ℓ divides m_G imply that

$$(34) \quad G \simeq GL_2(\mathbb{Z}_\ell) \times_\psi G(\ell),$$

where $\psi_\ell : GL_2(\mathbb{Z}_\ell) \twoheadrightarrow H$ and $\psi_{(\ell)} : G_{(\ell)} \twoheadrightarrow H$ are surjective homomorphisms onto a common nontrivial group H . Under the Galois correspondence, we have $GL_2(\mathbb{Z}_\ell) \simeq \text{Gal}(K(E[\ell^\infty])/K)$, $G_{(\ell)} \simeq \text{Gal}(K(E_{\text{tors},(\ell)})/K)$ and $H \simeq \text{Gal}(F/K)$,

where $F := K(E[\ell^\infty]) \cap K(E_{\text{tors},(\ell)}) \neq K$. Thus, the corresponding field diagram is as follows.

$$(35) \quad \begin{array}{ccc} K(E[\ell^\infty]) & & K(E_{\text{tors},(\ell)}) \\ & \searrow & \swarrow \\ & F & \\ & | & \\ & K & \end{array}$$

We first claim that

$$(36) \quad F \cap K(\mu_{\ell^\infty}) \neq K.$$

We separate the verification of (36) into cases.

Case: $\ell \geq 5$. By Lemma 4.10, we see that either $\text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ occurs in H (and thus occurs in $G_{(\ell)}$), or H is abelian and $F \subseteq K(\mu_{\ell^\infty})$. If $\ell \geq 7$ then, by (31) we see that H must be abelian and $F \subseteq K(\mu_{\ell^\infty})$, verifying (36). If $\ell = 5$, we consider the further quotient induced by reduction modulo 5:

$$H \simeq \frac{\text{GL}_2(\mathbb{Z}_5)}{\ker \psi_5} \rightarrow \frac{\text{GL}_2(\mathbb{Z}/5\mathbb{Z})}{(\ker \psi_5)(5)} =: H(5).$$

Since the kernel of this quotient is pro-solvable, we see that if $\text{PSL}_2(\mathbb{Z}/5\mathbb{Z}) \simeq A_5$ occurs in H , then it must occur in $H(5)$, and a computer calculation shows that we then must have

$$(\ker \psi_5)(5) \subseteq \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in (\mathbb{Z}/5\mathbb{Z})^\times \right\},$$

and thus

$$\langle \text{SL}_2(\mathbb{Z}_5), \ker \psi_5 \rangle \subseteq \left\{ g \in \text{GL}_2(\mathbb{Z}_5) : \left(\frac{\det(g) \pmod 5}{5} \right) = 1 \right\}.$$

By the Galois correspondence, we then have

$$F \cap K(\mu_{5^\infty}) = K(E[5^\infty])^{\langle \text{SL}_2(\mathbb{Z}_5), \ker \psi_5 \rangle} \supseteq K(\sqrt{5}) \neq K,$$

where we are using the fact that $G(5) = \text{GL}_2(\mathbb{Z}/5\mathbb{Z})$, which precludes the possibility that $K(\sqrt{5}) = K$. Thus in any case, (36) also holds for $\ell = 5$.

Case: $\ell = 3$. As in the previous case, we have that (34) holds with $\ell = 3$. By Galois theory, we have that

$$F := K(E[3^\infty])^{\ker \psi_3} \supseteq K(E[3^\infty])^{\langle \text{SL}_2(\mathbb{Z}_3), \ker \psi_3 \rangle} = K(\mu_{3^\infty}) \cap F.$$

As in the previous case, since $\ker \psi_3 \neq GL_2(\mathbb{Z}_3)$, we have $F \neq K$. The following lemma will then imply that $K(\mu_{3^\infty}) \cap F \neq K$.

Lemma 4.11. *Let $N \trianglelefteq GL_2(\mathbb{Z}_3)$ be a closed normal subgroup which satisfies $\langle SL_2(\mathbb{Z}_3), N \rangle = GL_2(\mathbb{Z}_3)$. Then $N = GL_2(\mathbb{Z}_3)$.*

Proof. A computer calculation shows that, if $H \trianglelefteq GL_2(\mathbb{Z}/9\mathbb{Z})$ is a normal subgroup satisfying

$$\langle SL_2(\mathbb{Z}/9\mathbb{Z}), H \rangle = GL_2(\mathbb{Z}/9\mathbb{Z}),$$

then $H = GL_2(\mathbb{Z}/9\mathbb{Z})$. Taking N as in the statement of the lemma and setting $H := N(9)$, we see that $N(9) = GL_2(\mathbb{Z}/9\mathbb{Z})$, and applying (14) with $\beta = 1$, we conclude that $N = GL_2(\mathbb{Z}_3)$. □

Applying Lemma 4.11 with $N = \ker \psi_3$, we find that $K(\mu_{3^\infty}) \cap F \neq K$, since $F \neq K$, verifying (36) in the $\ell = 3$ case as well.

Finally, we observe that (36) implies the conclusion of Lemma 4.4. Indeed, assume that $\ell \nmid \Delta_K$. Since $G_\ell = GL_2(\mathbb{Z}_\ell)$, we have $K \cap \mathbb{Q}(\mu_{\ell^\infty}) = \mathbb{Q}$, and so any prime $\mathfrak{L} \subseteq \mathcal{O}_K$ over ℓ is totally ramified in $K(\mu_{\ell^\infty})$, hence ramified in $F \cap K(\mu_{\ell^\infty})$. Thus, by (35), \mathfrak{L} is ramified in $K(E_{\text{tors},(\ell)})$. By Theorem 4.1, we find that $\ell \mid N_{K/\mathbb{Q}}(\Delta_E)$, finishing the proof. □

Proof of Lemma 4.5. The proof of Lemma 4.5 will make use of the following sublemma.

Lemma 4.12. *Let K be a number field for which $2 \nmid \Delta_K$ and let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal lying over 2. Let $\alpha \in \mathcal{O}_K - \{0\}$ be any element for which $\mathfrak{p} \nmid \alpha \mathcal{O}_K$. Then 2α is not a square in K^\times , so the field $K(\sqrt{2\alpha})$ is a quadratic extension of K . Furthermore, \mathfrak{p} ramifies in $K(\sqrt{2\alpha})$.*

Proof. Let $v_{\mathfrak{p}}$ denote the \mathfrak{p} -adic valuation on K , normalized so that $v_{\mathfrak{p}}(K^\times) = \mathbb{Z}$. Note that, since by assumption 2 is unramified in K and $v_{\mathfrak{p}}(\alpha) = 0$, we have

$$(37) \quad v_{\mathfrak{p}}(2\alpha) = v_{\mathfrak{p}}(2) + v_{\mathfrak{p}}(\alpha) = 1,$$

and so in particular 2α cannot be a square in K^\times , as asserted. Next, let $L := K(\sqrt{2\alpha})$, fix any prime $\mathfrak{P} \subseteq \mathcal{O}_L$ lying over \mathfrak{p} and let $v_{\mathfrak{P}}$ be the \mathfrak{P} -adic valuation on L , normalized so that it extends $v_{\mathfrak{p}}$ on K . By (37), we then have

$$v_{\mathfrak{P}}((2\alpha)^{1/2}) = \frac{1}{2} v_{\mathfrak{P}}(2\alpha) = \frac{1}{2}.$$

It follows that L is ramified over K at \mathfrak{p} , as asserted. □

We now proceed with the proof of Lemma 4.5. Since we are assuming that 4 divides r' , by Lemma 4.6 we may write $G(r')$ as a fibered product:

$$(38) \quad G(r') = G(4) \times_{\psi} G(r'_{(2)}).$$

Case: $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \{1_{r'_{(2)}}\} \not\subseteq G(r')$. In this case, either $G(4) \neq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ or $G(4) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ and the common quotient $\psi_2(G(4)) = \psi_{(2)}(G(r'_{(2)}))$ in (38) is nontrivial. If $G(4) \neq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, we find that $2 \leq [\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) : G(4)] \leq [\pi^{-1}(G(r'_{(2)})) : G(r')]$, and so the result of the lemma follows. If on the other hand $G(4) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, then the common quotient in (38) is nontrivial, and since

$$\begin{aligned}\pi^{-1}(G(r'_{(2)})) &= \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times G(r'_{(2)}), \\ G(r') &= \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times_{\psi} G(r'_{(2)}),\end{aligned}$$

we thus have $2 \leq [\pi^{-1}(G(r'_{(2)})) : G(r')]$, proving the lemma in this subcase as well.

Case: $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \{1_{r'_{(2)}}\} \subseteq G(r')$. In this case, (38) is a full product:

$$(39) \quad G(r') = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times G(r'_{(2)}).$$

By Lemma 3.6, either $G(8)$ is an index 2 subgroup of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ that surjects onto $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, or $G_2 = \mathrm{GL}_2(\mathbb{Z}_2)$. Let us treat the former subcase first. A computer search reveals that there are exactly 4 index 2 subgroups of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ that map surjectively onto $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, namely

$$\ker(\chi_8), \ker(\chi_8\chi_4), \ker(\chi_8\varepsilon), \ker(\chi_8\chi_4\varepsilon),$$

where $\chi_8 : \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) \rightarrow \{\pm 1\}$ (resp. $\chi_4 : \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) \rightarrow \{\pm 1\}$) denotes the Kronecker symbol associated to the quadratic field $\mathbb{Q}(\sqrt{2})$ (resp. to $\mathbb{Q}(\sqrt{-1})$), precomposed with the determinant map, and $\varepsilon : \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow \{\pm 1\}$ denotes the unique nontrivial character of order 2 on $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, precomposed with reduction modulo 2. We have

$$(40) \quad \begin{aligned}K(E[8])^{\ker(\chi_8)} &= K(\sqrt{2}), & K(E[8])^{\ker(\chi_8\varepsilon)} &= K(\sqrt{2\Delta_E}), \\ K(E[8])^{\ker(\chi_8\chi_4)} &= K(\sqrt{-2}), & K(E[8])^{\ker(\chi_8\chi_4\varepsilon)} &= K(\sqrt{-2\Delta_E}).\end{aligned}$$

Here, by $K(\sqrt{\pm 2\Delta_E})$ we mean the quadratic field $K(\sqrt{\pm 2\Delta(E_{\mathrm{Weier}})})$, where E_{Weier} is any fixed Weierstrass model of E and $\Delta(E_{\mathrm{Weier}}) \in K^\times$ denotes its discriminant (note that although $\Delta(E_{\mathrm{Weier}})$ depends on the choice of E_{Weier} , the quadratic field $K(\sqrt{\pm 2\Delta(E_{\mathrm{Weier}})})$ depends only on E). By (40), we thus have

$$G(8) = \ker(\chi_8) \Rightarrow \sqrt{2} \in K \quad \text{and} \quad G(8) = \ker(\chi_8\chi_4) \Rightarrow \sqrt{-2} \in K,$$

either of which imply that $2 \mid \Delta_K$. On the other hand, for any Weierstrass model E_{Weier} of E , we have

$$(41) \quad \begin{aligned}G(8) = \ker(\chi_8\varepsilon) &\Rightarrow \sqrt{2\Delta(E_{\mathrm{Weier}})} \in K, \\ G(8) = \ker(\chi_8\chi_4\varepsilon) &\Rightarrow \sqrt{-2\Delta(E_{\mathrm{Weier}})} \in K.\end{aligned}$$

Let us suppose for the sake of contradiction that

$$(42) \quad 2 \nmid \Delta_K N_{K/\mathbb{Q}}(\Delta_E).$$

Fix a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ lying over 2. By (42), we must have $\mathfrak{p} \nmid \Delta_E$, and we may thus find a Weierstrass model E_{Weier} of E satisfying $\mathfrak{p} \nmid \Delta(E_{\mathrm{Weier}})$. Applying Lemma 4.12 with $\alpha = \pm \Delta(E_{\mathrm{Weier}})$, we see that

$$\sqrt{\pm 2\Delta(E_{\mathrm{Weier}})} \notin K,$$

contradicting (41). Thus, we must have $2 \mid \Delta_K N_{K/\mathbb{Q}}(\Delta_E)$ whenever $G(8)$ has index 2 in $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$.

We now treat the second subcase, in which $G_2 = \mathrm{GL}_2(\mathbb{Z}_2)$. We evidently must have a nontrivial common quotient in

$$G_{r'} \simeq \mathrm{GL}_2(\mathbb{Z}_2) \times_{\psi} G_{r'_{(2)}}.$$

(If this fibered product were over a trivial quotient, then 2 would not divide m_G .) We note that any nontrivial finite quotient of $\mathrm{GL}_2(\mathbb{Z}_2)$ must have order divisible by 2 and that $\ker(G_{r'_{(2)}} \rightarrow G(r'_{(2)}))$ is a profinite group whose finite quotients each have order coprime with 2. It follows that the image of G under $\mathrm{id}_2 \times \pi_{(r'_{(2)})^\infty, r'_{(2)}}$ has the form

$$(43) \quad \mathrm{GL}_2(\mathbb{Z}_2) \times_{\psi} G(r'_{(2)}),$$

a fibered product with a common quotient of order divisible by 2 (and hence nontrivial). Consider the subgroup $N := \ker \psi_2 \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ where $\psi = (\psi_2, \psi_{(2)})$ in (43). The assumption $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \{1_{r'_{(2)}}\} \subseteq G(r')$ then implies that $N(4) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ (otherwise the mod r' image of (43) would have a nontrivial fibering between $G(4)$ and $G(r'_{(2)})$, contradicting (39)). By Lemma 3.6, we find that $[\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : N(8)] = 2$. By the same computation as mentioned in the previous subcase, we have

$$N(8) \in \{\ker(\chi_8), \ker(\chi_8\chi_4), \ker(\chi_8\varepsilon), \ker(\chi_8\chi_4\varepsilon)\},$$

and it follows by (40) and Galois theory that one of the fields $K(\sqrt{2})$, $K(\sqrt{-2})$, $K(\sqrt{2\Delta_E})$, or $K(\sqrt{-2\Delta_E})$ must be contained in $K(E_{\mathrm{tors}, (2)})$. By Lemma 4.12 and Theorem 4.1, it follows that, if $2 \nmid \Delta_K$ then 2 divides $N_{K/\mathbb{Q}}(\Delta_E)$. This finishes the proof of Lemma 4.5. \square

Acknowledgements

I would like to thank J. Mayle for thoughtful comments on a previous version and also the anonymous referee for carefully reading the manuscript and giving several helpful suggestions.

References

- [Bell et al. 2020] R. Bell, C. Blakestad, A. C. Cojocaru, A. Cowan, N. Jones, V. Matei, G. Smith, and I. Vogt, “Constants in Titchmarsh divisor problems for elliptic curves”, *Res. Number Theory* **6**:1 (2020), art. no. 1, 24 pp. [MR](#) [Zbl](#)
- [Bilu and Parent 2011] Y. Bilu and P. Parent, “Serre’s uniformity problem in the split Cartan case”, *Ann. of Math. (2)* **173**:1 (2011), 569–584. [MR](#) [Zbl](#)
- [Bilu et al. 2013] Y. Bilu, P. Parent, and M. Rebolledo, “Rational points on $X_0^+(p')$ ”, *Ann. Inst. Fourier (Grenoble)* **63**:3 (2013), 957–984. [MR](#) [Zbl](#)
- [Bourdon et al. 2019] A. Bourdon, O. Ejder, Y. Liu, F. Odumodu, and B. Viray, “On the level of modular curves that give rise to isolated j -invariants”, *Adv. Math.* **357** (2019), art. id. 106824, 33 pp. [MR](#) [Zbl](#)
- [Brau and Jones 2016] J. Brau and N. Jones, “Elliptic curves with 2-torsion contained in the 3-torsion field”, *Proc. Amer. Math. Soc.* **144**:3 (2016), 925–936. [MR](#) [Zbl](#)
- [Cojocaru 2005] A. C. Cojocaru, “On the surjectivity of the Galois representations associated to non-CM elliptic curves”, *Canad. Math. Bull.* **48**:1 (2005), 16–31. [MR](#) [Zbl](#)
- [Daniels 2015] H. B. Daniels, “An infinite family of Serre curves”, *J. Number Theory* **155** (2015), 226–247. [MR](#) [Zbl](#)
- [Daniels and González-Jiménez 2018] H. B. Daniels and E. González-Jiménez, “Serre’s constant of elliptic curves over the rationals”, preprint, 2018. To appear in *Exp. Math.* [arXiv](#)
- [Dokchitser and Dokchitser 2012] T. Dokchitser and V. Dokchitser, “Surjectivity of mod 2^n representations of elliptic curves”, *Math. Z.* **272**:3-4 (2012), 961–964. [MR](#) [Zbl](#)
- [Elkies 2006] N. D. Elkies, “Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9”, preprint, 2006. [arXiv](#)
- [Huppert 1967] B. Huppert, *Endliche Gruppen*, vol. I, Die Grundlehren der Mathematischen Wissenschaften **134**, Springer, 1967. [MR](#) [Zbl](#)
- [Jones 2009] N. Jones, “A bound for the torsion conductor of a non-CM elliptic curve”, *Proc. Amer. Math. Soc.* **137**:1 (2009), 37–43. [MR](#) [Zbl](#)
- [Jones 2019] N. Jones, “A bound for the conductor of an open subgroup of GL_2 associated to an elliptic curve”, preprint, 2019. [arXiv](#)
- [Lozano-Robledo 2013] A. Lozano-Robledo, “On the field of definition of p -torsion points on elliptic curves over the rationals”, *Math. Ann.* **357**:1 (2013), 279–305. [MR](#) [Zbl](#)
- [Mazur 1978] B. Mazur, “Rational isogenies of prime degree”, *Invent. Math.* **44**:2 (1978), 129–162. [MR](#) [Zbl](#)
- [Merel 1996] L. Merel, “Bornes pour la torsion des courbes elliptiques sur les corps de nombres”, *Invent. Math.* **124**:1-3 (1996), 437–449. [MR](#) [Zbl](#)
- [Morrow 2019] J. S. Morrow, “Composite images of Galois for elliptic curves over \mathbf{Q} and entanglement fields”, *Math. Comp.* **88**:319 (2019), 2389–2421. [MR](#) [Zbl](#)
- [Ogg 1967] A. P. Ogg, “Elliptic curves and wild ramification”, *Amer. J. Math.* **89** (1967), 1–21. [MR](#) [Zbl](#)
- [Ribet 1976] K. A. Ribet, “Galois action on division points of Abelian varieties with real multiplications”, *Amer. J. Math.* **98**:3 (1976), 751–804. [MR](#) [Zbl](#)
- [Serre 1968] J.-P. Serre, *Abelian l -adic representations and elliptic curves*, W. A. Benjamin, New York, 1968. [MR](#) [Zbl](#)

- [Serre 1972] J.-P. Serre, “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”, *Invent. Math.* **15**:4 (1972), 259–331. [MR](#) [Zbl](#)
- [Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, 1986. [MR](#) [Zbl](#)
- [Sutherland and Zywina 2017] A. V. Sutherland and D. Zywina, “Modular curves of prime-power level with infinitely many rational points”, *Algebra Number Theory* **11**:5 (2017), 1199–1229. [MR](#) [Zbl](#)
- [Weil 1940] A. Weil, “Sur les fonctions algébriques à corps de constantes fini”, *C. R. Acad. Sci. Paris* **210** (1940), 592–594. [MR](#) [Zbl](#)
- [Zywina 2010] D. Zywina, “Elliptic curves with maximal Galois action on their torsion points”, *Bull. Lond. Math. Soc.* **42**:5 (2010), 811–826. [MR](#) [Zbl](#)
- [Zywina 2015a] D. Zywina, “On the possible images of the mod ℓ representations associated to elliptic curves over \mathbb{Q} ”, preprint, 2015. [arXiv](#)
- [Zywina 2015b] D. Zywina, “Possible indices for the Galois image of elliptic curves over \mathbb{Q} ”, preprint, 2015. [arXiv](#)

Received October 18, 2019. Revised May 8, 2020.

NATHAN JONES
DEPARTMENT OF MATHEMATICS, STATISTICS, AND COMPUTER SCIENCE
UNIVERSITY OF ILLINOIS AT CHICAGO
CHICAGO, IL
UNITED STATES
ncjones@uic.edu

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

EDITORS

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Paul Balmer
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
balmer@math.ucla.edu

Wee Teck Gan
Mathematics Department
National University of Singapore
Singapore 119076
matgwt@nus.edu.sg

Sorin Popa
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
popa@math.ucla.edu

Paul Yang
Department of Mathematics
Princeton University
Princeton NJ 08544-1000
yang@math.princeton.edu

Matthias Aschenbrenner
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
matthias@math.ucla.edu

Daryl Cooper
Department of Mathematics
University of California
Santa Barbara, CA 93106-3080
cooper@math.ucsb.edu

Jiang-Hua Lu
Department of Mathematics
The University of Hong Kong
Pokfulam Rd., Hong Kong
jhlu@maths.hku.hk

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Kefeng Liu
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
liu@math.ucla.edu

Jie Qing
Department of Mathematics
University of California
Santa Cruz, CA 95064
qing@cats.ucsc.edu

PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org

SUPPORTING INSTITUTIONS

ACADEMIA SINICA, TAIPEI
CALIFORNIA INST. OF TECHNOLOGY
INST. DE MATEMÁTICA PURA E APLICADA
KEIO UNIVERSITY
MATH. SCIENCES RESEARCH INSTITUTE
NEW MEXICO STATE UNIV.
OREGON STATE UNIV.

STANFORD UNIVERSITY
UNIV. OF BRITISH COLUMBIA
UNIV. OF CALIFORNIA, BERKELEY
UNIV. OF CALIFORNIA, DAVIS
UNIV. OF CALIFORNIA, LOS ANGELES
UNIV. OF CALIFORNIA, RIVERSIDE
UNIV. OF CALIFORNIA, SAN DIEGO
UNIV. OF CALIF., SANTA BARBARA

UNIV. OF CALIF., SANTA CRUZ
UNIV. OF MONTANA
UNIV. OF OREGON
UNIV. OF SOUTHERN CALIFORNIA
UNIV. OF UTAH
UNIV. OF WASHINGTON
WASHINGTON STATE UNIVERSITY

These supporting institutions contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its contents or policies.


See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2020 is US \$520/year for the electronic version, and \$705/year for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by [Mathematical Reviews](#), [Zentralblatt MATH](#), [PASCAL CNRS Index](#), [Referativnyi Zhurnal](#), [Current Mathematical Publications](#) and [Web of Knowledge \(Science Citation Index\)](#).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW[®] from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2020 Mathematical Sciences Publishers

PACIFIC JOURNAL OF MATHEMATICS

Volume 308 No. 2 October 2020

Existence of steady multiple vortex patches to the vortex-wave system	257
DAOMIN CAO and GUODONG WANG	
Relations of rationality for special values of Rankin–Selberg L -functions of $GL_n \times GL_m$ over CM-fields	281
HARALD GROBNER and GUNJA SACHDEVA	
A bound for the conductor of an open subgroup of GL_2 associated to an elliptic curve	307
NATHAN JONES	
Topology of complexity one quotients	333
Yael KARSHON and SUSAN TOLMAN	
Flag Bott manifolds and the toric closure of a generic orbit associated to a generalized Bott manifold	347
SHINTARÔ KUROKI, EUNJEONG LEE, JONGBAEK SONG and DONG YOUP SUH	
Projective cases for the restriction of the oscillator representation to dual pairs of type I	393
SABINE J. LANG	
A remark on a trace Paley–Wiener theorem	407
GORAN MUIĆ	
Spectrum of the Laplacian and the Jacobi operator on rotational CMC hypersurfaces of spheres	419
OSCAR M. PERDOMO	
Mean curvature flow in a Riemannian manifold endowed with a Killing vector field	435
LIANGJUN WENG	
Green correspondence and relative projectivity for pairs of adjoint functors between triangulated categories	473
ALEXANDER ZIMMERMANN	