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

NATHAN JONES

Abstract. 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 $m$. In this note, 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 $E_{\text{tors}}$ denote its torsion subgroup. Denote by $G_K := \text{Gal}(\overline{K}/K)$ the absolute Galois group of $K$ and consider the Galois representation

$$\rho_{E,K} : G_K \rightarrow \text{Aut}(E_{\text{tors}}) \simeq GL_2(\hat{\mathbb{Z}})$$

defined by letting $G_K$ act on the torsion of $E$ and choosing a $\hat{\mathbb{Z}}$-basis thereof. A celebrated theorem of J.-P. Serre [15] states that, if $E$ has no complex multiplication, then the image of $\rho_{E,K}$ is open inside $GL_2(\hat{\mathbb{Z}})$, or equivalently that

$$\left[GL_2(\hat{\mathbb{Z}}) : \rho_{E,K}(G_K)\right] < \infty.$$

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

$$\ker\left(GL_2(\hat{\mathbb{Z}}) \rightarrow GL_2(\mathbb{Z}/m\mathbb{Z})\right) \subseteq \rho_{E,K}(G_K).$$

Definition 1.1. Given an open subgroup $G \subseteq GL_2(\hat{\mathbb{Z}})$, we define the positive integer $m_G$ by

$$m_G := \min\{m \in \mathbb{N} : \ker\left(GL_2(\hat{\mathbb{Z}}) \rightarrow GL_2(\mathbb{Z}/m\mathbb{Z})\right) \subseteq G\}$$

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 $m_{E,K}$.

The purpose of this note is to prove the following upper bound for $m_{E,K}$. In its statement, $\Delta_K$ denotes the absolute discriminant of the number field $K$, $\Delta_E$ 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

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

denotes the radical of the positive integer $m$. Given a non-zero 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

$$m_{E,K} \leq 2 \cdot \left[GL_2(\hat{\mathbb{Z}}) : \rho_{E,K}(G_K)\right] \cdot \text{rad}(|\Delta_K N_{K/\mathbb{Q}}(\Delta_E)|).$$

Remark 1.3. The bound in Theorem 1.2 both improves upon and generalizes a bound appearing in [8]. Furthermore, using results in [4], we may see that there are infinitely many elliptic curves $E$ over $\mathbb{Q}$ satisfying

$$m_{E,\mathbb{Q}} = 2 \cdot \left[GL_2(\hat{\mathbb{Z}}) : \rho_{E,\mathbb{Q}}(G_{\mathbb{Q}})\right] \cdot \text{rad}(|\Delta_E|).$$

Equation (1)

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

1
Thus, our bound for \( m_{E,K} \) is sharp when \( K = \mathbb{Q} \).

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 \( \rho_{E,K}(G_K) \subseteq \text{GL}_2(\hat{\mathbb{Z}}) \). 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 \( p \) reductions (see [10], [11], [9], [1], [2], and [21]) and also more recently its reductions at composite levels (see [5], [18] and [12]). In addition to this connection, Theorem 1.2 also has analytic relevance; for instance in [3] it is applied to the study of averages of constants appearing in various elliptic curve conjectures.

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

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

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 \( \text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}_3) \) (resp. under \( \text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}/3\mathbb{Z}) \)). The analysis proceeds a bit differently according to whether or not the condition

\[ 9 \mid m_G, \quad \text{SL}_2(\mathbb{Z}_3) \nsubseteq G_3 \quad \text{and} \quad G(3) = \text{GL}_2(\mathbb{Z}/3\mathbb{Z}) \]

holds.

**Proposition 1.4.** Let \( G \subseteq \text{GL}_2(\hat{\mathbb{Z}}) \) be an open subgroup and let \( m_G \) be as in Definition 1.1. We then have

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

where \( \text{rad}'(\cdot) \) is defined as in (2) and \( \pi : \text{GL}_2(\mathbb{Z}/m_G\mathbb{Z}) \to \text{GL}_2(\mathbb{Z}/\text{rad}'(m_G)\mathbb{Z}) \) denotes the canonical projection map. Assuming that (3) holds, we have

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

In contrast with Proposition 1.4, 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 Néron-Ogg-Shafarevich criterion for ramification in division fields.

**Proposition 1.5.** 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 (3) does not hold, we have

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

If (3) does hold, then

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

Since the index of a subgroup is preserved under taking the full pre-image, we have that

\[
\left[ \text{GL}_2(\mathbb{Z}/\text{rad}'(m_G)\mathbb{Z}) : G(\text{rad}'(m_G)) \right] = \left[ \text{GL}_2(\mathbb{Z}/m_G\mathbb{Z}) : \pi^{-1}(G(\text{rad}'(m_G))) \right],
\]

where \( \pi : \text{GL}_2(\mathbb{Z}/m_G\mathbb{Z}) \to \text{GL}_2(\mathbb{Z}/\text{rad}'(m_G)\mathbb{Z}) \) is the canonical projection map. Thus, Theorem 1.2 follows from Propositions 1.4 and 1.5.

Many of the ingredients that enter into the proof of Theorem 1.2 may be verified for algebraic groups other than \( \text{GL}_2 \). 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 \( \text{GSp}_{2g}(\hat{\mathbb{Z}}) \).
2. Notation and preliminaries

Throughout the paper, \( p \) and \( \ell \) 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

\[
\mathbb{N}_{\geq \alpha} := \{ n \in \mathbb{N} : n \geq \alpha \},
\quad \mathbb{Z}_{\geq \alpha} := \{ n \in \mathbb{Z} : n \geq \alpha \}.
\]

We recall that

\[
\mathbb{Z} \leftarrow \mathbb{Z}/m\mathbb{Z}
\]

is the inverse limit of the rings \( \mathbb{Z}/m\mathbb{Z} \) with respect to the canonical projection maps \( \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \). Under the isomorphism of the Chinese Remainder Theorem, we have that

\[
\mathbb{Z} \simeq \prod \mathbb{Z}_\ell,
\]

where \( \mathbb{Z}_\ell \) as usual denotes the ring of \( \ell \)-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 \( \mathbb{Z} \) corresponding under (4) to the following rings:

\[
\mathbb{Z}_m \simeq \prod_{\ell \mid m} \mathbb{Z}_\ell,
\quad \mathbb{Z}_{(m)} \simeq \prod_{\ell \nmid m} \mathbb{Z}_\ell.
\]

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

\[
\mathbb{Z} \simeq \mathbb{Z}_m \times \mathbb{Z}_{(m)},
\]

and projection maps

\[
\mathbb{Z} \to \mathbb{Z}_m,
\quad \mathbb{Z} \to \mathbb{Z}_{(m)}.
\]

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

\[
\text{GL}_2(\hat{\mathbb{Z}}) \simeq \text{GL}_2(\mathbb{Z}_m) \times \text{GL}_2(\mathbb{Z}_{(m)}) \simeq \prod \text{GL}_2(\mathbb{Z}_\ell)
\]

and we have projection maps

\[
\pi_m : \text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}_m),
\quad \pi_{(m)} : \text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}_{(m)}).
\]

In most cases we will denote any projection map simply by \( \pi \), but on some occasions we will decorate it with subscripts, such as in (5) or

\[
\pi_{m,\infty} : \text{GL}_2(\mathbb{Z}_m) \to \text{GL}_2(\mathbb{Z}/m\mathbb{Z}),
\quad \pi_{nm,n} : \text{GL}_2(\mathbb{Z}/nm\mathbb{Z}) \to \text{GL}_2(\mathbb{Z}/n\mathbb{Z}).
\]

The ring \( \hat{\mathbb{Z}} \) is a topological ring under the profinite topology, and the group \( \text{GL}_2(\hat{\mathbb{Z}}) \) inherits the structure of a profinite group. We recall that any open subgroup \( G \subseteq \text{GL}_2(\hat{\mathbb{Z}}) \) is a closed subgroup but not conversely. In general, given any closed subgroup \( G \subseteq \text{GL}_2(\hat{\mathbb{Z}}) \), we denote by \( G_m \subseteq \text{GL}_2(\mathbb{Z}_m) \) (resp. by \( G_{(m)} \subseteq \text{GL}_2(\mathbb{Z}_{(m)}) \)) its image under \( \pi_m \) (resp. under \( \pi_{(m)} \)) as in (5). We denote by \( G(m) \) the image of \( G \) under the canonical projection

\[
\text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}/m\mathbb{Z}).
\]

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

\[
m(d) := \prod_{d \mid f_{\text{ord}_d(m)}} \frac{m}{d}.
\]

Finally, we let

\[
id_m : \text{GL}_2(\mathbb{Z}_m) \to \text{GL}_2(\mathbb{Z}_m),
\quad \text{id}_{(m)} : \text{GL}_2(\mathbb{Z}_{(m)}) \to \text{GL}_2(\mathbb{Z}_{(m)}),
\]
denote the identity maps, and we let $1_m$ (resp. $1_{(m)}$) denote the identity element of $GL_2(\mathbb{Z}_m)$ (resp. of $GL_2(\mathbb{Z}/m\mathbb{Z})$). We may also at times denote by $1_m$ the identity element of $GL_2(\mathbb{Z}/m\mathbb{Z})$.

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 $\ell$ we define

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

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

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

For a number field $K$, we denote by $O_K$ its ring of integers, by $\Delta_K$ its absolute discriminant and by $N_{K/Q} : K \to Q$ the norm map. A critical issue that arises in the proof of Proposition 1.5 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 non-trivial 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

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

More generally, if $G_1$, $G_2$ and $H$ are groups and $\psi_1 : G_1 \to H$, $\psi_2 : G_2 \to H$ 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 $\psi$ is an abbreviation for the ordered pair $(\psi_1, \psi_2)$). 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 non-trivial group, where

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

denotes the restriction map.

3. PROOF OF PROPOSITION 1.5

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

$$m_G := \prod_\ell \ell^{\beta_\ell}. \quad (6)$$

In what follows we use the maps

$$\pi_{\ell^{\beta_1+1}, \ell^{\beta}} \times \text{id}_\ell : GL_2(\mathbb{Z}/\ell^{\beta+1}\mathbb{Z}) \times GL_2(\mathbb{Z}(\ell)) \to GL_2(\mathbb{Z}/\ell^{\beta}\mathbb{Z}) \times GL_2(\mathbb{Z}(\ell))$$

$$\pi_{\ell^{\infty}, \ell^{\beta+1}} \times \text{id}_\ell : GL_2(\mathbb{Z}(\ell)) \times GL_2(\mathbb{Z}(\ell)) \to GL_2(\mathbb{Z}/\ell^{\beta+1}\mathbb{Z}) \times GL_2(\mathbb{Z}(\ell))$$

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

$$\alpha_\ell := \begin{cases} 2 & \text{if } \ell = 2 \\ 1 & \text{if } \ell \geq 3. \end{cases} \quad (7)$$

The next lemma follows from ideas in [10], Lemma 3, IV-23. In its statement and henceforth, we will interpret $GL_2(\mathbb{Z}/\ell^0\mathbb{Z}) := \{1\}$ as the trivial group, so that $\ker \pi_{\ell,1} = GL_2(\mathbb{Z}/\ell\mathbb{Z})$.

**Lemma 3.1.** Let $G \subseteq GL_2(\hat{\mathbb{Z}})$ be a closed subgroup, let $\ell$ be a prime number, and let $\beta \in \mathbb{Z}_{\geq 0}$. Assume that

$$\forall \gamma \in [\beta, \max\{\beta, \alpha_\ell\}] \cap \mathbb{Z}, \quad \ker(\pi_{\ell^{\beta_1+1}, \ell^{\beta}} \times \{1\}) \subseteq \ker(\pi_{\ell^{\infty}, \ell^{\beta+1}} \times \text{id}_\ell)(G),$$

where $\alpha_\ell$ is as in (7). We then have

$$\ker(\pi_{\ell^{\infty}, \ell^{\beta}} \times \{1\}) \subseteq G.$$
Proof. Since $G \subseteq \text{GL}_2(\hat{\mathbb{Z}})$ is closed, it suffices to prove that, for each $n \in \mathbb{Z}_{2, \max \{ \beta, \alpha \}}$, one has
\[
\ker(\pi_{e^n+1,e^n}) \times \{1(e)\} \subseteq (\pi_{e^n+1,e^n+1} \times \text{id}_e)(G).
\] (8)
We prove this by induction on $n$ as follows (the base case $n = \max\{\beta, \alpha\}$ is true by hypothesis). First note that, for $n \geq 1$, we have
\[
\ker(\pi_{e^n+1,e^n}) = \{ I + e^n \tilde{X} \mod e^{n+1} : \tilde{X} \in M_{2 \times 2}(\mathbb{Z}_e) \}.
\] (9)
Thus, (8) may be reformulated as saying
\[
\forall X \in M_{2 \times 2}(\mathbb{F}_e), \exists \tilde{X} \in M_{2 \times 2}(\mathbb{Z}_e) \text{ such that } \tilde{X} \equiv X \mod e \Rightarrow g := (I + e^n \tilde{X}, 1(e)) \in G.
\] (10)
Our goal is to deduce that (10) continues to hold when $n$ is replaced by $n + 1$. Since $G$ is a group, $g^e \in G$, and one sees by considering the binomial expansion
\[
(I + e^n \tilde{X})^e = I + \frac{e}{1} e^n \tilde{X} + \frac{e^2}{2} e^{2n} \tilde{X}^2 + \ldots + \frac{e^{(e-1)n}}{e-1} e^{(e-1)n} \tilde{X}^{e-1} + e^en \tilde{X}^e
\] (11)
that
\[
(\pi_{e^n+2,e^n+2} \times \text{id}_e)(g^e) = (I + e^{n+1} \tilde{X} \mod e^{n+2}, 1(e)).
\]
Since $X$ in (11) was arbitrary, it follows by (9) that
\[
\ker(\pi_{e^n+2,e^n+1}) \times \{1(e)\} \subseteq (\pi_{e^n+2,e^n+1} \times \text{id}_e)(G),
\]
completing the induction and proving the lemma.

Definition 3.2. We define the exponents $\beta'_e = \beta'_e(G)$ by
\[
\beta'_e := \min\{ \beta \in \mathbb{Z}_{\geq 0} : \forall \gamma \in [\beta, \max\{\beta, \alpha\}] \cap \mathbb{Z}, \ker(\pi_{e^n+1,e^n}) \times \{1(e)\} \subseteq (\pi_{e^n+1,e^n+1} \times \text{id}_e)(G) \},
\]
where $\alpha_e$ is as in (7).

Corollary 3.3. We have $\beta_e = \beta'_e$, where $\beta_e$ is as in (6).

Proof. By Lemma 3.1, for each prime $e$ we have
\[
\ker(\pi_{e^n,e^n}) \times \{1(e)\} \subseteq G.
\]
Since $\ker \left( \text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}/\prod_\ell \ell^{\beta'_e} \mathbb{Z}) \right)$ is equal to the subgroup of $\text{GL}_2(\hat{\mathbb{Z}})$ generated by $\ker(\pi_{e^n,e^n}) \times \{1(e)\}$ as $e$ varies over all primes, we then have
\[
\ker \left( \text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}/\prod_\ell \ell^{\beta'_e} \mathbb{Z}) \right) \subseteq G.
\]
Thus, by (6) and Definition 1.1 we see that $\beta_e \leq \beta'_e$.

Conversely, suppose for the sake of contradiction that $\beta_e < \beta'_e$. By definition of $\beta_e$, we would then have
\[
\ker \left( \pi_{e^n+1,e^n} \right) \times \{1(e)\} \subseteq \ker \left( \pi_{e^n+1,e^n+1} \times \text{id}_e \right)(G).
\] (12)
Furthermore, since $\pi_{e^n+2,e^n}(\ker(\pi_{e^n+1,e^n})) = \ker(\pi_{e^n+1,e^n+1})$, we then see that (12) would then imply
\[
\forall \gamma \in [\beta'_e - 1, \max\{\beta'_e - 1, \alpha_e\}] \cap \mathbb{Z}, \ker(\pi_{e^n+1,e^n}) \times \{1(e)\} \subseteq (\pi_{e^n+1,e^n+1} \times \text{id}_e)(G),
\]
contradicting Definition 3.2. Thus, $\beta'_e \leq \beta_e$.

Remark 3.4. The “purely $e$-adic version” of Lemma 3.1 also follows by the same proof (without the $\text{GL}_2(\mathbb{Z}_e)$ factor). Precisely, for any prime $e$ and closed subgroup $G \subseteq \text{GL}_2(\mathbb{Z}_e)$, and any $\beta \in \mathbb{Z}_{\geq 0}$, one has
\[
\forall \gamma \in [\beta, \max\{\beta, \alpha_e\}] \cap \mathbb{Z}, \ker \left( \text{GL}_2(\mathbb{Z}/\ell^{\gamma+1} \mathbb{Z}) \to \text{GL}_2(\mathbb{Z}/\ell^{\gamma+1} \mathbb{Z}) \right) \subseteq G(\ell^{\gamma+1}) \Rightarrow \ker \left( \text{GL}_2(\mathbb{Z}_e) \to \text{GL}_2(\mathbb{Z}/\ell^{\beta_e} \mathbb{Z}) \right) \subseteq G.
\] (13)
We will also find it useful to have sufficient conditions to conclude that $\text{SL}_2(\mathbb{Z}_e) \subseteq G$ where $G \subseteq \text{GL}_2(\mathbb{Z}_e)$ is an arbitrary closed subgroup. The next lemma does so for $e$ odd, and gives us sufficient information to allow us to deal separately with the prime $e = 2$. As with Lemma 3.1, it can be largely deduced from arguments found in the proof of [16, Lemma 3, IV-23]; we reproduce those arguments here for the sake of completeness.
**Lemma 3.5.** Let $\ell$ be a prime number and let $G \subseteq \text{GL}_2(\mathbb{Z}_\ell)$ be a closed subgroup. If $\ell \geq 5$, then we have

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

If $\ell = 3$, we have

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

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

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

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

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

which amounts to showing that $\text{SL}_2(\mathbb{Z}_\ell) \subseteq [G, G]$, since the reverse inclusion is clearly true. We begin by first showing, by induction on $n$, that

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

(15)

The binomial expansion argument (11) 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

$$\det \left( I + \ell^n \tilde{X} \right) \equiv 1 + \ell^n \text{ tr} \tilde{X} \mod \ell^{n+1} \quad (n \geq 1).$$

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

$$\ker (\text{SL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})) = \{ I + \ell^n \tilde{X} \mod \ell^{n+1} : \tilde{X} \in M_{2 \times 2}(\mathbb{Z}_\ell) \},$$

where $M_{2 \times 2}(\mathbb{Z}_\ell) = \{ \tilde{X} \in M_{2 \times 2}(\mathbb{Z}_\ell) : \text{tr} \tilde{X} \equiv 0 \mod \ell \}$. In particular, ker ($\text{SL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$) is a 3-dimensional subspace of the 4-dimensional $\mathbb{Z}/\ell\mathbb{Z}$-vector space ker($\pi_{\ell\mathbb{Z}}$). It follows from this, together with the fact that $\left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right)$ and $\left( \begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right)$ reduced modulo $\ell$ generate $\text{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, that the set

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

satisfies

$$\langle I + \ell^n \mathcal{K} \mod \ell^{n+1} \rangle = \ker (\text{SL}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})) \quad (n \geq 0).$$

(17)

Fix $X \in \mathcal{K}$. Note that $I + \ell^0 X \mod \ell \in \text{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, 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 $\tilde{X}^2 \equiv 0 \mod \ell$, so $\tilde{X}^4 \equiv 0 \mod \ell^2$. Thus, since $\ell \geq 5$, we have

$$(I + \ell^0 \tilde{X})^\ell = I + \left( \frac{\ell}{1} \right) \tilde{X} + \left( \frac{\ell}{2} \right) \tilde{X}^2 + \cdots + \left( \frac{\ell}{\ell - 1} \right) \tilde{X}^{\ell - 1} + \tilde{X}^\ell \equiv I + \ell \tilde{X} \mod \ell^2,$$

and more generally,

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

(16)

Therefore (15) is established by induction on $n$.

We now proceed to verify (11) for $\ell$ an odd prime. When $\ell \geq 5$, the group $\text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is a non-abelian simple group (see e.g. [11] Ch. II, Hauptsatz 6.13), and the exact sequence

$$1 \longrightarrow \{ \pm I \} \longrightarrow \text{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \text{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow 1$$

does not split (see e.g. [20] Lemma 2.3). From this and a computer computation for the prime $\ell = 3$, we then find that

$$\ell \geq 5 \implies [G(\ell), G(\ell)] = \text{SL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

$$\ell = 3 \implies [\text{GL}_2(\mathbb{Z}/3\mathbb{Z}), \text{GL}_2(\mathbb{Z}/3\mathbb{Z})] = \text{SL}_2(\mathbb{Z}/3\mathbb{Z}).$$
Note that the commutator subgroup \([G, G] \subseteq G\) projects modulo \(\ell\) onto the commutator subgroup \([G(\ell), G(\ell)] = SL_2(\mathbb{Z}/\ell\mathbb{Z})\). We will prove by induction on \(n \in \mathbb{N}\) that
\[
[G(\ell^n), G(\ell^n)] = SL_2(\mathbb{Z}/\ell^n\mathbb{Z}) \quad (n \geq 1),
\] (18)
having just established the base case. Fix \(n \geq 1\) and assume that (18) holds. Pick any \(g \in G(\ell^{n+1})\) and \(\tilde{X} \in M_{2 \times 2}^{tr=0}(\mathbb{Z}_\ell)\), so that, by (13) and (10), we have \(I + \ell^n \tilde{X} \equiv I + \ell^n X \mod \ell^{n+1} \in G(\ell^{n+1})\). We then compute the commutator
\[
g(I + \ell^n \tilde{X})g^{-1}(I + \ell^n \tilde{X})^{-1} = g(I + \ell^n X)g^{-1}(I - \ell^n \tilde{X}) = I + \ell^n (g \tilde{X} g^{-1} - \tilde{X}) \mod \ell^{n+1}.
\] (19)
Consider the following computations in \(M_{2 \times 2}(\mathbb{Z}/\ell\mathbb{Z})\):
\[
\begin{pmatrix} dx & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & d \\ 0 & dx \end{pmatrix} = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix},
\]
\[
\begin{pmatrix} d & 0 \\ 0 & dx \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} d & 0 \\ 0 & dx \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix},
\]
\[
\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.
\]
It follows that, inside the additive 3-dimensional \(\mathbb{Z}/\ell\mathbb{Z}\)-vector space
\[
M_{2 \times 2}^{tr=0}(\mathbb{Z}/\ell\mathbb{Z}) := \{X \in M_{2 \times 2}(\mathbb{Z}/\ell\mathbb{Z}) : tr X = 0\},
\]
we have
\[
\ell \geq 5 \implies \{gXg^{-1} - X : g \in SL_2(\mathbb{Z}/\ell\mathbb{Z}), X \in M_{2 \times 2}^{tr=0}(\mathbb{Z}/\ell\mathbb{Z})\} = M_{2 \times 2}^{tr=0}(\mathbb{Z}/\ell\mathbb{Z}),
\]
\[
\ell = 3 \implies \{gXg^{-1} - X : g \in GL_2(\mathbb{Z}/3\mathbb{Z}), X \in M_{2 \times 2}^{tr=0}(\mathbb{Z}/3\mathbb{Z})\} = M_{2 \times 2}^{tr=0}(\mathbb{Z}/3\mathbb{Z}).
\]
Thus, varying \(g\) and \(\tilde{X}\) in (10), we see that
\[
ker (SL_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \to SL_2(\mathbb{Z}/\ell^n\mathbb{Z})) \subseteq [G(\ell^{n+1}), G(\ell^n)],
\]
verifying that (18) holds with \(n\) replaced by \(n + 1\), thus completing the induction step. Since \([G, G] \subseteq G \subseteq GL_2(\mathbb{Z}_\ell)\) are closed subgroups, we have therefore verified (13), proving Lemma 3.5 in case \(\ell\) is odd.

Now assume \(\ell = 2\) and note that (17) is still valid. By the hypothesis that \(G(4) = GL_2(\mathbb{Z}/4\mathbb{Z})\), for each \(X \in \mathcal{K}\) we may find a lift \(\tilde{X} \in M_{2 \times 2}(\mathbb{Z}_2)\) for which \(\tilde{X} \equiv X \mod 2\) and \(I + 2\tilde{X} \in G\). Again computing
\[
(I + 2\tilde{X})^2 = I + 4\tilde{X} + 4\tilde{X}^2 = I + 4\tilde{X} \mod 8,
\]
we see that \(ker (SL_2(\mathbb{Z}/8\mathbb{Z}) \to SL_2(\mathbb{Z}/4\mathbb{Z})) \subseteq G(8)\), and it follows that \([GL_2(\mathbb{Z}/8\mathbb{Z}) : G(8)] \leq 2\). Finally, if \(G(8) = GL_2(\mathbb{Z}/8\mathbb{Z})\), then (13) with \(\beta = 0\) implies that \(G = GL_2(\mathbb{Z}_2)\).

Next we will employ the following group theoretical lemma.

**Lemma 3.6.** Let \(G_1\) and \(G_2\) be finite groups and let \(\pi : G_1 \to G_2\) 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 \(N_1 \leq G_1\) and \(N_2 \leq G_2\) be normal subgroups satisfying \(\pi(N_1) = N_2\). Assume that
\[
gcd(\#N_1, \#ker \pi) = 1 \quad \text{and} \quad [N_1, ker \pi] = \{1\},
\] (20)
We then have
\[
N_1 \leq H_1 \iff N_2 \leq H_2.
\]

**Proof.** The implication \(\implies\) is immediate and does not require (20). For the converse, suppose that \(N_2 \leq H_2\) and let \(n_1 \in N_1\). Since \(N_2 \leq H_2\) and by our hypotheses, we may find \(k \in ker \pi\) so that \(n_1 k \in H_1\). Now by (20), we see that
\[
(n_1 k)^\# ker \pi = n_1^\# ker \pi \in H_1,
\]
which again by (20) implies that \(n_1 \in H_1\). Thus, \(N_1 \leq H_1\), proving the lemma.

Applying Lemma 3.6 in a special case, we obtain
Lemma 3.7. Let $G \subseteq \text{GL}_2(\mathbb{Z})$ be an open subgroup, let $m_G$ be as in Definition 1.1, and let $\text{rad}'(m_G)$ be defined by \footnote{2}{The (genus zero) modular curve associated with $G_2$ has been considered by N. Elkies \footnote{3}, who exhibited an explicit map from it to the $j$-line.}. For any prime $\ell$ and $d \in \mathbb{N}$, one has

$$\text{rad}'(m_G) \mid d \mid d\ell \mid m_G \implies \ell \text{ divides } \left[ \pi_{\ell d,\ell}(G(d)) : G(\ell d) \right].$$

Proof. We write $m := m_G$ and

$$d := \ell^{\delta} \cdot d(\ell), \quad m := \ell^{\beta} \cdot m(\ell)$$

(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 Definition 1.1 and Definition 3.2 we have

$$\ker(\pi_{\ell^{\delta},\ell^{\beta}}) \times \{1_{m(\ell)}\} \not\subseteq G(\ell^{\delta+1}m(\ell)).$$

We now apply Lemma 3.6 with

$$G_1 := \text{GL}_2(\mathbb{Z}/\ell^{\delta+1}m(\ell)\mathbb{Z}), \quad H_1 := G(\ell^{\delta+1}m(\ell)), \quad N_1 := \ker(\pi_{\ell^{\delta+1},\ell^{\beta'}}) \times \{1_{m(\ell)}\},$$

$$G_2 := \text{GL}_2(\mathbb{Z}/\ell^{\delta+1}d(\ell)\mathbb{Z}), \quad H_2 := G(\ell^{\delta+1}d(\ell)), \quad N_2 := \ker(\pi_{\ell^{\delta+1},\ell^{\beta'}}) \times \{1_{d(\ell)}\},$$

and $\pi : \text{GL}_2(\mathbb{Z}/\ell^{\delta+1}m(\ell)\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/\ell^{\delta+1}d(\ell)\mathbb{Z})$ the canonical projection map. The conclusion is that

$$\ker(\pi_{\ell^{\delta+1},\ell^{\beta'}}) \times \{1_{d(\ell)}\} \not\subseteq G(\ell^{\delta+1}d(\ell)).$$

Since $\ker(\pi_{\ell^{\delta+1},\ell^{\beta'}}) \times \{1_{d(\ell)}\} \simeq \ker(\pi_{\ell d,d})$ is an $\ell$-group, this proves the lemma.

Applying Lemma 3.7 prime by prime, for each prime $\ell$ dividing $m_G/\text{rad}'(m_G)$, we obtain

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

proving Proposition 1.4 by the case that (3) holds. In case (3) does not hold, we have $G(3) = \text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and, by Lemma 3.5, we must also have $\text{SL}_2(\mathbb{Z}/9\mathbb{Z}) \not\subseteq G(9)$. A computer search reveals that, up to conjugation in $\text{GL}_2(\mathbb{Z}/9\mathbb{Z})$, there are two subgroups $G_1, G_2 \subseteq \text{GL}_2(\mathbb{Z}/9\mathbb{Z})$ meeting these two criteria, and $G_1 \subseteq G_2$. Furthermore, $[\text{GL}_2(\mathbb{Z}/9\mathbb{Z}) : G_2] = 27$. From this it follows that $27$ divides $[\text{GL}_2(\mathbb{Z}/9\mathbb{Z}) : G(9)]$, and so

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

Now starting here and applying Lemma 3.7 prime by prime, we conclude the proof of Proposition 1.4 in the case that (3) holds.

4. Proof of Proposition 1.5

We now prove Proposition 1.5. The proof will rely, in part, on the following corollary to the Néron-Ogg-Shafarevich criterion (see for instance \footnote{13} or \footnote{17} Ch. 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 $\ell$ 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 $\ell$, the prime $\mathcal{L}$ is unramified in $K(E[m])$.

(c) The prime $\mathcal{L}$ is unramified in $K(E_{\text{tors}}(\ell))$.

We presently reduce the proof of Proposition 1.5 to the following four lemmas. The first lemma follows immediately from the classification subgroups of $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

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

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

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 $G := \rho_{E,K}(G_K) \subseteq \text{GL}_2(\widehat{\mathbb{Z}})$, and let $\ell$ be a prime number. For any positive integer $n$, we have

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

Consequently,

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

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 $G := \rho_{E,K}(G_K) \subseteq \text{GL}_2(\widehat{\mathbb{Z}})$, let $m_G$ be as in Definition 4.4 and let $\ell$ be an odd prime number dividing $m_G$. We then have

$$G_\ell = \text{GL}_2(\mathbb{Z}_\ell) \implies \ell \mid \Delta_K N_{K/Q}(\Delta_E).$$

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 $G := \rho_{E,K}(G_K) \subseteq \text{GL}_2(\widehat{\mathbb{Z}})$, let $m_G$ be as in Definition 4.4 and assume that 4 divides $m_G$. We then have

$$\text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \left\{1_{r'(2)}\right\} \subseteq G(r') \implies 4 \leq 2 \left[\pi^{-1} \left(\text{GL}_2(r'(2)) : G(r')\right)\right]$$

and

$$\text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \left\{1_{r'(2)}\right\} \subseteq G(r') \implies 2 \mid \Delta_K N_{K/Q}(\Delta_E).$$

Let us now deduce Proposition 4.2 from Lemmas 4.2 - 4.4, postponing the proofs of those lemmas until later. First, combining Lemma 4.2 with Lemmas 4.3 and 4.4 one concludes the following implications, for any prime $\ell \geq 5$ that divides $m_G$:

$$\text{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \not\subseteq G(\ell) \implies \ell \leq [\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : G(\ell)],$$

$$\text{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G(\ell) \implies \ell \mid \Delta_K N_{K/Q}(\Delta_E).$$

This implies that

$$r'_{(6)} \leq \prod_{\ell \geq 5, \ell \nmid r'} \frac{[\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : G(\ell)]}{\ell} \prod_{\ell \mid \Delta_K N_{K/Q}(\Delta_E)} \frac{1}{\text{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G(\ell)} \leq [\text{GL}_2(\mathbb{Z}/r'_{(6)}\mathbb{Z}) : G(r'_{(6)})] \text{rad} \left(\left|\Delta_K N_{K/Q}(\Delta_E)\right|\right)_{(6)}.$$  

If the prime $\ell = 3$ divides $m_G$ then either condition 3 holds or it does not hold. Let us first assume that 3 does not hold, i.e. we assume that it is not the case that 9 divides $m_G$, $G(3) = \text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and $\text{SL}_2(\mathbb{Z}_3) \not\subseteq G_3$. We then use Lemmas 4.2, 4.3 and 4.4 together with Lemma 3.5 to deduce the following implications:

$$\text{SL}_2(\mathbb{Z}/3\mathbb{Z}) \not\subseteq G(3) \implies 3 \leq [\text{GL}_2(\mathbb{Z}/3\mathbb{Z}) : G(3)],$$

$$\text{SL}_2(\mathbb{Z}/3\mathbb{Z}) \subseteq G(3) \neq \text{GL}_2(\mathbb{Z}/3\mathbb{Z}) \implies 3 \mid \Delta_K,$$

$$G(3) = \text{GL}_2(\mathbb{Z}/3\mathbb{Z}) \quad \text{and} \quad \text{SL}_2(\mathbb{Z}_3) \subseteq G_3 \neq \text{GL}_2(\mathbb{Z}_3) \implies 3 \mid \Delta_K,$$

$$G(3) = \text{GL}_2(\mathbb{Z}/3\mathbb{Z}) \quad \text{and} \quad G_3 = \text{GL}_2(\mathbb{Z}_3) \implies 3 \mid N_{K/Q}(\Delta_E).$$

Inserting this information into (21), we find that

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

On the other hand, in case 3 does hold, then we obviously have

$$\frac{r'_{(2)}}{3} = r'_{(6)} \leq [\text{GL}_2(\mathbb{Z}/r'_{(6)}\mathbb{Z}) : G(r'_{(6)})] \text{rad} \left(\left|\Delta_K N_{K/Q}(\Delta_E)\right|\right)_{(6)} 

\leq [\text{GL}_2(\mathbb{Z}/r'_{(2)}\mathbb{Z}) : G(r'_{(2)})] \text{rad} \left(\left|\Delta_K N_{K/Q}(\Delta_E)\right|\right)_{(2)}.$$
If $\ell = 2$ divides $m_G$, then either $4 \mid m_G$ or not. If $4 \mid m_G$, then multiplying both sides of (22) (resp. of (23)) by 2, we obtain the bound of Proposition 1.5. Now assume that $4 \mid m_G$. In this case, when (23) does not hold, we insert the result of Lemma 4.5 into (22), concluding that

$$r' = 4r_{(2)}' \leq 2[GL_2(\mathbb{Z}/r'\mathbb{Z}) : G(r')] \operatorname{rad} (|\Delta_K N_K/\mathbb{Q}(\Delta_E)|).$$

Likewise, in case condition (3) does hold, we insert these results into (23) and obtain

$$\frac{r'}{3} = \frac{4r_{(2)}'}{3} \leq 2[GL_2(\mathbb{Z}/r'\mathbb{Z}) : G(r')] \operatorname{rad} (|\Delta_K N_K/\mathbb{Q}(\Delta_E)|).$$

Thus we see that Lemmas 4.2, 4.5 indeed imply Proposition 1.5.

We now prove each of these lemmas. First we state an auxiliary lemma that is used throughout and may be found in [14, 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 $\operatorname{pr}_i : G_1 \times G_2 \rightarrow G_i$ the projection map onto the $i$-th factor. Let $G \subseteq G_1 \times G_2$ be a subgroup and assume that

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

Then there exists a group $\Gamma$ together with a pair of surjective homomorphisms

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

so that

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

4.1. **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 $\ell$ be any prime number.

(i) A subgroup $G(\ell) \subseteq GL_2(\mathbb{Z}/\ell\mathbb{Z})$ is called a **Borel subgroup** if it is conjugate in $GL_2(\mathbb{Z}/\ell\mathbb{Z})$ to the subgroup

$$B(\ell) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : b \in \mathbb{Z}/\ell\mathbb{Z}, a, d \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\}.$$  \hspace{1cm} (24)

(ii) A subgroup $G(\ell) \subseteq GL_2(\mathbb{Z}/\ell\mathbb{Z})$ is called a **normalizer of a split Cartan subgroup** if it is conjugate in $GL_2(\mathbb{Z}/\ell\mathbb{Z})$ to the subgroup

$$N_s(\ell) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, d \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\} \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} : b, c \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\}.$$  \hspace{1cm} (25)

If $\ell$ is odd, then $G(\ell)$ is called a **normalizer of a non-split Cartan subgroup** if it is conjugate in $GL_2(\mathbb{Z}/\ell\mathbb{Z})$ to the subgroup

$$N_{ns}(\ell) := \left\{ \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} : x, y \in \mathbb{Z}/\ell\mathbb{Z}, x^2 - \varepsilon y^2 \neq 0 \right\} \cup \left\{ \begin{pmatrix} x & -\varepsilon y \\ y & -x \end{pmatrix} : x, y \in \mathbb{Z}/\ell\mathbb{Z}, x^2 - \varepsilon y^2 \neq 0 \right\},$$  \hspace{1cm} (26)

where $\varepsilon$ is any fixed non-square in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. If $\ell = 2$, then $G(2)$ is called a normalizer of a non-split Cartan subgroup if $G(2) = GL_2(\mathbb{Z}/2\mathbb{Z})$.

(iii) A subgroup $G(\ell) \subseteq GL_2(\mathbb{Z}/\ell\mathbb{Z})$ is called an **exceptional group** if its image in $\operatorname{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ 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 [13].

**Lemma 4.8.** Let $G(\ell) \subseteq GL_2(\mathbb{Z}/\ell\mathbb{Z})$ 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 non-split Cartan subgroup.
4. $G(\ell)$ is an exceptional group.

10
Thus, by (28) we have

\[ \mathcal{E}_{A_1}(t) := \{ g \in \text{GL}_2(\mathbb{Z}/t\mathbb{Z}) : \varpi(g) \in A_1 \}, \]

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

| \( G(t) \) | \( B(t) \) | \( \mathcal{N}_S(t) \) | \( \mathcal{N}_{ns}(t) \) | \( \mathcal{E}_{A_1}(t) \) | \( \mathcal{E}_{S_4}(t) \) | \( \mathcal{E}_{A_5}(t) \) |
|----------------|-------------|----------------|----------------|----------------|----------------|----------------|
| \( \text{GL}_2(\mathbb{Z}/t\mathbb{Z}) : G(t) \) | \( t + 1 \) | \( \ell(t + 1)/2 \) | \( \ell(t - 1)/2 \) | \( \ell(\ell^2 - 1)/12 \) | \( \ell(\ell^2 - 1)/24 \) | \( \ell(\ell^2 - 1)/60 \) |

We note that \( \mathcal{N}_{ns}(2) = \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \), and also that each exceptional group only occurs for certain primes. 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 \( \text{GL}_2(\mathbb{Z}/t\mathbb{Z}) \) for that prime \( t \). The conclusion of Lemma 4.2 follows immediately from this table.

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

\[
\begin{array}{ccc}
\text{Gal}(K(E_{\text{tors}})/K) & \rightarrow & \text{Gal}(K(\mu_{\infty})/K), \\
\text{res} & \downarrow & \text{det}
\end{array}
\]

\[
\text{cyc} : \text{Gal}(K(\mu_{\infty})/K) \rightarrow \mathbb{Z}^\times
\]

denote respectively the restriction map and the cyclotomic character (the containment \( K(\mu_{\infty}) \subseteq K(E_{\text{tors}}) \) follows from the Weil Pairing [19], see also [17] Ch. III, [8]).

\[
\text{Gal}(K(E^{(q)})/K) \xrightarrow{\text{PE}_K} \text{GL}_2(\mathbb{Z}/t^n\mathbb{Z})
\]

By considering the commutative diagram (27) and Galois theory, we see that

\[
\text{SL}_2(\mathbb{Z}/t^n\mathbb{Z}) \subseteq G(t^n) \neq \text{GL}_2(\mathbb{Z}/t^n\mathbb{Z}) \Rightarrow \text{det}(G(t^n)) \neq (\mathbb{Z}/t^n\mathbb{Z})^\times \Rightarrow \mathbb{Q} \neq \mathbb{Q}(\mu_{t^n}) \cap K.
\]

Since \( \mathbb{Q}(\mu_{t^n}) \) is totally ramified at \( t \), it follows that \( t \) is then ramified in \( \mathbb{Q}(\mu_{t^n}) \cap K \), so \( t \) is ramified in \( K \), and thus \( t \) divides \( \Delta_K \).

4.3. **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 \( \Sigma \) a finite simple group. We say that \( \Sigma \) 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 \( G_1/N_1 \cong \Sigma \).

We further define

\[
\text{Occ}(G) := \{ \text{finite simple non-abelian groups } \Sigma : \Sigma \text{ occurs in } G \}.
\]

Note that any Jordan-Hölder factor of \( G \) occurs in \( G \) (but generally not vice versa). Also note that, if

\[
1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1
\]

is an exact sequence of profinite groups, then

\[
\text{Occ}(G) = \text{Occ}(G') \cup \text{Occ}(G'').
\]

Finally, as observed in [16] IV-25, one has that

\[
\text{Occ}(\text{GL}_2(\mathbb{Z}/t\mathbb{Z})) = \begin{cases} \\
\emptyset & \text{if } t \in \{2, 3\} \\
\{\text{PSL}_2(\mathbb{Z}/5\mathbb{Z})\} = \{A_5\} & \text{if } t = 5 \\
\{\text{PSL}_2(\mathbb{Z}/7\mathbb{Z})\} & \text{if } t > 5, t \equiv \pm 2 \pmod 5 \\
\{\text{PSL}_2(\mathbb{Z}/13\mathbb{Z}), A_5\} & \text{if } t > 5, t \equiv \pm 1 \pmod 5.
\end{cases}
\]

Thus, by (28) we have

\[
\text{Occ}(\text{GL}_2(\mathbb{Z}/t\mathbb{Z})) = \{A_5\} \cup \{\text{PSL}_2(\mathbb{Z}/p\mathbb{Z})\}_{p \neq t}.
\]
Lemma 4.10. Let \( \ell \geq 5 \) be a prime and let \( G \subseteq \text{GL}_2(\mathbb{Z}_\ell) \) be a closed subgroup satisfying \( \text{SL}_2(\mathbb{Z}/\ell \mathbb{Z}) \subseteq G(\ell) \). Suppose further that \( \psi : G \rightarrow H \) is a surjective group homomorphism onto a finite group \( H \). Then either

1. \( \text{PSL}_2(\mathbb{Z}/\ell \mathbb{Z}) \) occurs in \( H \), or
2. \( H \) is abelian and \( \text{SL}_2(\mathbb{Z}_\ell) \subseteq \ker \psi \).

Proof. As observed earlier, since \( \ell \geq 5 \), the group \( \text{PSL}_2(\mathbb{Z}/\ell \mathbb{Z}) \) is a simple non-abelian group, and we obviously have \( \{ \text{PSL}_2(\mathbb{Z}/\ell \mathbb{Z}) \} \subseteq \text{Occ}(\text{SL}_2(\mathbb{Z}/\ell \mathbb{Z})) \). Furthermore, by the hypothesis \( \text{SL}(\mathbb{Z}/\ell \mathbb{Z}) \subseteq G(\ell) \) together with (28), we see that \( \{ \text{PSL}_2(\mathbb{Z}/\ell \mathbb{Z}) \} \subseteq \text{Occ}(G(\ell)) \). Thus, again by (28), we have

\[
\{ \text{PSL}_2(\mathbb{Z}/\ell \mathbb{Z}) \} \subseteq \text{Occ}(G). \tag{30}
\]

Furthermore, we have that

\[
\pm(\ker \psi)(\ell) \cap \text{SL}_2(\mathbb{Z}/\ell \mathbb{Z}) = \begin{cases} \{ 1 \} & \text{or} \\ \text{PSL}_2(\mathbb{Z}/\ell \mathbb{Z}) & \end{cases} \tag{31}
\]

If the left-hand side of (31) is trivial, then \( \ker \psi \) is prosolvable (so that \( \text{Occ}(\ker \psi) = \emptyset \)), and considering the exact sequence

\[ 1 \rightarrow \ker \psi \rightarrow G \rightarrow H \rightarrow 1, \]

we see by (28) and (30) that \( \text{PSL}_2(\mathbb{Z}/\ell \mathbb{Z}) \) must occur in \( H \). If, on the other hand, we have \( \text{PSL}_2(\mathbb{Z}/\ell \mathbb{Z}) \) in (31), then \( \text{SL}_2(\mathbb{Z}/\ell \mathbb{Z}) \subseteq (\ker \psi)(\ell) \), which by Lemma 3.5 applied to \( G = \ker \psi \) implies that \( \text{SL}_2(\mathbb{Z}_\ell) \subseteq \ker \psi \). Thus \( H \) is abelian and \( \psi \) factors through the determinant map, as asserted. \( \Box \)

We now proceed with the proof of Lemma 4.4. By Lemma 4.6 the hypothesis that \( G_\ell = \text{GL}_2(\mathbb{Z}_\ell) \) and that \( \ell \) divides \( m_G \) imply that

\[ G = \text{GL}_2(\mathbb{Z}_\ell) \times_\psi G(\ell), \tag{32} \]

where \( \psi : \text{GL}_2(\mathbb{Z}_\ell) \rightarrow H \) and \( \psi : G(\ell) \rightarrow H \) are surjective homomorphisms onto a common non-trivial group \( H \). Under the Galois correspondence, we have \( \text{GL}_2(\mathbb{Z}_\ell) = \text{Gal}(K(E[\ell]) \mid K), G(\ell) = \text{Gal}(K(E_{\text{tors},(\ell)}) \mid K) \) and \( H = \text{Gal}(F \mid K) \), where \( F = K(E[\ell^\infty]) \cap K(E_{\text{tors},(\ell)}) \neq K \). Thus, the corresponding field diagram is as follows.

\[
\begin{array}{ccc}
K(E[\ell^\infty]) & \rightarrow & K(E_{\text{tors},(\ell)}) \\
\downarrow & & \downarrow \\
F & \rightarrow & K \\
\end{array}
\]

We first claim that

\[ F \cap K(\mu_{\ell^\infty}) \neq K. \tag{34} \]

We separate the verification of (34) 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 (29) we see that \( H \) must be abelian and \( F \subseteq K(\mu_{\ell^\infty}) \), verifying (34). If \( \ell = 5 \), we consider the further quotient induced by reduction modulo 5:

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

Since the kernel of this quotient is pro-solvable, we see that if \( \text{PSL}_2(\mathbb{Z}/5\mathbb{Z}) \cong A_5 \) 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

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

By the Galois correspondence, we then have

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

and thus

\[ F \cap K(\mu_{5^\infty}) \neq K. \]
Lemma 4.11. Let \( \psi : \ker \psi \subseteq \mathbb{Z}/(3^\infty) \) and so in particular \( 2 \leq \ker \psi \). As in the previous case, since \( \ker \psi \neq \mathbb{GL}_2(\mathbb{Z}/3) \), we have \( F \neq K \). The following lemma will then imply that \( K(\mu_{3^\infty}) \cap F \neq K \).

Lemma 4.12. Let \( N \subseteq \mathbb{GL}_2(\mathbb{Z}/3) \) be a closed normal subgroup satisfying \( \langle \mathbb{SL}_2(\mathbb{Z}/3), N \rangle = \mathbb{GL}_2(\mathbb{Z}/3) \). Then \( N = \mathbb{GL}_2(\mathbb{Z}/3) \).

Proof. A computer calculation shows that, if \( H \subseteq \mathbb{GL}_2(\mathbb{Z}/9) \) is a normal subgroup satisfying \( \langle \mathbb{SL}_2(\mathbb{Z}/9), H \rangle = \mathbb{GL}_2(\mathbb{Z}/9) \), then \( H = \mathbb{GL}_2(\mathbb{Z}/9) \). Taking \( N \) as in the statement of the lemma and setting \( H := N(9) \), we see that \( N(9) = \mathbb{GL}_2(\mathbb{Z}/9) \), and applying (13) with \( \beta = 1 \), we conclude that \( N = \mathbb{GL}_2(\mathbb{Z}/3) \).

Applying Lemma 4.11 with \( N = \ker \psi \), we find that \( K(\mu_{3^\infty}) \cap F \neq K \), since \( F \neq K \), verifying (34) in the \( \ell = 3 \) case as well.

Finally, we observe that (34) implies the conclusion of Lemma 4.3. Indeed, let \( \ell \) be any odd prime with \( \ell \nmid \Delta_K \). Since \( G_\ell = \mathbb{GL}_2(\mathbb{Z}/\ell) \), we have \( K \cap \mathbb{Q}(\mu_{\ell^\infty}) = \mathbb{Q} \), and so any prime \( \ell \subseteq \mathbb{O}_K \) over \( \ell \) is totally ramified in \( K(\mu_{\ell^\infty}) \), hence ramified in \( F \cap K(\mu_{\ell^\infty}) \). Thus, by (33), \( \ell \) is ramified in \( K(\mathbb{E}_{\text{tor},(\ell)}) \). By Theorem 4.1, we find that \( \ell \mid N_{K/\mathbb{Q}}(\Delta_K) \), finishing the proof.

4.4. Proof of Lemma 4.5. The proof of Lemma 4.3 will make use of the following sub-lemma.

Lemma 4.13. Let \( K \) be a number field for which \( 2 \nmid \Delta_K \) and let \( \mathfrak{p} \subseteq \mathbb{O}_K \) be a prime ideal lying over \( 2 \). Let \( \alpha \in \mathbb{O}_K - \{0\} \) be any element for which \( \mathfrak{p} \mid \alpha \mathbb{O}_K \). Then \( 2\alpha \) 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
\[
v_\mathfrak{p}(2\alpha) = v_\mathfrak{p}(2) + v_\mathfrak{p}(\alpha) = 1,
\]
and so in particular \( 2\alpha \) cannot be a square in \( K^\times \), as asserted. Next, let \( L := K(\sqrt{2\alpha}) \), fix any prime \( \mathfrak{P} \subseteq \mathbb{O}_L \) 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 (35), we then have
\[
v_\mathfrak{P} \left( (2\alpha)^{1/2} \right) = \frac{1}{2} v_\mathfrak{P}(2\alpha) = \frac{1}{2}.
\]
It follows that \( L \) is ramified over \( K \) at \( \mathfrak{p} \), as asserted.

We now proceed with the proof of Lemma 4.3. Since we are assuming that \( 4 \) divides \( r' \), by Lemma 4.6 we may write \( G(r') \) as a fibered product:
\[
G(r') = G(4) \times_\psi G(r'_2).
\]
Case: \( \mathbb{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \{1, r'_2(2)\} \subseteq G(r') \). In this case, either \( G(4) \neq \mathbb{GL}_2(\mathbb{Z}/4\mathbb{Z}) \) or \( G(4) = \mathbb{GL}_2(\mathbb{Z}/4\mathbb{Z}) \)
and the common quotient \( \psi_2(G(4)) = \psi_{(2)}(G(r'_2)) \) in (36) is nontrivial. If \( G(4) \neq \mathbb{GL}_2(\mathbb{Z}/4\mathbb{Z}) \), we find that \( 2 \leq \mathbb{GL}_2(\mathbb{Z}/4\mathbb{Z}) : G(4) \leq \lfloor \pi^{-1}(G(r'_2)) : G(r') \rfloor \), and so the result of the lemma follows. If on the other hand \( G(4) = \mathbb{GL}_2(\mathbb{Z}/4\mathbb{Z}) \), then the common quotient in (36) is nontrivial, and since
\[
\pi^{-1}(G(r'_2)) = \mathbb{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times G(r'_2),
\]
we thus have \( 2 \leq \lfloor \pi^{-1}(G(r'_2)) : G(r') \rfloor \), proving the lemma in this sub-case as well.
Case: \( \mathbb{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \{1, r'_2(2)\} \subseteq G(r') \). In this case, (30) is a full product:
\[
G(r') = \mathbb{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times G(r'_2).
\]
By Lemma 3.5, either \( G(8) \) is an index 2 subgroup of \( \text{GL}_2(\mathbb{Z}/8\mathbb{Z}) \) that surjects onto \( \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \), or \( G_2 = \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \). Let us treat the former subcase first. A computer search reveals that there are exactly 4 index 2 subgroups of \( \text{GL}_2(\mathbb{Z}/8\mathbb{Z}) \) that map surjectively onto \( \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \), namely

\[
\ker(\chi_8), \ker(\chi_8\chi_4), \ker(\chi_8\varepsilon), \ker(\chi_8\chi_4\varepsilon),
\]

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

\[
K(\mathbb{E}[8])^{\ker(\chi_8)} = K(\sqrt{2}), \quad K(\mathbb{E}[8])^{\ker(\chi_8\varepsilon)} = K(\sqrt{2\Delta_E}), \\
K(\mathbb{E}[8])^{\ker(\chi_8\chi_4)} = K(\sqrt{-2}), \quad K(\mathbb{E}[8])^{\ker(\chi_8\chi_4\varepsilon)} = K(\sqrt{-2\Delta_E}).
\tag{38}
\]

Here, by \( K(\sqrt{\pm 2\Delta}) \) we mean the quadratic field \( K(\sqrt{\pm 2\Delta(E_{\text{Weier}})}) \), where \( E_{\text{Weier}} \) is any fixed Weierstrass model of \( E \) and \( \Delta(E_{\text{Weier}}) \in \mathbb{K}^\times \) denotes its discriminant (note that although \( \Delta(E_{\text{Weier}}) \) depends on the choice of \( E_{\text{Weier}} \), the quadratic field \( K(\sqrt{\pm 2\Delta(E_{\text{Weier}})}) \) depends only on \( E \)). By \( \langle 39 \rangle \), we thus have

\[
G(8) = \ker(\chi_8) \implies \sqrt{2} \in K \quad \text{and} \quad G(8) = \ker(\chi_8\chi_4) \implies \sqrt{-2} \in K,
\]
either of which imply that \( 2 \mid \Delta_K \). On the other hand, for any Weierstrass model \( E_{\text{Weier}} \) of \( E \), we have

\[
G(8) = \ker(\chi_8\varepsilon) \implies \sqrt{2\Delta(E_{\text{Weier}})} \in K, \\
G(8) = \ker(\chi_8\chi_4\varepsilon) \implies \sqrt{-2\Delta(E_{\text{Weier}})} \in K.
\tag{39}
\]

Let us suppose for the sake of contradiction that

\[
2 \nmid \Delta_K N_{K/Q}(\Delta_E). \tag{40}
\]

Fix a prime ideal \( p \subseteq O_K \) lying over 2. By \( \langle 10 \rangle \), we must have \( p \nmid \Delta_E \), and we may thus find a Weierstrass model \( E_{\text{Weier}} \) of \( E \) satisfying \( p \nmid \Delta(E_{\text{Weier}}) \). Applying Lemma 4.12 with \( \alpha = \pm \Delta(E_{\text{Weier}}) \), we see that \( \sqrt{\pm 2\Delta(E_{\text{Weier}})} \notin K \), contradicting \( \langle 39 \rangle \). Thus, we must have \( 2 \nmid \Delta_K N_{K/Q}(\Delta_E) \) whenever \( G(8) \) has index 2 in \( \text{GL}_2(\mathbb{Z}/8\mathbb{Z}) \).

We now treat the second subcase, in which \( G_2 = \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \). We evidently must have a non-trivial common quotient in

\[
G_{r'} \simeq \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \psi G_{r'(2)}.
\]

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

\[
\text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \psi G(r'(2)), \tag{41}
\]

a fibered product with a common quotient of order divisible by 2 (and hence non-trivial). Consider the subgroup \( N := \ker(\psi_2) \subseteq \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \) where \( \psi = (\psi_2, \psi_2) \) in \( \langle 11 \rangle \). The assumption \( \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \{1, r'(2)\} \subseteq G(r') \) then implies that \( N(4) = \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \) (otherwise the mod \( r' \) image of \( \langle 11 \rangle \) would have a non-trivial fibered between \( G(4) \) and \( G(r'(2)) \), contradicting \( \langle 37 \rangle \)). By Lemma 3.3, we find that \( [\text{GL}_2(\mathbb{Z}/8\mathbb{Z}) : N(8)] = 2 \).

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 \( \langle 38 \rangle \) 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 \( K(E_{\text{tor},(2)}) \). By Lemma 4.12 and Theorem 4.1, it follows that, if \( 2 \nmid \Delta_K \) then 2 divides \( N_{K/Q}(\Delta_E) \). This finishes the proof of Lemma 4.15.
REFERENCES

[1] Y. Bilu and P. Parent, *Serre’s uniformity problem in the split Cartan case*, Annals of Mathematics, **173**, no. 1 (2011), 569–584.

[2] Y. Bilu, P. Parent and M. Rebolledo, *Rational points on $X_0^+(p^n)$*, Annales de l’Institut Fourier, **63**, no. 3 (2013), 957–984.

[3] 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*, preprint. Available at https://arxiv.org/abs/1706.03422

[4] H. Daniels, *An infinite family of Serre curves*, J. Number Theory **155** (2015), 226–247.

[5] T. Dokchitser and V. Dokchitser, *Surjectivity of mod $2^n$ representations of elliptic curves*, Math. Z. **272** (2012), 961–964.

[6] N. Elkies, *Elliptic curves with $3$-adic Galois representation surjective mod $3$ but not mod $9$*, preprint (2006).

[7] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der mathematischen Wissenschaften, **134**, Springer-Verlag, Berlin Heidelberg (1967).

[8] N. Jones, *A bound for the torsion conductor of an elliptic curve*, Proc. Amer. Math. Soc. **137** (2009), 37–43.

[9] A. Lozano-Robledo, *On the field of definition of $p$-torsion points on elliptic curves over the rationals*, Math. Annalen **357**, no. 1 (2013), 279–305.

[10] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44**, no. 2 (1978), 129–162.

[11] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **24**, no. 1 (1996), 437–449.

[12] J. Morrow, *Composite images of Galois for elliptic curves over $\mathbb{Q}$ and Entanglement fields*, preprint. Available at https://arxiv.org/abs/1707.04646

[13] A.P. Ogg, *Elliptic curves and wild ramification*, Amer. J. Math. **89**, no. 1 (1967), 1–21.

[14] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98**, no. 3 (1976), 751–804.

[15] J-P. Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[16] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Benjamin, New York-Amsterdam, 1968.

[17] J. Silverman, *The arithmetic of elliptic curves*, Springer, New York, 1986.

[18] A. Sutherland and D. Zywina, *Modular curves of prime-power level with infinitely many rational points*, Algebra & Number Theory **11**, no. 5 (2017), 1199–1229.

[19] A. Weil, *Sur les fonctions algébriques à corps de constantes finis*, C. R. Acad. Sci. Paris **210** (1940) 592–594.

[20] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), 811–826.

[21] D. Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, preprint. Available at https://arxiv.org/abs/1508.07660