GL_2-REPRESENTATIONS WITH MAXIMAL IMAGE

NATHAN JONES

ABSTRACT. We give a necessary and sufficient condition for the Galois representation on the torsion of a non-CM elliptic curve defined over $\mathbb{Q}$ to have image which is "as large as possible," given that it lies inside a fixed open subgroup $G \subseteq GL_2(\hat{\mathbb{Z}})$. Our results are applicable to a wider class of Galois representations.

1. INTRODUCTION

Let K be a number field and let E be an elliptic curve defined over K. Consider the action of $G_K := \mathrm{Gal}\,(\overline{K}/K)$ on the n-torsion $E[n]$ of E, which gives rise to a continuous group homomorphism (regarding $GL_2(\mathbb{Z}/n\mathbb{Z})$ with the discrete topology)

$$\varphi_{E,K,n} : G_K \longrightarrow \mathrm{Aut}(E[n]) \simeq GL_2(\mathbb{Z}/n\mathbb{Z}).$$

Taking the inverse limit over all $n \geq 1$ (ordered by divisibility), one may consider the action of G_K on

$$E_{\mathrm{tors}} := \bigcup_{n=1}^{\infty} E[n],$$

obtaining a continuous homomorphism

$$\varphi_{E,K} : G_K \longrightarrow \mathrm{Aut}(E_{\mathrm{tors}}) \simeq GL_2(\hat{\mathbb{Z}}),$$

where $GL_2(\hat{\mathbb{Z}}) = \varprojlim GL_2(\mathbb{Z}/n\mathbb{Z})$. As discussed in [10], it is of great interest to understand the image of $\varphi_{E,K}$. For example, if E is a fixed elliptic curve over $\mathbb{Q}$, the image $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}})$ plays a crucial role in a conjecture of Lang and Trotter which counts primes with fixed Frobenius trace. (This conjecture is still open, although an average version [4] has been obtained.)

Serre [14] proved that, when E has no complex multiplication, the image of $\varphi_{E,K}$ is open in $GL_2(\hat{\mathbb{Z}})$ (i.e. has finite index in $GL_2(\hat{\mathbb{Z}})$). He also noted that $\varphi_{E,K}$ can never be surjective when $K = \mathbb{Q}$, because of the following "cyclotomic obstruction." Let us introduce the notation

$$K(E[n]) := \overline{K}^{\ker \varphi_{E,K,n}} = K(\text{the } x \text{ and } y\text{-coordinates of all } P \in E[n]),$$
$$K(E_{\mathrm{tors}}) := \overline{K}^{\ker \varphi_{E,K}} = K(\text{the } x \text{ and } y\text{-coordinates of all } P \in E_{\mathrm{tors}}).$$

He noticed that if $K = \mathbb{Q}$, then for some positive integer $d = d_E \geq 1$ we have

$$\begin{aligned}\mathbb{Q}(\sqrt{\Delta_E}) &\subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(\mu_d) \\ &\subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[d]),\end{aligned}$$

which (by Galois theory) forces $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}}) \subsetneq GL_2(\hat{\mathbb{Z}})$. More precisely, we have that

$$\begin{aligned}\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}}) &\subseteq \left\{ g \in GL_2(\hat{\mathbb{Z}}) : \chi(g) = \varepsilon(g) \right\} \\ &=: GL_2(\hat{\mathbb{Z}})_{\chi=\varepsilon},\end{aligned} \tag{1}$$

where the "signature"

$$\varepsilon : GL_2(\hat{\mathbb{Z}}) \longrightarrow GL_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow GL_2(\mathbb{Z}/2\mathbb{Z})/[GL_2(\mathbb{Z}/2\mathbb{Z}), GL_2(\mathbb{Z}/2\mathbb{Z})] \simeq \{\pm 1\} \tag{2}$$

is the unique non-trivial character of $GL_2(\mathbb{Z}/2\mathbb{Z})$ pre-composed with reduction modulo 2 and

$$\chi : GL_2(\hat{\mathbb{Z}}) \longrightarrow \hat{\mathbb{Z}}^{\times} \longrightarrow \{\pm 1\}$$

is defined by $\chi(g) = \left(\frac{\Delta_E}{\det g}\right)$, where $\left(\frac{\Delta_E}{\cdot}\right)$ is the Kronecker symbol, i.e. the unique character which satisfies $\mathrm{Frob}_p(\sqrt{\Delta_E}) = \left(\frac{\Delta_E}{\mathrm{Frob}_p}\right)\sqrt{\Delta_E}$ for each p not dividing d. Serre also gave examples of elliptic curves E over $\mathbb{Q}$ for which $\varphi_{E,\mathbb{Q}}$ is "as surjective as possible modulo this obstruction," i.e. for which

$$\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}}) = GL_2(\hat{\mathbb{Z}})_{\chi=\varepsilon}. \tag{3}$$

Following Lang and Trotter, we call an elliptic curve E over $\mathbb{Q}$ a **Serre curve** if (3) holds. It has been shown (see [8]) that "almost all" elliptic curves E over $\mathbb{Q}$ are Serre curves (see also [11], which, building on [5], gives an asymptotic formula for the number of Serre curves of bounded height).

In the present paper, we consider the following generalization of this phenomenon. Fix once and for all a level $m \geq 1$ and a subgroup $G(m) \subseteq GL_2(\mathbb{Z}/m\mathbb{Z})$, and let $G := \pi^{-1}(G(m)) \subseteq GL_2(\hat{\mathbb{Z}})$ be the entire pre-image of $G(m)$ under the canonical projection. Suppose that we have found an elliptic curve E over $\mathbb{Q}$ for which the associated Galois representation maps into G:

$$\varphi_{E,\mathbb{Q}} : G_{\mathbb{Q}} \longrightarrow G. \tag{4}$$

Our goal is to describe the analogue of (1) in this context, thus making precise the notion that $\varphi_{E,\mathbb{Q}}$ is "as surjective onto G as possible" and allowing us to define the relative concept of a *G-Serre curve*. We will then prove a theorem which characterizes G-Serre curves in terms of checkable criteria at finite level.

There is a modular curve $X_{G(m)}$ whose $\mathbb{Q}$-rational points correspond to elliptic curves E over $\mathbb{Q}$ for which (4) holds (up to $GL_2(\hat{\mathbb{Z}})$-conjugation). When the genus of $X_{G(m)}$ is zero and $X_{G(m)}(\mathbb{Q}) \neq \emptyset$, one may fix a morphism

$$f : \mathbb{A}^1 \longrightarrow X_{G(m)},$$

and count the rational points $t_0 \in \mathbb{Q}$ for which $f(t_0)$ corresponds to a G-Serre curve (see Definition 2.7 in Section 2 below). One may use the same techniques as in [3] to prove that "almost all elliptic curves in a one-parameter family on $X_{G(m)}$ are G-Serre curves."

Finally, we remark that the techniques used in the current paper are exclusively group-theoretical. Consequently, our results are applicable in a wider context than we have stated here (see Theorem 2.11 in Section 2.1 below).

2. Statement of results

To motivate our definitions, we begin by re-examining (1) in more detail. Recall that, thanks to the Weil pairing (see [15]), the d-th cyclotomic field $\mathbb{Q}(\mu_d)$ is contained in $\mathbb{Q}(E[d])$. Furthermore, choosing a $\mathbb{Z}/d\mathbb{Z}$-basis of $E[d]$ (and thus an imbedding $\iota : \mathrm{Gal}\left(\mathbb{Q}(E[d])/\mathbb{Q}\right) \to GL_2(\mathbb{Z}/d\mathbb{Z})$), the following diagram is commutative:

$$\begin{array}{ccc} \mathrm{Gal}\left(\mathbb{Q}(E[d])/\mathbb{Q}\right) & \xrightarrow{\text{res}} & \mathrm{Gal}\left(\mathbb{Q}(\mu_d)/\mathbb{Q}\right) \\ \downarrow{\scriptstyle \iota} & & \downarrow \\ GL_2(\mathbb{Z}/d\mathbb{Z}) & \xrightarrow{\det} & (\mathbb{Z}/d\mathbb{Z})^*, \end{array} \tag{5}$$

where the unlabeled vertical arrow is the usual (canonical) isomorphism. Since

$$[GL_2(\mathbb{Z}/2\mathbb{Z}), GL_2(\mathbb{Z}/2\mathbb{Z})] = (\ker \varepsilon \mod 2) \subsetneq SL_2(\mathbb{Z}/2\mathbb{Z}),$$

we see (assuming $\varphi_{E,\mathbb{Q},2}(G_{\mathbb{Q}}) = GL_2(\mathbb{Z}/2\mathbb{Z})$) that

$$\mathbb{Q} = \mathbb{Q}(\mu_2) = \mathbb{Q}(E[2])^{SL_2(\mathbb{Z}/n\mathbb{Z})} \subsetneq \mathbb{Q}(E[2])^{[GL_2(\mathbb{Z}/2\mathbb{Z}), GL_2(\mathbb{Z}/2\mathbb{Z})]} = \mathbb{Q}(\sqrt{\Delta_E})$$

(here Δ_E denotes the minimal discriminant of E). Since $\mathbb{Q}(\sqrt{\Delta_E})$ is an abelian extension of $\mathbb{Q}$, it is contained in some $\mathbb{Q}(\mu_d)$, by the Kronecker-Weber Theorem. This containment, together with (5), implies (1).

This may be re-cast as follows. Let us denote the Galois representation $\varphi_{E,\mathbb{Q}}$ simply by φ. The commutator subgroup[1] $[\varphi(G_{\mathbb{Q}}), \varphi(G_{\mathbb{Q}})]$ satisfies

$$[\varphi(G_{\mathbb{Q}}), \varphi(G_{\mathbb{Q}})] \subseteq \varphi(G_{\mathbb{Q}}) \cap SL_2(\hat{\mathbb{Z}}). \tag{6}$$

[1]For a profinite group H, we are defining the commutator subgroup $[H, H]$ to be the *closure* of the subgroup generated by its set of commutators $\{xyx^{-1}y^{-1} : x, y \in H\}$.

Furthermore, one can show (see Corollary 5.12 with $G = \varphi(G_{\mathbb{Q}})$) that the index $\left[\varphi(G_{\mathbb{Q}}) \cap SL_2(\hat{\mathbb{Z}}) : [\varphi(G_{\mathbb{Q}}), \varphi(G_{\mathbb{Q}})]\right]$ is finite, which implies that there is a finite index subgroup $H_\varphi \subseteq \varphi(G_{\mathbb{Q}})$ so that

$$[\varphi(G_{\mathbb{Q}}), \varphi(G_{\mathbb{Q}})] = H_\varphi \cap \left(\varphi(G_{\mathbb{Q}}) \cap SL_2(\hat{\mathbb{Z}})\right).$$

By Galois theory, we have

$$\mathbb{Q}(E_{\text{tors}})^{H_\varphi} \cdot \mathbb{Q}^{\text{cyc}} = \mathbb{Q}(E_{\text{tors}})^{[\varphi(G_{\mathbb{Q}}), \varphi(G_{\mathbb{Q}})]} \supseteq \mathbb{Q}(E_{\text{tors}})^{\varphi(G_{\mathbb{Q}}) \cap SL_2(\hat{\mathbb{Z}})} = \mathbb{Q}^{\text{cyc}}.$$

Since $\mathbb{Q}(E_{\text{tors}})^{H_\varphi}$ is an abelian extension of $\mathbb{Q}$ and since $\mathbb{Q}^{\text{ab}} = \mathbb{Q}^{\text{cyc}}$, this implies that we must have equality in (6):

$$[\varphi(G_{\mathbb{Q}}), \varphi(G_{\mathbb{Q}})] = \varphi(G_{\mathbb{Q}}) \cap SL_2(\hat{\mathbb{Z}}).$$

This motivates the following definitions.

Definition 2.1. *A subgroup $H \subseteq GL_2(\hat{\mathbb{Z}})$ is called* ***commutator-thick*** *if*

$$[H, H] = H \cap SL_2(\hat{\mathbb{Z}}).$$

Definition 2.2. *A subgroup $H \subseteq GL_2(\hat{\mathbb{Z}})$ is called* ***determinant-surjective*** *if* $\det(H) = \hat{\mathbb{Z}}^\times$.

Remark 2.3. *The above discussion shows that $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}}) \subseteq GL_2(\hat{\mathbb{Z}})$ is always a commutator-thick, determinant-surjective subgroup.*

Recall that $G \subseteq GL_2(\hat{\mathbb{Z}})$ is a fixed subgroup of finite index, and imagine now that $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}}) \subseteq G$. The following definition captures the notion of $\varphi_{E,\mathbb{Q}}$ being "as surjective as possible onto G."

Definition 2.4. *We call a commutator-thick subgroup $H \subseteq G$ a* ***G-maximal commutator-thick subgroup of G*** *if $H \cap SL_2(\hat{\mathbb{Z}}) = [G, G]$.*

Our main result is the following theorem, which characterizes G-maximal commutator-thick subgroups of G in terms of criteria which are in practice checkable. Recall the set-up: $m \geq 1$ is any positive integer, $G(m) \subseteq GL_2(\mathbb{Z}/m\mathbb{Z})$ is an arbitrary subgroup, and $G := \pi^{-1}(G(m)) \subseteq GL_2(\hat{\mathbb{Z}})$ is the full pre-image of $G(m)$ under the natural projection. Define the positive integer m_0 by

$$m_0 := \text{lcm}\left(36, \left(\prod_{\substack{\ell \mid m \\ G(\ell) \text{ abelian}}} \ell^{2\text{ord}_\ell(m)+1}\right) \cdot \left(\prod_{\substack{\ell \mid m \\ G(\ell) \text{ non-abelian}}} \ell^{\text{ord}_\ell(m)+1}\right)\right) \tag{7}$$

Theorem 2.5. *Let $H \subseteq G$ be a determinant-surjective, commutator-thick subgroup of G. Then H is a G-maximal commutator-thick subgroup of G if and only if, for each $n \in \{m_0\} \cup \{\ell \text{ prime} : \ell \nmid m_0\}$, one has*

$$[H(n), H(n)] = [G(n), G(n)].$$

We remark that, since for all odd ℓ, $[GL_2(\mathbb{Z}/\ell\mathbb{Z}), GL_2(\mathbb{Z}/\ell\mathbb{Z})] = SL_2(\mathbb{Z}/\ell\mathbb{Z})$ (this follows from (10) below), Theorem 2.5 is equivalent to the following theorem.

Theorem 2.6. *Let $H \subseteq G$ be a determinant-surjective, commutator-thick subgroup of G. Then H is a G-maximal commutator-thick subgroup of G if and only if the following two conditions hold.*

1. *For each prime ℓ not dividing m_0, one has $SL_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq H(\ell)$.*
2. *One has $[H(m_0), H(m_0)] = [G(m_0), G(m_0)]$.*

Returning to our original example of an elliptic curve, we make the following definition.

Definition 2.7. *An elliptic curve E over $\mathbb{Q}$ which satisfies $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}}) \subseteq G$ is called a* ***G-Serre curve*** *if $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}})$ is a G-maximal commutator-thick subgroup*

If the group G is understood, one may refer to a G-Serre curve simply as a *relative Serre curve*. As an immediate corollary of Theorem 2.5, we will give a characterization of G-Serre curves. For any positive integer $n \geq 1$, define the following set of subgroups of $G(n)$:

$$\mathcal{M}_G(n) := \{H(n) \subseteq G(n) : [H(n), H(n)] \subsetneq [G(n), G(n)]\}.$$

Let $X(n)$ denote the complete modular curve of level n, which parametrizes elliptic curves, together with chosen $\mathbb{Z}/n\mathbb{Z}$-bases of $E[n]$. If H is a subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$ such that $-I \in H$ and the determinant map

$$\det : H \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

is surjective, then the quotient $X_H := X(n)/H$ is a curve over $\mathbb{Q}$. Furthermore, there is a one-to-one correspondence

$$X_H(\mathbb{Q})_{\text{non-cusp.}} \longleftrightarrow \{E/\mathbb{Q} : \varphi_{E,\mathbb{Q},n}(G_\mathbb{Q}) \subseteq H\}$$

between the non-cuspidal rational points of X_H and the set of ($\overline{\mathbb{Q}}$-isomorphism classes of) elliptic curves $E/\mathbb{Q}$ having the property that $\varphi_{E,\mathbb{Q},n}(G_\mathbb{Q})$ is contained in some conjugate of H in $GL_2(\mathbb{Z}/n\mathbb{Z})$.

Corollary 2.8. *Let E be an elliptic curve over $\mathbb{Q}$ for which $\varphi_{E,\mathbb{Q}}(G_\mathbb{Q}) \subseteq G$. Then E fails to be a G-Serre curve if and only if, for some $n \in \{m_0\} \cup \{\ell \text{ prime } : \ell \nmid m_0\}$ and some $H \in \mathcal{M}_G(n)$, E corresponds to a point in $X_H(\mathbb{Q})_{non\text{-}cusp.}$.*

Suppose we choose the group

$$G = \pi^{-1}(G(m)) \subseteq GL_2(\hat{\mathbb{Z}})$$

as above so that the corresponding modular curve $X_{G(m)}$ has genus zero and satisfies $X_{G(m)}(\mathbb{Q}) \neq \emptyset$, and suppose that

$$E : y^2 = x^3 + A(t)x + B(t) \qquad (A(t), B(t) \in \mathbb{Q}(t))$$

is an elliptic curve over $\mathbb{Q}(t)$ satisfying

$$\varphi_{E,\mathbb{Q}(t)}(G_{\mathbb{Q}(t)}) = G.$$

(Note in particular that E then defines a morphism $\mathbb{P}^1 \longrightarrow X_{G(m)}$.) For a real parameter $T \geq 0$, define the sets

$$\mathcal{F}_E(T) := \{t_0 \in \mathbb{Q} : \ \mathcal{H}(t_0) \leq T, \ E_{t_0}/\mathbb{Q} \text{ is an elliptic curve}\},$$
$$\mathcal{E}_{E,\text{non-}G\text{-Serre}}(T) := \{t_0 \in \mathcal{F}_E(T) : \ E_{t_0} \text{ is not a } G\text{-Serre curve}\},$$

where E_{t_0} denotes the specialization of E at t_0 and $\mathcal{H}(t_0)$ denotes the Mordell height of t_0, i.e. if we write $t_0 = a/b$ in lowest terms,

$$\mathcal{H}(a/b) := \max\{|a|, |b|\}.$$

Corollary 2.8 allows us to deduce the following generalization of [3, Main Theorem].

Theorem 2.9. *Let $\varepsilon > 0$ be arbitrary. One has*

$$|\mathcal{E}_{E,non\text{-}G\text{-}Serre}(T)| = O_{E,\varepsilon}(T^{1+\varepsilon}).$$

Since $|\mathcal{F}_E(T)| \asymp T^2$, Theorem 2.9 implies that "almost all specializations of E are G-Serre curves." The main theorem of [3] gives Theorem 2.9 when $G = GL_2(\hat{\mathbb{Z}})$, and also gives much better bounds in some cases. The proof of Theorem 2.9 proceeds along the same lines (with Corollary 2.8 replacing [3, Corollary 16]), and also gives better bounds in the appropriate cases. For the sake of brevity, Theorem 2.9 states only the weakest form of what one can deduce from Corollary 2.8, and (since its proof is exactly the proof of [3, Main Theorem], mutatis mutandis) we will not include it in the present paper.

Remark 2.10. *Suppose that $H \subseteq G$ is determinant-surjective and commutator-thick. Noting the exact sequence*

$$1 \longrightarrow H \cap SL_2(\hat{\mathbb{Z}}) \longrightarrow H \longrightarrow \hat{\mathbb{Z}}^\times \longrightarrow 1, \tag{8}$$

and that the kernel $H \cap SL_2(\hat{\mathbb{Z}}) = [H, H] \subseteq [G, G]$, it follows that, if H is a G-maximal commutator-thick subgroup of G in the sense of Definition 2.4, then H is also maximal (with respect to subset inclusion) among the commutator-thick subgroups of G. Furthermore, it follows from (8) *and the corresponding sequence with G replacing H that*

$$H \cap SL_2(\hat{\mathbb{Z}}) = [G, G] \iff [G : H] = \left[G \cap SL_2(\hat{\mathbb{Z}}) : [G, G]\right]. \tag{9}$$

Thus, Definition 2.4 is equivalent to H having minimal index in G.

2.1. **The general case.** The definitions and theorems we have described apply more generally to the following situation. Let $r \geq 1$ be a positive integer and let $\mathcal{G} \subseteq GL_r$ be any algebraic subgroup. Fix a positive integer $m \geq 1$ and an arbitrary subgroup $G(m) \subseteq \mathcal{G}(\mathbb{Z}/m\mathbb{Z})$, and let $G := \pi^{-1}_{\mathcal{G}(\hat{\mathbb{Z}})}(G(m)) \subseteq \mathcal{G}(\hat{\mathbb{Z}})$ denote the corresponding finite index subgroup of $\mathcal{G}(\hat{\mathbb{Z}})$. Furthermore, suppose that

$$\varphi : G_{\mathbb{Q}} \longrightarrow G$$

is any representation for which the composition

$$\det \circ \varphi : G_{\mathbb{Q}} \longrightarrow \hat{\mathbb{Z}}^{\times}$$

agrees with the cyclotomic character. Definitions 2.1, 2.2 and 2.4 (with $GL_2(\hat{\mathbb{Z}})$ and $SL_2(\hat{\mathbb{Z}})$ replaced by $GL_r(\hat{\mathbb{Z}})$ and $SL_r(\hat{\mathbb{Z}})$, respectively) each make sense for any subgroup $H \subseteq G$, and (for the same reason as in the GL_2 case) the image $\varphi(G_{\mathbb{Q}})$ must be commutator-thick and determinant-surjective.

Let us now make the following assumptions about the group $\mathcal{G}$. Let $\mathcal{S} := \mathcal{G} \cap SL_r$.

- A1 There is a finite set $\mathcal{P}_1$ of primes such that, for any prime $\ell \notin \mathcal{P}_1$, there is a simple group $P\mathcal{S}(\ell)$ and a surjective homomorphism $\varpi : \mathcal{S}(\mathbb{Z}/\ell\mathbb{Z}) \to P\mathcal{S}(\ell)$, with no proper subgroup $\mathcal{T}(\ell) \subsetneq \mathcal{S}(\mathbb{Z}/\ell\mathbb{Z})$ satisfying $\varpi(\mathcal{T}(\ell)) = P\mathcal{S}(\ell)$. Furthermore, if $\ell, \ell' \notin \mathcal{P}_1$ and $\ell' \neq \ell$, then $P\mathcal{S}(\ell')$ does not occur as a quotient of a subgroup of $\mathcal{S}(\mathbb{Z}_\ell)$.
- A2 There is a finite set $\mathcal{P}_2$ of primes such that, for any prime $\ell \notin \mathcal{P}_2$ there is no proper subgroup $\mathcal{T}(\ell^2) \subsetneq \mathcal{S}(\mathbb{Z}/\ell^2\mathbb{Z})$ satisfying $\pi(\mathcal{T}(\ell^2)) = \mathcal{S}(\mathbb{Z}/\ell\mathbb{Z})$, where $\pi : \mathcal{S}(\mathbb{Z}/\ell^2\mathbb{Z}) \to \mathcal{S}(\mathbb{Z}/\ell\mathbb{Z})$ denotes the canonical projection.
- A3 For every prime ℓ, the Lie algebra $\mathfrak{g}$ attached to the ℓ-adic lie group $\mathcal{G}(\mathbb{Z}_\ell)$ satisfies

  $$\langle CD - DC : C, D \in \mathfrak{g} \rangle = \{X \in \mathfrak{g} : \operatorname{tr} X = 0\},$$

  where we are viewing $\mathfrak{g} \subseteq M_{r\times r}(\mathbb{Z}_\ell)$ and interpreting the Lie bracket $[,]$ as $[C, D] = CD - DC$.

Having made these assumptions on $\mathcal{G}$, we put

$$m_0^{\text{gen}} := \operatorname{lcm}\left(\prod_{\ell \in \mathcal{P}_2 \cup \mathcal{P}_1} \ell^3 \, , \prod_{\substack{\ell \notin \mathcal{P}_2 \cup \mathcal{P}_1 \\ \ell | m}} \ell^{2\operatorname{ord}_\ell(m)+1} \right).$$

Our proof of Theorem 2.5, formulated generally, gives the following result.

Theorem 2.11. *Let $\mathcal{G} \subseteq GL_r$ be any algebraic subgroup satisfying assumptions A1, A2 and A3 above, $m \geq 1$ a positive integer, $G(m) \subseteq \mathcal{G}(\mathbb{Z}/m\mathbb{Z})$ any subgroup and $G = \pi^{-1}_{\mathcal{G}(\hat{\mathbb{Z}})}(G(m)) \subseteq \mathcal{G}(\hat{\mathbb{Z}})$ the corresponding finite index subgroup. Let $H \subseteq G$ be a determinant-surjective, commutator-thick subgroup. Then H is a G-maximal commutator-thick subgroup of G if and only if the following two conditions hold.*

1. *For each prime ℓ not dividing m_0^{gen}, one has $\mathcal{S}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq H(\ell)$.*
2. *One has $[H(m_0^{gen}), H(m_0^{gen})] = [G(m_0^{gen}), G(m_0^{gen})]$.*

2.2. **The case $G = GL_2(\hat{\mathbb{Z}})$.** We end this section by remarking on the situation when $G = GL_2(\hat{\mathbb{Z}})$. In this case, we have

$$[GL_2(\hat{\mathbb{Z}}), GL_2(\hat{\mathbb{Z}})] = SL_2(\hat{\mathbb{Z}}) \cap \ker \varepsilon, \tag{10}$$

where ε is defined in (2) (for a proof of this, see for instance [6]). Thus, putting $G = GL_2(\hat{\mathbb{Z}})$ in (9), we find that, for any elliptic curve E over $\mathbb{Q}$,

$$E \text{ is a Serre curve} \iff [GL_2(\hat{\mathbb{Z}}) : \varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}})] = 2$$

In particular,

$$E \text{ is a } GL_2(\hat{\mathbb{Z}})\text{-Serre curve} \iff E \text{ is a Serre curve.}$$

Thus, Theorem 2.6 has the following corollary, which improves [8, Lemma 5] to an "if and only-if" statement.

Corollary 2.12. *An elliptic curve E over $\mathbb{Q}$ is a Serre curve if and only if the following two conditions hold.*

1. *For each prime number $\ell \geq 5$, $SL_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq \varphi_{E,\mathbb{Q},\ell}(G_{\mathbb{Q}})$.*

(2) *One has* $[\varphi_{E,\mathbb{Q},36}(G_{\mathbb{Q}}), \varphi_{E,\mathbb{Q},36}(G_{\mathbb{Q}})] = SL_2(\mathbb{Z}/36\mathbb{Z}) \cap (\ker \varepsilon \mod 36)$.

Remark 2.13. *The fact that $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}})$ must be commutator-thick is a consequence of the Kronecker-Weber theorem, and so one cannot draw the same conclusion if E is defined over a number field $K \neq \mathbb{Q}$. Indeed, as shown in* [6] *(see also* [16]*), there are number fields K and elliptic curves E over K for which $\varphi_{E,K}(G_K) = GL_2(\hat{\mathbb{Z}})$, which by* (10) *is not commutator-thick.*

3. Notation and preliminaries

Throughout the paper, we will use the following notation. For positive integers n and m, we will write

$$n \mid m^{\infty}$$

to mean that, for every prime number p, if p divides n then p divides m. The symbols p and ℓ will always denote prime numbers. We use the usual notation

$$\hat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}$$

for the inverse limit of the projective system $\{\mathbb{Z}/n_1\mathbb{Z} \to \mathbb{Z}/n_2\mathbb{Z} : n_1, n_2 \geq 1,\ n_2 \mid n_1\}$. The Chinese remainder theorem gives an isomorphism

$$\hat{\mathbb{Z}} \simeq \prod_{\ell} \mathbb{Z}_{\ell},$$

where $\mathbb{Z}_{\ell}$ denotes the ring of ℓ-adic integers. We will often make implicit use of this isomorphism. For any fixed positive integer n, we will denote by $\mathbb{Z}_n$ (respectively $\mathbb{Z}_{(n)}$) the subring of $\hat{\mathbb{Z}}$ which corresponds under this isomorphism to $\prod_{\ell \mid n} \mathbb{Z}_{\ell}$ (respectively to $\prod_{\ell \nmid n} \mathbb{Z}_{\ell}$).

Given a subgroup $H \subseteq GL_2(\hat{\mathbb{Z}})$, we will denote by H_n (respectively by $H(n)$) the image of H under the canonical projection $GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}_n)$, (respectively under the canonical projection $GL_2(\hat{\mathbb{Z}}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$). We will overwork the symbol π, using it to denote any of the following canonical projections:

$$\begin{aligned} \pi : GL_2(\hat{\mathbb{Z}}) &\longrightarrow GL_2(\mathbb{Z}_n) \\ \pi : GL_2(\hat{\mathbb{Z}}) &\longrightarrow GL_2(\mathbb{Z}/n\mathbb{Z}) \\ \pi : GL_2(\mathbb{Z}/n_1\mathbb{Z}) &\longrightarrow GL_2(\mathbb{Z}/n_2\mathbb{Z}) \qquad (n_2 \mid n_1). \end{aligned}$$

We will use the symbol π_{SL_2} to refer to the restriction to SL_2 of any of these projections.

For a 2×2 matrix $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we denote by

$$g^{\mathrm{Ad}} := \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

the classical adjoint of g. Given a ring R, we use $M_{2\times 2}(R)$ to denote the ring of 2×2 matrices with entries in R. Furthermore, we set

$$M_{2\times 2}^{\mathrm{tr}=0}(R) := \{A \in M_{2\times 2}(R) : \mathrm{tr}\, A = 0\},$$

and, given a matrix $g \in M_{2\times 2}(R)$,

$$\mathcal{N}_g(R) := \{X \in M_{2\times 2}(R) : Xg = g^{\mathrm{Ad}}X\}.$$

Finally, for a pair of elements h and k in any group, we will use the standard notation for the commutator:

$$[h, k] := hkh^{-1}k^{-1}.$$

4. Examples and remarks

Before proving Theorem 2.5, we will give a few examples which illustrate some of the subtlety of this study. The first example highlights the fact that, even though there may exist a determinant-surjective, commutator-thick subgroup H of a given group G, there may nevertheless be no elliptic curve E over $\mathbb{Q}$ for which $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}}) \subseteq G$.

Example 4.1. *Let ℓ be a prime,*

$$G(\ell) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : \ b \in \mathbb{Z}/\ell\mathbb{Z};\ a, d \in (\mathbb{Z}/\ell\mathbb{Z})^\times \right\},$$

and $G = \pi^{-1}(G(\ell)) \subseteq GL_2(\hat{\mathbb{Z}})$. Even though there do exist commutator-thick, determinant-surjective subgroups $H \subseteq G$, Mazur has shown (see [9]*) that, for $\ell > 163$, there is no elliptic curve E over $\mathbb{Q}$ for which $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}}) \subseteq G$. More generally, when the index of G in $GL_2(\hat{\mathbb{Z}})$ is large enough, one expects that no subgroup of G arises as $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}})$ for E over $\mathbb{Q}$ (see* [14, § 4.3] *and* [1]*).*

The next example shows that there do exist finite index subgroups $G \subseteq GL_2(\hat{\mathbb{Z}})$ which have no commutator-thick, determinant-surjective subgroups.

Example 4.2. *Let ℓ be an odd prime and fix any element $\varepsilon \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ which is not a square, i.e. for which $\left(\frac{\varepsilon}{\ell}\right) = -1$. Let $\mathcal{C}_{ns}(\ell)$ denote the non-split Cartan subgroup*

$$\mathcal{C}_{ns}(\ell) := \left\{ \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} \right\} \subseteq GL_2(\mathbb{Z}/\ell\mathbb{Z}).$$

The group $G := \pi^{-1}(\mathcal{C}_{ns}(\ell)) \subseteq GL_2(\hat{\mathbb{Z}})$ has no subgroup H which is simultaneously commutator-thick and determinant-surjective.

Proof. If there were a commutator-thick, determinant-surjective subgroup $H \subseteq \pi^{-1}(\mathcal{C}_{\mathrm{ns}}(\ell))$ then there would necessarily be a group homomorphism $\psi : \hat{\mathbb{Z}}^\times \longrightarrow \mathcal{C}_{\mathrm{ns}}(\ell)$ for which the diagram

$$\begin{array}{ccc} \hat{\mathbb{Z}}^\times & = & \hat{\mathbb{Z}}^\times \\ {\scriptstyle\psi}\downarrow & & {\scriptstyle\mathrm{red}}\downarrow \\ \mathcal{C}_{\mathrm{ns}}(\ell) & \xrightarrow{\det} & (\mathbb{Z}/\ell\mathbb{Z})^\times \end{array} \tag{11}$$

commutes. We will show that such a homomorphism ψ cannot exist. Suppose for the sake of contradiction that such a ψ does exist. The group $\mathcal{C}_{\mathrm{ns}}(\ell)$ is a cyclic group of order $\ell^2 - 1$, from which it follows that ψ factors as

$$\hat{\mathbb{Z}}^\times \xrightarrow{\mathrm{red}} (\mathbb{Z}/\ell m'\mathbb{Z})^\times \xrightarrow{\psi} \psi((\mathbb{Z}/\ell m'\mathbb{Z})^\times) \subseteq \mathcal{C}_{\mathrm{ns}}(\ell),$$

where ℓ does not divide m'. Let g be a generator of $\mathcal{C}_{\mathrm{ns}}(\ell)$ and consider the image under ψ of $(\mathbb{Z}/\ell\mathbb{Z})^\times \times \{1\} \subseteq (\mathbb{Z}/\ell\mathbb{Z})^\times \times (\mathbb{Z}/m'\mathbb{Z})^\times$. By order considerations, we must have

$$\psi((\mathbb{Z}/\ell\mathbb{Z})^\times \times \{1\}) \subseteq \langle g^{\ell+1} \rangle,$$

from which it follows by (11) (since $g^{\ell+1}$ is a scalar matrix) that the canonical projection $(\mathbb{Z}/\ell m'\mathbb{Z})^\times \to (\mathbb{Z}/\ell\mathbb{Z})^\times$ maps into $[(\mathbb{Z}/\ell\mathbb{Z})^\times]^2$, a contradiction. Thus, there is no ψ making (11) commute, proving the assertion. □

Remark 4.3. *By Remark 2.3, the previous example shows that*

$$\nexists E/\mathbb{Q} \ \textit{ for which } \ \varphi_{E,\mathbb{Q},\ell}(G_{\mathbb{Q}}) \subseteq \mathcal{C}_{ns}(\ell).$$

Our third example illustrates, among other things, that the subspace $\mathcal{V} \subseteq M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})$ defined by the exact sequence

$$1 \to I + m\mathcal{V} \to H(\ell m) \to H(m) \to 1$$

may shrink when we replace m by a multiple of m. Let the split-Cartan subgroup $\mathcal{C}_{\mathrm{s}}(\mathbb{Z}/\ell^n\mathbb{Z})$ and the Borel subgroup $B(\mathbb{Z}/\ell^n\mathbb{Z})$ be defined as usual by

$$\mathcal{C}_{\mathrm{s}}(\mathbb{Z}/\ell^n\mathbb{Z}) := \left\{ \begin{pmatrix} x & 0 \\ 0 & z \end{pmatrix} \right\} \subseteq \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \right\} =: B(\mathbb{Z}/\ell^n\mathbb{Z}) \subseteq GL_2(\mathbb{Z}/\ell^n\mathbb{Z}).$$

Let $\chi^{(1)}_{\ell^n}, \chi^{(2)}_{\ell^n} : B(\mathbb{Z}/\ell^n\mathbb{Z}) \longrightarrow (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ be the characters defined by

$$\chi^{(1)}_{\ell^n}\left(\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \right) := x, \qquad \chi^{(2)}_{\ell^n}\left(\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \right) := z,$$

and let us use the same symbols to denote their corresponding restrictions to $\mathcal{C}_{\mathrm{s}}(\mathbb{Z}/\ell^n\mathbb{Z})$. Note that, if $\pi^{-1}(\mathcal{C}_{\mathrm{s}}(\mathbb{Z}/\ell\mathbb{Z})) \subseteq GL_2(\mathbb{Z}/\ell^2\mathbb{Z})$ denotes the full pre-image of $\mathcal{C}_{\mathrm{s}}(\mathbb{Z}/\ell\mathbb{Z})$, then there is a surjective group homomorphism

$$\mu : \pi^{-1}(\mathcal{C}_{\mathrm{s}}(\mathbb{Z}/\ell\mathbb{Z})) \longrightarrow \mathcal{C}_{\mathrm{s}}(\mathbb{Z}/\ell^2\mathbb{Z})$$
$$\mu\left(\begin{pmatrix} x+3a & 3b \\ 3c & z+3d \end{pmatrix} \right) := \begin{pmatrix} x+3a & 0 \\ 0 & x+3d \end{pmatrix}.$$

Finally, we use $\mathcal{L}_\ell : (\mathbb{Z}/\ell\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/3\mathbb{Z})^\times$ to denote the (unique) surjective homomorphism which sends a generator of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ to -1.

Example 4.4. *Suppose that $G \subseteq GL_2(\hat{\mathbb{Z}})$ is a subgroup with*

$$G(3\cdot 7\cdot 13) = \left\{ (g_3, g_7, g_{13}) \in \mathcal{C}_s(\mathbb{Z}/3\mathbb{Z}) \times B(\mathbb{Z}/7\cdot 13\mathbb{Z}) : \det(g_3) = \mathcal{L}_7(\chi^{(1)}_7(g_7)),\ \chi^{(1)}_3(g_3) = \mathcal{L}_{13}(\chi^{(1)}_{13}(g_{13})) \right\}.$$

It is possible that $G(9\cdot 7\cdot 13) \subseteq GL_2(\mathbb{Z}/9\cdot 7\cdot 13)$ is smaller than the full pre-image $\pi^{-1}(G(3\cdot 7\cdot 13)) \subseteq GL_2(\mathbb{Z}/9\cdot 7\cdot 13\mathbb{Z})$. For example, one could have

$$G(9\cdot 7\cdot 13) = \left\{ (g_9, g_7, g_{13}) \in \pi^{-1}(\mathcal{C}_s(\mathbb{Z}/3\mathbb{Z})) \times B(\mathbb{Z}/7\cdot 13\mathbb{Z})) : \det(g_9) = \theta_7(\chi^{(1)}_7(g_7)),\ \chi^{(1)}_9(\mu(g_9)) = \theta_{13}(\chi^{(1)}_{13}(g_{13})) \right\},$$

where $\theta_\ell : (\mathbb{Z}/\ell\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/9\mathbb{Z})^\times$ denotes any surjective homomorphism.

Suppose that $G = \pi^{-1}(G(9\cdot 7\cdot 13)) \subseteq GL_2(\hat{\mathbb{Z}})$, where $G(9\cdot 7\cdot 13)$ is as above. To see that $\pi(G(9\cdot 7\cdot 13)) = G(3\cdot 7\cdot 13)$, note that $\theta_\ell(\chi^{(1)}_\ell(g_\ell)) \mod 3 = \mathcal{L}_\ell(\chi^{(1)}_\ell(g_\ell))$. Also note that the exact sequence

$$1 \to I + 3M_{2\times 2}(\mathbb{Z}/3\mathbb{Z}) \to G(9) \to G(3) \to 1$$

has a larger kernel than

$$1 \to I + 3\cdot 7M^{\mathrm{tr}=0}_{2\times 2}(\mathbb{Z}/3\mathbb{Z}) \to G(9\cdot 7) \to G(3\cdot 7) \to 1,$$

whose kernel is still larger than

$$1 \to I + 3\cdot 7\cdot 13\left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \mod 3 \right\} \to G(9\cdot 7\cdot 13) \to G(3\cdot 7\cdot 13) \to 1.$$

Remark 4.5. *The **torsion conductor** m_E of an elliptic curve E over $\mathbb{Q}$ is defined in* [7] *to be the smallest positive integer $m \geq 1$ for which*

$$\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}}) = \pi^{-1}(\varphi_{E,\mathbb{Q},m}(G_{\mathbb{Q}})).$$

Example 4.4 highlights the fact that the determination of m_E can be very delicate. Indeed, suppose E is an elliptic curve over $\mathbb{Q}$ with $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}}) \subseteq \pi^{-1}(G(9\cdot 7\cdot 13)) \subseteq GL_2(\hat{\mathbb{Z}})$. One might, after separately calculating $\varphi_{E,\mathbb{Q},3\cdot 7\cdot 13}(G_{\mathbb{Q}})$ and $\varphi_{E,\mathbb{Q},9}(G_{\mathbb{Q}})$, mistakenly assume that $\varphi_{E,\mathbb{Q}}(G_{\mathbb{Q}})$ is a $\pi^{-1}(G(3\cdot 7\cdot 13))$-maximal commutator-thick subgroup of $\pi^{-1}(G(3\cdot 7\cdot 13))$.

5. Proof of Theorem 2.5

In this section, we will prove Theorem 2.5. We remark that many of the essential ideas are already present in the proof of the Proposition on page IV-19 of [13], wherein a slightly weaker hypothesis than that of Theorem 2.5 is used to deduce that H is an open subgroup of $GL_2(\hat{\mathbb{Z}})$. We begin with some preparatory lemmas.

5.1. **Preparatory lemmas.** Our first lemma will be used repeatedly throughout the paper.

Lemma 5.1. *(Goursat's Lemma) Let G_0 and G_1 be groups and $G \subseteq G_0 \times G_1$ a subgroup satisfying*

$$\pi_i(G) = G_i \qquad (i \in \{0,1\}),$$

where π_i denotes the canonical projection onto the i-th factor. Let $N_i := \pi_i(G \cap \ker \pi_{1-i})$. Then there is an isomorphism of groups $\psi : G_0/N_0 \to G_1/N_1$ (whose graph is induced by G) for which

$$G = \{(g_0, g_1) \in G_0 \times G_1 : \psi(g_0 N_0) = g_1 N_1\}.$$

Proof. See [12, Lemma (5.2.1)], which shows that the image of G in $G_0/N_0 \times G_1/N_1$ is the graph of an isomorphism ψ. Thus, $G \subseteq \{(g_0, g_1) \in G_0 \times G_1 : \psi(g_0 N_0) = g_1 N_1\}$. Now note that $N_0 \times N_1 \subseteq G$, from which the equality follows. □

Remark 5.2. *When applying Lemma 5.1 in this paper, we will usually formulate the conclusion equivalently as "then there exists a group Q and surjective homomorphisms $\psi_0 : G_0 \to Q$, $\psi_1 : G_1 \to Q$ for which $G = \{(g_0, g_1) \in G_0 \times G_1 : \psi_0(g_0) = \psi_1(g_1)\}$."*

The following corollary may be viewed as a "fibered version" of Lemma 5.1. Suppose now that G_0 and G_1 are groups, together with surjective homomorphisms

$$\eta_0 : G_0 \longrightarrow R, \quad \eta_1 : G_1 \longrightarrow R$$

onto a fixed group R. Let

$$G_0 \times_R G_1 := \{(g_0, g_1) \in G_0 \times G_1 : \eta_0(g_0) = \eta_1(g_1)\}$$

denote the fibered product of G_0 and G_1 over R.

Corollary 5.3. *Suppose that $G \subseteq G_0 \times_R G_1$ is any subgroup satisfying $\pi_i(G) = G_i$ for $i \in \{0,1\}$. Then there is a group Q together with a surjective homomorphisms $f : Q \to R$, $\psi_0 : G_0 \to Q$, and $\psi_1 : G_1 \to Q$ for which $f \circ \psi_i = \eta_i$ ($i \in \{0,1\}$), and*

$$G = \{(g_0, g_1) \in G_0 \times G_1 : \psi_0(g_0) = \psi_1(g_1)\}.$$

Proof. We apply Lemma 5.1 and note that there is a well-defined surjective group homomorphism

$$\begin{aligned} f : Q \simeq G_i/N_i &\to R \qquad\qquad (i \in \{0,1\}) \\ g_i N_i &\mapsto \eta_i(g_i). \end{aligned}$$

The corollary follows. □

5.2. **Lemmas for working in $GL_2(\mathbb{Z}_{m_0})$.**

Lemma 5.4. *Fix a prime number ℓ and let $X, Y \in GL_2(\mathbb{Z}_\ell)$. For any $n \geq 1$ and any matrices $C, D \in M_{2\times 2}(\mathbb{Z}_\ell)$, denote by $h := X(I + \ell^n C)$ and $k := Y(I + \ell^n D)$. Then one has*

$$\begin{aligned} [h,k] = [X,Y] &+ \ell^n \left(XY(DX^{-1} - X^{-1}D)Y^{-1} + X(CY - YC)X^{-1}Y^{-1} \right) \\ &\ell^{2n}(X(YC - CY)CX^{-1}Y^{-1} + X(YC - CY)X^{-1}DY^{-1} \\ &\quad + XY(X^{-1}D - DX^{-1})DY^{-1} + X(CYD - YDC)X^{-1}Y^{-1}) \\ &+ \ell^{3n} E_{h,k}, \end{aligned}$$

where $E_{h,k} \in M_{2\times 2}(\mathbb{Z}_\ell)$.

Proof. A calculation, using the series representation $(I + \ell^n C)^{-1} = I - \ell^n C + \ell^{2n} C^2 - \ell^{3n} C^3 + \dots$. □

For a fixed $g \in GL_2(\mathbb{Z}/\ell\mathbb{Z})$ which is not a scalar matrix, consider the map

$$\begin{aligned} \mathrm{Ad}_g : M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z}) &\longrightarrow M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z}) \\ A &\mapsto Ag - gA. \end{aligned}$$

Recall that we are using g^{Ad} to denote the classical adjoint of g.

Lemma 5.5. *Suppose that $g \in GL_2(\mathbb{Z}/\ell\mathbb{Z})$ is not a scalar matrix. Then we have*

$$Ad_g\left(M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})\right) = \mathcal{N}_g(\mathbb{Z}/\ell\mathbb{Z}) := \{X \in M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z}) : Xg = g^{Ad}X\}$$

and

$$Ad_g\left(M_{2\times 2}^{tr=0}(\mathbb{Z}/\ell\mathbb{Z})\right) = \begin{cases} \mathcal{N}_g(\mathbb{Z}/\ell\mathbb{Z}) & \text{if } \ell \neq 2 \text{ or if } \ell = 2 \text{ and } tr\, g \neq 0 \\ \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\} & \text{if } \ell = 2 \text{ and } tr\, g = 0. \end{cases}$$

Furthermore, $\mathcal{N}_g(\mathbb{Z}/\ell\mathbb{Z}) \subseteq M_{2\times 2}^{tr=0}(\mathbb{Z}/\ell\mathbb{Z})$ is a 2-dimensional $\mathbb{Z}/\ell\mathbb{Z}$-vector subspace.

Proof. Let $A \in M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})$ be arbitrary. Using that $gg^{\mathrm{Ad}} = \det g \cdot I$ is a scalar matrix, we find that

$$(Ag - gA)g = g^{\mathrm{Ad}}(Ag - gA) \iff Ag(g + g^{\mathrm{Ad}}) = (g + g^{\mathrm{Ad}})Ag,$$

which, since $g + g^{\mathrm{Ad}} = \operatorname{tr} g \cdot I$ is a scalar matrix, verifies that $\mathrm{Ad}_g\left(M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})\right) \subseteq \mathcal{N}_g(\mathbb{Z}/\ell\mathbb{Z})$. To see equality, we compare dimensions: $\ker \mathrm{Ad}_g = \mathbb{Z}/\ell\mathbb{Z} \cdot I + \mathbb{Z}/\ell\mathbb{Z} \cdot g$ has dimension 2, and one checks that the defining equation $Xg = g^{\mathrm{Ad}}X$ cuts out a 2-dimensional subspace of $M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})$.

Regarding $\mathrm{Ad}_g(M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/\ell\mathbb{Z}))$, one simply checks that

$$\dim_{\mathbb{Z}/\ell\mathbb{Z}}((\mathbb{Z}/\ell\mathbb{Z} \cdot I + \mathbb{Z}/\ell\mathbb{Z} \cdot g) \cap M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/\ell\mathbb{Z})) = \begin{cases} 1 & \text{if } \ell \neq 2 \text{ or if } \ell = 2 \text{ and } \operatorname{tr} g \neq 0 \\ 2 & \text{if } \ell = 2 \text{ and } \operatorname{tr} g = 0 \end{cases}$$

and that, for $g \in GL_2(\mathbb{Z}/2\mathbb{Z})$ with $\operatorname{tr} g = 0$, the image $\mathrm{Ad}_g(M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/2\mathbb{Z}))$ is as stated.

Finally, to see that $\mathcal{N}_g(\mathbb{Z}/\ell\mathbb{Z}) \subseteq M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/\ell\mathbb{Z})$, note that

$$\mathcal{N}_g(\mathbb{Z}/\ell\mathbb{Z}) = g^{-1}\mathcal{N}_g(\mathbb{Z}/\ell\mathbb{Z}) = g^{-1}\mathrm{Ad}_g\left(M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})\right) = \{g^{-1}Ag - A : A \in M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})\} \subseteq M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/\ell\mathbb{Z}).$$

□

Recall that an integer m_0 is called *square-full* if, for each prime ℓ, one has

$$\ell \mid m_0 \implies \ell^2 \mid m_0.$$

Lemma 5.6. *Suppose that m_0 is a positive square-full integer, $H \subseteq SL_2(\mathbb{Z}_{m_0})$ is any subgroup, M is any multiple of m_0 satisfying $m_0 \mid M \mid m_0^\infty$, and ℓ is any prime divisor of m_0. Let $A \in M_{2\times 2}^{tr=0}(\mathbb{Z}/\ell\mathbb{Z})$ be arbitrary, and in case $4 \mid m_0$ but $8 \nmid m_0$, assume additionally that $A^2 = 0$. We then have*

$$I + \frac{m_0}{\ell}A \in H(m_0) \implies I + \frac{M}{\ell}A \in H(M).$$

Proof. The proof is by induction on M, the base case $M = m_0$ being trivial. If $M > m_0$, then there is a prime p dividing m for which $m_0 \mid M/p$. By induction, we have that

$$I + \frac{m_0}{\ell}A \in H(m_0) \implies I + \frac{M/p}{\ell}A \in H\left(M/p\right).$$

Case: $p \neq \ell$. One has

$$H(M) \subseteq \{(h_0, h_1) \in H\left(\frac{M}{p}\right) \times H\left(\frac{M}{\ell}\right) : \pi_0(h_0) = \pi_1(h_1)\}, \tag{12}$$

where $\pi_0 : H\left(\frac{M}{p}\right) \to H\left(\frac{M}{\ell p}\right)$ and $\pi_1 : H\left(\frac{M}{\ell}\right) \to H\left(\frac{M}{\ell p}\right)$ are the natural projections. By Corollary 5.3, there must be a group Q, a surjective group homomorphism $f : Q \to H\left(\frac{M}{\ell p}\right)$ and surjective group homomorphisms

$$\psi_0 : H\left(\frac{M}{p}\right) \longrightarrow Q, \quad \psi_1 : H\left(\frac{M}{\ell}\right) \longrightarrow Q$$

for which $f \circ \psi_i = \pi_i$ $(i \in \{0, 1\})$ and

$$H(M) = \{\{(h_0, h_1) \in H\left(\frac{M}{p}\right) \times H\left(\frac{M}{\ell}\right) : \psi_0(h_0) = \psi_1(h_1)\},$$

Furthermore, since the degrees of π_0 and π_1 are relatively prime, we see that Q must be equal to $H\left(\frac{M}{\ell p}\right)$, $\psi_i = \pi_i$, and (12) is in fact an equality. It follows that $I + \frac{M}{\ell}(p^*A) \in H(M)$ (where p^* denotes the multiplicative inverse of p modulo ℓ), and, since H is a group, that $I + \frac{M}{\ell}A \in H(M)$.

Case: $p = \ell$**.** Now we have $I + \frac{M}{\ell^2}A \in H\left(\frac{M}{\ell}\right)$. Let $I + \frac{M}{\ell^2}A + \frac{M}{\ell}B \in H(M)$ be any lift, and note that

$$\begin{aligned}\left(I + \frac{M}{\ell^2}A + \frac{M}{\ell}B\right)^\ell &\equiv \left(I + \frac{M}{\ell^2}A\right)^\ell \mod M \\ &\equiv I + \frac{M}{\ell}A \mod M.\end{aligned}$$

(Note that this computation requires $A^2 = 0$ if $\ell = 2$ and $2 \mid \frac{M}{2^2}$ but $4 \nmid \frac{M}{2^2}$.) This concludes the proof of Lemma 5.6. □

The following lemma is a corollary of Lemmas 5.4, 5.5 and 5.6.

Lemma 5.7. *Let $m \geq 1$ be any positive integer, $H(m) \subseteq GL_2(\mathbb{Z}/m\mathbb{Z})$ any subgroup and $H = \pi^{-1}(H(m)) \subseteq GL_2(\hat{\mathbb{Z}})$ the corresponding subgroup of finite index. Suppose that m_0 is any positive square-full integer satisfying the following two properties:*

- *For each prime ℓ dividing m with $H(\ell)$ non-abelian, $\ell^{ord_\ell(m)+1} \mid m_0$.*
- *For each prime ℓ dividing m with $H(\ell)$ abelian, $\ell^{2ord_\ell(m)+1} \mid m_0$.*

Then, for each prime ℓ dividing m_0, we have

$$I + \frac{m_0}{\ell}M_{2\times 2}^{tr=0}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq [H(m_0), H(m_0)]. \tag{13}$$

Proof. We begin by noting that, by Lemma 5.6, we may without loss of generality assume that, for each prime ℓ dividing m_0,

$$\ell \nmid m \Longrightarrow \ell^3 \nmid m_0.$$

Assuming this, let us fix a prime ℓ dividing m_0 and write $m_0 = \ell^{m_\ell} \cdot m_0'$, where $\ell \nmid m_0'$. By Lemma 5.1, there is a group Q and surjective homomorphisms $\psi_0 : H(\ell^{m_\ell}) \to Q$, $\psi_1 : H(m_0') \to Q$ for which, under the isomorphism of the Chinese remainder theorem,

$$\begin{aligned}H(m_0) &= \{(h_0, h_1) \in H(\ell^{m_\ell}) \times H(m_0') : \psi_0(h_0) = \psi_1(h_1)\} \\ &=: H(\ell^{m_\ell}) \times_Q H(m_0').\end{aligned}$$

Note that, under this isomorphism,

$$I + \frac{m_0}{\ell}M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq H(m_0) \iff (I + \ell^{m_\ell - 1}M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/\ell\mathbb{Z}), I) \subseteq H(\ell^{m_\ell}) \times_Q H(m_0').$$

In order to show (13), we will produce a set $T \subseteq H(\ell^{m_\ell}) \times_Q H(m_0')$ for which the group generated by $[T, T]$ contains $(I + \ell^{m_\ell - 1}M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/\ell\mathbb{Z}), I)$:

$$(I + \ell^{m_\ell - 1}M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/\ell\mathbb{Z}), I) \subseteq \langle [(h, h'), (k, k')] : (h, h'), (k, k') \in T \rangle. \tag{14}$$

In case $H(\ell)$ is not abelian, choose any two elements $Z, \tilde{Z} \in H(\ell^{m_\ell})$ which do not commute with one another modulo ℓ (and consequently for which $\mathcal{N}_Z(\mathbb{Z}/\ell\mathbb{Z}) \neq \mathcal{N}_{\tilde{Z}}(\mathbb{Z}/\ell\mathbb{Z})$), and find elements $Z', \tilde{Z}' \in H(m_0')$ for which $(Z, Z'), (\tilde{Z}, \tilde{Z}') \in H(\ell^{m_\ell}) \times_Q H(m_0')$. To uniformize the notation, let us define the exponent n_ℓ by

$$n_\ell := \begin{cases} \mathrm{ord}_\ell(m) & \text{if } \ell \mid m \\ 1 & \text{otherwise.} \end{cases}$$

Then one can in fact take

$$T := \begin{cases} \{(I + \ell^{n_\ell}C, I) : C \in M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})\} \cup \{(Z, Z'), (\tilde{Z}, \tilde{Z}')\} & \text{if } H(\ell) \text{ is not abelian} \\ \{(I + \ell^{n_\ell}C, I) : C \in M_{2\times 2}(\mathbb{Z}/\ell^{n_\ell+1}\mathbb{Z})\} & \text{if } H(\ell) \text{ is abelian.} \end{cases}$$

To see that $T \subseteq H(\ell^{m_\ell}) \times_Q H(m_0')$, note that every element of $(I + \ell^{n_\ell} M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z}), I)$ is congruent to I modulo m, and similarly with $(I + \ell^{n_\ell} M_{2\times 2}(\mathbb{Z}/\ell^{n_\ell+1}\mathbb{Z}), I)$. The containment (14) follows from Lemmas 5.4 and 5.5, as follows. In case $H(\ell)$ is non-abelian, then by Lemma 5.4 (with $n = n_\ell$, $X = I$, $Y = Z$ and $D = 0$) we have that

$$[(I + \ell^{n_\ell} D, I), (Z, Z')] = (I + \ell^{n_\ell}((CZ - ZC)Z^{-1}), I).$$

By Lemma 5.5, we find that, varying $C \in M_{2\times 2}(\mathbb{Z}/\ell\mathbb{Z})$ shows that $I + \frac{m_0}{\ell}\mathcal{N}_Z(\mathbb{Z}/\ell\mathbb{Z}) \subseteq [H(m_0), H(m_0)]$. Similarly, $I + \frac{m_0}{\ell}\mathcal{N}_{\tilde{Z}}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq [H(m_0), H(m_0)]$, from which (14) follows by dimension considerations. In case $H(\ell)$ is abelian, we again use Lemma 5.4 (with $n = n_\ell$ and $X = Y = I$), concluding that

$$[(I + \ell^{n_\ell} C, I), (I + \ell^{n_\ell} D, I)] = (I + \ell^{2n_\ell}(CD - DC), I).$$

Varying C and D modulo ℓ, we conclude (14), as before. This finishes the proof of Lemma 5.7. □

The following key lemma is a corollary of Lemma 5.6.

Lemma 5.8. *Let m_0 be any positive square-full integer and $S \subseteq SL_2(\mathbb{Z}/m_0\mathbb{Z})$ any subgroup satisfying*

$$\forall \ell \mid m_0, \quad I + \frac{m_0}{\ell} M_{2\times 2}^{tr=0}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq S. \tag{15}$$

in case $4 \mid m_0$ but $8 \nmid m_0$, assume additionally that $S(2) = SL_2(\mathbb{Z}/2\mathbb{Z})$. Suppose that $K \subseteq SL_2(\mathbb{Z}_{m_0})$ is any closed subgroup for which $K(m_0) = S$. Then we must have

$$K = \pi_{SL_2}^{-1}(S).$$

Proof. Since K is closed, it suffices to show that $K(M) = \pi^{-1}(S) \subseteq SL_2(\mathbb{Z}/M\mathbb{Z})$, for any positive integer M satisfying $m_0 \mid M \mid m_0^\infty$. This is proved by induction on M, the base case $M = m_0$ being trivial. If $M > m_0$, then there is a prime ℓ for which $m_0 \mid (M/\ell)$. By induction, $K(M/\ell) = \pi^{-1}(S) \subseteq SL_2(\mathbb{Z}/(M/\ell)\mathbb{Z})$, and thus $I + (M/\ell^2)M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq K(M/\ell)$. Considering the exact sequence

$$1 \longrightarrow I + (M/\ell)M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/M\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/(M/\ell)\mathbb{Z}) \longrightarrow 1,$$

we see that $K(M) = \pi^{-1}(S)$ if and only if $I + (M/\ell)M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/\ell\mathbb{Z}) \subseteq K(M)$. This last containment follows from (15) and Lemma 5.6. In case $\ell = 2$ and $8 \nmid M/\ell$, we note that, as observed in [13, Lemma 3, p. IV-23] (see also [16, Lemma A.2]), $I + (M/2)M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/2\mathbb{Z})$ may be generated as an $SL_2(\mathbb{Z}/2\mathbb{Z})$-module (the $SL_2(\mathbb{Z}/2\mathbb{Z})$-action given by conjugation) by matrices $I+(M/2)A \in I+(M/2)M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/2\mathbb{Z})$ with $A^2 = 0$. □

5.3. **Lemmas for working in $GL_2(\mathbb{Z}_{(m_0)})$.**

Lemma 5.9. *Let $\ell \geq 5$ be a prime number, and let $n \geq 1$ be any positive integer exponent. Suppose that $N \trianglelefteq SL_2(\mathbb{Z}/\ell^n\mathbb{Z})$ is a normal subgroup. Then either there is a surjective group homomorphism $SL_2(\mathbb{Z}/\ell^n\mathbb{Z})/N \longrightarrow PSL_2(\mathbb{Z}/\ell\mathbb{Z})$, or else $N = SL_2(\mathbb{Z}/\ell^n\mathbb{Z})$.*

Proof. The proof proceeds by induction on n. If $n = 1$, then consider the image

$$\pm N/\{\pm I\} \subseteq PSL_2(\mathbb{Z}/\ell\mathbb{Z})$$

of N under the canonical surjection $SL_2(\mathbb{Z}/\ell\mathbb{Z}) \to PSL_2(\mathbb{Z}/\ell\mathbb{Z})$. Since $\ell \geq 5$, $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ is a simple group, and so

$$\pm N/\{\pm I\} = \begin{cases} \{1\} & \text{or} \\ PSL_2(\mathbb{Z}/\ell\mathbb{Z}). \end{cases} \tag{16}$$

In the first case we have $N \subseteq \{\pm 1\}$ and so $SL_2(\mathbb{Z}/\ell\mathbb{Z})/N \in \{SL_2(\mathbb{Z}/\ell\mathbb{Z}), PSL_2(\mathbb{Z}/\ell\mathbb{Z})\}$, which clearly has $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ as a quotient. In the second case of (16), we have that $\pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in N$, which implies that $\{\pm I\} \subseteq N$, and so $N = SL_2(\mathbb{Z}/\ell\mathbb{Z})$, as asserted, concluding the verification of the base case.

Now assume the statement of Lemma 5.9 for some exponent $n \geq 1$ and let $N \trianglelefteq SL_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$ be any normal subgroup. By the inductive hypothesis, the image of N under reduction modulo ℓ^n either has $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ as a quotient, or else is equal to $SL_2(\mathbb{Z}/\ell^n\mathbb{Z})$. In the first case, $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ is also a quotient of $SL_2(\mathbb{Z}/\ell^{n+1}/\mathbb{Z})/N$, and in the second case, [13, Lemma 3, p. IV-23] implies that $N = SL_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$. This concludes the proof of Lemma 5.9. □

The following lemma is a consequence of the previous one.

Lemma 5.10. *Let m_0 be any integer divisible by 6 and suppose that $K \subseteq SL_2(\mathbb{Z}_{(m_0)})$ is any closed subgroup satisfying*

$$\forall \ell \nmid m_0, \quad K(\ell) = SL_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Then $K = SL_2(\mathbb{Z}_{(m_0)})$.

Proof. Since K is closed, it suffices to show that, for each integer M with $\gcd(m_0, M) = 1$, $K(M) = SL_2(\mathbb{Z}/M\mathbb{Z})$. We prove this by induction on the number of prime divisors ℓ of M. The base case where $M = \ell^n$ is a prime power follows immediately from [13, Lemma 3, p. IV-23]. For the induction step, suppose that M is divisible by more than one prime and write $M = \ell^n M'$, where $\ell \nmid M'$ and $M' > 1$. By induction, we have that

$$K(M') = SL_2(\mathbb{Z}/M'\mathbb{Z}) \quad \text{and} \quad K(\ell^n) = SL_2(\mathbb{Z}/\ell^n\mathbb{Z}).$$

By Lemma 5.1, there is a common quotient group Q, together with surjective homomorphisms

$$\psi_0 : K(M') \longrightarrow Q, \quad \psi_1 : K(\ell^n) \longrightarrow Q,$$

such that under the isomorphism of the Chinese remainder theorem, we have

$$K(M) = \{(h_0, h_1) \in K(M') \times K(\ell^n) : \psi_0(h_0) = \psi_1(h_1)\}.$$

Now we apply Lemma 5.9 (with $N = \ker \psi_1$), concluding that either Q has $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ as a quotient, or else $Q = 1$. But since M' is not divisible by ℓ, Q cannot have $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ as a quotient, and so $Q = 1$ and $K(M) = SL_2(\mathbb{Z}/M\mathbb{Z})$, finishing the proof of Lemma 5.10. □

Lemma 5.11. *For any prime $\ell \geq 5$, one has*

$$[SL_2(\mathbb{Z}/\ell\mathbb{Z}), SL_2(\mathbb{Z}/\ell\mathbb{Z})] = SL_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Proof. This follows from (10). □

Corollary 5.12. *Under the isomorphism $GL_2(\hat{\mathbb{Z}}) = GL_2(\mathbb{Z}_{m_0}) \times GL_2(\mathbb{Z}_{(m_0)})$ of the Chinese remainder theorem, we have*

$$[G, G] = \pi_{SL_2}^{-1}([G(m_0), G(m_0)]) \times SL_2(\mathbb{Z}_{(m_0)}).$$

In particular, the index of $[G, G]$ in $SL_2(\hat{\mathbb{Z}})$ is finite.

Proof. Since $G = G_{m_0} \times GL_2(\mathbb{Z}_{(m_0)})$, it follows that $[G, G] = [G_{m_0}, G_{m_0}] \times [GL_2(\mathbb{Z}_{(m_0)}), GL_2(\mathbb{Z}_{(m_0)})]$. Lemmas 5.7 and 5.8 imply that

$$[G_{m_0}, G_{m_0}] = \pi_{SL_2}^{-1}([G(m_0), G(m_0)]).$$

Also, it follows from Lemma 5.11 that the reduction of $[GL_2(\mathbb{Z}_{(m_0)}), GL_2(\mathbb{Z}_{(m_0)})]$ modulo any prime ℓ not dividing m_0 is $SL_2(\mathbb{Z}/\ell\mathbb{Z})$. Using Lemma 5.10, we conclude that $[GL_2(\mathbb{Z}_{(m_0)}), GL_2(\mathbb{Z}_{(m_0)})] = SL_2(\mathbb{Z}_{(m_0)})$. □

5.4. **A key proposition.** Putting together the lemmas of the previous section, we now deduce the following proposition.

Proposition 5.13. *Let $m \geq 1$ be any positive integer, $G(m) \subseteq GL_2(\mathbb{Z}/m\mathbb{Z})$ any subgroup and $G = \pi^{-1}(G(m)) \subseteq GL_2(\hat{\mathbb{Z}})$ the corresponding finite index subgroup. Define m_0 by (7), and suppose that $H' \subseteq SL_2(\hat{\mathbb{Z}})$ is any closed subgroup satisfying the following two hypotheses:*

A. *For each prime ℓ not dividing m_0, $H'(\ell) = SL_2(\mathbb{Z}/\ell\mathbb{Z})$.*
B. *One has $H'(m_0) = [G(m_0), G(m_0)]$.*

Then, $H' = [G, G]$.

Proof. By Lemmas 5.7 and 5.8, it follows from property B that

$$H'_{m_0} = \pi_{SL_2}^{-1}([G(m_0), G(m_0)]) = [G_{m_0}, G_{m_0}].$$

On the other hand, by Lemma 5.10, it follows from property A that

$$H'_{(m_0)} = SL_2(\mathbb{Z}_{(m_0)}).$$

By Lemma 5.1, there is a group Q and surjective homomorphisms $\psi_0 : [G_{m_0}, G_{m_0}] \to Q$ and $\psi_1 : SL_2(\mathbb{Z}_{(m_0)}) \to Q$ for which

$$H' = \{(h_0, h_1) \in [G_{m_0}, G_{m_0}] \times SL_2(\mathbb{Z}_{(m_0)}) : \psi_0(h_0) = \psi_1(h_1)\}.$$

Given Corollary 5.12, we now only need to show that $Q = \{1\}$. Consider the subgroup $\ker \psi_2 \subseteq SL_2(\mathbb{Z}_{(m_0)})$, and its projection $\ker \psi_2(\ell) \subseteq SL_2(\mathbb{Z}/\ell\mathbb{Z})$. By Lemma 5.9, either $SL_2(\mathbb{Z}/\ell\mathbb{Z})/\ker \psi_2(\ell)$ has $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ as a quotient, or $\ker \psi_2(\ell) = SL_2(\mathbb{Z}/\ell\mathbb{Z})$. If $SL_2(\mathbb{Z}/\ell\mathbb{Z})/\ker \psi_2(\ell)$ had $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ as a quotient, then so would Q, and hence so would $[G_{m_0}, G_{m_0}]$, contradicting the fact that $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ only occurs as a quotient of a subgroup of $GL_2(\mathbb{Z}_{m_0})$ if $\ell \mid m_0$ (see [13, p. IV-25]). Thus we see that, for each prime $\ell \nmid m_0$, $\ker \psi_2(\ell) = SL_2(\mathbb{Z}/\ell\mathbb{Z})$. By Lemma 5.10, it follows that $\ker \psi_2 = SL_2(\mathbb{Z}_{(m_0)})$, and so $Q = 1$ and $H' = [G, G]$, finishing the proof of Proposition 5.13. □

5.5. **Proof of Theorem 2.5.** As remarked in Section 2, Theorem 2.5 is equivalent to Theorem 2.6. We will now deduce Theorem 2.6 from Proposition 5.13. Note that, if H is any commutator-thick subgroup of G, then

$$H \text{ is a } G\text{-maximal commutator-thick subgroup of } G \iff [G, G] \subseteq H.$$

The "only if" part of Theorem 2.6 then follows, since, by Lemma 5.11, we have

$$[G(\ell), G(\ell)] = [GL_2(\mathbb{Z}/\ell\mathbb{Z}), GL_2(\mathbb{Z}/\ell\mathbb{Z})] = SL_2(\mathbb{Z}/\ell\mathbb{Z}).$$

We proceed to prove the "if" part, i.e. we will show that

$$H \text{ satisfyes hypotheses 1 and 2 of Theorem 2.6} \implies [G, G] \subseteq H.$$

This follows by applying Proposition 5.13 with $H' = [H, H]$. Properties A and B of the proposition follow from Hypotheses 1 and 2 of Theorem 2.6, since, by Lemma 5.11, one has $[H, H](\ell) = [H(\ell), H(\ell)] = SL_2(\mathbb{Z}/\ell\mathbb{Z})$.

6. The group $GL_2(\hat{\mathbb{Z}})_{\chi=\varepsilon}$ is commutator-thick

We will now use Lemmas from Section 5 to deduce the commutator-thickness of the group $GL_2(\hat{\mathbb{Z}})_{\chi=\varepsilon}$, further clarifying the situation where $G = GL_2(\hat{\mathbb{Z}})$.

Proposition 6.1. *The group $GL_2(\hat{\mathbb{Z}})_{\chi=\varepsilon}$ is commutator-thick if and only if χ is non-trivial.*

Proof. Let n_χ be the conductor of χ and put $G := GL_2(\hat{\mathbb{Z}})_{\chi=\varepsilon}$. Note that $G = \pi^{-1}(G(m))$, where $m = \operatorname{lcm}(2, n_\chi)$. Since the argument is slightly different when n_χ is a power of 2, we treat the cases separately.

Case: $n_\chi \notin \{1, 4, 8\}$

This case is equivalent to the existence of an odd prime ℓ dividing n_χ. Define m_0 as usual by (7). Our first claim is that

$$[G(m_0), G(m_0)] = SL_2(\mathbb{Z}/m_0\mathbb{Z}) \cap (\ker \varepsilon \mod m_0). \tag{17}$$

Notice that, by Proposition 5.13 and (10), this will imply Proposition 6.1 for the case $n_\chi \notin \{1, 4, 8\}$.

To see (17), first write $m_0 = 2^\beta \cdot m_1$, where $m_1 > 1$ is odd. Define the characters

$$\chi_2 : (\mathbb{Z}/2^\beta\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m_0\mathbb{Z})^\times \longrightarrow \{\pm 1\}$$
$$\chi_{m_1} : (\mathbb{Z}/m_1\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m_0\mathbb{Z})^\times \longrightarrow \{\pm 1\}$$

to be the composition of χ and the canonical embedding

$$(\mathbb{Z}/2^\beta\mathbb{Z})^\times \to (\mathbb{Z}/2^\beta\mathbb{Z})^\times \times \{1\} \subseteq (\mathbb{Z}/2^\beta\mathbb{Z})^\times \times (\mathbb{Z}/m_1\mathbb{Z})^\times \simeq (\mathbb{Z}/m_0\mathbb{Z})^\times$$

(respectively $(\mathbb{Z}/m_1\mathbb{Z})^\times \to (\mathbb{Z}/m_0\mathbb{Z})^\times$). Then one has

$$\chi(n) = \chi_2(n_2) \cdot \chi_{m_1}(n_{m_1}),$$

where $(\mathbb{Z}/m_0\mathbb{Z})^\times \ni n \leftrightarrow (n_2, n_{m_1}) \in (\mathbb{Z}/2^\beta\mathbb{Z})^\times \times (\mathbb{Z}/m_1\mathbb{Z})^\times$ under the isomorphism of the Chinese remainder theorem, and so, under this isomorphism,

$$GL_2(\mathbb{Z}/m_0\mathbb{Z})_{\chi=\varepsilon} = \{(g_2, g_{m_1}) \in GL_2(\mathbb{Z}/2^\beta\mathbb{Z}) \times GL_2(\mathbb{Z}/m_1\mathbb{Z}) : \chi_2(g_2)\varepsilon(g_2) = \chi_{m_1}(g_{m_1})\}.$$

Let $X, Y \in GL_2(\mathbb{Z}/m_1\mathbb{Z})$ be arbitrary. We will show that

$$(1, XYX^{-1}Y^{-1}) \in [G(m_0), G(m_0)]. \tag{18}$$

If $\chi_{m_1}(X) = \chi_{m_1}(Y)$, then one can find a single element $Z \in GL_2(\mathbb{Z}/2^\beta\mathbb{Z})$ for which $(Z, X), (Z, Y) \in GL_2(\mathbb{Z}/m_0\mathbb{Z})_{\chi=\varepsilon}$, which verifies (18). If on the other hand $\chi_{m_1}(X) \neq \chi_{m_1}(Y)$, then one of them must be equal to 1, and so (if, say, $\chi_{m_1}(X) = 1$), we find that $(I, X), (Z, Y) \in G(m_0)$ for an appropriately chosen $Z \in GL_2(\mathbb{Z}/2^\beta\mathbb{Z})$, verifying (18) in this case. It follows that $\{1\} \times SL_2(\mathbb{Z}/m_1\mathbb{Z}) \subseteq [G(m_0), G(m_0)]$, and, since (10) implies that $[GL_2(\mathbb{Z}/2^\beta\mathbb{Z}), GL_2(\mathbb{Z}/2^\beta\mathbb{Z})] = SL_2(\mathbb{Z}/2^\beta\mathbb{Z}) \cap (\ker\varepsilon \mod 2^\beta)$, (17) follows.

Case: $n_\chi \in \{4, 8\}$

In this case, $G = G_2 \times GL_2(\mathbb{Z}_{(2)})$, and so it suffices to show that

$$[G_2, G_2] = \ker\varepsilon \cap SL_2(\mathbb{Z}_2). \tag{19}$$

If $n_\chi = 4$, then from the exact sequence

$$1 \longrightarrow I + 2M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/2\mathbb{Z}) \longrightarrow G(4) \longrightarrow GL_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow 1$$

and its specialization

$$1 \longrightarrow I + 2M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/2\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/4\mathbb{Z}) \cap (\ker\varepsilon \mod 4) \longrightarrow \ker\varepsilon \mod 2 \longrightarrow 1,$$

we conclude by Lemma 5.8 that (19) follows from

$$I + 2M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}/2\mathbb{Z}) \subseteq [G(4), G(4)]. \tag{20}$$

To prove (20), fix any $Z \in M_{2\times 2}(\mathbb{Z}_2)$ with $\operatorname{tr} Z \equiv 1 \mod 2$. If we apply Lemma 5.4 with $\ell = 2$, $n = 1$, $X = I$, $Y = Z$, and $D = 0$, then by Lemma 5.5 (varying $C \in M_{2\times 2}^{\mathrm{tr}=0}(\mathbb{Z}_2)$), we see that

$$I + 2\mathcal{N}_Z(\mathbb{Z}/2\mathbb{Z}) = I + 2\left(\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}\right) \subseteq [G(4), G(4)].$$

Now do the same, but with $Z \in M_{2\times 2}(\mathbb{Z}_2)$ lift of $\begin{pmatrix}1&1\\0&1\end{pmatrix} \in GL_2(\mathbb{Z}/2\mathbb{Z})$, concluding that

$$I + 2\begin{pmatrix}1&0\\0&1\end{pmatrix} \in [G(4), G(4)].$$

The containment (20) follows, by dimension considerations. The case $n_\chi = 8$ is done in much the same way.

Case: $n_\chi = 1$

In this case, since χ is trivial, we have $G = \ker\varepsilon$. Since $\ker\varepsilon \mod 2$ is abelian, we have that

$$[G(2), G(2)] = \{1\} \subsetneq \ker\varepsilon \mod 2,$$

but since $(\ker\varepsilon \cap SL_2(\hat{\mathbb{Z}})) \mod 2 = \ker\varepsilon \mod 2$, we see that G cannot be commutator-thick.

□

7. Acknowledgments

Much of the research leading to this paper was done while visiting the Hausdorff Research Institute for Mathematics and subsequently the Max Planck Institute for Mathematics (both in Bonn, Germany). I would like to thank each of these institutes for providing stimulating work environments. I would also like to thank D. Zywina for comments on a previous version.

References

[1] K. Arai, *On uniform lower bound of the Galois images associated to elliptic curves*, Journal de théorie des nombres de Bordeaux, **20** no. 1 (2008), 23–43.

[2] Y. Bilu and P. E. Parent, *Serre's uniformity problem in the split Cartan case*, to appear in Annals of Math (Available at http://arxiv.org/abs/0807.4954).

[3] A. Cojocaru, D. Grant and N. Jones, *Serre curves in one-parameter families*, preprint (Available at http://olemiss.edu/working/ncjones).

[4] C. David and F. Papalardi, *Average frobenius distributions of elliptic curves*, International Math. Research Notices, **4** (1999), 165–183.

[5] D. Grant, *A Formula for the Number of Elliptic Curves with Exceptional Primes*, Compos. Math. **122** (2000), 151–164.

[6] A. Greicius, *Elliptic curves with surjective global Galois representation*, Ph.D. dissertation, University of California at Berkeley (2007).

[7] N. Jones, *A bound for the torsion conductor of a non-CM elliptic curve*, Proceedings of the Amer. Math. Soc. **137** (2009), 37-43.

[8] N. Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), 1547-1570.

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

[10] B. Mazur, *Rational points on modular curves*, in Lecture notes in Math. **601**, Springer, NY 1977, 107–148.

[11] V. Radhakrishnan, *An asymptotic formula for the number of non-Serre curves in a two-parameter family of elliptic curves*, Ph.D. dissertation, University of Colorado at Boulder (2008).

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

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

[14] ———- *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[16] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, preprint. (Available at http://www.math.upenn.edu/∼zywina).