Rigidity in elliptic curve local-global principles

by

JACOB MAYLE (Winston-Salem, NC)

1. Introduction. Let $E$ be an elliptic curve over a number field $K$. For a prime ideal $p \subseteq \mathcal{O}_K$ of good reduction for $E$, we write $E_p$ to denote the reduction of $E$ modulo $p$. We say that a property holds for $E$ locally everywhere if it holds for each reduced elliptic curve $E_p$. Given a property that holds locally everywhere, it is natural to ask if some corresponding property holds globally. If so, such an implication is referred to as a local-global principle.

Two well-known local-global principles address the following questions. Fix a prime number $\ell$.

(A) If $E$ has nontrivial rational $\ell$-torsion locally everywhere, must $E$ have nontrivial rational $\ell$-torsion?

(B) If $E$ admits a rational $\ell$-isogeny locally everywhere, must $E$ admit a rational $\ell$-isogeny?

It turns out that the answer to both of these questions is “no”. For instance, consider the elliptic curves over $\mathbb{Q}$ with LMFDB [14] labels $11.a1$ and $2450.i1$. They are given by the minimal Weierstrass equations

$$E_{11.a1} : y^2 + y = x^3 - x^2 - 7820x - 263580,$$

$$E_{2450.i1} : y^2 + xy = x^3 - x^2 - 107x - 379.$$

These curves provide counterexamples for the above questions. The curve $E_{11.a1}$ has nontrivial rational 5-torsion at every prime of good reduction, but has trivial rational 5-torsion itself. The curve $E_{2450.i1}$ admits a rational 7-isogeny at every prime of good reduction, but does not admit a rational 7-isogeny itself.

2020 Mathematics Subject Classification: Primary 11G05; Secondary 11F80.
Key words and phrases: local-global, elliptic curves, Galois representations.
Received 1 January 2023; revised 7 June 2023.
Published online 18 September 2023.

DOI: 10.4064/aa230101-29-6 [1] © Instytut Matematyczny PAN, 2023
Further analysis of the above counterexamples reveals some structure. One sees that $E_{11.a1}$ is isogenous to an elliptic curve $E'_{11.a1}$ that has nontrivial rational 5-torsion. In addition, the curve $E_{2450.i1}$ admits a 7-isogeny not over $\mathbb{Q}$, but over $\mathbb{Q}(\sqrt{-7})$. With these examples in mind, there is the prospect of powerful local-global principles stemming from questions (A) and (B).

Indeed, Serge Lang proposed and Katz proved a local-global principle that corresponds to (A) and deals more generally with composite level. In its statement below, we write “locally almost everywhere” to mean a mildly relaxed variant of “locally everywhere” in which the corresponding local condition is only asserted to hold for a set of prime ideals of density 1, in the sense of natural density (which we shall define shortly).

**Theorem 1.1 (Katz, 1981 [12]).** Fix an integer $m \geq 2$. If the condition $|E_p(\mathcal{O}_K/p)| \equiv 0 \pmod{m}$ holds locally almost everywhere, then $E$ is $K$-isogenous to an elliptic curve $E'/K$ for which $|E'_{\text{tors}}(K)| \equiv 0 \pmod{m}$.

In fact, we shall only consider the case where $m$ is prime, which dates back to two exercises of Serre [19, pp. I-2 and IV-6]. Much more recently, Sutherland established a local-global principle associated with (B).

**Theorem 1.2 (Sutherland, 2012 [21]).** Fix a prime number $\ell$ for which $\sqrt{\frac{-1}{\ell}} \notin K$. Suppose that the condition that $E_p$ admits an $\mathcal{O}_K/p$-rational $\ell$-isogeny holds locally almost everywhere. Then there exists a quadratic extension $L/K$ such that $E$ admits an $L$-rational $\ell$-isogeny. Further, if $\ell = 2, 3$ or $\ell \equiv 1 \pmod{4}$, then in fact $E$ admits a $K$-rational $\ell$-isogeny.

Sutherland’s result sparked an outpouring of research. Notably, Anni [1] showed that in Theorem 1.2, $L$ may be taken to be $K(\sqrt{-\ell})$ and gave an explicit upper bound (depending on $K$) on the prime numbers $\ell$ for which there exists an elliptic curve $E/K$ that admits a rational $\ell$-isogeny locally everywhere, but not globally. Vogt [23] gave an extension of Sutherland’s result to composite level. Other authors made contributions as well, such as Banwait–Cremona [4] and Etropolski [10]. Recently, there has been increased interest in probabilistic local-global principles [8] and extensions to higher-dimensional abelian varieties [3, 7, 15].

In this paper, we prove that for a given elliptic curve over a number field and prime number $\ell$, a failure of either of the “locally everywhere” conditions of (A) or (B) must be fairly substantial. This phenomenon is a consequence of the properties of the general linear group $\text{GL}_2(\ell)$, as we shall see. Moreover, it contrasts the elliptic curve local-global principles of Katz and Sutherland with, for instance, the familiar local-global principle of Hasse–Minkowski. As an example, consider the equation

$$x^2 + y^2 = 3.$$
It fails to have solutions locally everywhere and hence has no solutions over $\mathbb{Q}$. However, the failure is quite limited. In fact, (1.1) has no solutions over $\mathbb{Q}_2$ or $\mathbb{Q}_3$ but has solutions over $\mathbb{R}$ and $\mathbb{Q}_p$ for each $p \geq 5$.

To discuss this feature of the prime-level local-global principles of Katz and Sutherland more precisely, we fix some standard notation and terminology from algebraic number theory. Let $\mathcal{O}_K$ denote the ring of integers of $K$ and let $\mathcal{P}_K$ denote the set of prime ideals of $\mathcal{O}_K$. For a prime ideal $p \in \mathcal{P}_K$, denote its residue field by $\mathbb{F}_p := \mathcal{O}_K/p$ and its norm by $Np := |\mathbb{F}_p|$. For a subset $\mathcal{A} \subseteq \mathcal{P}_K$ and a positive real number $x$, define

$$\mathcal{A}(x) := \{p \in \mathcal{A} : Np \leq x\}.$$  

The natural density of $\mathcal{A}$ is defined to be the following limit (provided it exists):

$$(1.2) \quad \delta(\mathcal{A}) := \lim_{x \to \infty} \frac{|\mathcal{A}(x)|}{|\mathcal{P}_K(x)|}.$$  

Let $N_E \subseteq \mathcal{O}_K$ be the conductor of $E/K$. The subsets of $\mathcal{P}_K$ that are relevant to our study are the following:

$$(1.3) \quad S_{E,\ell}^1 := \{p \in \mathcal{P}_K : p \nmid N_E \quad \text{and} \quad \text{$E_p$ has an $\mathbb{F}_p$-rational point of order $\ell$}\},$$

$$(1.4) \quad S_{E,\ell} := \{p \in \mathcal{P}_K : p \nmid N_E \quad \text{and} \quad \text{$E_p$ has an $\mathbb{F}_p$-rational isogeny of degree $\ell$}\}.$$  

With these sets defined and the above notation in mind, we now state our main theorem.

**Theorem 1.3.** Let $K$ be a number field, $E/K$ be an elliptic curve, and $\ell$ be a prime number.

1. If there exists a prime ideal $p \subseteq \mathcal{O}_K$ of good reduction for $E$ such that $E_p$ does not have an $\mathbb{F}_p$-rational point of order $\ell$, then $\delta(S_{E,\ell}^1) \leq \frac{3}{4}$.
2. If there exists a prime ideal $p \subseteq \mathcal{O}_K$ of good reduction for $E$ such that $E_p$ does not admit an $\mathbb{F}_p$-rational isogeny of degree $\ell$, then $\delta(S_{E,\ell}) \leq \frac{3}{4}$.

Moreover, if $\ell = 2$, then the quantity $\frac{3}{4}$ may be replaced with $\frac{2}{3}$ in both (1) and (2) above.

We prove this theorem in Section 5 by applying the Chebotarev density theorem and Propositions 5.2 and 5.3, which are purely group-theoretic. We complete the proofs of the two group-theoretic propositions by considering subgroups of $\text{GL}_2(\ell)$ case-by-case in Sections 6 and 7, following Dickson’s well-known classification.

Our result weakens the hypotheses of Theorems 1.1 and 1.2 for each reducing the density at which the local condition of its statement must hold from 1 down to $\frac{3}{4}$ (or $\frac{2}{3}$ in the case of $\ell = 2$). Perhaps more to the point, our result
may be viewed as one about the rigidity of the “locally everywhere” conditions of (A) and (B). Roughly speaking, a collection is termed rigid if its elements are determined by less information than expected. A well-known example is the subset of complex analytic functions among all complex functions. Another example, articulated by Jones [11], is the subset of power maps among all set functions \( K \to K \), for a Galois number field \( K \). In our case, for an odd prime \( \ell \), the two parts of Theorem 1.3 are equivalent to the assertion that (1′) \( E/K \) has nontrivial rational \( \ell \)-torsion locally everywhere if and only if \( \delta(S_{E,\ell}^1) > \frac{3}{4} \), and (2′) \( E/K \) admits a rational \( \ell \)-isogeny locally everywhere if and only if \( \delta(S_{E,\ell}) > \frac{3}{4} \). In this sense, for a number field \( K \) and prime number \( \ell \), the subset of elliptic curves over \( K \) that satisfy the “locally everywhere” condition of (A) (respectively (B)) is rigid among the set of all elliptic curves over \( K \).

The related matter of computing the densities \( \delta(S_{E,\ell}^1) \) and \( \delta(S_{E,\ell}) \) is straightforward in light of [22]. As we shall see, for a given elliptic curve \( E/K \) and prime number \( \ell \), these densities are determined by the image of the mod \( \ell \) Galois representation of \( E \) in \( GL_2(\ell) \). In Section 8, we list the values of \( \delta(S_{E,\ell}^1) \) and \( \delta(S_{E,\ell}) \) corresponding to all 63 of the known (and conjecturally all) mod \( \ell \) Galois images of elliptic curves over the rationals without complex multiplication.

2. Preliminaries on Galois representations. In this section, we recall some basic facts about Galois representations of elliptic curves. Let \( E \) be an elliptic curve over a perfect field \( K \). Let \( \overline{K} \) be an algebraic closure of \( K \) and let \( \ell \) be a prime number.

The \( \ell \)-torsion subgroup of \( E(\overline{K}) \), denoted \( E[\ell] \), is a \( \mathbb{Z}/\ell\mathbb{Z} \)-vector space of rank 2. The absolute Galois group \( G_K := \text{Gal}(\overline{K}/K) \) acts coordinate-wise on \( E[\ell] \). This action is encoded in the group homomorphism

\[
\rho_{E,\ell} : G_K \to \text{Aut}(E[\ell]) \cong GL_2(\ell),
\]

which is known as the mod \( \ell \) Galois representation of \( E \). Here \( GL_2(\ell) \) denotes the general linear group over \( \mathbb{F}_\ell \), and the isomorphism \( \text{Aut}(E[\ell]) \cong GL_2(\ell) \) is determined by a choice of \( \mathbb{Z}/\ell\mathbb{Z} \)-basis of \( E[\ell] \). The mod \( \ell \) Galois image of \( E \), denoted \( G_E(\ell) \), is the image of \( \rho_{E,\ell} \). Because \( \rho_{E,\ell} \) and \( G_E(\ell) \) depend on a choice of basis for \( E[\ell] \), we recognize that we may only speak sensibly of these objects up to conjugation in \( GL_2(\ell) \).

Let \( K(E[\ell]) \) denote the \( \ell \)-division field of \( E \), that is, the Galois extension of \( K \) obtained by adjoining to \( K \) the affine coordinates of the points of \( E[\ell] \). Observe that \( \text{Gal}(\overline{K}/K(E[\ell])) \) is the kernel of \( \rho_{E,\ell} \). Thus, by the first isomorphism theorem and Galois theory,

\[
\tilde{\rho}_{E,\ell} : \text{Gal}(K(E[\ell])/K) \cong G_E(\ell)
\]

is an isomorphism, where \( \tilde{\rho}_{E,\ell} \) is the restriction of \( \rho_{E,\ell} \) to \( \text{Gal}(K(E[\ell])/K) \).
The Galois image $G_E(\ell) \subseteq \text{GL}_2(\ell)$ is of central interest to us since it detects the presence of nontrivial rational $\ell$-torsion of $E$ and rational $\ell$-isogenies admitted by $E$. We shall describe precisely how in the following lemma. First, recall that the Borel subgroup and first Borel subgroup of $\text{GL}_2(\ell)$ are, respectively,

\begin{align*}
B(\ell) &:= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, d \in \mathbb{F}_\ell^\times \text{ and } b \in \mathbb{F}_\ell \right\}, \\
B_1(\ell) &:= \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} : d \in \mathbb{F}_\ell^\times \text{ and } b \in \mathbb{F}_\ell \right\}.
\end{align*}

**Lemma 2.1.** With the notation above,

1. $E$ has nontrivial $K$-rational $\ell$-torsion if and only if $G_E(\ell)$ is conjugate to a subgroup of $B_1(\ell)$,
2. $E$ admits a $K$-rational $\ell$-isogeny if and only if $G_E(\ell)$ is conjugate to a subgroup of $B(\ell)$.

**Proof.** (1) Let $P \in E(K)$ be a point of order $\ell$. Then $P \in E[\ell]$ and we may choose a point $Q \in E[\ell]$ such that $\{P, Q\}$ is a $\mathbb{Z}/\ell\mathbb{Z}$-basis of $E[\ell]$. For each $\sigma \in G_K$, we have

$$\sigma(P) = P \quad \text{and} \quad \sigma(Q) = bP + dQ$$

for some $b, d \in \mathbb{Z}/\ell\mathbb{Z}$ (depending on $\sigma$). Hence,

$$\rho_{E,\ell}(\sigma) = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in B_1(\ell).$$

Thus $G_E(\ell) \subseteq B_1(\ell)$, with respect to the basis $\{P, Q\}$.

Conversely, assume that $G_E(\ell)$ is conjugate to a subgroup of $B_1(\ell)$. Let $\{P, Q\}$ be a $\mathbb{Z}/\ell\mathbb{Z}$-basis of $E[\ell]$ that realizes $G_E(\ell) \subseteq B_1(\ell)$. Then $\sigma(P) = P$ for each $\sigma \in G_K$, so $P \in E(K)$. Thus $P$ is a nontrivial $K$-rational $\ell$-torsion point of $E$.

(2) Let $\phi : E \to E'$ be a $K$-rational $\ell$-isogeny. Then ker $\phi \subseteq E(K)$ is cyclic of order $\ell$. Let $P$ be a generator of ker $\phi$. Then $P \in E[\ell]$ and we may choose a point $Q \in E[\ell]$ such that $\{P, Q\}$ is a $\mathbb{Z}/\ell\mathbb{Z}$-basis of $E[\ell]$. For each $\sigma \in G_K$, we have

$$\sigma(P) = aP \quad \text{and} \quad \sigma(Q) = bP + dQ$$

for some $a, b, d \in \mathbb{Z}/\ell\mathbb{Z}$ (depending on $\sigma$). Hence,

$$\rho_{E,\ell}(\sigma) = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B(\ell).$$

Thus $G_E(\ell) \subseteq B(\ell)$, with respect to the basis $\{P, Q\}$. 

Conversely, assume that $G_E(\ell)$ is conjugate to a subgroup of $\mathcal{B}(\ell)$. Let \{P, Q\} be a $\mathbb{Z}/\ell\mathbb{Z}$-basis of $E[\ell]$ that realizes $G_E(\ell) \subseteq \mathcal{B}(\ell)$. Let $\Phi$ denote the subgroup of $E(K)$ generated by $P$. Then $\Phi$ is cyclic of order $\ell$, so the natural isogeny $E \to E/\Phi$ is a $K$-rational $\ell$-isogeny of $E$. \hfill \Box

3. Preliminaries on $\text{GL}_2(\ell)$. Let $\ell$ be an odd prime number. The main objective of this section is to state two important classification results for $\text{GL}_2(\ell)$: the classification of its subgroups (originally due to Dickson) and the classification of its conjugacy classes. We start by recalling some standard notation and terminology.

We write $\mathcal{Z}(\ell)$ to denote the center of $\text{GL}_2(\ell)$, which consists precisely of the scalar matrices of $\text{GL}_2(\ell)$. The \textit{projective linear group} over $\mathbb{F}_\ell$ is the quotient $\text{PGL}_2(\ell) := \text{GL}_2(\ell)/\mathcal{Z}(\ell)$, and $\pi : \text{GL}_2(\ell) \twoheadrightarrow \text{PGL}_2(\ell)$ denotes the quotient map. We denote the image of a matrix $\gamma \in \text{GL}_2(\ell)$ in $\text{PGL}_2(\ell)$ by $\overline{\gamma}$. Similarly, we denote the image of a subset $S \subseteq \text{GL}_2(\ell)$ in $\text{PGL}_2(\ell)$ by $\overline{S}$. In particular, the \textit{projective special linear group} over $\mathbb{F}_\ell$ is $\text{PSL}_2(\ell) := \text{SL}_2(\ell)$, where $\text{SL}_2(\ell)$ denotes the special linear group over $\mathbb{F}_\ell$.

The \textit{split Cartan subgroup} of $\text{GL}_2(\ell)$ and its normalizer are, respectively,
\[
\mathcal{C}_s(\ell) := \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{F}_\ell^\times \right\} \quad \text{and} \quad \mathcal{C}_s^+(\ell) := \mathcal{C}_s(\ell) \cup \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mathcal{C}_s(\ell).
\]

Fix a nonsquare $\varepsilon \in \mathbb{F}_\ell^\times \setminus \mathbb{F}_\ell^{\times 2}$. The \textit{nonsplit Cartan subgroup} of $\text{GL}_2(\ell)$ and its normalizer are, respectively,
\[
\mathcal{C}_{ns}(\ell) := \left\{ \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_\ell \text{ and } (a, b) \neq (0, 0) \right\},
\]
\[
\mathcal{C}_{ns}^+(\ell) := \mathcal{C}_{ns}(\ell) \cup \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mathcal{C}_{ns}(\ell).
\]

Note that different choices of $\varepsilon \in \mathbb{F}_\ell^\times \setminus \mathbb{F}_\ell^{\times 2}$ give rise to conjugate subgroups, so the conjugacy classes of $\mathcal{C}_{ns}(\ell)$ and $\mathcal{C}_{ns}^+(\ell)$ in $\text{GL}_2(\ell)$ are well-defined.

The Borel subgroup $\mathcal{B}(\ell)$ was defined in \cite[2.1]{2}. Also, let $A_n$ and $S_n$ denote the alternating group and symmetric group, respectively, on $n$ elements. With notation set, we now state Dickson’s classification \cite[9]{6}.

**Proposition 3.1.** Let $\ell$ be an odd prime and $G \subseteq \text{GL}_2(\ell)$ be a subgroup. If $\ell$ does not divide $|G|$, then

\begin{align*}
\text{Cs}: \quad & G \text{ is conjugate to a subgroup of } \mathcal{C}_s(\ell); \\
\text{Cn}: \quad & G \text{ is conjugate to a subgroup of } \mathcal{C}_{ns}(\ell), \text{ but not of } \mathcal{C}_s(\ell); \\
\text{Ns}: \quad & G \text{ is conjugate to a subgroup of } \mathcal{C}_s^+(\ell), \text{ but not of } \mathcal{C}_s(\ell) \text{ or } \mathcal{C}_{ns}(\ell); \\
\text{Nn}: \quad & G \text{ is conjugate to a subgroup of } \mathcal{C}_{ns}(\ell), \text{ but not of } \mathcal{C}_s^+(\ell) \text{ or } \mathcal{C}_{ns}(\ell); \\
\text{A4}: \quad & \overline{G} \text{ is isomorphic to } A_4;
\end{align*}
S4: $G$ is isomorphic to $S_4$; or
A5: $G$ is isomorphic to $A_5$.

If $\ell$ divides $|G|$, then

- **B:** $G$ is conjugate to a subgroup of $B(\ell)$, but not of $C_s(\ell)$;
- **SL:** $G$ equals $\text{PSL}_2(\ell)$; or
- **GL:** $G$ equals $\text{PGL}_2(\ell)$.

**Proof.** See, for instance, [20, Section 2]. □

A subgroup $G \subseteq \text{GL}_2(\ell)$ has type $Cs, Cn, Ns$, etc. according to its position in the classification.

Eigenvalues will play a central role in our study. For a matrix $\gamma \in \text{GL}_2(\ell)$ we shall, in particular, be interested only in the eigenvalues of $\gamma$ that lie in $F_\ell$. The existence of such eigenvalues may be detected by the discriminant of $\gamma$, by which we mean the discriminant of the characteristic polynomial of $\gamma$:

$$\Delta(\gamma) := \text{disc}(\det(\gamma - xI)) = (\text{tr} \gamma)^2 - 4 \det \gamma.$$

Further, define the quadratic character $\chi : \text{GL}_2(\ell) \rightarrow \{0, \pm 1\}$ by

$$\chi(\gamma) := \left( \frac{\Delta(\gamma)}{\ell} \right),$$

where $\left( \cdot \right)$ denotes the Legendre symbol. Now since $\gamma$ has an eigenvalue in $F_\ell$ if and only if its characteristic polynomial splits over $F_\ell$, we see that

$$\gamma \text{ has an eigenvalue in } F_\ell \iff \chi(\gamma) \neq -1.$$

The conjugacy classes of $\text{GL}_2(\ell)$ are well-known (see, e.g., [13, XVIII, Section 12] or [22, Table 1]). In Table 1, we list the conjugacy classes of $\text{GL}_2(\ell)$ with the associated values of det, tr, $\chi$, and rational eigenvalues.

**Table 1.** Conjugacy classes of $\text{GL}_2(\ell)$ (“R.e.” stands for “Rational eigenvalues”)

<table>
<thead>
<tr>
<th>Representative of class</th>
<th>No. of classes</th>
<th>Size of class</th>
<th>det</th>
<th>tr</th>
<th>$\chi$</th>
<th>R.e.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\begin{pmatrix} a &amp; 0 \ 0 &amp; a \end{pmatrix}$</td>
<td>$0 &lt; a &lt; \ell$</td>
<td>$\ell - 1$</td>
<td>$1$</td>
<td>$a^2$</td>
<td>$2a$</td>
<td>$0$</td>
</tr>
<tr>
<td>$\begin{pmatrix} a &amp; 1 \ 0 &amp; a \end{pmatrix}$</td>
<td>$0 &lt; a &lt; \ell$</td>
<td>$\ell - 1$</td>
<td>$(\ell + 1)(\ell - 1)$</td>
<td>$a^2$</td>
<td>$2a$</td>
<td>$0$</td>
</tr>
<tr>
<td>$\begin{pmatrix} a &amp; 0 \ 0 &amp; b \end{pmatrix}$</td>
<td>$0 &lt; a &lt; b &lt; \ell$</td>
<td>$\frac{1}{2}(\ell - 1)(\ell - 2)$</td>
<td>$\ell(\ell + 1)$</td>
<td>$ab$</td>
<td>$a + b$</td>
<td>$1$</td>
</tr>
<tr>
<td>$\begin{pmatrix} a &amp; \varepsilon b \ b &amp; a \end{pmatrix}$</td>
<td>( \begin{cases} 0 \leq a &lt; \ell \ 0 &lt; b \leq \frac{\ell - 1}{2} \end{cases} )</td>
<td>$\frac{1}{2}\ell(\ell - 1)$</td>
<td>$\ell(\ell - 1)$</td>
<td>$a^2 - \varepsilon b^2$</td>
<td>$2a$</td>
<td>$-1$</td>
</tr>
</tbody>
</table>

4. **Reduction to group theory.** In this section, we use Lemma 2.1 and the Chebotarev density theorem to reduce our problem from one of
arithmetic geometry to one of group theory. Let \( \ell \) be a prime number and define the following subsets of \( \text{GL}_2(\mathbb{F}_\ell) \):

\[
I_1(\ell) := \{ \gamma \in \text{GL}_2(\mathbb{F}_\ell) : \gamma \text{ has 1 as an eigenvalue} \},
\]

\[
I(\ell) := \{ \gamma \in \text{GL}_2(\mathbb{F}_\ell) : \gamma \text{ has some eigenvalue in } \mathbb{F}_\ell \}.
\]

We record a quick observation that connects the sets \( I_1(\ell) \) and \( I(\ell) \) with the subgroups \( B_1(\ell) \) and \( B(\ell) \).

**Lemma 4.1.** Let \( G \subseteq \text{GL}_2(\mathbb{F}_\ell) \) be a cyclic subgroup and let \( \gamma \) be a generator of \( G \). Then

1. \( G \) is conjugate to a subgroup of \( B_1(\ell) \) if and only if \( \gamma \in I_1(\ell) \),
2. \( G \) is conjugate to a subgroup of \( B(\ell) \) if and only if \( \gamma \in I(\ell) \).

**Proof.** (1) Suppose \( G \) is conjugate to a subgroup of \( B_1(\ell) \). Then \( \gamma \) is, in particular, conjugate to some matrix in \( B_1(\ell) \). Thus, since eigenvalues are invariant under conjugation, 1 is an eigenvalue of \( \gamma \), and so \( \gamma \in I_1(\ell) \). Conversely, assume that \( \gamma \in I_1(\ell) \). As 1 is an eigenvalue of \( \gamma \), it must be that \( \gamma \) is conjugate to some matrix in \( B_1(\ell) \). Hence \( G \), being generated by \( \gamma \), is conjugate to a subgroup of \( B_1(\ell) \).

(2) This follows similarly to (1). ■

For a subgroup \( G \subseteq \text{GL}_2(\mathbb{F}_\ell) \), we define the proportions

\[
\mathcal{F}_1(G) := \frac{|G \cap I_1(\ell)|}{|G|} \quad \text{and} \quad \mathcal{F}(G) := \frac{|G \cap I(\ell)|}{|G|}.
\]

In words, \( \mathcal{F}_1(G) \) is the proportion of matrices in \( G \) that have 1 as an eigenvalue, and \( \mathcal{F}(G) \) is the proportion of matrices in \( G \) that have some eigenvalue in \( \mathbb{F}_\ell \). In the translation of our problem to group theory, \( \mathcal{F}_1(G) \) and \( \mathcal{F}(G) \) become the central objects of study. We describe precisely how in the next proposition, but first we set up some preliminaries for its proof.

Let \( L/K \) be a finite extension of number fields. Given a prime ideal \( p \in P_K \) that is unramified in \( L/K \), we write \( \text{Frob}_p \in \text{Gal}(L/K) \) to denote the Frobenius element associated with \( p \), which is defined up to conjugation. For a conjugation-stable subset \( C \subseteq \text{Gal}(L/K) \), the Chebotarev density theorem states that

\[
\delta(\{ p \in P_K : p \text{ is unramified in } L/K \text{ and } \text{Frob}_p \in C \}) = \frac{|C|}{|\text{Gal}(L/K)|}.
\]

For an elliptic curve \( E \) over a number field \( K \) and a prime number \( \ell \), we define the set of bad prime ideals:

\[
\mathcal{D}_{E,\ell} := \{ p \in P_K : p \text{ is ramified in } K(E[\ell])/K \text{ or } p \mid N_E \}.
\]

Let \( p \in P_K \setminus \mathcal{D}_{E,\ell} \) be a good prime and let \( E_p \) denote the reduction of \( E \) at \( p \). As \( K(E[\ell])/K \) is unramified at \( p \), we may consider a Frobenius element \( \text{Frob}_p \in \text{Gal}(K(E[\ell])/K) \). The Galois group \( \text{Gal}(\mathbb{F}_p(E_p[\ell])/\mathbb{F}_p) \) is a finite
cyclic group, generated by the image of Frobp. Thus GEp(ℓ) is the cyclic group generated by \( \tilde{\rho}_{E,\ell}(\text{Frob}_p) \), up to conjugation in GL\(_2\)(ℓ).

**Proposition 4.2.** Let \( K \) be a number field, \( E/K \) be an elliptic curve, and \( \ell \) be a prime number. Write \( G_E(\ell) \) to denote the mod \( \ell \) Galois image of \( E \). Let \( S_{E,\ell}^1 \) and \( S_{E,\ell} \) be as defined in (1.3) and (1.4). Then

\[
\delta(S_{E,\ell}^1) = F_1(G_E(\ell)) \quad \text{and} \quad \delta(S_{E,\ell}) = F(G_E(\ell)).
\]

**Proof.** We define two conjugation-stable subsets of \( \text{Gal}(K(E[\ell])/K) \):

\[
\mathcal{C}_{E,\ell}^1 := \{ \sigma \in \text{Gal}(K(E[\ell])/K) : \tilde{\rho}_{E,\ell}(\sigma) \in \mathcal{T}_1(\ell) \},
\]

\[
\mathcal{C}_{E,\ell} := \{ \sigma \in \text{Gal}(K(E[\ell])/K) : \tilde{\rho}_{E,\ell}(\sigma) \in \mathcal{I}(\ell) \}.
\]

In addition, we define two subsets of \( \mathcal{P}_K \):

\[
\mathcal{T}_{E,\ell}^1 := \{ p \in \mathcal{P}_K : p \text{ is unramified in } K(E[\ell])/K \text{ and } \text{Frob}_p \in \mathcal{C}_{E,\ell}^1 \},
\]

\[
\mathcal{T}_{E,\ell} := \{ p \in \mathcal{P}_K : p \text{ is unramified in } K(E[\ell])/K \text{ and } \text{Frob}_p \in \mathcal{C}_{E,\ell} \}.
\]

By Lemmas 2.1 and 4.1, the sets \( S_{E,\ell}^1 \) (resp. \( S_{E,\ell} \)) and \( T_{E,\ell}^1 \) (resp. \( T_{E,\ell} \)) agree up to the finite set of bad primes \( D_{E,\ell} \). Thus, in particular,

\[
\delta(S_{E,\ell}^1) = \delta(T_{E,\ell}^1) \quad \text{and} \quad \delta(S_{E,\ell}) = \delta(T_{E,\ell}).
\]

Now applying the Chebotarev density theorem to \( T_{E,\ell}^1 \) and \( T_{E,\ell} \), we find that

\[
\delta(T_{E,\ell}^1) = \frac{|C_{E,\ell}^1|}{|\text{Gal}(K(E[\ell])/K)|} = \frac{|G_E(\ell) \cap \mathcal{T}_1(\ell)|}{|G_E(\ell)|} = F_1(G_E(\ell)),
\]

\[
\delta(T_{E,\ell}) = \frac{|C_{E,\ell}|}{|\text{Gal}(K(E[\ell])/K)|} = \frac{|G_E(\ell) \cap \mathcal{I}(\ell)|}{|G_E(\ell)|} = F(G_E(\ell)).
\]

Combining these with (4.1) completes the proof. \( \blacksquare \)

5. Group-theoretic propositions and proof of main theorem.

Proposition 4.2 offers us a bridge between the realms of arithmetic geometry and group theory. Given it, our main objects of study are now \( F_1(G) \) and \( F(G) \). Explicitly, our goal is to show that as \( G \) varies among all subgroups of GL\(_2\), these proportions never take on a value in the open interval \( \left( \frac{2}{3}, 1 \right) \) when \( \ell \) is an odd prime and in \( \left( \frac{2}{3}, 1 \right) \) when \( \ell = 2 \). We start with \( \ell = 2 \), simply proceeding “by hand” in this case.

**Remark 5.1.** By inspection of each of the six matrices of GL\(_2\), we find that

\[
\mathcal{I}(2) = \mathcal{I}(2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}.
\]

Given this, we now compute \( F_1(G) \) and \( F(G) \) for each of the six subgroups of GL\(_2\), recording our results in Table 2. From the table, we observe that
if $F_1(G) \neq 1$ (resp. $F(G) \neq 1$), then $F_1(G) \leq \frac{2}{3}$ (resp. $F(G) \leq \frac{2}{3}$).

<table>
<thead>
<tr>
<th>Subgroup $G$</th>
<th>$F_1(G)$</th>
<th>$F(G)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>${(\frac{1}{0}, \frac{0}{1})}$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>${(\frac{1}{0}, \frac{0}{1}), (\frac{0}{1}, \frac{1}{0})}$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>${(\frac{1}{0}, \frac{1}{1}), (\frac{0}{1}, \frac{1}{0})}$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>${(\frac{1}{0}, \frac{1}{1}), (\frac{1}{1}, \frac{1}{1})}$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>${(\frac{1}{0}, \frac{1}{1}), (\frac{1}{1}, \frac{0}{1}), (\frac{0}{1}, \frac{1}{1})}$</td>
<td>$\frac{1}{3}$</td>
<td>$\frac{1}{3}$</td>
</tr>
<tr>
<td>$GL_2(2)$</td>
<td>$\frac{2}{3}$</td>
<td>$\frac{2}{3}$</td>
</tr>
</tbody>
</table>

We now state our main group-theoretic propositions, which we shall prove in Sections 6 and 7. The first proposition concerns $F(G)$.

**Proposition 5.2.** Let $\ell$ be an odd prime and $G \subseteq GL_2(\ell)$ be a subgroup. We have

$$F(G) = \begin{cases} 
1 & \text{if } G \text{ is of type Cs or B,} \\
\frac{1}{|G|} & \text{if } G \text{ is of type Cn}, \\
\frac{\ell+3}{2(\ell+1)} & \text{if } G \text{ is of type SL}, \\
\frac{\ell+2}{2(\ell+1)} & \text{if } G \text{ is of type GL},
\end{cases}$$

and

$$F(G) \in \left\{ \begin{array}{l}
\{\frac{1}{2}, \frac{3}{4}, 1\} & \text{if } G \text{ is of type Ns}, \\
\{\frac{1}{|G|}, \frac{1}{4} + \frac{1}{|G|}, \frac{1}{2} + \frac{1}{|G|}\} & \text{if } G \text{ is of type Nn}, \\
\{\frac{1}{12}, \frac{7}{8}, \frac{3}{4}, 1\} & \text{if } G \text{ is of type A4}, \\
\{\frac{1}{24}, \frac{7}{8}, \frac{3}{5}, \frac{5}{2}, \frac{3}{4}, 1\} & \text{if } G \text{ is of type S4}, \\
\{\frac{1}{60}, \frac{4}{15}, \frac{7}{20}, \frac{5}{12}, \frac{3}{5}, \frac{3}{4}, 1\} & \text{if } G \text{ is of type A5}.
\end{array} \right\}$$

Further, if $G$ is of type Cn, Nn, SL, or GL, then $F(G) \leq \frac{3}{4}$. In all cases, if $F(G) \neq 1$, then $F(G) \leq \frac{3}{4}$.

**Proof.** This result is the combination of Lemmas 6.2, 6.3, 6.5, 6.6, 6.7, 6.8, 6.10, 6.11, 6.12, and Remark 6.9.

Next is our group-theoretic proposition about $F_1(G)$. A quick observation reduces the number of cases that we must consider. Because $I_1(\ell) \subseteq I(\ell)$, we have $F_1(G) \leq F(G)$. Since $F(G) \leq \frac{2}{3}$ by the above proposition when $G$ is of type Cn, Nn, SL, or GL, we already know that $F_1(G) \leq \frac{3}{4}$ for each of these types. Thus in the following proposition, we need only consider subgroups of type Cs, Ns, B, A4, S4, and A5.
Proposition 5.3. Let $\ell$ be an odd prime and $G \subseteq \text{GL}_2(\ell)$ be a subgroup. If $\mathcal{F}_1(G) \neq 1$, then
\[
\mathcal{F}_1(G) \leq \begin{cases} 
\frac{1}{2} + \frac{1}{|G|} & \text{if } G \text{ is of type } Cs \text{ or } Ns, \\
\frac{1}{2} + \frac{\ell}{|G|} & \text{if } G \text{ is of type } B, \\
\frac{3}{4} & \text{if } G \text{ is of type } A_4, S_4, \text{ or } A_5,
\end{cases}
\]
In all cases, if $\mathcal{F}_1(G) \neq 1$, then $\mathcal{F}_1(G) \leq \frac{3}{4}$.

Proof. This result is the combination of Lemmas 7.2, 7.4, 7.5, 7.7, 7.9, 7.10, and Remark 7.6.

The work carried out in Sections 6 and 7 completes the proofs of the above propositions. We now prove our main theorem, given the two propositions.

Proof of Theorem 1.3. We prove part (1), noting that (2) follows in the same way. Suppose that the condition that $E$ has nontrivial rational $\ell$-torsion locally everywhere fails. Let $p \in \mathcal{P}_K$ be a prime ideal of good reduction for $E$ with the property that the reduction $E_p$ has trivial $F_p$-rational $\ell$-torsion. Then, by Lemma 2.1, the group $G_E(p) \subseteq \text{GL}_2(\ell)$ is not conjugate to a subgroup of $B_1(\ell)$. Thus by Lemma 4.1(1), we have $\tilde{\rho}_{E,\ell}(\text{Frob}_p) \not\in I_1(\ell)$. As a result, $G_E(\ell) \cap I_1(\ell)$ is a proper subset of $G_E(\ell)$, and so $\mathcal{F}_1(G_E(\ell)) \neq 1$. Thus if $\ell$ is an odd prime, then by Propositions 4.2 and 5.3, we have $\delta(S_{E,\ell}) = \mathcal{F}_1(G_E(\ell)) \leq \frac{3}{4}$. If $\ell = 2$, then Remark 5.1 gives $\mathcal{F}_1(G) \leq \frac{2}{3}$ and hence $\delta(S_{E,\ell}) \leq \frac{2}{3}$.

6. Proof of Proposition 5.2. In this section, we prove the lemmas that are referenced in our proof of Proposition 5.2. We begin with several observations that will be useful at times. From here on, $\ell$ denotes an odd prime number.

Lemma 6.1.
1. For $\gamma \in \text{GL}_2(\ell)$, we have $\gamma \in I(\ell)$ if and only if $\chi(\gamma) \neq -1$, where $\chi$ is defined in (3.1).
2. For $\gamma \in \text{GL}_2(\ell)$, we have $\gamma \in I(\ell)$ if and only if $\gamma^2 \in I(\ell) \setminus \mathbb{Z}_{nr}(\ell)$, where $\mathbb{Z}_{nr}(\ell) := \{(a \ 0 \\ 0 \ a) : a \in F_{\ell}^* \setminus F_{\ell}^{\times 2}\}$.
3. For $\gamma_1, \gamma_2 \in \text{GL}_2(\ell)$, if $\gamma_1$ is conjugate to $\gamma_2$ in $\text{PGL}_2(\ell)$, then $\gamma_1 \in I(\ell)$ if and only if $\gamma_2 \in I(\ell)$.
4. For a subgroup $G \subseteq \text{GL}_2(\ell)$, we have
\[
\mathcal{F}(G) = \frac{|G \cap I(\ell)|}{|G|}.
\]
5. For subgroups $G_1, G_2 \subseteq \text{GL}_2(\ell)$, if $\overline{G}_1$ is conjugate to $\overline{G}_2$ in $\text{PGL}_2(\ell)$, then $\mathcal{F}(G_1) = \mathcal{F}(G_2)$. In particular, if $G_1$ and $G_2$ are conjugate in $\text{GL}_2(\ell)$, then $\mathcal{F}(G_1) = \mathcal{F}(G_2)$. 
Proof. (1) We have already seen this in \([3.2]\).

(2) Suppose that \(\gamma \in I(\ell)\) and that \(\lambda \in \mathbb{F}_\ell\) is an eigenvalue of \(\gamma\). Then \(\lambda^2 \in \mathbb{F}_\ell\) is an eigenvalue of \(\gamma^2\), so \(\gamma^2 \in I(\ell)\). Now note that if \(\gamma^2 \in Z_{nr}(\ell)\), then as \(\lambda^2\) is an eigenvalue, we must have \(\gamma^2 = \begin{pmatrix} \lambda^2 & 0 \\ 0 & \lambda^2 \end{pmatrix} \notin Z_{nr}(\ell)\). We now prove the converse via its contrapositive. Suppose that \(\gamma \notin I(\ell)\). From the classification of conjugacy classes of \(GL_2(\ell)\) given in Table 1, we see that \(\gamma\) is conjugate in \(GL_2(\ell)\) to a matrix of the form \(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\) for some \(a \in \mathbb{F}_\ell\) and \(b \in \mathbb{F}_\ell^\times\). Thus \(\gamma^2\) is conjugate to \(\begin{pmatrix} a^2 + b^2 & 2ab \\ 2ab & a^2 + b^2 \end{pmatrix}\) and we may calculate

\[
\chi(\gamma^2) = \left(\frac{2(a^2 + b^2) - 4(a^2 - b^2)^2}{\ell}\right) = \left(\frac{16a^2b^2}{\ell}\right) = \left(\frac{a}{\ell}\right)^2.
\]

If \(a \neq 0\), then \(\chi(\gamma^2) = -1\) so \(\gamma^2 \notin I(\ell)\) and we are done. On the other hand, if \(a = 0\), then \(\gamma^2\) is conjugate, and hence equal, to the scalar matrix \(\begin{pmatrix} b^2 & 0 \\ 0 & b^2 \end{pmatrix}\) \(\in Z_{nr}(\ell)\) and we are done as well.

(3) Since \(\overline{\gamma}_1\) is conjugate to \(\overline{\gamma}_2\) in \(PGL_2(\ell)\), we have \(\gamma_0\gamma_1\gamma_0^{-1} = \alpha\gamma_2\) for some \(\alpha \in \mathbb{F}_\ell^\times\) and \(\gamma_0 \in GL_2(\ell)\). In particular, \(\gamma_1\) has an eigenvalue in \(\mathbb{F}_\ell\) if and only if \(\gamma_2\) has an eigenvalue in \(\mathbb{F}_\ell\).

(4) In this part, we abuse notation to let \(\pi : G \to \overline{G}\) denote the restriction of \(GL_2(\ell) \to PGL_2(\ell)\) to \(G\). It follows from (3) that for a matrix \(\gamma\), either \(\pi^{-1}(\gamma) \subseteq I(\ell)\) or \(\pi^{-1}(\gamma) \cap I(\ell) = \emptyset\) according to whether \(\gamma \in I(\ell)\) or not. In addition, \(|\pi^{-1}(\gamma)| = |\ker \pi| = |G|/|\overline{G}|\). With these observations, we calculate

\[
\mathcal{F}(G) = \frac{1}{|G|} \sum_{\gamma \in G \cap I(\ell)} |\pi^{-1}(\gamma)| = \frac{1}{|\overline{G}|} \sum_{\gamma \in G \cap I(\ell)} 1 = \frac{|G \cap I(\ell)|}{|\overline{G}|}.
\]

(5) This follows from (3) and (4). \(\square\)

We now proceed case-by-case along Dickson’s classification of subgroups of \(GL_2(\ell)\). Throughout, \(G\) denotes a subgroup of \(GL_2(\ell)\). By Lemma 6.1(5), the value of \(\mathcal{F}(G)\) is invariant on conjugating \(G\) in \(GL_2(\ell)\). Thus if \(G\) is of type \(B\), \(C_s\), \(C_n\), \(N_s\), \(N_n\), or \(\mathcal{B}\), it suffices to assume that \(G\) itself is contained in \(C_s(\ell)\), \(C_{ns}(\ell)\), \(C_{ns}^+(\ell)\) but not \(C_s(\ell)\), \(C_{ns}^+(\ell)\) but not \(C_{ns}(\ell)\), or \(\mathcal{B}(\ell)\), respectively. If \(G\) is of type \(SL\) or \(GL\), it suffices to assume that \(G\) is equal to \(SL_2(\ell)\) or \(GL_2(\ell)\), respectively. When \(G\) is of one of the types mentioned in this paragraph, we shall make the appropriate assumption listed here without further mention.

6.1. Cartan and Borel subgroups

Lemma 6.2. If \(G\) is of type \(C_s\) or \(B\), then \(\mathcal{F}(G) = 1\).

Proof. This follows immediately since a matrix of the form \(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\) has eigenvalues \(a, d \in \mathbb{F}_\ell\). \(\square\)

Lemma 6.3. If \(G\) is of type \(C_n\), then \(\mathcal{F}(G) = 1/|\overline{G}|\).
Proof. For a matrix \( \gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C_{ns}(\ell) \), we calculate
\[
\chi(\gamma) = \left( \frac{(2a)^2 - 4(a^2 - b^2\varepsilon)}{\ell} \right) = \left( \frac{4b^2\varepsilon}{\ell} \right) = - \left( \frac{b}{\ell} \right)^2.
\]
Thus \( \gamma \in \mathcal{I}(\ell) \) if and only if \( b = 0 \). Hence \( C_{ns}(\ell) \cap \mathcal{I}(\ell) = \mathcal{Z}(\ell) \), and so
\[
\text{(6.1)} \quad \mathcal{G} \cap \mathcal{I}(\ell) = \mathcal{G} \cap \mathcal{Z}(\ell).
\]
Consequently, \( \mathcal{G} \cap \mathcal{I}(\ell) \subseteq \mathcal{Z}(\ell) = \{ \mathcal{T} \} \) so Lemma 6.1(4) gives \( \mathcal{F}(\mathcal{G}) = \frac{1}{|\mathcal{G}|} \). ■

6.2. Normalizers of Cartan subgroups. Here we first prove a straightforward auxiliary lemma.

Lemma 6.4. If \( \gamma \in C_s(\ell) \) (resp. \( \gamma \in C_{ns}(\ell) \)) and \( \gamma_0 \in C_s^+(\ell) \setminus C_s(\ell) \) (resp. \( \gamma_0 \in C_{ns}^+(\ell) \setminus C_{ns}(\ell) \)), then
\[
\Delta(\gamma \gamma_0) = \det(\gamma)\Delta(\gamma_0).
\]

Proof. For given matrices \( \gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C_s(\ell), \gamma_0 := \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \in C_s^+(\ell) \setminus C_s(\ell), \) we calculate
\[
\Delta(\gamma \gamma_0) = 4abcd = \det(\gamma)\Delta(\gamma_0).
\]
Next, for given matrices \( \gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C_{ns}(\ell), \gamma_0 := \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \in C_{ns}^+(\ell) \setminus C_{ns}(\ell), \) we calculate
\[
\Delta(\gamma \gamma_0) = 4(a^2 - b^2\varepsilon)(c^2 - d^2\varepsilon) = \det(\gamma)\Delta(\gamma_0). \quad \blacksquare
\]

Lemma 6.5. If \( G \) is of type \( \mathbb{N}_s \), then \( \mathcal{F}(G) \in \{ \frac{1}{2}, \frac{3}{4}, 1 \} \).

Proof. Write \( G_c := G \cap C_s(\ell) \) and \( G_n := G \setminus G_c \). We are assuming that \( G_n \neq \emptyset \), so we may fix a matrix \( \gamma_0 \in G_n \). Right multiplication by \( \gamma_0 \) gives a bijection \( G_c \to G_n \). Thus \( |G_c| = |G_n| = \frac{1}{2}|G| \) and in fact
\[
G_n = \{ \gamma \gamma_0 : \gamma \in G_c \}.
\]
Hence, by Lemmas 6.1(1) and 6.4 we have
\[
|G_n \cap \mathcal{I}(\ell)| = \left| \left\{ \gamma \gamma_0 : \gamma \in G_c \text{ and } \chi(\gamma \gamma_0) \neq -1 \right\} \right|
= \left\{ \gamma \gamma_0 : \gamma \in G_c \text{ and } \left( \frac{\det(\gamma)}{\ell} \right) = \chi(\gamma_0) \right\}.
\]
Noting that \( \chi(\gamma_0) \) is fixed and \( \left( \frac{\det(\gamma)}{\ell} \right) : G_c \to \{ \pm 1 \} \) is a homomorphism, we find that
\[
|G_n \cap \mathcal{I}(\ell)| = \left| \left\{ \gamma \in G_c : \left( \frac{\det(\gamma)}{\ell} \right) = \chi(\gamma_0) \right\} \right|
= \left\{ 0, \frac{1}{2}|G_c|, |G_c| \right\} = \left\{ 0, \frac{1}{4}|G|, \frac{1}{2}|G| \right\}.
\]
Therefore
\[
\mathcal{F}(G) = \frac{|G_c \cap \mathcal{I}(\ell)| + |G_n \cap \mathcal{I}(\ell)|}{|G|} = \frac{1}{2}|G| + \frac{|G_n \cap \mathcal{I}(\ell)|}{|G|} \in \left\{ \frac{1}{2}, \frac{3}{4}, 1 \right\}. \quad \blacksquare
\]
Lemma 6.6. If \( G \) is of type \( \mathbb{N}n \), then \( \mathcal{F}(G) \in \{ \frac{1}{|G|}, \frac{1}{4} + \frac{1}{|G|}, \frac{1}{2} + \frac{1}{|G|} \} \).

Proof. Write \( G_c := G \cap \mathcal{C}_{ns}(\ell) \) and \( G_n := G \setminus G_c \). We note that by (6.1),

\[
|G_c \cap \mathcal{I}(\ell)| = |G \cap \mathcal{I}(\ell)| = \frac{|G|}{|G|}.
\]

Since \( G_n \neq \emptyset \), we may fix a matrix \( \gamma_0 \in G_n \). Right multiplication by \( \gamma_0 \) gives a bijection \( G_c \to G_n \). Thus \( |G_c| = |G_n| = \frac{1}{2}|G| \) and \( G_n = \{ \gamma \gamma_0 : \gamma \in G_c \} \).

As in the preceding proof, Lemmas 6.1(1) and 6.4 show

\[
G_n \cap \mathcal{I}(\ell) = \{ \gamma \gamma_0 : \gamma \in G_c \text{ and } \left( \frac{\det \gamma}{\ell} \right) = \chi(\gamma_0) \}.
\]

Noting that \( \chi(\gamma_0) \) is fixed and \( \left( \frac{\det(\cdot)}{\ell} \right) : G_c \to \{ \pm 1 \} \) is a homomorphism, we find that

\[
|G_n \cap \mathcal{I}(\ell)| = \left| \left\{ \gamma \gamma_0 : \gamma \in G_c, \left( \frac{\det \gamma}{\ell} \right) = \chi(\gamma_0) \right\} \right|/\frac{1}{2}|G_c| = \frac{1}{4} |G| / \frac{1}{2} |G|.
\]

Combining (6.2) and (6.3), we obtain

\[
\mathcal{F}(G) = \frac{|G_c \cap \mathcal{I}(\ell)| + |G_n \cap \mathcal{I}(\ell)|}{|G|} = \frac{|G_c| + |G_n \cap \mathcal{I}(\ell)|}{|G|} \in \left\{ \frac{1}{|G|}, \frac{1}{4} + \frac{1}{|G|}, \frac{1}{2} + \frac{1}{|G|} \right\}.
\]

6.3. Subgroups containing the special linear group

Lemma 6.7. If \( G \) is of type \( \text{SL} \), then \( \mathcal{F}(G) = \frac{\ell+3}{2(\ell+1)} \).

Proof. We proceed by counting the complement of \( \mathcal{I}(\ell) \) in \( \text{SL}_2(\ell) \). Referencing Table I, we see that

\[
\text{SL}_2(\ell) \setminus \mathcal{I}(\ell) = \bigcup_{0 < a < \ell, \ 0 < b \leq (\ell-1)/2, \ \ a^2 - \varepsilon b^2 \equiv 1 \pmod{\ell}} \left[ \begin{pmatrix} a & b \varepsilon \\ b & a \end{pmatrix} \right],
\]

where \([\gamma]\) denotes the \( \text{GL}_2(\ell) \)-conjugacy class of \( \gamma \). It is well-known (e.g. [18, Problem 22 of Section 3.2]) that

\[
|\{(a, b) \in \mathbb{F}_\ell \oplus \mathbb{F}_\ell : a^2 - \varepsilon b^2 = 1\}| = \ell - \left( \frac{\varepsilon}{\ell} \right) = \ell + 1.
\]

Realizing that solutions to \( a^2 - \varepsilon b^2 = 1 \) come in pairs \((\pm x, y)\) and disregarding the pair \((\pm 1, 0)\), we deduce that \( |U| = \frac{1}{2}(\ell-1) \) where

\[
U := \{ (a, b) : 0 \leq a < \ell, \ 0 < b \leq \frac{1}{2}(\ell-1), \ a^2 - \varepsilon b^2 \equiv 1 \pmod{\ell} \}.
\]
Thus \( \text{SL}_2(\ell) \setminus \mathcal{I}(\ell) \) is the union of \( \frac{1}{2}(\ell - 1) \) conjugacy classes, each of size \( \ell(\ell - 1) \). Hence,

\[
\mathcal{F}(\text{SL}_2(\ell)) = 1 - \frac{|\text{SL}_2(\ell) \setminus \mathcal{I}(\ell)|}{|\text{SL}_2(\ell)|} = 1 - \frac{\frac{1}{2}(\ell - 1) \cdot \ell(\ell - 1)}{\ell(\ell^2 - 1)} = \frac{\ell + 3}{2(\ell + 1)}. \tag{6.4}
\]

**Lemma 6.8.** If \( G \subseteq \text{GL}_2(\ell) \) is a subgroup of type \( \text{GL} \), then \( \mathcal{F}(G) = \frac{\ell + 2}{2(\ell + 1)} \).

**Proof.** We proceed by counting the complement of \( \mathcal{I}(\ell) \) in \( \text{GL}_2(\ell) \). Referencing Table 1, we see that

\[
\text{GL}_2(\ell) \setminus \mathcal{I}(\ell) = \bigcup_{0 \leq a < \ell} \left[ \left( \begin{array}{cc} a & b \varepsilon \\ b & a \end{array} \right) \right].
\]

Thus \( \text{GL}_2(\ell) \setminus \mathcal{I}(\ell) \) is the union of \( \frac{1}{2} \ell(\ell - 1) \) conjugacy classes, each of size \( \ell(\ell - 1) \). Hence,

\[
\mathcal{F}(\text{GL}_2(\ell)) = 1 - \frac{|\text{GL}_2(\ell) \setminus \mathcal{I}(\ell)|}{|\text{GL}_2(\ell)|} = 1 - \frac{\frac{1}{2} \ell(\ell - 1) \cdot \ell(\ell - 1)}{(\ell^2 - 1)(\ell^2 - \ell)} = \frac{\ell + 2}{2(\ell + 1)}. \tag{6.5}
\]

**Remark 6.9.** If \( G \) is of type \( \text{C}_n \), \( \text{N}_n \), \( \text{SL} \), or \( \text{GL} \), then \( \mathcal{F}(G) \leq \frac{3}{4} \). Indeed, if \( G \) is of type \( \text{C}_n \) or \( \text{N}_n \), we note that \( |G| \geq 2 \) or \( |G| \geq 4 \), respectively. The inequality now follows directly from Lemmas 6.3 and 6.6 respectively. For \( G \) of type \( \text{SL} \) or \( \text{GL} \), apply Lemmas 6.7 and 6.8 and note that \( \frac{\ell + 2}{2(\ell + 1)} \leq \frac{\ell + 3}{2(\ell + 1)} \leq \frac{3}{4} \) for all \( \ell \geq 3 \).

**6.4. Exceptional subgroups.** We first introduce some notation that is useful in dealing with the **exceptional subgroups**, i.e., those of type \( \text{A}_4 \), \( \text{S}_4 \), and \( \text{A}_5 \). Let \( G \subseteq \text{GL}_2(\ell) \) be a subgroup and let \( H \) be a group that is isomorphic to \( \overline{G} \subseteq \text{PGL}_2(\ell) \). Let \( \phi : \overline{G} \rightarrow H \) be an isomorphism. For each \( h \in H \), we define

\[
\delta_h := \begin{cases} 
1 & \text{if } \phi^{-1}(h) \in \overline{G} \cap \overline{\mathcal{I}(\ell)}, \\
0 & \text{if } \phi^{-1}(h) \not\in \overline{G} \cap \overline{\mathcal{I}(\ell)}. 
\end{cases}
\]

Let \( h_1, \ldots, h_n \in H \) be representatives of the conjugacy classes of \( H \). For each \( i \in \{1, \ldots, n\} \), we write \([h_i]\) to denote the conjugacy class of \( h_i \) in \( H \). By parts (3) and (4) of Lemma 6.1, we deduce that

\[
(6.4) \quad \mathcal{F}(G) = \frac{\sum_i \delta_{h_i} |\text{C}_{h_i}|}{|\overline{G}|}.
\]

We record that if \( 1_H \) denotes the identity element of \( H \), then since \( \phi^{-1}(1_H) = \overline{T} \in \overline{G} \cap \overline{\mathcal{I}(\ell)} \), we have \( \delta_{1_H} = 1 \).

**Lemma 6.10.** If \( G \subseteq \text{GL}_2(\ell) \) is a subgroup of type \( \text{A}_4 \), then \( \mathcal{F}(G) \in \{ \frac{1}{12}, \frac{1}{3}, \frac{3}{4}, 1 \} \).
Proof. Let \( \phi : G \to A_4 \) be an isomorphism and define \( \delta_h \) for each \( h \in A_4 \) as above. The conjugacy classes of \( A_4 \) are \([()],[(12)(34)],[(123)],[(124)]\), of sizes 1, 3, 4 and 4, respectively. Observe that \((123)^2 = (132) \in [(124)]\). Hence, by Lemma 6.1(2,3), we have \( \delta_{(124)} = \delta_{(123)} \). Putting this information together with (6.4), we get
\[
\mathcal{F}(G) = \frac{1 \cdot \delta(()) + 3 \cdot \delta_{(12)(34)} + 4 \cdot \delta_{(123)} + 4 \cdot \delta_{(124)}}{12}
\]
Iterating over all \( \delta_{(12)(34)}, \delta_{(123)} \in \{0,1\} \) leads to the desired result.

Lemma 6.11. If \( G \subseteq \text{GL}_2(\ell) \) is a subgroup of type \( S_4 \), then \( \mathcal{F}(G) \in \{ \frac{1}{24}, \frac{7}{24}, \frac{3}{8}, \frac{5}{12}, \frac{5}{24}, \frac{3}{4}, 1 \} \).

Proof. Let \( \phi : G \to S_4 \) be an isomorphism and define \( \delta_h \) for each \( h \in S_4 \) as above. The conjugacy classes of \( S_4 \) are \([()],[(12)],[(12)(34)],[(123)],[(1234)]\), of sizes 1, 6, 3, 8, and 6, respectively. Observe that \((1234)^2 = (13)(24) \in [(12)(34)]\). Hence, by Lemma 6.1(2,3), we have \( \delta_{(12)(34)} = \delta_{(1234)} \). Thus by (6.4),
\[
\mathcal{F}(G) = \frac{1 \cdot \delta(()) + 6 \cdot \delta_{(12)} + 3 \cdot \delta_{(12)(34)} + 8 \cdot \delta_{(123)} + 6 \cdot \delta_{(1234)}}{24}
\]
Iterating over all \( \delta_{(12)}, \delta_{(12)(34)}, \delta_{(123)} \in \{0,1\} \) gives the desired result.

Lemma 6.12. If \( G \subseteq \text{GL}_2(\ell) \) is a subgroup of type \( A_5 \), then \( \mathcal{F}(G) \in \{ \frac{1}{60}, \frac{4}{15}, \frac{7}{20}, \frac{5}{12}, \frac{5}{10}, \frac{3}{3}, \frac{3}{4}, 1 \} \).

Proof. Let \( \phi : G \to A_5 \) be an isomorphism and define \( \delta_h \) for each \( h \in A_5 \) as above. The conjugacy classes of \( A_5 \) are \([()],[(12)(34)],[(123)],[(1234)],[(12354)]\), of sizes 1, 15, 20, 12, and 12, respectively. Observe that \((12345)^2 = (13524) \in [(12354)]\). Hence, by Lemma 6.1(2,3), we deduce \( \delta_{(12345)} = \delta_{(12354)} \). Thus by (6.4),
\[
\mathcal{F}(G) = \frac{1 \cdot \delta(()) + 15 \cdot \delta_{(12)(34)} + 20 \cdot \delta_{(123)} + 12 \cdot \delta_{(12345)} + 12 \cdot \delta_{(12354)}}{60}
\]
Iterating over all \( \delta_{(12)(34)}, \delta_{(123)}, \delta_{(12345)} \in \{0,1\} \) gives the desired result.

7. Proof of Proposition 5.3. In this section, we prove the lemmas that are referenced in our proof of Proposition 5.3. We start with some observations that will be occasionally useful. As before, \( \ell \) denotes an odd prime throughout.
LEMMA 7.1.
(1) For $\gamma \in \text{GL}_2(\ell)$, we have $\gamma \in I_1(\ell)$ if and only if $\det \gamma + 1 = \text{tr} \gamma$.
(2) For subgroups $G_1, G_2 \subseteq \text{GL}_2(\ell)$, if $G_1$ is conjugate to $G_2$ in $\text{GL}_2(\ell)$, then $\mathcal{F}_1(G_1) = \mathcal{F}_1(G_2)$.

Proof. (1) Note that $\gamma \in I_1(\ell)$ if and only if 1 is a root of the characteristic polynomial of $\gamma$, which is given by $p_\gamma(x) = x^2 - \text{tr} \gamma \cdot x + \det \gamma$. As $p_\gamma(1) = 1 - \text{tr} \gamma + \det \gamma$, we see that 1 is a root of the characteristic polynomial of $\gamma$ if and only if $\det \gamma + 1 = \text{tr} \gamma$.

(2) This follows from the fact that a matrix’s eigenvalues are invariant under conjugation in $\text{GL}_2(\ell)$. ■

We now give a lemma that places a restrictive upper bound on $\mathcal{F}_1(G)$, provided that $|G \cap Z(\ell)|$ is large. Although the bound holds for arbitrary subgroups of $\text{GL}_2(\ell)$, we shall only employ it in the exceptional cases.

LEMMA 7.2. If $G \subseteq \text{GL}_2(\ell)$ is a subgroup, then

$$\mathcal{F}_1(G) \leq \frac{2}{|G \cap Z(\ell)|} - \frac{1}{|G|}.$$ 

In particular, if $|G \cap Z(\ell)| \geq 3$, then $\mathcal{F}_1(G) \leq \frac{2}{3}$.

Proof. For a matrix $\gamma \in \text{GL}_2(\ell)$ and scalar $\lambda \in \mathbb{F}_p^\times$, the eigenvalues of the product $\lambda \gamma$ are the eigenvalues of $\gamma$, multiplied by $\lambda$. Thus, since matrices in $\text{GL}_2(\ell)$ have at most two eigenvalues, in each of the $|\overline{G}|$ fibers of the projection $G \to \overline{G}$, there exist at most two matrices contained in $I_1(\ell)$. In fact, the kernel of $G \to \overline{G}$ contains only a single matrix in $I_1(\ell)$, the identity matrix. Applying these observations, we obtain

$$\mathcal{F}_1(G) = \frac{|G \cap I_1(\ell)|}{|G|} \leq \frac{2(|\overline{G}| - 1) + 1}{|G|} = \frac{2}{|G|/|\overline{G}|} - \frac{1}{|G|}.$$ 

Finally, notice that $|G \cap Z(\ell)| = |G|/|\overline{G}|$, by the first isomorphism theorem applied to $\pi : G \to \overline{G}$. ■

Subgroups $G \subseteq \text{GL}_2(\ell)$ for which $|G \cap Z(\ell)| \leq 2$ are problematic from the point of view of the previous lemma. In the case of $|G \cap Z(\ell)| = 2$, we may say something more that will be useful when considering exceptional subgroups. In order to do so, we introduce the following subset of $\overline{G}$:

$$\overline{G}_2 := \{ \gamma \in \overline{G} : \text{the order of } \gamma \text{ is } 2 \}.$$ 

LEMMA 7.3. If $G \subseteq \text{GL}_2(\ell)$ is a subgroup for which $|G \cap Z(\ell)| = 2$, then

$$\mathcal{F}_1(G) \leq \frac{2|\overline{G}_2| + |\overline{G} \setminus \overline{G}_2|}{|G|}.$$ 

Proof. The scalar group $\overline{Z}(\ell)$ is cyclic of order $\ell - 1$. Its one (and only) subgroup of order 2 is $\{ \pm I \}$. Hence, since $|G \cap Z(\ell)| = 2$, we see that
\(G \cap \mathcal{Z}(\ell) = \{\pm I\}\). Fix \(\overline{\gamma} \in \overline{G}\) and note that its fiber under \(G \to \overline{G}\) is \(\{\pm \gamma\}\). If \(\{\pm \gamma\} \subseteq \mathcal{I}_1(\ell)\), then the eigenvalues of \(\gamma\) are 1 and \(-1\), so \(\gamma\) is conjugate to \(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\) in \(\text{GL}_2(\ell)\). In particular, the order of both \(\gamma\) in \(G\) and \(\overline{\gamma}\) in \(\overline{G}\) is 2. We conclude that the fiber of each matrix in \(\overline{G} \setminus \overline{G}_2\) contains at most one matrix in \(\mathcal{I}_1(\ell)\). Thus, we have the inequality that is claimed in the statement of the lemma.

We now proceed case-by-case, considering subgroups of type \(\mathsf{Cs}, \mathsf{Ns}, \mathsf{B}, \mathsf{A}_4, \mathsf{A}_5, \) and \(\mathsf{S}_4\) in Dickson’s classification. By Lemma 7.1, we may (and do) make the assumptions described in the paragraph immediately preceding Section 6.1.

### 7.1. Split Cartan and Borel subgroups.

For a subgroup \(G \subseteq \mathcal{B}(\ell)\), we define for \(i = 1, 4\) the homomorphism \(\psi_i : G \to \mathbb{F}_\ell^\times\) given by \(\begin{pmatrix} a_1 & a_2 \\ 0 & a_4 \end{pmatrix} \mapsto a_i\).

We observe that \(G \cap \mathcal{I}_1(\ell) = \ker \psi_1 \cup \ker \psi_4\) and thus

\[
|G \cap \mathcal{I}_1(\ell)| = |\ker \psi_1| + |\ker \psi_4| - |\ker \psi_1 \cap \ker \psi_4|.
\]

**Lemma 7.4.** If \(G\) is of type \(\mathsf{Cs}\) and \(\mathcal{F}_1(G) \neq 1\), then \(\mathcal{F}_1(G) \leq \frac{1}{2} + \frac{1}{|G|}\).

**Proof.** Let each \(\psi_i : G \to \mathbb{F}_\ell^\times\) be defined for \(G\) as above. As \(\ker \psi_1 \cap \ker \psi_4 = \{I\}\), by (7.1) we have

\[
|G \cap \mathcal{I}_1(\ell)| = |\ker \psi_1| + |\ker \psi_4| - |\ker \psi_1 \cap \ker \psi_4|.
\]

The subgroup of \(G\) generated by \(\ker \psi_1 \cup \ker \psi_4\) has order \(|\ker \psi_1| |\ker \psi_4|\), so \(|\ker \psi_1| |\ker \psi_4| \leq |G|\). Thus,

\[
|\ker \psi_1| + |\ker \psi_4| \leq |\ker \psi_1| + \frac{|G|}{|\ker \psi_1|}.
\]

Now if \(|\ker \psi_1| = |\ker \psi_4| = 1\), then \(\mathcal{F}_1(G) = \frac{1}{|G|}\) by (7.2) and we are done. So assume, without loss of generality, that \(|\ker \psi_1| > 1\). Because \(\ker \psi_1 \subseteq G \cap \mathcal{I}_1(\ell)\) and \(\mathcal{F}_1(G) \neq 1\), we further have \(|\ker \psi_1| < |G|\). As \(|\ker \psi_1|\) is an integer that divides \(|G|\) and satisfies the inequalities \(1 < |\ker \psi_1| < |G|\), we see that

\[
|\ker \psi_1| + \frac{|G|}{|\ker \psi_1|} \leq \frac{1}{2}|G| + 2.
\]

Now by combining (7.2)−(7.4), we conclude that

\[
\mathcal{F}_1(G) = \frac{|G \cap \mathcal{I}_1(\ell)|}{|G|} \leq \left(\frac{1}{2}|G| + 2\right) - 1 = \frac{1}{2} + \frac{1}{|G|}.
\]

**Lemma 7.5.** If \(G\) is of type \(\mathsf{B}\) and \(\mathcal{F}_1(G) \neq 1\), then \(\mathcal{F}_1(G) \leq \frac{1}{2} + \frac{\ell}{|G|}\).

**Proof.** As \(G \subseteq \mathcal{B}(\ell)\) and \(\ell\) divides \(|G|\), we have \(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G\). Thus,

\[
\ker \psi_1 \cap \ker \psi_4 = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_\ell \right\}.
\]
Hence, by (7.1), we see that

\[ |G \cap I(\ell)| = |\ker \psi_1| + |\ker \psi_4| - \ell. \tag{7.5} \]

The subgroup of \(G\) generated by \(\ker \psi_1 \cup \ker \psi_4\) has order \(\frac{1}{\ell}|\ker \psi_1||\ker \psi_4|\), so \(\frac{1}{\ell}|\ker \psi_1||\ker \psi_4| \leq |G|\). Thus,

\[ |\ker \psi_1| + |\ker \psi_4| - \ell \leq |\ker \psi_1| + \frac{|G|}{\ell|\ker \psi_1|} - \ell \]

\[ = \ell \left( \frac{1}{\ell} |\ker \psi_1| + \frac{1}{\ell} |G| \right) - 1. \]

Now if \(|\ker \psi_1| = |\ker \psi_4| = \ell\), then \(F_1(G) = \frac{\ell}{|G|}\) by (7.5) and we are done. So assume, without loss of generality, that \(|\ker \psi_1| > \ell\). Because \(\ker \psi_1 \subseteq G \cap I_1(\ell)\) and \(F_1(G) \neq 1\), we further have \(|\ker \psi_1| < |G|\). Since \(\frac{1}{\ell}|\ker \psi_1|\) is an integer that divides \(\frac{1}{\ell}|G|\) and satisfies the inequalities \(1 < \frac{1}{\ell}|\ker \psi_1| < \frac{1}{\ell}|G|\), we see that

\[ \frac{1}{\ell}|\ker \psi_1| + \frac{1}{\ell}|G| \leq \frac{1}{2} \cdot \frac{1}{\ell}|G| + 2. \tag{7.7} \]

Now by combining (7.5)–(7.7), we conclude that

\[ F_1(G) = \frac{|G \cap I_1(\ell)|}{|G|} \leq \ell \left( \frac{1}{2\ell} |G| + 2 \right) \leq \frac{1}{2} + \ell \frac{1}{|G|}. \]

The above lemma leaves open the possibility of a subgroup \(G\) of type B satisfying \(\frac{3}{4} < F_1(G) < 1\) in the single case when \(\frac{1}{\ell}|G| = 3\). As we see in the following remark, this case in fact presents no issues.

**Remark 7.6.** If in the above lemma the quantity \(\frac{1}{\ell}|G|\) is prime, then \(F_1(G) = \frac{\ell}{|G|}\). Indeed, for \(i = 1, 4\) we see that \(\frac{1}{\ell}|\ker \psi_i|\) divides \(\frac{1}{\ell}|G|\) and satisfies the inequalities \(1 \leq |\ker \psi_i| \leq \frac{1}{\ell}|G|\). Thus \(|\ker \psi_i| \in \{\ell, |G|\}\) for each \(i = 1, 4\). As noted in the proof of the lemma, if \(|\ker \psi_1| = |\ker \psi_4| = \ell\), then \(F(G) = \frac{\ell}{|G|}\). The case of \(|\ker \psi_1| = |\ker \psi_4| = |G|\) cannot occur since then the inequality \(\frac{1}{\ell}|\ker \psi_1||\ker \psi_4| \leq |G|\) is violated. Both of the remaining cases are excluded by the assumptions of the lemma, since in each we have \(F(G) = \frac{|G| + \ell - \ell}{\ell} = 1\).

### 7.2. Normalizer of the split Cartan subgroup

**Lemma 7.7.** If \(G \subseteq GL_2(\ell)\) is a subgroup of type \(\mathfrak{Ns}\) for which \(F_1(G) \neq 1\), then \(F_1(G) \leq \frac{1}{2} + \frac{1}{|G|} \).
Proof. Write \( G_c := G \cap \mathcal{C}_s(\ell) \) and \( G_n := G \setminus G_c \). If \( G_n \cap I_1(\ell) = \emptyset \), then we are done as by Lemma 7.4, \( \mathcal{F}_1(G) = \frac{|G_c \cap I_1(\ell)| + |G_n \cap I_1(\ell)|}{|G|} \leq \frac{1}{2} \frac{|G_c| + 1}{|G|} + 0 = \frac{1}{4} \frac{|G| + 1}{|G|} = \frac{1}{4} + \frac{1}{|G|} \).

So we shall assume that \( G_n \cap I_1(\ell) \neq \emptyset \). Say \( \gamma_0 \in G_n \cap I_1(\ell) \) and note that \( \text{tr} \gamma_0 = 0 \) and \( \text{tr}(\gamma_0) = 0 \). Hence Lemma 7.4(1) gives

\[
\gamma \gamma_0 \in I_1(\ell) \iff \det(\gamma \gamma_0) = -1 \iff \det \gamma = 1.
\]

Thus,

\[ G_n \cap I_1(\ell) = \{ \gamma \gamma_0 : \gamma \in G_c \cap \text{SL}_2(\ell) \} \text{.} \]

Either \( |G_c : G_c \cap \text{SL}_2(\ell)| \geq 2 \) or \( G_c = G_c \cap \text{SL}_2(\ell) \). In the former case, we are done as then

\[
\mathcal{F}_1(G) = \frac{|G_c \cap I_1(\ell)| + |G_n \cap I_1(\ell)|}{|G|} \leq \frac{1}{2} \frac{|G_c| + 1}{|G|} + \frac{1}{2} \frac{|G_c|}{|G|} = \frac{1}{2} + \frac{1}{|G|} \text{.}
\]

So we consider the case of \( G_c = G_c \cap \text{SL}_2(\ell) \). Clearly, \( \mathcal{C}_s(\ell) \cap \text{SL}_2(\ell) \cap I_1(\ell) = \{ I \} \), so in particular \( G_c \cap I_1(\ell) = \{ I \} \). Hence, in this case, we also have the bound

\[
\mathcal{F}_1(G) = \frac{|G_c \cap I_1(\ell)| + |G_n \cap I_1(\ell)|}{|G|} = \frac{1 + |G_n|}{|G|} = \frac{1 + \frac{1}{2} |G|}{|G|} = \frac{1}{2} + \frac{1}{|G|} \text{.}
\]

7.3. Exceptional subgroups. We finally consider \( G \subseteq \text{GL}_2(\ell) \) an exceptional subgroup. We split our consideration into three cases: \( |G \cap \mathcal{Z}(\ell)| = 1 \), \( |G \cap \mathcal{Z}(\ell)| = 2 \), and \( |G \cap \mathcal{Z}(\ell)| \geq 3 \). It is not clear (at least to the author) whether the first of these three cases may occur, so we pose the following question: Does there exist an exceptional subgroup \( G \subseteq \text{GL}_2(\ell) \) for which \( G \cap \mathcal{Z}(\ell) = \{ I \} \)?

Lacking an affirmative answer, we start by considering the (possibly vacuous) case of \( G \cap \mathcal{Z}(\ell) = \{ I \} \). We proceed via conjugacy class considerations, as in Lemmas 6.10-6.12. First, two quick observations.

**Lemma 7.8.** For \( \gamma \in \text{GL}_2(\ell) \),

(1) \( \gamma \in I_1(\ell) \) implies \( \gamma^2 \in I_1(\ell) \),

(2) \( \gamma^2 = I \) implies \( \gamma \in I_1(\ell) \) or \( \gamma = -I \).

**Proof.** (1) This is clear, since if 1 is an eigenvalue of \( \gamma \), then \( 1^2 \) is an eigenvalue of \( \gamma^2 \).
(2) Here the minimal polynomial of $\gamma$ divides $X^2 - I$. Thus only if the minimal polynomial of $\gamma$ equals $X + I$ may we have $\gamma \notin \mathcal{I}_1(\ell)$. But then $\gamma = -I$. ■

**Lemma 7.9.** If $G \subseteq \text{GL}_2(\ell)$ is an exceptional subgroup for which $G \cap Z(\ell) = \{I\}$ and $\mathcal{F}_1(G) \neq 1$, then $\mathcal{F}_1(G) \leq \frac{3}{4}$.

**Proof.** We have three cases to consider as $G$ may be isomorphic to $A_4$, $S_4$, or $A_5$. Below, we write $[\gamma]$ to denote the conjugacy class of a matrix $\gamma$ in $G$.

First assume that $G \cong A_4$. The conjugacy classes of $A_4$ have sizes $1, 3, 4, 6, 8, 12, 24$ and $48$. Fix $\gamma \in G$ with $\gamma \notin \mathcal{I}_1(\ell)$. Then $\gamma \neq I$, so its conjugacy class $[\gamma]$ has size at least $3$. Therefore $[\gamma] \cap \mathcal{I}_1(\ell) = \emptyset$, so $\mathcal{F}_1(G) \leq \frac{12-3}{12} = \frac{3}{4}$.

Now assume that $G \cong S_4$. The conjugacy classes of $S_4$ have sizes $1, 3, 6, 8, 12, 48$. Fix $\gamma \in G$ with $\gamma \notin \mathcal{I}_1(\ell)$. Note that the conjugacy class of size $3$ consists of elements of order $2$. Thus, by Lemma $7.8(2)$ and our assumption that $G \cap Z(\ell) = \{I\}$, we see that the size of $[\gamma]$ is at least $6$. Hence $\mathcal{F}_1(G) \leq \frac{24-6}{24} = \frac{3}{4}$.

Finally assume that $G \cong A_5$. The conjugacy classes of $A_5$ have sizes $1, 5, 20, 12, 60$. Fix $\gamma \in G$ with $\gamma \notin \mathcal{I}_1(\ell)$. If the size of $[\gamma]$ is $15$ or $20$, then we are done as then $\mathcal{F}_1(G) \leq \frac{60-15}{60} = \frac{3}{4}$. So we shall assume that $[\gamma]$ is one of the conjugacy classes of size $12$. Let $\gamma_0 \in G$ be such that $[\gamma_0]$ is the other conjugacy class of $G$ of size $12$. Then $\gamma_0^2 \in [\gamma]$, so by the contrapositive of Lemma $7.8(1)$, we have $\gamma_0 \notin \mathcal{I}_1(\ell)$. Thus $([\gamma] \cup [\gamma_0]) \cap \mathcal{I}_1(\ell) = \emptyset$. Consequently, $\mathcal{F}_1(G) \leq \frac{60-12}{60} = \frac{3}{4}$. ■

We turn to the case of $|G \cap Z(\ell)| = 2$. Here we proceed via Lemma $7.3$.

**Lemma 7.10.** If $G \subseteq \text{GL}_2(\ell)$ is an exceptional subgroup with $|G \cap Z(\ell)| = 2$, then

$$\mathcal{F}_1(G) \leq \begin{cases} \frac{5}{8} & \text{if } G \text{ is of type } A_4 \text{ or } A_5, \\ \frac{11}{16} & \text{if } G \text{ is of type } S_4. \end{cases}$$

**Proof.** First assume $G$ is of type $A_4$. The group $A_4$ has $12$ elements, of which three have order $2$. Thus, by Lemma $7.3$, we see that $\mathcal{F}_1(G) \leq \frac{2 \cdot 3 + (12-3)}{24} = \frac{5}{8}$. We obtain the upper bounds for the other cases similarly. Specifically, apply Lemma $7.3$ on noting that $A_5$ has $60$ elements, of which $15$ have order $2$, and that $S_4$ has $24$ elements, of which nine have order $2$. ■

Finally, we note that the case of $|G \cap Z(\ell)| \geq 3$ has already been handled via Lemma $7.2$.

**8. Densities for non-CM elliptic curves over the rationals.** Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. For a prime number $\ell$, let $G_{E, \ell}$ denote the image of the mod $\ell$ Galois representation $\rho_{E, \ell}$:
Gal(O/Q) → GL₂(ℓ). Serre’s open image theorem \cite{20, Théorème 3} gives \(G_E(\ell) = GL_2(\ell)\) for all sufficiently large \(\ell\). If \(G_E(\ell) = GL_2(\ell)\), then

\[
\delta(S^1_{E,\ell}) = \frac{\ell^2 - 2}{(\ell^2 - 1)(\ell - 1)} \quad \text{and} \quad \delta(S_{E,\ell}) = \frac{\ell + 2}{2(\ell + 1)},
\]

as we see by Proposition 4.2 and a calculation of \(F_1(GL_2(\ell))\) and \(F(GL_2(\ell))\) (the latter is carried out in Lemma 6.8 and the former follows similarly).

A prime \(\ell\) is exceptional for \(E\) if \(G_E(\ell) \neq GL_2(\ell)\), and in this instance, the group \(G_E(\ell)\) is called an exceptional image for \(\ell\). All exceptional images are known \cite{24} for \(\ell \leq 11\). For primes \(\ell \geq 13\), as a result of systematic computations \cite{22} and significant partial results (e.g. \cite{2, 5, 6, 16, 17, 20}), it is conjectured that all exceptional images are known and that \(G_E(\ell) = GL_2(\ell)\) for \(\ell > 37\).

<table>
<thead>
<tr>
<th>(G_E(\ell))</th>
<th>(\delta(S^1_{E,\ell}))</th>
<th>(\delta(S_{E,\ell}))</th>
<th>(G_E(\ell))</th>
<th>(\delta(S^1_{E,\ell}))</th>
<th>(\delta(S_{E,\ell}))</th>
</tr>
</thead>
<tbody>
<tr>
<td>2Cs</td>
<td>1</td>
<td>1</td>
<td>5B.4.2</td>
<td>1</td>
<td>11B.1.6</td>
</tr>
<tr>
<td>2B</td>
<td>1</td>
<td>1</td>
<td>5Nn</td>
<td>3</td>
<td>11B.1.5</td>
</tr>
<tr>
<td>2Cn</td>
<td>(\frac{1}{3})</td>
<td>(\frac{1}{3})</td>
<td>5B</td>
<td>(\frac{7}{5})</td>
<td>1</td>
</tr>
<tr>
<td>3Cs.1.1</td>
<td>1</td>
<td>1</td>
<td>5S4</td>
<td>(\frac{19}{5})</td>
<td>(\frac{5}{12})</td>
</tr>
<tr>
<td>3Cs</td>
<td>(\frac{3}{4})</td>
<td>(\frac{3}{4})</td>
<td>7Ns.2.1</td>
<td>(\frac{7}{4})</td>
<td>1</td>
</tr>
<tr>
<td>3B.1.1</td>
<td>1</td>
<td>1</td>
<td>7Ns.3.1</td>
<td>(\frac{11}{36})</td>
<td>1</td>
</tr>
<tr>
<td>3B.1.2</td>
<td>1</td>
<td>1</td>
<td>7B.1.1</td>
<td>(\frac{1}{4})</td>
<td>1</td>
</tr>
<tr>
<td>3Ns</td>
<td>(\frac{5}{24})</td>
<td>(\frac{5}{24})</td>
<td>7B.1.3</td>
<td>(\frac{1}{4})</td>
<td>1</td>
</tr>
<tr>
<td>3B</td>
<td>(\frac{3}{24})</td>
<td>(\frac{3}{24})</td>
<td>7B.1.2</td>
<td>(\frac{1}{4})</td>
<td>1</td>
</tr>
<tr>
<td>3Nn</td>
<td>(\frac{3}{24})</td>
<td>(\frac{3}{24})</td>
<td>7B.1.5</td>
<td>(\frac{1}{4})</td>
<td>1</td>
</tr>
<tr>
<td>5Cs.1.1</td>
<td>1</td>
<td>1</td>
<td>7B.1.6</td>
<td>(\frac{1}{4})</td>
<td>1</td>
</tr>
<tr>
<td>5Cs.1.3</td>
<td>(\frac{5}{24})</td>
<td>(\frac{5}{24})</td>
<td>7B.1.4</td>
<td>(\frac{1}{4})</td>
<td>1</td>
</tr>
<tr>
<td>5Cs.4.1</td>
<td>(\frac{5}{24})</td>
<td>(\frac{5}{24})</td>
<td>7Ns</td>
<td>(\frac{17}{12})</td>
<td>(\frac{3}{4})</td>
</tr>
<tr>
<td>5Ns.2.1</td>
<td>(\frac{5}{24})</td>
<td>(\frac{5}{24})</td>
<td>7B.6.1</td>
<td>(\frac{17}{12})</td>
<td>1</td>
</tr>
<tr>
<td>5Cs</td>
<td>(\frac{7}{16})</td>
<td>(\frac{7}{16})</td>
<td>7B.6.3</td>
<td>(\frac{1}{2})</td>
<td>1</td>
</tr>
<tr>
<td>5B.1.1</td>
<td>1</td>
<td>1</td>
<td>7B.6.2</td>
<td>(\frac{1}{2})</td>
<td>(\frac{5}{15})</td>
</tr>
<tr>
<td>5B.1.2</td>
<td>1</td>
<td>1</td>
<td>7Nn</td>
<td>(\frac{3}{4})</td>
<td>(\frac{5}{15})</td>
</tr>
<tr>
<td>5B.1.4</td>
<td>(\frac{1}{2})</td>
<td>(\frac{1}{2})</td>
<td>7B.2.1</td>
<td>(\frac{1}{2})</td>
<td>(\frac{5}{15})</td>
</tr>
<tr>
<td>5B.1.3</td>
<td>(\frac{1}{2})</td>
<td>(\frac{1}{2})</td>
<td>7B.2.3</td>
<td>(\frac{1}{2})</td>
<td>(\frac{5}{15})</td>
</tr>
<tr>
<td>5Ns</td>
<td>(\frac{11}{12})</td>
<td>(\frac{11}{12})</td>
<td>7B</td>
<td>(\frac{11}{12})</td>
<td>(\frac{1}{2})</td>
</tr>
<tr>
<td>5B.4.1</td>
<td>(\frac{5}{8})</td>
<td>(\frac{5}{8})</td>
<td>11B.1.4</td>
<td>(\frac{1}{2})</td>
<td>(\frac{5}{15})</td>
</tr>
</tbody>
</table>

We reproduce from \cite{22} Table 3 the conjecturally complete list of 63 exceptional images in the first column of the table above. For each exceptional image \(G\), we list in columns two and three the associated values of \(\delta(S^1_{E,\ell})\) and \(\delta(S_{E,\ell})\) for elliptic curves \(E/Q\) with \(G_E(\ell) = G\). These densities are straightforward and fast to compute as, by Proposition 4.2, we simply need to compute the proportions \(F_1(G)\) and \(F(G)\).
Recall that Sutherland [21] considered the local-global question (B) of the introduction. He found that for elliptic curves over \(\mathbb{Q}\), a counterexample can only occur for \(\ell = 7\). Further, an elliptic curve \(E/\mathbb{Q}\) is a counterexample to (B) if and only if the \(j\)-invariant of \(E\) is \(\frac{2268945}{128}\). The mod 7 Galois image of such an \(E\) is either \(7\text{Ns.2.1}\) or \(7\text{Ns.3.1}\) [22, Remark 6.5]. Note that in either case, \(\delta(S_{E,7}) = 1\) yet neither subgroup is conjugate to a subgroup of \(B(7)\).

Acknowledgements. I would like to thank the referee for their helpful comments and corrections. In addition, I would like to thank my Ph.D. advisor, Nathan Jones, for his support throughout this project.

References


Jacob Mayle
Department of Mathematics
Wake Forest University
Winston-Salem, NC 27104, USA
E-mail: maylej@wfu.edu