Massachusetts Institute of Technology

CARTAN IMAGES AND ℓ-TORSION POINTS OF ELLIPTIC CURVES WITH RATIONAL j-INVARIANT

ORON Y. PROPP

ABSTRACT. Let ℓ be an odd prime and d a positive integer. We determine when there exists a degree-d number field K and an elliptic curve E/K with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$ for which $E(K)_{\text{tors}}$ contains a point of order ℓ. We also determine when there exists such a pair (K, E) for which the image of the associated mod-ℓ Galois representation is contained in a Cartan subgroup or its normalizer, conditionally on a conjecture of Sutherland. We do the same under the stronger assumption that E is defined over $\mathbb{Q}$.

1. INTRODUCTION

Let E be an elliptic curve over a number field K with algebraic closure $\overline{K}$. For an odd prime ℓ, let $E[\ell]$ denote the ℓ-torsion subgroup of $E(\overline{K})$, which we recall is a free rank-2 $\mathbb{Z}/\ell\mathbb{Z}$-module. The absolute Galois group $\text{Gal}(\overline{K}/K)$ acts on $E[\ell]$ via its action on the coordinates of its points, which induces a continuous Galois representation

$$\rho_{E,\ell} \colon \text{Gal}(\overline{K}/K) \to \text{Aut}(E[\ell]) \simeq \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

where the isomorphism with $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ depends on a choice of a $\mathbb{Z}/\ell\mathbb{Z}$-basis of $E[\ell]$. Thus, we may regard the image of $\rho_{E,\ell}$ as a subgroup of $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ determined up to conjugacy. Moreover, $\rho_{E,\ell}$ factors through the finite Galois group $\text{Gal}(K(E[\ell])/K)$, where the ℓ-torsion field $K(E[\ell])$ is obtained by adjoining to K the coordinates of all ℓ-torsion points of E.

The problem of identifying the possible images of these Galois representations is closely related to that of determining the possible torsion subgroups and isogenies admitted by elliptic curves over a particular number field. Mazur famously classified the possible torsion subgroups $E(\mathbb{Q})_{\text{tors}}$ in [25] and the possible ℓ-isogenies of an elliptic curve $E/\mathbb{Q}$ in [26]. Kamienny, Kenku and Momose generalized Mazur's results on torsion subgroups to quadratic number fields in [22, 23], and though no complete characterization for higher-degree number fields is known, there has been recent progress towards characterizing the cubic case [6, 17, 18, 29, 30, 35], the quartic case [7, 14, 19, 28], and the quintic case [8, 12]. In particular, the set of torsion subgroups that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves defined over number fields of degree d has been determined for $d = 3, 4, 5, 6$ [10, 20, 21]. The growth of torsion subgroups of elliptic curves upon base change was further studied in [13, 16]. Using Galois representations, Lozano-Robledo has explicitly characterized the set of primes ℓ for which an elliptic curve $E/\mathbb{Q}$ has a point of order ℓ over a number field of degree at most d, assuming a positive answer to Serre's uniformity problem [24]. The same was done by Najman for cyclic ℓ-isogenies of elliptic curves with rational j-invariant [27].

We aim to give a more precise characterization of the degrees of number fields over which elliptic curves exhibit certain properties deducible from the images of their Galois representations. Recently, Sutherland developed an algorithm to efficiently compute Galois images of elliptic curves, and conjectured the following stronger version of Serre's uniformity problem in [34, Conj. 1.1] based on data from some 140 million elliptic curves, including all curves of conductor up to 400,000 [9]:

Conjecture 1.1 (Sutherland). *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let ℓ be a prime. Then the image of $\rho_{E,\ell}$ is either equal to $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or conjugate to one of the 63 exceptional groups listed in Table 1 (see also [34, Tables 3,4]).*

Combining this conjecture with the precise characterization of Galois images for elliptic curves over $\mathbb{Q}$ with complex multiplication (CM) given in [36, Thm. 1.14-1.16], we are able to deduce the possible subgroups of $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ arising as images of $\rho_{E,\ell}$ for base changes of elliptic curves $E/\mathbb{Q}$ to a number field K, and

ℓ	Index	Generators
2	6	
	3	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	2	$\left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)$
3	24	$\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
	12	$\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
	8	$\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	8	$\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	6	$\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}0&2\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
	4	$\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	3	$\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}2&1\\2&2\end{smallmatrix}\right)$
5	120	$\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
	120	$\left(\begin{smallmatrix}3&0\\0&4\end{smallmatrix}\right)$
	60	$\left(\begin{smallmatrix}4&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
	30	$\left(\begin{smallmatrix}2&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\3&0\end{smallmatrix}\right)$
	30	$\left(\begin{smallmatrix}2&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
	24	$\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	24	$\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	24	$\left(\begin{smallmatrix}4&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	24	$\left(\begin{smallmatrix}3&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	15	$\left(\begin{smallmatrix}0&4\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)$
	12	$\left(\begin{smallmatrix}4&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	12	$\left(\begin{smallmatrix}4&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	10	$\left(\begin{smallmatrix}1&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}2&3\\4&2\end{smallmatrix}\right)$
	6	$\left(\begin{smallmatrix}2&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	5	$\left(\begin{smallmatrix}0&3\\3&4\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}3&0\\4&4\end{smallmatrix}\right)$
7	112	$\left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\4&0\end{smallmatrix}\right)$
	56	$\left(\begin{smallmatrix}3&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\4&0\end{smallmatrix}\right)$
	48	$\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	48	$\left(\begin{smallmatrix}3&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	48	$\left(\begin{smallmatrix}2&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	48	$\left(\begin{smallmatrix}5&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	48	$\left(\begin{smallmatrix}6&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$

ℓ	Index	Generators
	48	$\left(\begin{smallmatrix}4&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	28	$\left(\begin{smallmatrix}0&6\\1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}3&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right)$
	24	$\left(\begin{smallmatrix}6&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
7	24	$\left(\begin{smallmatrix}6&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}3&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	24	$\left(\begin{smallmatrix}6&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	21	$\left(\begin{smallmatrix}1&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}2&5\\4&2\end{smallmatrix}\right)$
	16	$\left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	16	$\left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}3&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	8	$\left(\begin{smallmatrix}3&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&3\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	120	$\left(\begin{smallmatrix}4&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
11	120	$\left(\begin{smallmatrix}6&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	120	$\left(\begin{smallmatrix}5&0\\0&7\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	120	$\left(\begin{smallmatrix}7&0\\0&5\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	60	$\left(\begin{smallmatrix}10&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}4&0\\0&6\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	60	$\left(\begin{smallmatrix}10&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}5&0\\0&7\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	55	$\left(\begin{smallmatrix}1&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}3&5\\8&3\end{smallmatrix}\right)$
	91	$\left(\begin{smallmatrix}3&0\\12&9\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}9&5\\0&6\end{smallmatrix}\right)$
	56	$\left(\begin{smallmatrix}3&0\\0&9\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	56	$\left(\begin{smallmatrix}3&0\\0&9\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	56	$\left(\begin{smallmatrix}3&0\\0&9\end{smallmatrix}\right),\left(\begin{smallmatrix}4&0\\0&7\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	56	$\left(\begin{smallmatrix}3&0\\0&9\end{smallmatrix}\right),\left(\begin{smallmatrix}7&0\\0&4\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
13	42	$\left(\begin{smallmatrix}5&0\\0&8\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	42	$\left(\begin{smallmatrix}5&0\\0&8\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	42	$\left(\begin{smallmatrix}5&0\\0&8\end{smallmatrix}\right),\left(\begin{smallmatrix}4&0\\0&7\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	28	$\left(\begin{smallmatrix}4&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	28	$\left(\begin{smallmatrix}4&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	14	$\left(\begin{smallmatrix}2&0\\0&7\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
17	72	$\left(\begin{smallmatrix}4&0\\0&13\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&10\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	72	$\left(\begin{smallmatrix}4&0\\0&13\end{smallmatrix}\right),\left(\begin{smallmatrix}6&0\\0&9\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
37	114	$\left(\begin{smallmatrix}8&0\\0&14\end{smallmatrix}\right),\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$
	114	$\left(\begin{smallmatrix}8&0\\0&14\end{smallmatrix}\right),\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$

TABLE 1. Known exceptional images of $\rho_{E,\ell}$ for non-CM elliptic curves $E/\mathbb{Q}$ (for $\ell \le 11$, the list is complete) [34, Tables 3,4]. The first column lists the prime ℓ; the second column lists the index of the subgroup G in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$; and the third lists generators for G, as matrices acting on column vectors from the left.

for elliptic curves E/K with $j(E) \in \mathbb{Q}$, assuming $j(E) \ne 0, 1728$.[1] Thus, all results in this paper hold unconditionally for elliptic curves with CM.
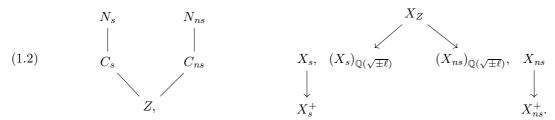
Let C_s and C_{ns} denote the split and nonsplit Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, and N_s and N_{ns} their normalizers. Also, let Z denote the center of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, that is, the subgroup of scalar matrices, and let

$$
(1.1) \quad
\begin{aligned}
\mathcal{P} &:= \{\ell : \left(\tfrac{-D}{\ell}\right) = 1 \text{ for all } D \in \{3,4,7,8,11,19,43,67,163\}\} = \{15073, 18313, 38833, \ldots\}, \\
\mathcal{Q} &:= \{\ell : \left(\tfrac{-D}{\ell}\right) = -1 \text{ for all } D \in \{3,4,7,8,11,19,43,67,163\}\} = \{3167, 8543, 14423, \ldots\}.
\end{aligned}
$$

---

[1]For $\ell = 2$, all conjugacy classes of subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ occur as the image of $\rho_{E,\ell}$ for some elliptic curve $E/\mathbb{Q}$, so we ignore this case henceforth.

Let M be either Z, C_s, C_{ns}, N_s, or N_{ns}. We say that a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *belongs to* M if it is conjugate to a subgroup of M, but not to a subgroup of any other of these five subgroups contained in M. For example, if M is Z, this amounts to requiring that G consists only of scalars; if M is N_s, then G must be conjugate to a subgroup of N_s but not to any subgroup of C_s. The inclusions among these five subgroups are depicted in the following diagram on the left:

$$(1.2)$$

$$
\begin{array}{ccc}
N_s & & N_{ns} \\
| & & | \\
C_s & & C_{ns} \\
& \searrow \quad \swarrow & \\
& Z, &
\end{array}
\qquad
\begin{array}{c}
X_Z \\
\swarrow \qquad \searrow \\
X_s, \ (X_s)_{\mathbb{Q}(\sqrt{\pm\ell})} \qquad (X_{ns})_{\mathbb{Q}(\sqrt{\pm\ell})}, \ X_{ns} \\
\downarrow \qquad\qquad\qquad\qquad \downarrow \\
X_s^+ \qquad\qquad\qquad\qquad X_{ns}^+.
\end{array}
$$

Now, to any subgroup M of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ containing $-I$, we can associate a modular curve X_M defined over the field $K_M := \mathbb{Q}(\zeta_\ell)^{\det M}$; thus, $X_s := X_{C_s}$, $X_{ns} := X_{C_{ns}}$, $X_s^+ := X_{N_s}$, and $X_{ns}^+ := X_{N_{ns}}$ are defined over $\mathbb{Q}$, whereas X_Z is defined over $\mathbb{Q}(\sqrt{\pm\ell}) \subseteq \mathbb{Q}(\zeta_\ell)$. The curve X_M is smooth, projective, and geometrically irreducible, and comes with a natural morphism of K_M-schemes

$$\pi_M \colon X_M \longrightarrow X(1)_{K_M} = \operatorname{Spec} K_M[j] \cup \{\infty\} = \mathbb{P}^1_{K_M}$$

with the property that, for an elliptic curve E/K_M with $j(E) \neq 0, 1728$, the image $\rho_{E,\ell}(\operatorname{Gal}(\overline{K_M}/K_M))$ is conjugate to a subgroup of M in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ if and only if $j(E) \in K_M$ is the image of some K_M-point of X_M under π_M [36]. The diagram on the right in (1.2) shows the morphisms of these modular curves corresponding to the inclusions in the diagram on the left.

Our first result determines the degrees of number fields K over which the image of the Galois representation attached to an elliptic curve can belong to each of these subgroups M, or equivalently, the degrees of K-points on the modular curves X_M:

Theorem 1.2. *Assume Conjecture 1.1. Let ℓ be an odd prime, and let M be one of the subgroups Z, C_s, C_{ns}, N_s, or N_{ns} of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. There exists a set $\mathcal{S}_M(\ell)$, identified explicitly in Table 2, such that the following holds: there exists a degree-d number field K and an elliptic curve $E/\mathbb{Q}$ with $j(E) \neq 0, 1728$ for which $\rho_{E,\ell}(\operatorname{Gal}(\overline{K}/K))$ belongs to M if and only if $s \mid d$ for some $s \in \mathcal{S}_M(\ell)$. The set $\mathcal{S}_M(\ell)$ satisfies the same condition with $E/\mathbb{Q}$ replaced by an elliptic curve E/K with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$.*

Consequently, there exists a non-cuspidal K-point on the modular curve X_M that is not in the image of any of the morphisms in (1.2) for some degree-d number field K if and only if $s \mid d$ for some $s \in \mathcal{S}_M(\ell)$.

ℓ	Z	C_s	C_{ns}	N_s	N_{ns}
3	2	1	2	1	1
5	4	1	2	1	1
7	$6, 14, 16$	$2, 3, 7$	2	1	1
13	$24, 28, 52$	$2, 13$	2	1	1
17	$32, 36, 272$	$2, 17$	2	1	1
37	$72, 76, 1332$	$2, 37$	2	1	1
$11, 19, 43, 67, 163$	$2(\ell-1), 2\ell, 2(\ell+1)$	$2, \ell$	2	1	1
$\in \mathcal{P}$	$2(\ell-1)$	2	$\ell-1$	1	$(\ell-1)/2$
$\in \mathcal{Q}$	$2(\ell+1)$	$\ell+1$	2	$(\ell+1)/2$	1
other	$2(\ell-1), 2(\ell+1)$	2	2	1	1

TABLE 2. Values of $\mathcal{S}_M(\ell)$ (see Theorem 1.2).

We also identify analogous sets $\mathcal{S}_M^{\mathrm{CM}}(\ell)$ and $\mathcal{S}_M^{\text{non-CM}}(\ell)$ for elliptic curves with and without CM, listed in Tables 3 and 4, respectively. To replace "belonging" in the theorem with the ordinary notion of containment, and remove the corresponding restriction related to the morphisms in (1.2), simply take unions of the $\mathcal{S}_M(\ell)$

ℓ	Z	C_s	C_{ns}	N_s	N_{ns}
$3, 7, 11, 19, 43, 67, 163$	$2(\ell-1), 2\ell, 2(\ell+1)$	$2, \ell$	2	1	1
$\in \mathcal{P}$	$2(\ell-1)$	2	$\ell-1$	1	$(\ell-1)/2$
$\in \mathcal{Q}$	$2(\ell+1)$	$\ell+1$	2	$(\ell+1)/2$	1
other	$2(\ell-1), 2(\ell+1)$	2	2	1	1

TABLE 3. Values of $\mathcal{S}_M^{\mathrm{CM}}(\ell)$ (see Theorem 1.2).

ℓ	Z	C_s	C_{ns}	N_s	N_{ns}
3	2	1	2	1	1
5	4	1	2	1	1
7	$6, 14, 16$	$2, 3, 7$	2	1	1
11	$24, 110$	$11, 12$	2	6	1
13	$24, 52$	$6, 8, 13$	12	$3, 4$	$6, 26$
17	272	17	272	153	136
37	1332	37	1332	703	666
other	$\ell(\ell+1)(\ell-1)$	$\ell(\ell+1)$	$\ell(\ell-1)$	$\ell(\ell+1)/2$	$\ell(\ell-1)/2$

TABLE 4. Values of $\mathcal{S}_M^{\mathrm{non\text{-}CM}}(\ell)$ (see Theorem 1.2).

along the subgroup inclusion lattice in (1.2) (e.g., replace $\mathcal{S}_{N_{ns}}(\ell)$ with $\mathcal{S}_{N_{ns}}(\ell) \cup \mathcal{S}_{C_{ns}}(\ell) \cup \mathcal{S}_Z(\ell)$). For interpretations of the latter statement on modular curves in terms of moduli data, see the table on page 2 of [32].

Our next result characterizes the degrees of abelian sub-extensions of ℓ-torsion fields $\mathbb{Q}(E[\ell])$:

Theorem 1.3. *Assume Conjecture 1.1. Given an odd prime ℓ, there exists a set $\mathcal{K}(\ell)$, identified explicitly in (3.5), such that the following holds: there exists a degree-d number field K contained in the ℓ-torsion field of an elliptic curve $E/\mathbb{Q}$ with $j(E) \neq 0, 1728$ for which $\mathbb{Q}(E[\ell])/K$ is an abelian extension precisely when $d \in \mathcal{K}(\ell)$. The set $\mathcal{K}(\ell)$ satisfies the same condition with $E/\mathbb{Q}$ replaced by an elliptic curve E/K with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$.*

As above, we explicitly identify analogous subsets $\mathcal{K}^{\mathrm{CM}}(\ell), \mathcal{K}^{\mathrm{non\text{-}CM}}(\ell) \subseteq \mathcal{K}(\ell)$ for elliptic curves with and without CM, listed in (3.5). Note that Theorem 1.2 already implies that there exists a degree-d number field K and an elliptic curve $E/\mathbb{Q}$ with $j(E) \neq 0, 1728$ for which the extension $\mathbb{Q}(E[\ell])/(K \cap \mathbb{Q}(E[\ell])$ is abelian precisely when $r \mid d$ for some $r \in \mathcal{S}_Z(\ell) \cup \mathcal{S}_{C_s}(\ell) \cup \mathcal{S}_{C_{ns}}(\ell)$; as in the statement of Theorem 1.2, E may be replaced by an elliptic curve E/K with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$. However, Theorem 1.3 provides a more precise characterization of abelian subfields of ℓ-torsion fields by identifying when $\mathbb{Q}(E[\ell])/K$ is abelian, rather than $\mathbb{Q}(E[\ell])/(K \cap \mathbb{Q}(E[\ell]))$. Table 5 illustrates the first result for all pairs (ℓ, d) with $\ell \leq 97$ and $d \leq 45$; a light square indicates that such a number field and elliptic curve exist, and a dark square indicates that they do not [31]. In particular, as shown unconditionally in [15, Thm. 1.1], $\mathbb{Q}(E[\ell])/\mathbb{Q}$ can only be abelian for $\ell = 3, 5$, though naturally for any elliptic curve $E/\mathbb{Q}$ with CM there exists a quadratic field K for which $\mathbb{Q}(E[\ell])/K$ is abelian.

Finally, we have the following result, which is a refinement of [24, Thm. 1.7] on degrees of number fields over which elliptic curves with rational j-invariant contain torsion points of order ℓ:

Theorem 1.4. *Assume Conjecture 1.1. Given an odd prime ℓ, there exists a set $\mathcal{T}(\ell)$, identified explicitly in Table 6, such that the following holds: there exists a degree-d number field K and an elliptic curve E/K with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$ for which $E(K)_{\mathrm{tors}}$ contains a point of order ℓ if and only if $t \mid d$ for some $t \in \mathcal{T}(\ell)$.*

The analogous result for elliptic curves defined over $\mathbb{Q}$ is proven unconditionally in [16, Cor. 6.1]; our methods can be easily made to give a proof of this case, which we omit, instead reproducing the resultant sets $\mathcal{T}_{\mathbb{Q}}(\ell)$ in Table 6. We again identify analogous sets $\mathcal{T}^{\mathrm{CM}}(\ell), \mathcal{T}_{\mathbb{Q}}^{\mathrm{CM}}(\ell), \mathcal{T}^{\mathrm{non\text{-}CM}}(\ell), \mathcal{T}_{\mathbb{Q}}^{\mathrm{non\text{-}CM}}(\ell)$ for elliptic curves with and without CM, listed with $\mathcal{T}(\ell)$ and $\mathcal{T}_{\mathbb{Q}}(\ell)$. These results agree with, and in some cases
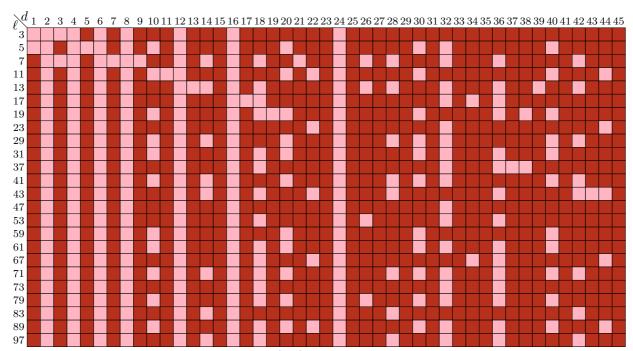
TABLE 5. Light squares identify pairs (ℓ, d) for which there exists a degree-d number field K contained in the ℓ-torsion field of an elliptic curve $E/\mathbb{Q}$ (or E/K) with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$ such that $\mathbb{Q}(E[\ell])/K$ is abelian (see Theorem 1.3).

ℓ	$\mathcal{T}(\ell)$	$\mathcal{T}^{\mathrm{CM}}(\ell)$	$\mathcal{T}^{\mathrm{non\text{-}CM}}(\ell)$
3	1	1	1
5	1	4	1
7	1	3	1
11	5	5	5
13	2, 3	12	2, 3
17	4	16	4
37	6	36	6
19, 43, 67, 163	$(\ell - 1)/2$	$(\ell - 1)/2$	$(\ell^2 - 1)/2$
$\in \mathcal{Q}$	$(\ell^2 - 1)/2$	$(\ell^2 - 1)/2$	$(\ell^2 - 1)/2$
other	$\ell - 1$	$\ell - 1$	$(\ell^2 - 1)/2$

TABLE 6. Values of $\mathcal{T}(\ell)$, $\mathcal{T}^{\mathrm{CM}}(\ell)$, and $\mathcal{T}^{\mathrm{non\text{-}CM}}(\ell)$ (see Theorem 1.4).

sharpen, recent work on CM elliptic curves [3, 4, 5]. For instance, [4, Thm. 1.5] and [5, Thm. 1.2] imply that there exists a number field of odd degree d over which a CM elliptic curve attains an ℓ-torsion point if and only if $\ell \equiv 3 \bmod 4$ and d is divisible by $h_\ell \cdot \frac{\ell - 1}{2}$, where h_ℓ denotes the class number of $\mathbb{Q}(\sqrt{-\ell})$ (see also [3, Thm. 6.2]). But by Theorem 1.4, for certain primes $\ell \equiv 3 \bmod 4$, all odd degrees d divisible by $h_\ell \cdot \frac{\ell - 1}{2}$ have this property even if we restrict to CM elliptic curves E with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$; for other primes $\ell \equiv 3 \bmod 4$, no such degrees do. Table 8 illustrates this phenomenon for all such $\ell \leq 83$. The entries in its final column can also be derived from [4, 5]: they are "all" when $h_\ell = 1$ and "none" when $h_\ell > 1$.

ℓ	$\mathcal{T}_{\mathbb{Q}}(\ell)$	$\mathcal{T}_{\mathbb{Q}}^{\mathrm{CM}}(\ell)$	$\mathcal{T}_{\mathbb{Q}}^{\text{non-CM}}(\ell)$
3	1	1	1
5	1	8	1
7	1	3	1
11	5	5	5
13	3, 4	24	3, 4
17	8	32	8
37	12	72	12
$19, 43, 67, 163$	$(\ell-1)/2$	$(\ell-1)/2$	$\ell^2 - 1$
$\in \mathcal{Q}$	$\ell^2 - 1$	$\ell^2 - 1$	$\ell^2 - 1$
other	$2(\ell-1)$	$2(\ell-1)$	$\ell^2 - 1$

TABLE 7. Values of $\mathcal{T}_{\mathbb{Q}}(\ell)$, $\mathcal{T}_{\mathbb{Q}}^{\mathrm{CM}}(\ell)$, and $\mathcal{T}_{\mathbb{Q}}^{\text{non-CM}}(\ell)$ (see Theorem 1.4).

ℓ	$h_\ell \cdot \frac{\ell-1}{2}$	$\mathcal{T}^{\mathrm{CM}}(\ell)$	Degrees
3	1	1	all
7	3	3	all
11	5	5	all
19	9	9	all
23	33	22	none
31	45	30	none
43	21	21	all
47	115	46	none
59	87	58	none
67	33	33	all
71	245	70	none
79	195	78	none
83	123	82	none

TABLE 8. Primes $\ell \equiv 3 \bmod 4$, along with whether "all" or "none" of the odd numbers d divisible by $h_\ell \cdot \frac{\ell-1}{2}$ have the property that there exists a degree-d number field over which a CM elliptic curve E with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$ attains an ℓ-torsion point.

2. BACKGROUND

Let ℓ be an odd prime, and let $\mathrm{GL}_2(\ell) := \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and $\mathrm{SL}_2(\ell) := \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. The center of $\mathrm{GL}_2(\ell)$ is the subgroup

$$Z(\ell) := \{ \left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix} \right) : x \in \mathbb{F}_\ell^\times \} \simeq \mathbb{F}_\ell^\times,$$

and we let $\mathrm{PGL}_2(\ell) := \mathrm{GL}_2(\ell)/Z(\ell)$. Let

$$C_s(\ell) := \{ \left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix} \right) : xy \neq 0 \} \leq \mathrm{GL}_2(\ell),$$
$$C_{ns}(\ell) := \{ \left(\begin{smallmatrix} x & \epsilon y \\ y & x \end{smallmatrix} \right) : (x, y) \neq (0, 0) \} \leq \mathrm{GL}_2(\ell),$$

be the *split Cartan group* and *nonsplit Cartan group*, respectively, for some fixed non-quadratic residue $\epsilon \in \mathbb{F}_\ell^\times$. We refer to their conjugates in $\mathrm{GL}_2(\ell)$ as *split* and *nonsplit Cartan groups*, respectively. Note that we have $C_s(\ell) \simeq \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$ and $C_{ns}(\ell) \simeq \mathbb{F}_{\ell^2}^\times$. Both $C_s(\ell)$ and $C_{ns}(\ell)$ are index-2 subgroups of their normalizers

$$N_s(\ell) := C_s \cup \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right) C_s, \qquad N_{ns}(\ell) := C_{ns} \cup \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix} \right) C_{ns}.$$

We denote the matrices in $N_s(\ell)$ and $N_{ns}(\ell)$ by

$$\mathcal{D}_s(x,y) := \left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right), \qquad \mathcal{A}_s(x,y) := \left(\begin{smallmatrix} 0 & x \\ y & 0 \end{smallmatrix}\right),$$
$$\mathcal{D}_{ns}(x,y) := \left(\begin{smallmatrix} x & \epsilon y \\ y & x \end{smallmatrix}\right), \qquad \mathcal{A}_{ns}(x,y) := \left(\begin{smallmatrix} x & -\epsilon y \\ y & -x \end{smallmatrix}\right).$$

The *Borel group* $B(\ell) \leq \mathrm{GL}_2(\ell)$ is the subgroup of upper triangular matrices; we refer to its conjugates in $\mathrm{GL}_2(\ell)$ as *Borel groups*. We refer to $\mathrm{GL}_2(\ell)$, the Borel groups, the Cartan subgroups, and their normalizers collectively as *standard subgroups* of $\mathrm{GL}_2(\ell)$.

The following proposition, originally due to Dickson [11], classifies subgroups of $\mathrm{GL}_2(\ell)$ in terms of their images in $\mathrm{PGL}_2(\ell)$:

Proposition 2.1. *Let ℓ be an odd prime and G be a subgroup of $\mathrm{GL}_2(\ell)$ with image H in $\mathrm{PGL}_2(\ell)$. If G contains an element of order ℓ, then either G is conjugate to a subgroup of the Borel group $B(\ell)$, or $\mathrm{SL}_2(\ell)$ is contained in G. Otherwise, one of the following holds:*

(1) *H is cyclic and a conjugate of G lies in $C_s(\ell)$ or $C_{ns}(\ell)$;*
(2) *H is dihedral and a conjugate of G lies in $N_s(\ell)$ or $N_{ns}(\ell)$, but not in $C_s(\ell)$ or $C_{ns}(\ell)$;*
(3) *H is isomorphic to A_4, S_4, or A_5, and no conjugate of G is contained in the normalizer of any Cartan subgroup.*

Proof. See [33, §2]. $\qquad\qquad\square$

An integer $n \in S \subseteq \mathbb{Z}_{>0}$ is said to be *div-minimal in S* if it is a minimal element of S in the divisibility lattice of integers. A subgroup $H \in S \subseteq \{G : G \leq \mathrm{GL}_2(\ell)\}$ is said to be *div-minimal in S* if $\#H$ is div-minimal in $\{\#G : G \in S\}$. The terms "div-maximal," "div-minima," and so forth, are defined as expected. The set S is often omitted if it is clear from context. Note that an element of a set S can be both div-minimal and div-maximal.

3. Proof of Theorems 1.2 and 1.3

Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) \neq 0, 1728$, and let K be a degree-d number field. The intersection $K \cap \mathbb{Q}(E[\ell])$ with the ℓ-torsion field of E is a number field of degree r dividing d. Conversely, for any degree-r number field L that is a subfield of $\mathbb{Q}(E[\ell])$, and d divisible by r, there exists a degree-d number field L' such that $L' \cap \mathbb{Q}(E[\ell]) = L$ (e.g., adjoin to L a root of $x^{d/r} - p$ for some prime p unramified in both L and $\mathbb{Q}(E[\ell])$). Since

$$(3.1) \qquad \rho_{E,\ell}(\mathrm{Gal}(\overline{K}/K)) \simeq \mathrm{Gal}(\mathbb{Q}(E[\ell])/(K \cap \mathbb{Q}(E[\ell]))) \leq \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \simeq \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$$

is an index-r subgroup, it suffices to determine which index-r subgroups of each possible image $G_E(\ell) := \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ belong to each standard subgroup in question. That is, we would like to identify the sets $\mathcal{I}(G_E(\ell); M(\ell))$ for each $M \in \{Z, C_s, C_{ns}, N_s, N_{ns}\}$, where we have let

$$(3.2) \qquad \mathcal{I}(G_1, \ldots, G_n; M) := \{[G_i : H] : H \leq G_i \text{ such that } H \text{ belongs to } M, \text{ for some } 1 \leq i \leq n\}$$

for any $G_1, \ldots, G_n \leq \mathrm{GL}_2(\ell)$ and standard subgroup M.

If E does not have CM, then $G_E(\ell)$ is either $\mathrm{GL}_2(\ell)$ or one of the 63 exceptional groups listed in Table 1 by our assumption of Conjecture 1.1. Let $\mathrm{Excep}(\ell)$ denote the set of exceptional subgroups of $\mathrm{GL}_2(\ell)$. The results for each subgroup in Table 1 were computed [31, 34] using Magma [2], and the unions of these sets of indices over each $\mathrm{Excep}(\ell)$ are the sets $\mathcal{I}(\mathrm{Excep}(\ell); M(\ell))$ appearing in Table 9. The analogous sets $\mathcal{I}(\mathrm{GL}_2(\ell); M(\ell))$ are determined in §3.1, and appear in Table 10. There, and henceforth, we define

$$(3.3) \qquad \Delta(r \in L \mid s \in U) := \Delta(L, U) := \{n \in \mathbb{Z}_{>0} : r \mid n \mid s \text{ for some } r \in L, s \in U\}$$

for any nonempty $L, U \subseteq \mathbb{Z}_{>0}$; we also let

$$(3.4) \qquad \Pi(n) := \{p \mid n\}, \qquad \Pi_{\mathrm{odd}}(n) := \{p \mid n : p > 2\},$$

and ν_2 denote the usual 2-adic valuation.

Now suppose E has CM. Following [36], define subgroups

$$G(\ell) := \{\left(\begin{smallmatrix} a & b \\ 0 & \pm a \end{smallmatrix}\right) : a \in \mathbb{F}_\ell^\times, b \in \mathbb{F}_\ell\},$$
$$H_1(\ell) := \{\left(\begin{smallmatrix} a & b \\ 0 & \pm a \end{smallmatrix}\right) : a \in (\mathbb{F}_\ell^\times)^2, b \in \mathbb{F}_\ell\},$$
$$H_2(\ell) := \{\left(\begin{smallmatrix} \pm a & b \\ 0 & a \end{smallmatrix}\right) : a \in (\mathbb{F}_\ell^\times)^2, b \in \mathbb{F}_\ell\},$$

and recall the definitions of (1.1). By [36, Prop. 1.14], if $\ell \in \mathcal{P}$ (resp. $\ell \in \mathcal{Q}$) then $G_E(\ell)$ is conjugate to $N_s(\ell)$ (resp. $N_{ns}(\ell)$); if $\ell \in \{3, 7, 11, 19, 43, 67, 163\}$ (i.e., the set of odd primes ℓ such that the imaginary quadratic field $\mathbb{Q}(\sqrt{-\ell})$ has class number 1) then $G_E(\ell)$ is conjugate to either $N_s(\ell)$, $N_{ns}(\ell)$, $G(\ell)$, $H_1(\ell)$, or $H_2(\ell)$, and moreover each of these cases occurs for some such E (as a simple Magma computation [31] shows that $\left\{ \left(\frac{-D}{\ell} \right) : D \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\} \right\} = \{-1, 0, 1\}$ for all $\ell \in \{3, 7, 11, 19, 43, 67, 163\}$); and otherwise $G_E(\ell)$ is conjugate to either $N_s(\ell)$ or $N_{ns}(\ell)$, with each case occurring for some such E. The sets $\mathcal{I}(N_s(\ell); M(\ell))$, $\mathcal{I}(N_{ns}(\ell); M(\ell))$, and $\mathcal{I}(G(\ell), H_1(\ell), H_2(\ell); M(\ell))$ are determined in §3.2, §3.3, and §3.4, respectively, and appear in Table 10.

Now let K be a degree-d number field, and E/K be an elliptic curve with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$. Then E is either a base change of an elliptic curve over $\mathbb{Q}$, or a quadratic twist of such a curve. By [34, Cor. 5.25], the images $\rho_{E,\ell}(\mathrm{Gal}(\overline{K}/K))$ which may arise in this case are precisely the groups G arising for base changes of elliptic curves $E/\mathbb{Q}$, along with their *twists*: these are the group $\langle G, -1 \rangle$ and its index-2 subgroups that do not contain -1. The following lemma shows that a subgroup of $\mathrm{GL}_2(\ell)$ and its twists always belong to the same subgroup, and therefore all results above hold when $E/\mathbb{Q}$ is replaced by an elliptic curve E/K with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$.

Lemma 3.1. *Let $G \le \mathrm{GL}_2(\ell)$, let H be a twist of G, and let M be Z, C_s, C_{ns}, N_s, or N_{ns}. Then G belongs to M if and only if H belongs to M.*

Proof. Let H be an index-2 subgroup of $\langle G, -1 \rangle$ not containing -1, and suppose $H \le M$. Then H is an index-2 subgroup of $\langle H, -1 \rangle \simeq H \times \{\pm 1\}$, so since $\langle H, -1 \rangle \subseteq \langle G, -1 \rangle$, it follows that $\langle H, -1 \rangle = \langle G, -1 \rangle$. But $-1 \in M$ (as is true of all standard subgroups of $\mathrm{GL}_2(\ell)$), hence $G \le \langle H, -1 \rangle \le M$. Conversely, if $G \le M$, then $H \le \langle G, -1 \rangle \le M$ as $-1 \in M$, so altogether $H \le M$ if and only if $G \le M$. Since the above argument respects conjugacy, the conclusion follows by definition. The same proof applies if $H = \langle G, -1 \rangle$. $\square$

Finally, let

$$\mathcal{E}_M^{\mathrm{CM}}(\ell) := \begin{cases} \mathcal{I}(N_s(\ell); M(\ell)) & \text{if } \ell \in \mathcal{P}, \\ \mathcal{I}(N_{ns}(\ell); M(\ell)) & \text{if } \ell \in \mathcal{Q}, \\ \mathcal{I}(N_s(\ell), N_{ns}(\ell), G(\ell), H_1(\ell), H_2(\ell); M(\ell)) & \text{if } \ell \in \{3, 7, 11, 19, 43, 67, 163\}, \\ \mathcal{I}(N_s(\ell), N_{ns}(\ell); M(\ell)) & \text{otherwise.} \end{cases}$$

$$\mathcal{E}_M^{\mathrm{non\text{-}CM}}(\ell) := \mathcal{I}(\mathrm{Excep}(\ell); M(\ell)) \cup \mathcal{I}(\mathrm{GL}_2(\ell); M(\ell)), \qquad \mathcal{E}_M(\ell) := \mathcal{E}_M^{\mathrm{CM}} \cup \mathcal{E}_M^{\mathrm{non\text{-}CM}}.$$

Altogether, we have proven the following result:

Theorem 3.2. *Assume Conjecture 1.1. Let ℓ be an odd prime, and let $M \in \{C_s, C_{ns}, N_s, N_{ns}\}$. There exists a degree-$d$ number field K and an elliptic curve $E/\mathbb{Q}$ with K a subfield of $\mathbb{Q}(E[\ell])$ such that $\rho_{E,\ell}(\mathrm{Gal}(\overline{K}/K)))$ belongs to $M(\ell)$ if and only if $d \in \mathcal{E}_M(\ell)$. The same is true if E is replaced by an elliptic curve E/K with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$.*

Naturally, to restrict to an elliptic curve with or without CM, we may simply replace $\mathcal{E}_M(\ell)$ by $\mathcal{E}_M^{\mathrm{CM}}(\ell)$ or $\mathcal{E}_M^{\mathrm{non\text{-}CM}}(\ell)$, respectively. To obtain Theorem 1.2, it remains to choose the div-minimal elements of $\mathcal{E}_M(\ell)$, by (3.1). Doing so yields the sets $\mathcal{S}_M(\ell)$ in Table 2; the sets $\mathcal{S}_M^{\mathrm{CM}}(\ell)$ and $\mathcal{S}_M^{\mathrm{non\text{-}CM}}(\ell)$ are obtained similarly.

For Theorem 1.3, note that the Cartan subgroups are the maximal abelian subgroups of $\mathrm{GL}_2(\ell)$ not containing an element of order ℓ; by [34, Lem. 3.3], the maximal abelian subgroup of $\mathrm{GL}_2(\ell)$ containing an element of order ℓ is given up to conjugacy by the *ramified Cartan group*

$$C_r(\ell) := \{ \left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix} \right) : a \in \mathbb{F}_\ell^\times, b \in \mathbb{F}_\ell \}.$$

Thus, it remains to determine the sets $\mathcal{I}(G_E(\ell); C_r(\ell))$ for each G_E appearing in Table 10; note that since $Z(\ell) \subseteq C_r(\ell)$, we say that a subgroup belongs to $C_r(\ell)$ if it is conjugate to a subgroup of $C_r(\ell)$, but not to a subgroup of $Z(\ell)$. These sets appear in Tables 9 and 10 and are determined in Lemma 3.3 below. It then follows from (3.1) that

$$\begin{aligned} \mathcal{K}(\ell) &= \mathcal{E}_Z(\ell) \cup \mathcal{E}_{C_s}(\ell) \cup \mathcal{E}_{C_{ns}}(\ell) \cup \mathcal{E}_{C_r}(\ell), \\ (3.5) \qquad \mathcal{K}^{\mathrm{CM}}(\ell) &= \mathcal{E}_Z^{\mathrm{CM}}(\ell) \cup \mathcal{E}_{C_s}^{\mathrm{CM}}(\ell) \cup \mathcal{E}_{C_{ns}}^{\mathrm{CM}}(\ell) \cup \mathcal{E}_{C_r}^{\mathrm{CM}}(\ell), \\ \mathcal{K}^{\mathrm{non\text{-}CM}}(\ell) &= \mathcal{E}_Z^{\mathrm{non\text{-}CM}}(\ell) \cup \mathcal{E}_{C_s}^{\mathrm{non\text{-}CM}}(\ell) \cup \mathcal{E}_{C_{ns}}^{\mathrm{non\text{-}CM}}(\ell) \cup \mathcal{E}_{C_r}^{\mathrm{non\text{-}CM}}(\ell), \end{aligned}$$

which is the desired explicit identification.

ℓ	$Z(\ell)$	$C_s(\ell)$
3	$\Delta(2 \mid 12, 16)$	$\Delta(1 \mid 6, 8)$
5	$\Delta(4 \mid 80, 96)$	$\Delta(1 \mid 40, 48) \setminus \{3\}$
7	$\Delta(6, 14, 16 \mid 72, 96, 252)$	$\Delta(2, 3, 7 \mid 36, 48, 84, 126)$
11	$\Delta(24, 110 \mid 220, 240)$	$\Delta(11, 12 \mid 44, 110, 120)$
13	$\Delta(24, 52 \mid 288, 1872)$	$\Delta(6, 8, 13 \mid 96, 144, 624, 936)$
17	$\Delta(272 \mid 1088)$	$\Delta(17 \mid 544)$
37	$\Delta(1332 \mid 15984)$	$\Delta(37 \mid 5328, 7992)$
other	$\varnothing$	$\varnothing$

ℓ	$C_{ns}(\ell)$	$N_s(\ell)$	$N_{ns}(\ell)$	$C_r(\ell)$
3	$\Delta(2 \mid 4)$	$\Delta(1 \mid 4)$	$\Delta(1 \mid 6, 8)$	$\Delta(2 \mid 4)$
5	$\Delta(2 \mid 12, 32)$	$\Delta(1 \mid 12)$	$\Delta(1 \mid 40, 48) \setminus \{5\}$	$\Delta(4 \mid 16)$
7	$\Delta(2 \mid 18, 24)$	$\Delta(1 \mid 18, 24)$	$\Delta(1 \mid 36, 48, 126)$	$\Delta(2 \mid 26)$
11	$\Delta(2 \mid 60, 80)$	$\Delta(6 \mid 60)$	$\Delta(1 \mid 110, 120) \setminus \{11, 22\}$	$\Delta(10 \mid 20)$
13	$\Delta(12 \mid 36)$	$\Delta(3, 4 \mid 36)$	$\Delta(6, 26 \mid 144, 936)$	$\Delta(4 \mid 144)$
17	$\varnothing$	$\varnothing$	$\Delta(136 \mid 544)$	$\Delta(16 \mid 64)$
37	$\varnothing$	$\varnothing$	$\Delta(666 \mid 7992)$	$\Delta(36 \mid 432)$
other	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$

TABLE 9. The set $\mathcal{I}(\mathrm{Excep}(\ell); M(\ell))$ of indices of subgroups G of some exceptional image $G_E(\ell) = \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ listed in Table 1 such that G belongs to $M(\ell)$, for the standard subgroups $M = Z, C_s, C_{ns}, N_s, N_{ns}, C_r$. Regarding notation, see (3.3).

Lemma 3.3. *The set of indices of subgroups G of $G_E(\ell)$ such that G belongs to $C_r(\ell)$ is the set of positive integers divisible by $\ell^2 - 1$ (resp. 2) and dividing $(\ell + 1)(\ell - 1)^2$ (resp. $2(\ell - 1)$) if G_E is GL_2 (resp. G, H_1, or H_2), and the empty set if G_E is N_s or N_{ns}.*

Proof. A subgroup of $\mathrm{GL}_2(\ell)$ belongs to $C_r(\ell)$ if and only if it is contained in $C_r(\ell)$ and contains $\langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right) \rangle$; the set of indices of such subgroups is evidently

$$\Delta([\mathrm{GL}_2(\ell) : C_r(\ell)] \mid [\mathrm{GL}_2(\ell) : \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right) \rangle]) = \Delta(\# \mathrm{GL}_2(\ell)/\ell(\ell - 1) \mid \# \mathrm{GL}_2(\ell)/\ell),$$

as desired.

Since $C_r(\ell) \subseteq G(\ell)$, we have

$$\mathcal{I}(G(\ell); C_r(\ell)) = \Delta((\ell^2 - 1)/[\mathrm{GL}_2(\ell) : G(\ell)] \mid (\ell + 1)(\ell - 1)^2/[\mathrm{GL}_2(\ell) : G(\ell)]) = \Delta(2 \mid 2(\ell - 1)).$$

The computations for $H_1(\ell)$ and $H_2(\ell)$ are analogous, and taking unions gives the result when G_E is allowed to be any of these three subgroups.

For the cases where $G_E(\ell)$ is $N_s(\ell)$ or $N_{ns}(\ell)$, it suffices to note that neither of these subgroups contains an element of order ℓ. $\square$

3.1. Full image.

Lemma 3.4. *The set of indices of subgroups G of $\mathrm{GL}_2(\ell)$ such that G belongs to $Z(\ell)$ is the set of positive integers divisible by $\ell(\ell + 1)(\ell - 1)$ and dividing $\ell(\ell + 1)(\ell - 1)^2$.*

Proof. Since finite abelian groups have subgroups of every order dividing the order of the group, and $\# Z(\ell) = \ell - 1$, it follows that

$$\mathcal{I}(\mathrm{GL}_2(\ell); Z(\ell)) = \{[\mathrm{GL}_2(\ell) : G] : G \leq Z(\ell)\} = \Delta(\ell(\ell + 1)(\ell - 1)^2/\# Z(\ell) \mid \ell(\ell + 1)(\ell - 1)^2),$$

as desired. $\square$

Lemma 3.5. *The set of indices of subgroups G of $\mathrm{GL}_2(\ell)$ such that G belongs to $C_s(\ell)$ is the set of positive integers divisible by $\ell(\ell + 1)$ and dividing an element of*

$$\{\ell(\ell + 1)(\ell - 1)^2/q : q \in \Pi(\ell - 1)\}.$$

G_E	M	$\mathcal{I}(G_E(\ell); M(\ell))$
GL$_2$	Z	$\Delta(\ell(\ell+1)(\ell-1) \mid \ell(\ell+1)(\ell-1)^2)$
	C_s	$\Delta(\{\ell(\ell+1)\}, \{\ell(\ell+1)(\ell-1)^2/q : q \in \Pi(\ell-1)\})$
	C_{ns}	$\Delta(\{\ell(\ell-1)\}, \{\ell(\ell+1)(\ell-1)^2/q : q \in \Pi_{\mathrm{odd}}(\ell+1) \cup \{2^{\nu_2(\ell-1)+1}\}\})$
	N_s	$\Delta(\{\ell(\ell+1)/2\}, \{\ell(\ell+1)(\ell-1)^2/2q : q \in \Pi_{\mathrm{odd}}(\ell-1) \cup \{4 \text{ if } 4 \mid (\ell-1), \text{ else } 2\}\})$
	N_{ns}	$\Delta(\ell(\ell-1)/2 \mid \ell(\ell+1)(\ell-1)^2/2)$
	C_r	$\Delta(\ell^2-1 \mid (\ell+1)(\ell-1)^2)$
N_s	Z	$\Delta(2(\ell-1) \mid 2(\ell-1)^2)$
	C_s	$\Delta(\{2\}, \{2(\ell-1)^2/q : q \in \Pi(\ell-1)\})$
	C_{ns}	$\Delta(\ell-1 \mid (\ell-1)^2/2^{\nu_2(\ell-1)})$
	N_s	$\Delta(\{1\}, \{(\ell-1)^2/q : q \in \Pi_{\mathrm{odd}}(\ell-1) \cup \{4 \text{ if } 4 \mid (\ell-1), \text{ else } 2\}\})$
	N_{ns}	$\Delta((\ell-1)/2 \mid (\ell-1)^2)$
	C_r	$\varnothing$
N_{ns}	Z	$\Delta(2(\ell+1) \mid 2(\ell^2-1))$
	C_s	$\Delta(\ell+1 \mid \ell^2-1)$
	C_{ns}	$\Delta(\{2\}, \{2(\ell^2-1)/q : q \in \Pi_{\mathrm{odd}}(\ell+1) \cup \{2^{\nu_2(\ell-1)+1}\}\})$
	N_s	$\Delta((\ell+1)/2 \mid (\ell^2-1)/2^{\nu_2(\ell-1)})$
	N_{ns}	$\Delta(1 \mid (\ell^2-1))$
	C_r	$\varnothing$
G, H_1, H_2	Z	$\Delta(2\ell \mid 2\ell(\ell-1))$
	C_s	$\Delta(\ell \mid \ell(\ell-1))$
	C_{ns}	$\varnothing$
	N_s	$\varnothing$
	N_{ns}	$\Delta(\ell \mid \ell(\ell-1))$
	C_r	$\Delta(2 \mid 2(\ell-1))$

TABLE 10. The set of indices of subgroups G of $G_E(\ell)$ such that G belongs to $M(\ell)$, for each possible non-exceptional image $G_E(\ell) = \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ and for the standard subgroups $M = Z, C_s, C_{ns}, N_s, N_{ns}, C_r$ (the final row should be interpreted in the manner of (3.2)). Regarding notation, see (3.3, 3.4).

Proof. Since $C_s(\ell) \simeq \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$, it contains non-scalar subgroups of every order dividing $\#C_s(\ell) = (\ell-1)^2$ except for 1, which corresponds to the trivial subgroup. The div-minimal such orders are therefore the prime divisors of $\ell-1$, and the proof concludes as in Lemma 3.4. $\square$

Lemma 3.6. *The set of indices of subgroups G of $\mathrm{GL}_2(\ell)$ such that G belongs to $C_{ns}(\ell)$ is the set of positive integers divisible by $\ell(\ell-1)$ and dividing an element of*
$$\{\ell(\ell+1)(\ell-1)^2/q : q \in \Pi_{\mathrm{odd}}(\ell+1) \cup \{2^{\nu_2(\ell-1)+1}\}\}.$$

Proof. Since $\#C_{ns}(\ell) = \ell^2-1$, we again have
$$\{[\mathrm{GL}_2(\ell) : G] : G \leq C_{ns}(\ell)\} = \Delta(\ell(\ell-1) \mid \ell(\ell+1)(\ell-1)^2),$$
however, certain subgroups of $C_{ns}(\ell)$ may instead lie in the standard subgroup $Z(\ell)$. Any div-minimal non-scalar subgroup G of $C_{ns}(\ell)$ with $2 \nmid \#G$ has trivial intersection with $Z(\ell)$, hence is isomorphic to its image in $\mathrm{PGL}_2(\ell)$, which has order dividing $\#C_{ns}(\ell)/(\ell-1) = \ell+1$. Since G must be non-trivial, we have $\#G \in \Pi_{\mathrm{odd}}(\ell+1)$, and all such possibilities for $\#G$ are realized as $C_{ns}(\ell)$ is cyclic.

Otherwise, if $\#G$ is even, then G must contain an element $\gamma = \mathcal{D}_{ns}(x,y) \in C_{ns}(\ell) \setminus Z(\ell)$ squaring to an element of $Z(\ell)$; the only such elements are those for which $x = 0$, which square to an element of $\epsilon Z(\ell)^2$, i.e., the non-square elements of $Z(\ell)$. Picking a primitive root $\alpha \in \mathbb{F}_\ell^\times$, we see that G is div-minimal when $\gamma^2 = \mathcal{D}_{ns}(\alpha^{(\ell-1)/2^{\nu_2(\ell-1)}}, 0)$ and $G = \langle \gamma \rangle$, that is, $\#G = 2^{\nu_2(\ell-1)+1}$.

Thus, the div-maximal indices in $\mathrm{GL}_2(\ell)$ of a non-diagonalizable subgroup of $C_{ns}(\ell)$ are
$$\{\ell(\ell+1)(\ell-1)^2/q : q \in \Pi_{\mathrm{odd}}(\ell+1) \cup \{2^{\nu_2(\ell-1)+1}\}\},$$

and $C_{ns}(\ell)$ contains subgroups of all intermediate indices as it is cyclic. $\qquad\square$

Lemma 3.7. *Let* $G := (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, *where*

$$\varphi \colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}), \qquad \tau \mapsto \begin{cases} \alpha \mapsto \beta, \\ \beta \mapsto \alpha, \end{cases}$$

for generators τ, α, *and* β *of* $\mathbb{Z}/2\mathbb{Z}$ *and the first and second copies of* $\mathbb{Z}/n\mathbb{Z}$, *respectively. Then for any* $H \leq G$ *containing* $(1, \tau)$, *we have*

$$\{\#K : H \leq K \leq G\} = \Delta(\#H \mid \#G).$$

Proof. Let H be a subgroup of G containing $(0, \tau)$. Then $(h, \tau) \in H$ if and only if $(h, 0) \in H$ as we may perform the group operation with $(0, \pm\tau)$ on the right. It follows that $H \simeq \pi_1(H) \rtimes_\varphi \langle \tau \rangle$, where π_1 denotes projection onto the first coordinate of the semi-direct product and $\pi_1(H) \leq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. For any $d \mid [G : H]$, we would like to show that there exists some subgroup $H \leq K \leq G$ with $[H : K] = d$. Iterating, we may assume that $p = d$ is prime. By Goursat's lemma [1, Thm. 4], $\pi_1(H)$ is given by the fiber product

$$\mathbb{Z}/m_1\mathbb{Z} \times_{\mathbb{Z}/r\mathbb{Z}} \mathbb{Z}/m_2\mathbb{Z} = \{(x, y) \in \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} : \psi_1(x) = \psi_2(y)\}$$

for some $r \mid m_i \mid n$, where the maps $\psi_i \colon \mathbb{Z}/m_i\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}$ are surjective for $i = 1, 2$. Since $\pi_1(H)$ must be $\varphi(\tau)$-invariant, it follows that $m_1 = m = m_2$ as $\varphi(\tau)$ maps each cyclic factor of $\pi_1(H)$ bijectively to the other. This condition is also sufficient: we have $(j \cdot \frac{n}{m}\alpha, k \cdot \frac{n}{m}\beta) \in \pi_1(H)$ if and only if $j \equiv k \bmod r$, which is true if and only if $\varphi(\tau)(j \cdot \frac{n}{m}\alpha, k \cdot \frac{n}{m}\beta) = (k \cdot \frac{n}{m}\alpha, j \cdot \frac{n}{m}\beta) \in \pi_1(H)$. Thus,

$$\#\pi_1(H) = \#\mathbb{Z}/r\mathbb{Z} \cdot \#\ker(\psi_1) \cdot \#\ker(\psi_2) = r \cdot \frac{m}{r} \cdot \frac{m}{r} = \frac{m^2}{r},$$

and so p divides

$$[G : H] = \frac{\#G}{\#H} = \frac{2n^2}{2m^2/r} = r\left(\frac{n}{m}\right)^2.$$

It follows that either $p \mid r$ or $p \mid \frac{n}{m}$.

In the former case, let $\kappa \colon \mathbb{Z}/r\mathbb{Z} \to \mathbb{Z}/(r/p)\mathbb{Z}$ be the unique quotient map, and let $K_1 := \mathbb{Z}/m\mathbb{Z} \times_{\mathbb{Z}/(r/p)\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$ with maps $\kappa \circ \psi_i \colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/(r/p)\mathbb{Z}$. As before, K_1 is $\varphi(\tau)$-invariant, and $\#K_1 = \frac{m^2}{r/p} = p \cdot \#\pi_1(H)$. Moreover, $\pi_1(H) \leq K_1$, since $\psi_1(x) = \psi_2(y)$ implies $(\kappa \circ \psi_1)(x) = (\kappa \circ \psi_2)(y)$ for $(x, y) \in \pi_1(H)$. It follows that $K := K_1 \rtimes_\varphi \langle \tau \rangle$ is a subgroup of G containing H as an index-p subgroup, as desired.

For the latter case, let $K_1 := \mathbb{Z}/pm\mathbb{Z} \times_{\mathbb{Z}/pr\mathbb{Z}} \mathbb{Z}/pm\mathbb{Z}$ (clearly $p \mid \frac{n}{r}$ as well) with maps $\psi_i' \colon \mathbb{Z}/pm\mathbb{Z} \to \mathbb{Z}/pr\mathbb{Z}$ for $i = 1, 2$. Then K_1 is again $\varphi(\tau)$-invariant, and $\#K_1 = \frac{(pm)^2}{pr} = p \cdot \#\pi_1(H)$. Moreover, $\pi_1(H) \leq K_1$, as the following diagram commutes for $i = 1, 2$, where we have let $\gamma := \psi_i(\frac{n}{m}\alpha)$ and $\gamma' := \psi_i'(\frac{n}{pm}\alpha)$ be generators of $\mathbb{Z}/r\mathbb{Z}$ and $\mathbb{Z}/pr\mathbb{Z}$, respectively:

$$\begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} \lhook\joinrel\longrightarrow \mathbb{Z}/pm\mathbb{Z} & & \frac{n}{m}\alpha \longmapsto p \cdot \frac{n}{pm}\alpha \\ \downarrow{\scriptstyle\psi_i} \qquad\qquad \downarrow{\scriptstyle\psi_i'} & & \downarrow \qquad\qquad \downarrow \\ \mathbb{Z}/r\mathbb{Z} \longrightarrow \mathbb{Z}/pr\mathbb{Z}, & & \gamma \longmapsto p\gamma'. \end{array}$$

Thus, $K := K_1 \rtimes_\varphi \langle \tau \rangle$ is again a subgroup of G containing H as an index-p-subgroup, and this completes the proof. $\qquad\square$

Lemma 3.8. *The set of indices of subgroups* G *of* $\mathrm{GL}_2(\ell)$ *such that* G *belongs to* $N_s(\ell)$ *is the set of positive integers divisible by* $\ell(\ell + 1)/2$ *and dividing an element of*

$$\left\{\ell(\ell + 1)(\ell - 1)^2/2q : q \in \Pi_{\mathrm{odd}}(\ell - 1) \cup \begin{cases} \{4\} & \text{if } 4 \mid (\ell - 1), \\ \{2\} & \text{otherwise.} \end{cases}\right\}.$$

Proof. Since $\#N_s(\ell) = 2(\ell - 1)^2$, we have

$$\{[\mathrm{GL}_2(\ell) : G] : G \leq N_s(\ell)\} \subseteq \Delta(\ell(\ell + 1)/2 \mid \ell(\ell + 1)(\ell - 1)^2),$$

however, certain subgroups of $N_s(\ell)$ may instead lie in the standard subgroup $C_s(\ell)$. Thus, any subgroup G belonging to $N_s(\ell)$ must be non-abelian, so it contains an anti-diagonal element; since any anti-diagonal

element of $N_s(\ell)$ has even order, $\#G$ is even. If $\#G = 4$, then G is abelian, hence conjugate to a subgroup of $C_s(\ell)$ or $C_{ns}(\ell)$; thus, if the former is not true, then G must be cyclic. If $\ell \equiv 1 \bmod 4$, then any element of $N_s(\ell)$ of order 4 is diagonalizable by Lemma 3.6, so such a G must be conjugate to a subgroup of $C_s(\ell)$. In this case,

$$(3.6) \qquad\qquad\qquad \langle \mathcal{A}_s(1,1), \mathcal{D}_s(1,-1) \rangle \simeq D_8$$

is a non-abelian subgroup of order 8, hence div-minimal. Otherwise, if $\ell \equiv 3 \bmod 4$, pick a primitive root $\alpha \in \mathbb{F}_\ell^\times$; the subgroup $\langle \mathcal{A}_s(\alpha, \alpha^{(\ell-3)/2}) \rangle$ is cyclic of order 4, and cannot be conjugate to a subgroup of $C_s(\ell)$ as $-1 \in \mathbb{F}_\ell^\times$ is not a square, so it is div-minimal.

Now, for each $q \in \Pi_{\mathrm{odd}}(\ell-1)$, the subgroup

$$\langle \mathcal{A}_s(1,1), \mathcal{D}_s(\alpha^{(\ell-1)/q}, \alpha^{-(\ell-1)/q}) \rangle \simeq D_{2q}$$

is non-abelian and of order $2q$, hence div-minimal. Thus,

$$(3.7) \qquad\qquad 2 \cdot (\Pi_{\mathrm{odd}}(\ell-1) \cup \{4 \text{ if } 4 \mid (\ell-1), \text{ else } 2\})$$

is the set of div-minima of $\mathcal{I}(\mathrm{GL}_2(\ell); N_s(\ell))$, for which the corresponding div-minimal subgroups each contain $\mathcal{A}_s(1,1)$ (if $\ell \equiv 3 \bmod 4$, then this is not the case for the div-minimal subgroup of order 4; however, any other integer in $\Delta(4 \mid 2(\ell-1)^2)$ will either be divisible by some other element of (3.7), or divisible by 8. Since the order-8 subgroup (3.6) contains $\mathcal{A}_s(1,1)$, the rest of the argument goes through unchanged). Since

$$N_s \simeq (\mathbb{Z}/(\ell-1)\mathbb{Z} \times \mathbb{Z}/(\ell-1)\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$$

with the non-trivial element $\mathcal{A}_s(1,1) \in \mathbb{Z}/2\mathbb{Z}$ corresponding to the automorphism in Lemma 3.7, it follows that

$$\Delta(\{\ell(\ell+1)/2\}, \{\ell(\ell+1)(\ell-1)^2/2q : q \in \Pi_{\mathrm{odd}}(\ell-1) \cup \{4 \text{ if } 4 \mid (\ell-1), \text{ else } 2\}\})$$

is in fact the set of possible indices of subgroups of $\mathrm{GL}_2(\ell)$ belonging to $N_s(\ell)$. $\qquad\square$

Lemma 3.9. *Let $G := \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi A$, where A is abelian. Then for any $H \leq G$ containing A, we have*

$$\{\#K : H \leq K \leq G\} = \Delta(\#H \mid \#G).$$

The same is true for any $H \leq G$ projecting trivially onto A.

Proof. As in Lemma 3.7, the projection $\pi_1(H)$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$, hence for any $d \mid [G : H] = n/\#\pi_1(H)$, there exists a unique subgroup $K_1 \leq \mathbb{Z}/n\mathbb{Z}$ of order $d \cdot \#\pi_1(H)$ containing $\pi_1(H)$. Letting α be a generator of $\mathbb{Z}/n\mathbb{Z}$, observe that any automorphism of $\mathbb{Z}/n\mathbb{Z}$ is of the form $\alpha \mapsto \alpha^i$, where $(i, n) = 1$, hence any cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ is $\varphi(a)$-invariant for each $a \in A$. Thus, $K := K_1 \rtimes_\varphi A$ is a subgroup of G containing H as an index-d subgroup, as desired.

For the second assertion, note that any $d \mid [G : H]$ factors as a product of $d_1 \mid [\mathbb{Z}/n\mathbb{Z} : \pi_1(H)]$ and $d_2 \mid \#A$. Letting K_1 be the unique order $d_1 \cdot \#\pi_1(H)$ subgroup of $\mathbb{Z}/n\mathbb{Z}$ containing $\pi_1(H)$ and K_2 be a subgroup of A of order d_2, we see that $K := K_1 \rtimes_\varphi K_2$ is again a subgroup of G containing H as an index-d subgroup. $\qquad\square$

Lemma 3.10. *Let $H \leq G$ such that $H \not\leq N$, for some index-2 subgroup N of G. Then $[H : H \cap N] = 2$.*

Proof. Let $\gamma \in H \cap (G \setminus N)$. Then $G = N \sqcup \gamma N$, and left multiplication by γ is a bijective map of sets on G, mapping N to γN and vice versa. Thus, $\gamma \cdot (H \cap N) \subset H \cap \gamma N$ has cardinality $\#(H \cap N)$, hence $[H : H \cap N] \geq 2$. Moreover, $\gamma \cdot (H \cap \gamma N) \subset H \cap N$ has cardinality $\#(H \cap \gamma N)$, hence $[H : H \cap N] \leq 2$, and the result follows. $\qquad\square$

Lemma 3.11. *The set of indices of subgroups G of $\mathrm{GL}_2(\ell)$ such that G belongs to $N_{ns}(\ell)$ is the set of positive integers divisible by $\ell(\ell-1)/2$ and dividing $\ell(\ell+1)(\ell-1)^2/2$.*

Proof. Since $\#N_{ns}(\ell) = 2(\ell^2-1)$, we have

$$\{[\mathrm{GL}_2(\ell) : G] : G \leq N_{ns}(\ell)\} \subseteq \Delta(\ell(\ell-1)/2 \mid \ell(\ell+1)(\ell-1)^2),$$

however, certain subgroups of $N_{ns}(\ell)$ may instead lie in the standard subgroup $C_{ns}(\ell)$. By Lemma 3.10, any subgroup of $N_{ns}(\ell)$ that is not contained in $C_{ns}(\ell)$ must have order divisible by 2. One such order-2 subgroup is $\langle \mathcal{A}_{ns}(1,0) \rangle$ (which is not conjugate to $\langle \mathcal{D}_{ns}(1,0) \rangle$, the unique order-2 subgroup of $C_{ns}(\ell)$), so by Lemma 3.9, the set of possible indices of subgroups of $\mathrm{GL}_2(\ell)$ belonging to $N_{ns}(\ell)$ is

$$\Delta([\mathrm{GL}_2(\ell) : N_{ns}(\ell)] \mid \#\mathrm{GL}_2(\ell)/2),$$

as desired. $\qquad\square$

3.2. Normalizer of a split Cartan.

Lemma 3.12. *The set of indices of subgroups G of $N_s(\ell)$ such that G belongs to $Z(\ell)$ is the set of positive integers divisible by $2(\ell-1)$ and dividing $2(\ell-1)^2$.*

Proof. Since finite abelian groups have subgroups of every order dividing the order of the groups, it follows that

$$\mathcal{I}(N_s(\ell); Z(\ell)) = \{[N_s(\ell) : G] : G \leq Z(\ell)\} = \Delta([N_s(\ell) : Z(\ell)] \mid \#N_s(\ell)),$$

as desired. $\qquad\square$

Lemma 3.13. *The set of indices of subgroups G of $N_s(\ell)$ such that G belongs to $C_s(\ell)$ is the set of positive integers divisible by 2 and dividing an element of*

$$\{2(\ell-1)^2/q : q \in \Pi(\ell-1)\}.$$

Proof. The result follows as in Lemma 3.5 after noting that $[N_s(\ell) : C_s(\ell)] = 2$. $\qquad\square$

Lemma 3.14. *The set of indices of subgroups G of $N_s(\ell)$ such that G belongs to $C_{ns}(\ell)$ is the set of positive integers divisible by $\ell-1$ and dividing $(\ell-1)^2/2^{\nu_2(\ell-1)}$.*

Proof. Let $\alpha \in \mathbb{F}_\ell^\times$ be a primitive root. Clearly, $\langle \mathcal{A}_s(1,\alpha) \rangle \leq N_s(\ell)$ has order $2(\ell-1)$, hence it is an index-$(\ell-1)$ subgroup belonging to $C_{ns}(\ell)$ (as the maximal cyclic subgroups of $C_s(\ell)$ are of order $\ell-1$). Since any anti-diagonal element of $N_s(\ell)$ squares to a diagonal element, $2(\ell-1)$ is the maximal order of an element of $N_s(\ell)$, hence any subgroup of $N_s(\ell)$ belonging to $C_{ns}(\ell)$ has index divisible by $\ell-1$ in $N_s(\ell)$. Now, since $\mathcal{A}_s(1,\alpha)^2 \in Z(\ell)$ (the same is true for any other order $2(\ell-1)$ cyclic subgroup of $N_s(\ell)$), a subgroup of $\langle \mathcal{A}_s(1,\alpha) \rangle$ is conjugate to a subgroup of $Z(\ell)$ if and only if its order divides $\ell-1$; thus, a subgroup of $\langle \mathcal{A}_s(1,\alpha) \rangle$ is not conjugate to a subgroup of $Z(\ell)$ if and only if it contains the unique subgroup of order $2^{\nu_2(\ell-1)+1}$. Since $\langle \mathcal{A}_s(1,\alpha) \rangle$ is cyclic, it contains a unique subgroup of each possible order, and therefore

$$\Delta(\ell-1 \mid 2(\ell-1)^2/2^{\nu_2(\ell-1)+1})$$

is indeed the set of indices of subgroups of $N_s(\ell)$ belonging to $C_{ns}(\ell)$. $\qquad\square$

Lemma 3.15. *The set of indices of subgroups G of $N_s(\ell)$ such that G belongs to $N_s(\ell)$ is the set of positive integers dividing an element of*

$$\{(\ell-1)^2/q : q \in \Pi_{\mathrm{odd}}(\ell-1) \cup \{4 \text{ if } 4 \mid (\ell-1), \text{ else } 2\}\}.$$

Proof. By Lemma 3.8, this is obtained by dividing all indices of $\mathcal{I}(\mathrm{GL}_2(\ell); N_s(\ell))$ by

$$[\mathrm{GL}_2(\ell) : N_s(\ell)] = \frac{\ell(\ell+1)}{2},$$

as

$$\{G \leq \mathrm{GL}_2(\ell) : G \text{ belongs to } N_s(\ell)\} = \{G \leq N_s(\ell) : G \text{ belongs to } N_s(\ell)\},$$

which clearly yields the desired set. $\qquad\square$

Lemma 3.16. *The set of indices of subgroups G of $N_s(\ell)$ such that G belongs to $N_{ns}(\ell)$ is the set of positive integers divisible by $(\ell-1)/2$ and dividing $(\ell-1)^2$.*

Proof. Observe that

$$Z(\ell) \cdot \{\mathcal{D}_s(1,1), \mathcal{D}_s(1,-1), \mathcal{A}_s(\epsilon,1), \mathcal{A}_s(-\epsilon,1)\} = N_s(\ell) \cap N_{ns}(\ell) \leq N_s(\ell)$$

is a subgroup of order $4(\ell-1)$ contained in $N_{ns}(\ell)$, isomorphic to $\mathbb{Z}/2(\ell-1)\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. By Lemma 3.10, any subgroup of $N_{ns}(\ell)$ is either contained in $C_{ns}(\ell)$ or has an index-2 subgroup contained in $C_{ns}(\ell)$, hence by Lemma 3.14, $\#G \mid 2 \cdot 2(\ell-1) = 4(\ell-1)$ for any $G \leq N_s(\ell)$ belonging to $N_{ns}(\ell)$. Moreover, by Lemma 3.10, any subgroup of $N_s(\ell)$ belonging to $N_{ns}(\ell)$ must have order divisible by 2; as in Lemma 3.11, one such order-2 subgroup is $\langle \mathcal{A}_{ns}(1,0) \rangle$, so by Lemma 3.9, the set of possible indices of subgroups of $N_s(\ell)$ belonging to $N_{ns}(\ell)$ is

$$\Delta(\#N_s(\ell)/4(\ell-1) \mid \#N_s(\ell)/2),$$

as desired. $\qquad\square$

3.3. **Normalizer of a non-split Cartan.**

Lemma 3.17. *The set of indices of subgroups G of $N_{ns}(\ell)$ such that G belongs to $C_s(\ell)$ is the set of positive integers divisible by $2(\ell+1)$ and dividing $2(\ell^2-1)$.*

Proof. The result follows as in Lemma 3.12 after noting that $Z(\ell) = \{\mathcal{D}_{ns}(x,0) : x \in \mathbb{F}_\ell^\times\} \leq N_{ns}(\ell)$. $\qquad\square$

Lemma 3.18. *The set of indices of subgroups G of $N_{ns}(\ell)$ such that G belongs to $C_s(\ell)$ is the set of positive integers divisible by $\ell+1$ and dividing ℓ^2-1.*

Proof. Clearly,

$$(3.8) \qquad Z(\ell) \cdot \{\mathcal{D}_{ns}(1,0), \mathcal{A}_{ns}(1,0)\} = N_{ns}(\ell) \cap C_s(\ell) \leq N_{ns}(\ell)$$

is a subgroup of order $2(\ell-1)$ (isomorphic to $\mathbb{Z}/(\ell-1)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) belonging to $C_s(\ell)$. For any $G \leq N_{ns}(\ell)$ belonging to $C_s(\ell)$, the proof of Lemma 3.11 shows that G is conjugate to a subgroup of

$$Z(\ell) \cdot \{\mathcal{D}_s(1,1), \mathcal{A}_s(1,1)\} \subseteq N_s(\ell),$$

since G has exponent dividing $\ell-1$. This group is further conjugate to (3.8) (via $\left(\begin{smallmatrix}1&1\\-1&1\end{smallmatrix}\right)$), so $\#G \mid 2(\ell-1)$. Now, a subgroup of (3.8) belongs to $C_s(\ell)$ if and only if contains a multiple of $\mathcal{A}_{ns}(1,0)$, that is, if and only if its order is divisible by 2. Thus,

$$\mathcal{I}(N_{ns}(\ell); C_s(\ell)) = \Delta(\#N_{ns}(\ell)/(2(\ell-1)) \mid \#N_{ns}(\ell)/2),$$

as desired. $\qquad\square$

Lemma 3.19. *The set of indices of subgroups G of $N_{ns}(\ell)$ such that G belongs to $C_{ns}(\ell)$ is the set of positive integers divisible by 2 and dividing an element of*

$$\{2(\ell^2-1)/q : q \in \Pi_{\text{odd}}(\ell+1) \cup \{2^{\nu_2(\ell-1)+1}\}\}.$$

Proof. The proof is as that of Lemma 3.15, applied to Lemma 3.6. $\qquad\square$

Lemma 3.20. *The set of indices of subgroups G of $N_{ns}(\ell)$ such that G belongs to $N_s(\ell)$ is the set of positive integers divisible by $(\ell+1)/2$ and dividing $(\ell^2-1)/2^{\nu_2(\ell-1)}$.*

Proof. Observe that

$$Z(\ell) \cdot \{\mathcal{D}_{ns}(1,0), \mathcal{D}_{ns}(0,1), \mathcal{A}_{ns}(1,0), \mathcal{A}_{ns}(0,1)\} = N_{ns}(\ell) \cap N_s(\ell) \leq N_{ns}(\ell)$$

is a subgroup of order $4(\ell-1)$ contained in $N_s(\ell)$. Moreover, by Lemma 3.10, any subgroup of $N_s(\ell)$ is either contained in $C_s(\ell)$ or has an index-2 subgroup contained in $C_s(\ell)$, hence by Lemma 3.18, $\#G \mid 2 \cdot 2(\ell-1) = 4(\ell-1)$ for any $G \leq N_{ns}(\ell)$ belonging to $N_s(\ell)$. Now, any subgroup of $N_{ns}(\ell)$ belonging to $N_s(\ell)$ of order $4(\ell-1)$ is conjugate to $N_{ns}(\ell) \cap N_s(\ell)$, so it suffices to find the div-minimal subgroups of $N_{ns}(\ell) \cap N_s(\ell)$ belonging to $N_s(\ell)$. Any such subgroup is either cyclic and generated by a non-diagonalizable matrix or non-abelian. Thus, in the first case, it must be generated by an element of $Z(\ell) \cdot \mathcal{D}_{ns}(0,1)$, or, if $\ell \equiv 1 \bmod 4$, an element of $Z(\ell) \cdot \mathcal{A}_{ns}(0,1)$; regardless, the div-minimal order is $2^{\nu_2(\ell-1)+1}$ as in Lemma 3.6. In the latter case, it must be generated by two elements, each from a distinct set in

$$\{Z(\ell) \cdot \mathcal{D}_{ns}(0,1), Z(\ell) \cdot \mathcal{A}_{ns}(1,0), Z(\ell) \cdot \mathcal{A}_{ns}(0,1)\}.$$

However, given any two such elements, multiplying them gives an element of the unchosen set, hence we may suppose without loss of generality that our subgroup is given by $\langle \gamma, \delta \rangle$, where $\gamma \in Z(\ell) \cdot \mathcal{D}_{ns}(0,1)$ and $\delta \in Z(\ell) \cdot \mathcal{A}_{ns}(1,0)$. By Lemma 3.10, $\#\langle \gamma, \delta \rangle$ is div-minimal when $\#(\langle \gamma, \delta \rangle \cap C_s(\ell))$ is, so since $2 \mid \#\langle \delta \rangle$, we may assume $\delta = \mathcal{A}_{ns}(1,0)$, and since $2^{\nu_2(\ell-1)+1} \mid \#\langle \gamma \rangle$ as in Lemma 3.6, we may assume $\gamma = \mathcal{D}_{ns}(0, \beta)$, where $\beta^2 = \epsilon^{-1}\alpha^{(\ell-1)/2^{\nu_2(\ell-1)}}$ and $\alpha \in \mathbb{F}_\ell^\times$ is a primitive root. Now, since $\gamma \delta \gamma^{-1} = \mathcal{A}_{ns}(-1,0) \in \langle \gamma, \delta \rangle$, it follows that

$$\#(\langle \gamma, \delta \rangle \cap C_s(\ell)) = \#(\{\mathcal{D}_{ns}(1,0), \mathcal{D}_{ns}(-1,0), \mathcal{A}_{ns}(1,0), \mathcal{A}_{ns}(-1,0)\} \cdot \langle \gamma^2 \rangle)$$

$$= \frac{\#\langle \mathcal{A}_{ns}(1,0), \mathcal{A}_{ns}(-1,0)\rangle \cdot \#\langle \gamma^2 \rangle}{\#(\langle \mathcal{A}_{ns}(1,0), \mathcal{A}_{ns}(-1,0)\rangle \cap \langle \gamma^2 \rangle)}$$

$$= \frac{4 \cdot 2^{\nu_2(\ell-1)}}{2}$$

$$= 2^{\nu_2(\ell-1)+1},$$

so Lemma 3.10 implies that

$$\#\langle\gamma,\delta\rangle = 2\cdot\#(\langle\gamma,\delta\rangle\cap C_s(\ell)) = 2\cdot 2^{\nu_2(\ell-1)+1} = 2^{\nu_2(\ell-1)+2},$$

which is divisible by $2^{\nu_2(\ell-1)+1}$, the div-minimal order in the first case. Thus, by Lemma 3.9, we have

$$\mathcal{I}(N_{ns}(\ell); N_s(\ell)) = \Delta(\#N_{ns}(\ell)/(4(\ell-1)) \mid \#N_{ns}(\ell)/2^{\nu_2(\ell-1)+1}),$$

as desired. $\qquad\square$

Lemma 3.21. *The set of indices of subgroups G of $N_{ns}(\ell)$ such that G belongs to $N_{ns}(\ell)$ is the set of positive integers dividing ℓ^2-1.*

Proof. The proof is as that of Lemma 3.15, applied to Lemma 3.11. $\qquad\square$

3.4. Borel cases.

Lemma 3.22. *Let $G \leq B(\ell)$, and suppose that G does not contain an element of order ℓ. Then G is conjugate to a subgroup of $C_s(\ell)$.*

Proof. Let H denote the image of G in $\mathrm{PGL}_2(\ell)$, and observe that $S := \{x : \left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right) \in H\}$ forms a subgroup of $\mathbb{F}_\ell^\times$, of which we let a be a generator (as it must be cyclic). Then there exists some $\gamma := \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in H$, and for any n, we have

$$\gamma^n = \begin{pmatrix} a^n & b(1+a+\cdots+a^{n-1}) \\ 0 & 1 \end{pmatrix},$$

so $a \neq 1$ unless $b = 0$, as otherwise $\mathrm{ord}(\gamma) = \ell$ (and all its lifts to $B(\ell)$ have order divisible by ℓ). If $a \neq 1$, then $1 + a + \cdots + a^{n-1} = 0$ if and only if

$$(1-a)(1+a+\cdots+a^{n-1}) = 1 - a^n = 0,$$

that is, $\mathrm{ord}(a) \mid n$, from which it follows that $\mathrm{ord}(\gamma) = \mathrm{ord}(a) \mid (\ell-1)$. Letting $\gamma' := \left(\begin{smallmatrix} a' & b' \\ 0 & 1 \end{smallmatrix}\right) \in H$ and r be such that $a^{-r} = a'$ (which exists as $a' \in S$), we have

$$\gamma^r\gamma' = \begin{pmatrix} a^r a' & a^r b' + b(1+a+\cdots+a^{r-1}) \\ 0 & 1 \end{pmatrix},$$

and so $b' = -ba^{-r}(1+a+\cdots+a^{n-1})$ since otherwise $\gamma^r\gamma'$ has order ℓ as above. But then $\gamma' = \gamma^{-r}$, implying that $H = \langle\gamma\rangle$ is cyclic. Since every element of $B(\ell)$ has an eigenvalue in $\mathbb{F}_\ell$, whereas no element of $C_{ns}(\ell) \setminus Z(\ell)$ has any eigenvalues over $\mathbb{F}_\ell$ (as those of $\mathcal{D}_{ns}(x,y) \in C_{ns}(\ell)$ are $x \pm y\sqrt{\epsilon} \in \overline{\mathbb{F}_\ell}$), G is conjugate to a subgroup of $C_s(\ell)$ by Proposition 2.1, as desired. $\qquad\square$

Lemma 3.23. *The set of indices of subgroups G of $G(\ell)$, $H_1(\ell)$, or $H_2(\ell)$ such that G belongs to a standard subgroup $M(\ell)$ is the set of positive integers divisible by 2ℓ (resp. ℓ) and dividing $2\ell(\ell-1)$ (resp. $\ell(\ell-1)$) if M is Z (resp. C_s); the empty set if M is C_{ns} or N_s; and the set of positive integers divisible by ℓ and dividing $\ell(\ell-1)$ if M is N_{ns}.*

Proof. Evidently, $[G(\ell) : G(\ell) \cap C_s(\ell)] = \ell$, and since $G(\ell)$ contains an element of order ℓ, any subgroup of $G(\ell)$ conjugate to a subgroup of $C_s(\ell)$ must have index divisible by ℓ in $G(\ell)$. Since

$$G(\ell) \cap C_s(\ell) = Z(\ell) \cdot \{\mathcal{D}_s(1,1), \mathcal{D}_s(1,-1)\},$$

the proof of Lemma 3.18 shows that

$$\mathcal{I}(G(\ell); C_s(\ell)) = \Delta(\ell \mid \#G(\ell)/2) = \Delta(\ell \mid \ell(\ell-1)).$$

Also, $\mathcal{I}(G(\ell); Z(\ell)) = \Delta(2\ell \mid 2\ell(\ell-1))$ as before. Performing the analogous computations for $H_1(\ell)$ and $H_2(\ell)$ and taking unions gives the result if M is Z or C_s.

For the case where M is C_{ns}, observe that any subgroup of $C_{ns}(\ell)$ conjugate to a subgroup of $C_s(\ell)$ is contained in $Z(\ell)$: an element $\mathcal{D}_{ns}(x,y) \in C_{ns}(\ell)$ is diagonalizable if and only if

$$(2x)^2 - 4(x^2 - \epsilon y^2) = 4\epsilon y^2 \in (\mathbb{F}_\ell)^2,$$

that is, $y = 0$. Thus, $\mathcal{I}(G(\ell), H_1(\ell), H_2(\ell); C_{ns}(\ell)) = \varnothing$ by Lemma 3.22.

The case where M is N_s is immediate from Lemma 3.22.

For the case where M is N_{ns}, we must identify the non-scalar subgroups of $G(\ell)$ that are conjugate to a subgroup of $N_{ns}(\ell)$. These cannot contain an element of order ℓ, so we may assume that they are subgroups of

$$G(\ell) \cap C_s(\ell) = Z(\ell) \cdot \{\mathcal{D}_{ns}(1,0), \mathcal{A}_{ns}(1,0)\} \subseteq N_{ns}(\ell).$$

It immediately follows that $\mathcal{I}(G(\ell); N_{ns}(\ell) = \mathcal{I}(G(\ell); C_s(\ell))$; performing a similar analysis for $H_1(\ell)$ and $H_2(\ell)$ and taking unions then gives the desired result. $\qquad\square$

4. Proof of Theorem 1.4

Let E/K be an elliptic curve, for some number field K. The Mordell–Weil group $E(K)$ contains a point of order ℓ if and only if $\rho_{E,\ell}(\mathrm{Gal}(\overline{K}/K))$ fixes a nonzero element of $\mathbb{F}_\ell^2$. Thus, as in the proof of Theorem 1.2, there exists a degree-d number field K and an elliptic curve $E/\mathbb{Q}$ for which $E(K)$ contains a point of order ℓ if and only if $\rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ contains a degree-t subgroup fixing a nonzero element of $\mathbb{F}_\ell^2$ for some $t \mid d$. The same is true of an elliptic curve E/K with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$ if and only if $\rho_{E,\ell}(\mathrm{Gal}(\overline{K}/K))$ is a twist of a degree-t subgroup of $\rho_{E',\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ for some elliptic curve $E'/\mathbb{Q}$ and $t \mid d$, and it fixes a nonzero element of $\mathbb{F}_\ell^2$. For a subgroup $G \le \mathrm{GL}_2(\ell)$, define

$$\mathcal{I}(G_1, \ldots, G_n) := \{[G_i : H] : H \le G_i \text{ such that } H'v = v \text{ for some } 0 \ne v \in \mathbb{F}_\ell^2,$$
(4.1)
$$\text{twist } H' \text{ of } H, \text{ and } 1 \le i \le n\},$$

$$\mathcal{I}_\mathbb{Q}(G_1, \ldots, G_n) := \{[G_i : H] : H \le G_i \text{ such that } Hv = v \text{ for some } 0 \ne v \in \mathbb{F}_\ell^2 \text{ and } 1 \le i \le n\},$$

and let div-min(S) denote the div-minima of a set S. By the above, it remains to determine the sets

$$\mathcal{T}(\ell) = \text{div-min} \bigcup_{E/\mathbb{Q}} \mathcal{I}(G_E(\ell)), \qquad \mathcal{T}_\mathbb{Q}(\ell) = \text{div-min} \bigcup_{E/\mathbb{Q}} \mathcal{I}_\mathbb{Q}(G_E(\ell)),$$

where the elliptic curves in each union are assumed to satisfy $j(E) \ne 0, 1728$. We begin by determining the sets div-min $\mathcal{I}(G_E(\ell))$ individually for every possible image $G_E(\ell) = \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$; the sets div-min $\mathcal{I}_\mathbb{Q}(G_E(\ell))$ may be determined analogously.

If E does not have CM, then $G_E(\ell)$ is either $\mathrm{GL}_2(\ell)$ or one of the 63 exceptional groups listed in Table 1 by our assumption of Conjecture 1.1. The results for each exceptional subgroup were computed [31,34] using Magma, and the div-minima of the unions of the two sets (4.1) of indices over each $\mathrm{Excep}(\ell)$ are the sets $\mathcal{I}(\mathrm{Excep}(\ell))$ and $\mathcal{I}_\mathbb{Q}(\mathrm{Excep}(\ell))$, respectively, listed in Table 11. The set div-min $\mathcal{I}(\mathrm{GL}_2(\ell))$ is determined by Lemma 4.1 below, and appears in Table 12.

Now suppose E has CM. As in the proof of Theorems 1.2 and 1.3, $G_E(\ell)$ is conjugate to $N_s(\ell)$ (resp. $N_{ns}(\ell)$) if $\ell \in \mathcal{P}$ (resp. $\ell \in \mathcal{Q}$); to either $N_s(\ell)$, $N_{ns}(\ell)$, $G(\ell)$, $H_1(\ell)$, or $H_2(\ell)$ if $\ell \in \{3, 7, 11, 19, 43, 67, 163\}$, with each case occurring for some such E; and otherwise to either $N_s(\ell)$ or $N_{ns}(\ell)$, with each case again occurring for some such E [36, Prop. 1.14]. The set div-min $\mathcal{I}(N_s(\ell))$ is determined by Lemma 4.2; the set div-min$(\mathcal{I}(N_{ns}(\ell))$ by Lemma 4.3; and the set div-min $\mathcal{I}(G(\ell), H_1(\ell), H_2(\ell))$ by Lemma 4.4. All appear in Table 12.

Finally, the sets appearing in Tables 7 and 6 are determined by letting $\mathcal{T}(\ell)$ be the div-minima of the set

$$\mathcal{I}(\mathrm{Excep}(\ell), \mathrm{GL}_2(\ell)) \cup \begin{cases} \mathcal{I}(N_s(\ell)) & \text{if } \ell \in \mathcal{P}, \\ \mathcal{I}(N_{ns}(\ell)) & \text{if } \ell \in \mathcal{Q}, \\ \mathcal{I}(N_s(\ell), N_{ns}(\ell), G(\ell), H_1(\ell), H_2(\ell)) & \text{if } \ell \in \{3, 7, 11, 19, 43, 67, 163\}, \\ \mathcal{I}(N_s(\ell), N_{ns}(\ell)) & \text{otherwise.} \end{cases},$$

and similarly for the sets $\mathcal{T}^{\mathrm{CM}}(\ell)$ and $\mathcal{T}^{\mathrm{non\text{-}CM}}(\ell)$.

We now turn to the task of proving the lemmas used above, which will complete the proof of Theorem 1.4.

Lemma 4.1. *The set of indices of subgroups G of $\mathrm{GL}_2(\ell)$ such that a twist of G fixes a nonzero element of $\mathbb{F}_\ell^2$ has div-minima $\{(\ell^2 - 1)/2\}$.*

Proof. Any subgroup of $\mathrm{GL}_2(\ell)$ fixing each element of a 1-dimensional $\mathbb{F}_\ell$-subspace of $\mathbb{F}_\ell^2$ must be conjugate to a subgroup fixing $\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle$. Such a subgroup must be upper triangular, with a 1 in the upper left-hand entry of each matrix, hence it is a subgroup of

$$T := \{ \left(\begin{smallmatrix} 1 & a \\ 0 & b \end{smallmatrix}\right) : a \in \mathbb{F}_\ell, b \in \mathbb{F}_\ell^\times \} \le B(\ell) \le \mathrm{GL}_2(\ell),$$

ℓ	div-min $\mathcal{I}(\mathrm{Excep}(\ell))$	div-min $\mathcal{I}_\mathbb{Q}(\mathrm{Excep}(\ell))$
$2,3,5,7$	1	1
11	5	5
13	$2,3$	$3,4$
17	4	8
37	6	12
other	$\varnothing$	$\varnothing$

TABLE 11. div-Minima of the set of indices of subgroups G of some exceptional image $G_E(\ell) = \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ listed in Table 1 such that a twist of G (or, in the third column, G itself) fixes a nonzero vector of $\mathbb{F}_\ell^2$.

G_E	div-min $\mathcal{I}(G_E(\ell))$	div-min $\mathcal{I}_\mathbb{Q}(G_E(\ell))$
GL_2	$(\ell^2-1)/2$	ℓ^2-1
N_s	$\ell-1$	$2(\ell-1)$
N_{ns}	$(\ell^2-1)/2$	ℓ^2-1
G, H_1, H_2	$(\ell-1)/2$	$(\ell-1)/2$

TABLE 12. div-Minima of the set of indices of subgroups G of $G_E(\ell)$ such that a twist of G (or, in the third column, G itself) fixes a nonzero vector of $\mathbb{F}_\ell^2$, for each non-exceptional possible image $G_E(\ell) = \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ (the final row should be interpreted in the manner of (4.1)).

which has order $\ell(\ell-1)$, hence index ℓ^2-1 in $\mathrm{GL}_2(\ell)$.

Now, since -1 does not fix any nontrivial element of $\mathbb{F}_\ell^2$, we need only consider index-2 subgroups $H \leq \langle G, -1 \rangle$ with $-1 \notin H$, where $H \leq T$ and $G \leq \mathrm{GL}_2(\ell)$, by the previous paragraph. Both $[\mathrm{GL}_2(\ell) : H]$ and $[\mathrm{GL}_2(\ell) : G]$ are either $[\mathrm{GL}_2(\ell) : \langle G, -1 \rangle]$ or $2 \cdot [\mathrm{GL}_2(\ell) : \langle G, -1 \rangle]$, and evidently $[\mathrm{GL}_2(\ell) : G]$ is div-minimal when $-1 \in G$ and $[\mathrm{GL}_2(\ell) : H] = 2 \cdot [\mathrm{GL}_2(\ell) : G]$. Taking $G = \langle T, -1 \rangle$ then gives a subgroup of $\mathrm{GL}_2(\ell)$ of index $(\ell^2-1)/2$ with $[G : T] = 2$. For any other such G and H, we have

$$(\ell^2-1) \mid [\mathrm{GL}_2(\ell) : T] \mid [\mathrm{GL}_2(\ell) : H] \mid 2 \cdot [\mathrm{GL}_2(\ell) : G],$$

implying $(\ell^2-1)/2 \mid [\mathrm{GL}_2(\ell) : G]$, as desired. $\qquad\square$

Lemma 4.2. *The set of indices of subgroups G of $N_s(\ell)$ such that a twist of G fixes a nonzero element of $\mathbb{F}_\ell^2$ has div-minima $\{(\ell-1)\}$.*

Proof. The proof is identical to that of Lemma 4.1, with $\mathrm{GL}_2(\ell)$ replaced by $N_s(\ell)$ and T replaced by each of the subgroups identified in [24, Lem. 6.6] in turn. $\qquad\square$

Lemma 4.3. *The set of indices of subgroups G of $N_{ns}(\ell)$ such that a twist of G fixes a nonzero element of $\mathbb{F}_\ell^2$ has div-minima $\{(\ell^2-1)/2\}$.*

Proof. The proof is identical to that of Lemma 4.1, with $\mathrm{GL}_2(\ell)$ replaced by $N_{ns}(\ell)$ and T replaced by each of the subgroups identified in [24, Lem. 7.4] in turn. $\qquad\square$

Lemma 4.4. *Suppose $\ell \equiv 3 \bmod 4$. The set of indices of subgroups G of $G(\ell)$, $H_1(\ell)$, or $H_2(\ell)$ such that a twist of G fixes a nonzero element of $\mathbb{F}_\ell^2$ has div-minima $\{(\ell-1)/2\}$.*

Proof. The characteristic polynomial of an element $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \in G(\ell)$ is $(\lambda - a)^2$, hence it has eigenvalue 1 if and only if $a = 1$. Similarly, the characteristic polynomial of an element $\left(\begin{smallmatrix} a & b \\ 0 & -a \end{smallmatrix}\right) \in G(\ell)$ is $\lambda^2 - a^2$, hence it has eigenvalue 1 if and only if $a = \pm 1$. If $a = -1$, then it fixes every element of the space $\langle \left(\begin{smallmatrix} b \\ -1 \\ 1 \end{smallmatrix}\right) \rangle$, hence it is the only nontrivial element of $G(\ell)$ fixing every element of this space, and $\langle \left(\begin{smallmatrix} -1 & b \\ 0 & 1 \end{smallmatrix}\right) \rangle \leq G(\ell)$ is a subgroup of

order 2. Otherwise, if $a = 1$, then both types of elements fix every element of $\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix} \right) \rangle$, and together they form the index-$(\ell - 1)$ subgroup

$$\{ \left(\begin{smallmatrix} 1 & b \\ 0 & \pm 1 \end{smallmatrix} \right) : b \in \mathbb{F}_\ell \} \leq G(\ell),$$

which is maximal as its order, 2ℓ, is divisible by 2.

The same reasoning shows that the subgroup $\{ \left(\begin{smallmatrix} 1 & b \\ 0 & \pm 1 \end{smallmatrix} \right) : b \in \mathbb{F}_\ell \} \leq H_1(\ell)$ is maximal, and it also has order 2ℓ, hence index $(\ell - 1)/2$.

For $H_2(\ell)$, we obtain the same characteristic polynomials, but in this case elements $\left(\begin{smallmatrix} -a & b \\ 0 & a \end{smallmatrix} \right) \in G(\ell)$ with $a = 1$ each generate order-2 subgroups fixing $\langle \left(\begin{smallmatrix} b-1 \\ 1 \end{smallmatrix} \right) \rangle$, and the elements of $H_2(\ell)$ with upper left-hand entry 1 form a subgroup of order ℓ, since $\ell \equiv 3 \bmod 4$ by assumption and therefore $-1 \notin (\mathbb{F}_\ell^\times)^2$. Thus, the two div-minimal indices of such subgroups of $H_2(\ell)$ are $\ell - 1$ and $\ell(\ell - 1)/2$.

Repeating the proof of Lemma 4.1 with $\mathrm{GL}_2(\ell)$ replaced by $G(\ell)$ and T replaced by each of the subgroups of $G(\ell)$ identified above in turn shows that $\mathcal{I}(G(\ell)) = \{(\ell - 1)/2\}$. Since $-1 \notin H_1(\ell), H_2(\ell)$ as $\ell \equiv 3 \bmod 4$ by assumption, any twist of a subgroup H of $H_1(\ell)$ or $H_2(\ell)$ is a subgroup of H, hence $\mathcal{I}(H_1(\ell)) = \mathcal{I}_\mathbb{Q}(H_1(\ell)) = \{(\ell - 1)/2\}$ and $\mathcal{I}(H_2(\ell)) = \mathcal{I}_\mathbb{Q}(H_2(\ell)) = \{\ell - 1, \ell(\ell - 1)/2\}$. Thus, among $G(\ell)$, $H_1(\ell)$, and $H_2(\ell)$, the div-minimal index is $(\ell - 1)/2$. $\qquad\square$

References

[1] D. D. Anderson and V. Camillo. Subgroups of direct products of groups, ideals and subrings of direct products of rings, and Goursat's lemma. In *Rings, modules and representations*, volume 480 of *Contemp. Math.*, pages 1–12. Amer. Math. Soc., Providence, RI, 2009.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24:235–265, 1997.

[3] Abbey Bourdon and Pete L. Clark. Torsion points and Galois representations on CM elliptic curves. *arXiv:1612.03229*, 2016.

[4] Abbey Bourdon, Pete L. Clark, and James Stankewicz. Torsion points on CM elliptic curves over real number fields. *Trans. Amer. Math. Soc. (to appear)*.

[5] Abbey Bourdon and Paul Pollack. Torsion subgroups of CM elliptic curves over odd degree number fields. *Int. Math. Res. Not. IMRN. (to appear)*.

[6] Peter Bruin and Filip Najman. A criterion to rule out torsion groups for elliptic curves over number fields. *Res. Number Theory*, 2:23, 2016.

[7] Michael Chou. Torsion of rational elliptic curves over quartic Galois number fields. *J. Number Theory*, 160:603–628, 2016.

[8] Pete L. Clark, Patrick Corn, Alex Rice, and James Stankewicz. Computation on elliptic curves with complex multiplication. *LMS J. Comput. Math.*, 17(1):509–535, 2014.

[9] John E. Cremona. Elliptic curves over $\mathbb{Q}$. available at *http://www.lmfdb.org/EllipticCurve/Q/*, 2016.

[10] Maarten Derickx and Andrew V. Sutherland. Torsion subgroups of elliptic curves over quintic and sextic number fields. *Proc. Amer. Math. Soc. (to appear)*.

[11] Leonard E. Dickson. *Linear groups with an exposition of Galois field theory*. Cosimo Classics 2007 reprint of original publication by B. G. Teubner, Leipzig, 1901.

[12] Enrique González-Jiménez. Complete classification of the torsion structures of rational elliptic curves over quintic number fields. *Journal of Algebra (to appear)*.

[13] Enrique González-Jiménez and Álvaro Lozano-Robledo. On the minimal degree of definition of p-primary torsion subgroups of elliptic curves. *Math. Res. Lett. (to appear)*.

[14] Enrique González-Jiménez and Álvaro Lozano-Robledo. On the torsion of rational elliptic curves over quartic fields. *Math. Comp. (to appear)*.

[15] Enrique González-Jiménez and Álvaro Lozano-Robledo. Elliptic curves with abelian division fields. *Math. Z.*, 283(3-4):835–859, 2016.

[16] Enrique González-Jiménez and Filip Najman. Growth of torsion groups of elliptic curves upon base change. *arXiv:1609.02515*, 2016.

[17] Daeyeol Jeon. Families of elliptic curves over cyclic cubic number fields with prescribed torsion. *Math. Comp.*, 85(299):1485–1502, 2016.

[18] Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee. Families of elliptic curves over cubic number fields with prescribed torsion subgroups. *Math. Comp.*, 80(273):579–591, 2011.

[19] Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee. Infinite families of elliptic curves over dihedral quartic number fields. *J. Number Theory*, 133(1):115–122, 2013.

[20] Daeyeol Jeon, Chang Heon Kim, and Euisung Park. On the torsion of elliptic curves over quartic number fields. *J. London Math. Soc. (2)*, 74(1):1–12, 2006.

[21] Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer. On the torsion of elliptic curves over cubic number fields. *Acta Arith.*, 113(3):291–301, 2004.

[22] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

[23] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988.

[24] Álvaro Lozano-Robledo. On the field of definition of p-torsion points on elliptic curves over the rationals. *Math. Ann.*, 357(1):279–305, 2013.
[25] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.
[26] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.
[27] Filip Najman. Isogenies of non-CM elliptic curves with rational j-invariants over number fields. *Math. Proc. Cambridge Philos. Soc. (to appear)*.
[28] Filip Najman. Exceptional elliptic curves over quartic fields. *Int. J. Number Theory*, 8(5):1231–1246, 2012.
[29] Filip Najman. Torsion of elliptic curves over cubic fields. *J. Number Theory*, 132(1):26–36, 2012.
[30] Filip Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. *Math. Res. Letters*, (23):245–272, 2016.
[31] Oron Y. Propp. GitHub repository related to *Cartan images and ℓ-torsion points of elliptic curves with rational j-invariant*, available at https://github.com/oronpropp/ecdegsets. 2017.
[32] Marusia Rebolledo and Christian Wuthrich. A moduli interpretation for the non-split Cartan modular curve. *Glasgow Mathematical Journal (to appear)*, 2017.
[33] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.
[34] Andrew V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma*, 4:e4 (79 pages), 2016.
[35] Jian Wang. On the cyclic torsion of elliptic curves over cubic number fields. *arXiv:1502.06873*, 2017.
[36] David J. Zywina. On the possible images of the mod-ℓ representations associated to elliptic curves over $\mathbb{Q}$. *arXiv:1508.07660*, 2015.

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
E-mail address: opropp@mit.edu