EXPLICIT KUMMER THEORY FOR ELLIPTIC CURVES

DAVIDE LOMBARDO AND SEBASTIANO TRONTO

ABSTRACT. Let E be an elliptic curve defined over a number field K, let $\alpha \in E(K)$ be a point of infinite order, and let $N^{-1}\alpha$ be the set of N-division points of α in $E(\overline{K})$. We prove strong effective and uniform results for the degrees of the Kummer extensions $[K(E[N], N^{-1}\alpha) : K(E[N])]$. When $K = \mathbb{Q}$, and under a minimal assumption on α, we show that the inequality $[\mathbb{Q}(E[N], N^{-1}\alpha) : \mathbb{Q}(E[N])] \geqslant cN^2$ holds with a constant c independent of both E and α.

1. INTRODUCTION

1.1. **Setting.** Let E be an elliptic curve defined over a number field K (for which we fix an algebraic closure $\overline{K}$) and let $\alpha \in E(K)$ be a point of infinite order. The purpose of this paper is to study the extensions of K generated by the division points of α; in order to formally introduce these extensions we need to set some notation.

Given a positive integer M, we denote by $E[M]$ the group of M-torsion points of E, that is, the set $\{P \in E(\overline{K}) : MP = 0\}$ equipped with the group law inherited from E. Moreover, we denote by K_M the *M-th torsion field* $K(E[M])$ of E, namely, the finite extension of K obtained by adjoining the coordinates of all the M-torsion points of E. For each positive integer N dividing M, we let $N^{-1}\alpha := \left\{\beta \in E(\overline{K}) \mid N\beta = \alpha\right\}$ denote the set of N-division points of α and set

$$K_{M,N} := K(E[M], N^{-1}\alpha).$$

The field $K_{M,N}$ is called the (M, N)-*Kummer extension* of K (related to α), and both K_M and $K_{M,N}$ are finite Galois extensions of K.

It is a classical question to study the degree of $K_{M,N}$ over K_M as M, N vary, see for example [4, Théorème 5.2], [11, Lemme 14], or Ribet's foundational paper [23]. In particular, it is known that there exists an integer $C = C(E/K, \alpha)$, depending only on E/K and α, such that

$$\frac{N^2}{[K_{M,N} : K_M]} \quad \text{divides} \quad C$$

for every pair of positive integers (M, N) with $N \mid M$.

The aim of this paper is to give an explicit version of this result, and to show that it can even be made uniform when the base field is $K = \mathbb{Q}$. Our first result is that, under the assumption $\mathrm{End}_K(E) = \mathbb{Z}$, the integer C can be bounded (explicitly) in terms of the ℓ-adic Galois representations attached to E and of divisibility properties of the point α, and that this statement becomes false if we remove the hypothesis $\mathrm{End}_K(E) = \mathbb{Z}$.

On the other hand, the assumption $\mathrm{End}_{\mathbb{Q}}(E) = \mathbb{Z}$ is always satisfied when $K = \mathbb{Q}$, and we show that in this case C can be taken to be independent of E and α, provided that α and all its translates by torsion points are not divisible by any $n > 1$ in the group $E(\mathbb{Q})$. This is a rather surprising statement, especially given that such a strong uniformity result is not known for the closely connected problem of studying the degrees of the torsion fields K_M over K.

1.2. **Main results.** Our main results are the following.

Theorem 1.1. *Assume that* $\mathrm{End}_K(E) = \mathbb{Z}$*. There is an explicit constant* C*, depending only on* α *and on the* ℓ*-adic torsion representations associated to* E *for all primes* ℓ*, such that*

$$\frac{N^2}{[K_{M,N} : K_M]} \quad \textit{divides} \quad C$$

for all pairs of positive integers (M, N) *with* N *dividing* M*.*

The proof gives an explicit expression for C that depends on computable parameters associated with E and α. We also show that all these quantities can be bounded effectively in terms of standard invariants of the elliptic curve and of the height of α, see Remark 5.19.

Theorem 1.2. *There is a universal constant* C *with the following property. Let* $E/\mathbb{Q}$ *be an elliptic curve, and let* $\alpha \in E(\mathbb{Q})$ *be a point such that the class of* α *in the free abelian group* $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$ *is not divisible by any* $n > 1$*. Then*

$$\frac{N^2}{[\mathbb{Q}_{M,N} : \mathbb{Q}_M]} \quad \textit{divides} \quad C$$

for all pairs of positive integers (M, N) *with* N *dividing* M*.*

1.3. **Structure of the paper.** We start with some necessary general preliminaries in Section 2, leading up to a factorisation of the constant C of Theorem 1.1 as a product of certain contributions which we dub the *ℓ-adic* and *adelic* failures (corresponding to E, α, and a fixed prime ℓ). In the same section we also introduce some of the main actors of this paper, in the form of several Galois representations associated with the torsion and Kummer extensions. In Section 3 we then recall some important properties of the torsion representations that will be needed in the rest of the paper. In Sections 4 and 5 we study the ℓ-adic and adelic failures respectively. In Section 6 we show that one cannot hope to naïvely generalise some of the results in section 4 to CM curves. Finally, in Section 7 we prove Theorem 1.2 by establishing several auxiliary results about the Galois cohomology of the torsion modules $E[M]$ that might have an independent interest.

1.4. **Acknowledgements.** It is a pleasure to thank Antonella Perucca for suggesting the problem that led to this paper, for her constant support, and for her useful comments. We are grateful to Peter Bruin for many interesting discussions, and to Peter Stevenhagen and Francesco Campagna for useful correspondence about the results of section 5.1.

2. PRELIMINARIES

2.1. **Notation and definitions.** The letter K will always denote a number field, E an elliptic curve defined over K, and α a point of infinite order in $E(K)$.

For n a positive integer, we denote by ζ_n a primitive root of unity of order n.

Given a prime ℓ, we denote by v_ℓ the usual ℓ-adic valuation on $\mathbb{Q}$ and on $\mathbb{Q}_\ell$. If X is a vector in $\mathbb{Z}_\ell^n$ or a matrix in $\mathrm{Mat}_{m\times n}(\mathbb{Z}_\ell)$, we call *valuation* of X, denoted by $v_\ell(X)$, the minimum of the ℓ-adic valuations of its coefficients.

We shall often use divisibility conditions involving the symbols ℓ^∞ (where ℓ is a prime) and ∞. Our convention is that every power of ℓ divides ℓ^∞, every positive integer divides ∞, and ℓ^∞ divides ∞.

Recall from the Introduction that we denote by K_M the field $K(E[M])$ generated by the coordinates of the M-torsion points of E, and by $K_{M,N}$ (for $N \mid M$) the field $K(E[M], N^{-1}\alpha)$. We extend this notation by setting $K_{\ell^\infty} = \bigcup_n K_{\ell^n}$, $K_\infty = \bigcup_M K_M$, and more generally, for $M, N \in \mathbb{N}_{>0} \cup \{\ell^\infty, \infty\}$ with $N \mid M$,

$$K_M = \bigcup_{d|M} K_d, \quad K_{M,N} = \bigcup_{d|M} \bigcup_{\substack{e|d \\ e|N}} K_{d,e}$$

If H is a subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, we denote by $\mathbb{Z}_\ell[H]$ the sub-$\mathbb{Z}_\ell$-algebra of $\mathrm{Mat}_2(\mathbb{Z}_\ell)$ generated by the elements of H.

Let G be a (profinite) group. We write G' for its derived subgroup, namely, the subgroup of G (topologically) generated by commutators, and $G^{\mathrm{ab}} = G/G'$ for its abelianisation, namely, its largest abelian (profinite) quotient. We say that a finite simple group S *occurs* in a profinite group G if there are closed subgroups H_1, H_2 of G, with $H_1 \triangleleft H_2$, such that H_2/H_1 is isomorphic to S. Finally, we denote by $\exp G$ the exponent of a finite group G, namely, the smallest integer $e \geqslant 1$ such that $g^e = 1$ for every $g \in G$.

2.2. **The ℓ-adic and adelic failures.** We start by observing that it is enough to restrict our attention to the case $N = M$:

Remark 2.1. Suppose that there is a constant $C \geqslant 1$ satisfying

$$\frac{M^2}{[K_{M,M} : K_M]} \quad \text{divides} \quad C$$

for all positive integers M. Then for any $N \mid M$, since $[K_{M,M} : K_{M,N}]$ divides $(M/N)^2$, we have that

$$\frac{N^2}{[K_{M,N} : K_M]} = \frac{N^2[K_{M,M} : K_{M,N}]}{[K_{M,M} : K_M]} \quad \text{divides} \quad \frac{M^2}{[K_{M,M} : K_M]},$$

which in turn divides C.

Elementary field theory gives

$$\begin{aligned}\frac{N^2}{[K_{N,N} : K_N]} &= \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \frac{\ell^{2n_\ell}}{[K_{N,\ell^{n_\ell}} : K_N]} = \\ &= \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \frac{\ell^{2n_\ell}}{[K_{\ell^{n_\ell},\ell^{n_\ell}} : K_{\ell^{n_\ell}}]} \cdot \frac{[K_{\ell^{n_\ell},\ell^{n_\ell}} : K_{\ell^{n_\ell}}]}{[K_{N,\ell^{n_\ell}} : K_N]} = \\ &= \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} \frac{\ell^{2n_\ell}}{[K_{\ell^{n_\ell},\ell^{n_\ell}} : K_{\ell^{n_\ell}}]} \cdot [K_{\ell^{n_\ell},\ell^{n_\ell}} \cap K_N : K_{\ell^{n_\ell}}]\end{aligned}$$

where $n_\ell = v_\ell(N)$. To see why the first equality holds, recall that the degree $[K_{N,\ell^{n_\ell}} : K_N]$ is a power of ℓ, so the fields $K_{N,\ell^{n_\ell}}$ are linearly disjoint over K_N, and clearly they generate all of $K_{N,N}$.

Definition 2.2. Let ℓ be a prime and N a positive integer. Let $n := v_\ell(N)$. We call

$$A_\ell(N) := \frac{\ell^{2n}}{[K_{\ell^n,\ell^n} : K_{\ell^n}]}$$

the *ℓ-adic failure* at N and

$$B_\ell(N) := \frac{[K_{\ell^n,\ell^n} : K_{\ell^n}]}{[K_{N,\ell^n} : K_N]} = [K_{\ell^n,\ell^n} \cap K_N : K_{\ell^n}]$$

the *adelic failure* at N (related to ℓ). Notice that both $A_\ell(N)$ and $B_\ell(N)$ are powers of ℓ.

Example 2.3. It is clear that the ℓ-adic failure $A_\ell(N)$ can be nontrivial, that is, different from 1. Suppose for example that $\alpha = \ell\beta$ for some $\beta \in E(K)$: then we have

$$K_{\ell^n,\ell^n} = K_{\ell^n}(\ell^{-n}\alpha) = K_{\ell^n}(\ell^{-n+1}\beta),$$

and the degree of this field over K_{ℓ^n} is at most $\ell^{2(n-1)}$, so $\ell^2 \mid A_\ell(N)$. In Example 4.4 we will show that the ℓ-adic failure can be non-trivial also when α is strongly ℓ-indivisible (see Definition 4.1).

Example 2.4. We now show that the adelic failure $B_\ell(N)$ can be non-trivial as well. Consider the elliptic curve E over $\mathbb{Q}$ given by the equation

$$y^2 = x^3 + x^2 - 44x - 84$$

and with Cremona label 624f2 (see [32, label 624f2]). One can show that $E(\mathbb{Q}) \cong \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2$, so that the curve has full rational 2-torsion, and that a generator of the free part of $E(\mathbb{Q})$ is given by $P = (-5, 6)$. The 2-division points of P are given by $(1 + \sqrt{-3}, -3 + 7\sqrt{-3})$, $(-11 + 3\sqrt{-3}, 27 + 15\sqrt{-3})$, and their Galois conjugates, so they are defined over $\mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}_3$, and we have $B_2(6) := [\mathbb{Q}_{2,2} \cap \mathbb{Q}_6 : \mathbb{Q}_2] = [\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$.

These computations have been checked with SageMath [34].

2.3. **The torsion, Kummer and arboreal representations.** In this section we introduce three representations of the absolute Galois group of K that will be our main tool for studying the extensions $K_{M,N}$. For further information about these representations see for example [12, Section 3], [5], and [17].

2.3.1. *The torsion representation.* Let N be a positive integer. The group $E[N]$ of N-torsion points of E is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2. Since the multiplication-by-N map is defined over K, the absolute Galois group of K acts $\mathbb{Z}/N\mathbb{Z}$-linearly on $E[N]$, and we get a homomorphism

$$\tau_N : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{Aut}(E[N]).$$

The field fixed by the kernel of τ_N is exactly the N-th torsion field K_N. Thus, after fixing a $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N]$, the Galois group $\mathrm{Gal}(K_N \mid K)$ is identified with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ which we denote by H_N.

As N varies, and provided that we have made compatible choices of bases, these representations form a compatible projective system, so we can pass to the limit over powers of a fixed prime ℓ to obtain the *ℓ-adic torsion representation* $\tau_{\ell^\infty} : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$. We can also take the limit over all integers N (ordered by divisibility) to obtain the *adelic torsion representation* $\tau_\infty : \mathrm{Gal}(\overline{K} \mid K) \to \mathrm{GL}_2(\hat{\mathbb{Z}})$. We denote by H_{ℓ^∞} (resp. H_∞) the image of τ_{ℓ^∞} (resp. τ_∞). The group H_{ℓ^∞} (resp. H_∞) is isomorphic to $\mathrm{Gal}(K_{\ell^\infty} \mid K)$ (resp. $\mathrm{Gal}(K_\infty \mid K)$).

One can also pass to the limit on the torsion subgroups themselves, obtaining the *ℓ-adic Tate module* $T_\ell E = \varprojlim_n E[\ell^n] \cong \mathbb{Z}_\ell^2$ and the *adelic Tate module* $TE = \varprojlim_M E[M] \cong \hat{\mathbb{Z}}^2 \cong \prod_\ell \mathbb{Z}_\ell^2$.

2.3.2. *The Kummer representation.* Let M and N be positive integers with $N \mid M$. Let $\beta \in E(\overline{K})$ be a point such that $N\beta = \alpha$. For any $\sigma \in \mathrm{Gal}(\overline{K} \mid K_M)$ we have that $\sigma(\beta) - \beta$ is an N-torsion point, so the following map is well-defined:

$$\begin{array}{rccc} \kappa_N : & \mathrm{Gal}(\overline{K} \mid K_M) & \to & E[N] \\ & \sigma & \mapsto & \sigma(\beta) - \beta. \end{array}$$

Since any other N-division point β' of α satisfies $\beta' = \beta + T$ for some $T \in E[N]$, and the coordinates of T belong to $K_N \subseteq K_M$, the map κ_N does not depend on the choice of β. It is also immediate to check that κ_N is a group homomorphism, and that the field fixed by its kernel is exactly the (M, N)-Kummer extension of K. Fixing a basis of $E[N]$ we can identify the Galois group $\mathrm{Gal}(K_{M,N} \mid K_M)$ with a subgroup of $(\mathbb{Z}/N\mathbb{Z})^2$. It is then clear that $K_{M,N}$ is an abelian extension of K_M of degree dividing N^2, and the Galois group of this extension has exponent dividing N.

In the special case $M = N$ we denote by V_N the image of $\mathrm{Gal}\,(K_{N,N} \mid K_N)$ in $(\mathbb{Z}/N\mathbb{Z})^2$.

By passing to the limit in the previous constructions we also obtain the following:

- There is an ℓ-adic Kummer representation $\kappa_{\ell^\infty} : \mathrm{Gal}(\overline{K} \mid K_{\ell^\infty}) \to T_\ell E$ which factors via a map $\mathrm{Gal}(K_{\ell^\infty,\ell^\infty} \mid K_{\ell^\infty}) \to T_\ell E$ (still denoted by κ_{ℓ^∞}).
- The image V_{ℓ^∞} of κ_{ℓ^∞} is a sub-$\mathbb{Z}_\ell$-module of $T_\ell E \cong \mathbb{Z}_\ell^2$, isomorphic to $\mathrm{Gal}(K_{\ell^\infty,\ell^\infty} \mid K_{\ell^\infty})$ as a profinite group. We therefore identify $\mathrm{Gal}(K_{\ell^\infty,\ell^\infty} \mid K_{\ell^\infty})$ with V_{ℓ^∞}.

- We can identify the Galois group $\mathrm{Gal}(K_{\infty,\ell^\infty} \mid K_\infty)$ with a $\mathbb{Z}_\ell$-submodule W_{ℓ^∞} of V_{ℓ^∞} (hence also of $T_\ell E$) via the representation κ_{ℓ^∞}.
- We can identify the Galois group $\mathrm{Gal}(K_{\infty,\infty} \mid K_\infty)$ with a sub-$\hat{\mathbb{Z}}$-module W_∞ of $TE \cong \hat{\mathbb{Z}}^2$.

Notice that W_{ℓ^∞} is the projection of W_∞ in $\mathbb{Z}_\ell^2$, and since W_{ℓ^∞} is a pro-ℓ group and there are no nontrivial continuous morphisms from a pro-ℓ group to a pro-ℓ' group for $\ell \neq \ell'$ we have $W_\infty = \prod_\ell W_{\ell^\infty}$.

2.3.3. *The arboreal representation.* Fix a sequence $\{\beta_i\}_{i\in\mathbb{N}}$ of points in $E(\overline{K})$ such that $\beta_1 = \alpha$ and $N\beta_M = \beta_{M/N}$ for all pairs of positive integers (N, M) with $N \mid M$. For every $N \geqslant 1$ fix furthermore a $\mathbb{Z}/N\mathbb{Z}$-basis $\{T_1^N, T_2^N\}$ of $E[N]$ in such a way that $NT_1^M = T_1^{M/N}$ and $NT_2^M = T_2^{M/N}$ for every pair of positive integers (N, M) with $N \mid M$. For every $N \geqslant 1$, the map

$$\begin{aligned} \omega_N : \mathrm{Gal}(K_{N,N} \mid K) &\to (\mathbb{Z}/N\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \\ \sigma &\mapsto (\sigma(\beta_N) - \beta_N, \tau_N(\sigma)) \end{aligned}$$

is an injective homomorphism (similarly to [12, Proposition 3.1]) and thus identifies the group $\mathrm{Gal}(K_{N,N} \mid K)$ with a subgroup of $(\mathbb{Z}/N\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

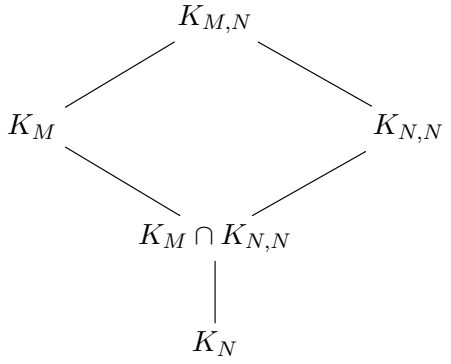
It will be important for our applications to notice that V_N comes equipped with an action of H_N coming from the fact that V_N is the (abelian) kernel of the natural map $\mathrm{Gal}(K_{N,N} \mid K) \to H_N$. More precisely, the action of $h \in H_N$ on $v \in V_N$ is given by conjugating the element $(v, \mathrm{Id}) \in (\mathbb{Z}/N\mathbb{Z})^2 \rtimes \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by $(0, h)$. Explicitly, we have

$$(0, h)(v, \mathrm{Id})(0, h)^{-1} = (hv, h)(0, h^{-1}) = (hv, \mathrm{Id}),$$

so that the action of H_N on V_N is induced by the natural action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $(\mathbb{Z}/N\mathbb{Z})^2$. We obtain similar statements by suitably passing to the limit in N:

Lemma 2.5. *For every positive integer N, the group V_N is an H_N-submodule of $(\mathbb{Z}/N\mathbb{Z})^2$ for the natural action of $H_N \leqslant \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $V_N \leqslant (\mathbb{Z}/N\mathbb{Z})^2$. Similarly, both V_{ℓ^∞} and W_{ℓ^∞} are H_{ℓ^∞}-modules.*

Remark 2.6. Let $N \in \mathbb{N} \cup \{\ell^\infty\}$ and $M \in \mathbb{N} \cup \{\ell^\infty, \infty\}$ with $N \mid M$. Then $\mathrm{Gal}(K_{M,N} \mid K_M)$ can be identified with a subgroup of V_N: this follows from inspection of the diagram



which shows that $\mathrm{Gal}(K_{M,N} \mid K_M)$ is isomorphic to $\mathrm{Gal}(K_{N,N} \mid K_M \cap K_{N,N})$, which in turn is clearly a subgroup of $\mathrm{Gal}(K_{N,N} \mid K_N) \cong V_N$.

2.4. **Curves with complex multiplication.** If $\mathrm{End}_{\overline{K}}(E) \neq \mathbb{Z}$ we say that E *has complex multiplication*, or CM for short. In this case $\mathrm{End}_{\overline{K}}(E)$ is an order in an imaginary quadratic field, called *the CM-field of* E. The torsion representations in the CM case have been studied for example in [9] and [10].

In this case, the image of the torsion representation τ_{ℓ^∞} is closely related to the *Cartan subgroup of* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *corresponding to* $\mathrm{End}_{\overline{K}}(E)$, defined as follows:

Definition 2.7. Let F be a reduced $\mathbb{Q}_\ell$-algebra of degree 2 and let $\mathcal{A}_\ell$ be a $\mathbb{Z}_\ell$-order in F. The *Cartan subgroup* corresponding to $\mathcal{A}_\ell$ is the group of units of $\mathcal{A}_\ell$, which we embed in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ by fixing a $\mathbb{Z}_\ell$-basis of $\mathcal{A}_\ell$ and considering the left multiplication action of $\mathcal{A}_\ell^\times$. If $\mathcal{A}$ is an order in an imaginary quadratic number field, the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathcal{A}$ is defined by taking $\mathcal{A}_\ell = \mathcal{A} \otimes \mathbb{Z}_\ell$ in the above.

More precisely, when E/K is an elliptic curve with CM, the image of the ℓ-adic torsion representation τ_{ℓ^∞} is always contained (up to conjugacy in $\mathrm{GL}_2(\mathbb{Z}_\ell)$) in the normaliser of the Cartan subgroup corresponding to $\mathrm{End}_{\overline{K}}(E)$, and is contained in the Cartan subgroup itself if and only if the complex multiplication is defined over the base field K.

In order to have a practical representation of Cartan subgroups, we recall the following definition from [18]:

Definition 2.8. Let C be a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. We say that $(\gamma, \delta) \in \mathbb{Z}_\ell^2$ are *parameters for* C if C is conjugated in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ to the subgroup

$$\left\{ \begin{pmatrix} x & \delta y \\ y & x + \gamma y \end{pmatrix} : x, y \in \mathbb{Z}_\ell,\ v_\ell(x(x+\gamma y) - \delta y^2) = 0 \right\}. \tag{1}$$

Parameters for C always exist, see [18, §2.3].

Remark 2.9 ([18, Remark 9])**.** One may always assume that γ, δ are integers. Furthermore, one can always take $\gamma \in \{0, 1\}$, and $\gamma = 0$ if $\ell \neq 2$.

We also recall the following explicit description of the normaliser of a Cartan subgroup [18, Lemma 14]:

Lemma 2.10. *A Cartan subgroup has index 2 in its normaliser. If* C *is as in* (1)*, its normaliser* N *in* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *is the disjoint union of* C *and* $C' := \begin{pmatrix} 1 & \gamma \\ 0 & -1 \end{pmatrix} \cdot C$.

3. Properties of the torsion representation

Torsion representations are studied extensively in the literature; we have in particular the following fundamental theorem of Serre [27], which applies to all elliptic curves (defined over number fields) without complex multiplication:

Theorem 3.1 (Serre)**.** *If* $\mathrm{End}_{\overline{K}}(E) = \mathbb{Z}$*, then* H_∞ *is open in* $\mathrm{GL}_2(\hat{\mathbb{Z}})$*. Equivalently, the index of* H_N *in* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *is bounded independently of* N.

There is also a CM analogue of Theorem 3.1, which is more easily stated by introducing the following definition:

Definition 3.2. Let E/K be an elliptic curve and ℓ be a prime number. We say that the image of the ℓ-adic representation is *maximal* if one of the following holds:

- E does not have CM over $\overline{K}$ and $H_{\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$.
- E has CM over K by an order $\mathcal{A}$ in the imaginary quadratic field F, the prime ℓ is unramified in F and does not divide $[\mathcal{O}_F : \mathcal{A}]$, and H_{ℓ^∞} is conjugated to the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathcal{A}$.
- E has CM over $\overline{K}$ (but not over K) by an order $\mathcal{A}$ in the imaginary quadratic field F, the prime ℓ is unramified in F and does not divide $[\mathcal{O}_F : \mathcal{A}]$, and H_{ℓ^∞} is conjugated to the normaliser of the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathcal{A}$.

Theorem 3.3 ([27, Corollaire on p.302])**.** *Let E/K be an elliptic curve admitting CM over $\overline{K}$. Then the ℓ-adic representation attached to E/K is maximal for all but finitely many primes ℓ.*

In the rest of this section we recall various important properties of the torsion representations: we shall need results that describe both the asymptotic behaviour of the $\mathrm{mod}\,\ell^n$ torsion representation as $n \to \infty$ (§3.1 and 3.2) and the possible images of the $\mathrm{mod}\,\ell$ representations attached to elliptic curves defined over the rationals (§3.3).

3.1. **Maximal growth.** We recall some results on the growth of the torsion extensions from [17, §2.3].

Proposition 3.4. *Let ℓ be a prime number. Let $\delta = 2$ if E has complex multiplication and $\delta = 4$ otherwise. There exists a positive integer n_ℓ such that*

$$\#H_{\ell^{n+1}}/\#H_{\ell^n} = \ell^\delta \qquad \text{for every } n \geqslant n_\ell.$$

Proof. This follows from Theorem 3.1 in the non-CM case and from classical results in the CM case. See also [17, Lemma 10 and Remark 13] for a more general result. □

Definition 3.5. We call an integer n_ℓ as in Proposition 3.4 a *parameter of maximal growth for the ℓ-adic torsion representation*. We say that it is *minimal* if $n_\ell - 1$ is not a parameter of maximal growth; when $\ell = 2$, we require that the minimal parameter be at least 2.

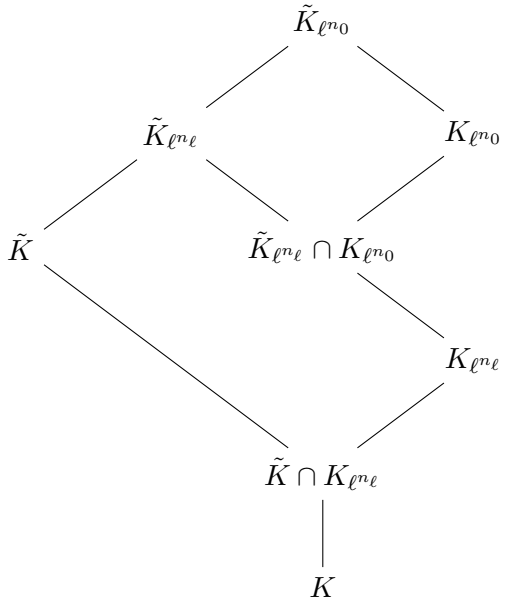
Remark 3.6. The assumption $n_\ell \geqslant 2$ when $\ell = 2$ will be needed to apply [17, Theorem 12].

Remark 3.7. Given an explicit elliptic curve E/K and a prime ℓ, the problem of determining the optimal value of n_ℓ can be solved effectively (see [17, Remark 13]). However, computing n_ℓ can be challenging in practice, because the naïve algorithm requires the determination of the Galois groups of the splitting fields of several large-degree polynomials. The situation is usually better for smaller primes ℓ, and especially for $\ell = 2$, for which the 2-torsion tower is known essentially explicitly (see [25] for a complete classification result when $K = \mathbb{Q}$, and [35] for a description of the 2-torsion tower of a given elliptic curve over a number field).

In Section 5 we will need to bound the minimal parameter of maximal growth for the ℓ-adic torsion representation defined over certain extensions of the base field. We will do so with the help of the following Lemma:

Lemma 3.8. *Let $\tilde{K}$ be a finite extension of K. Let n_ℓ (resp. $\tilde{n}_\ell$) be the minimal parameter of maximal growth for the ℓ-adic torsion representation attached to E/K (resp. $E/\tilde{K}$). Then $\tilde{n}_\ell \leqslant n_\ell + v_\ell([\tilde{K} : K])$.*

Proof. Let $n_0 := n_\ell + v_\ell([\tilde{K} : K]) + 1$ and consider the following diagram:



Since clearly $[\tilde{K}_{\ell^{n_\ell}} \cap K_{\ell^{n_0}} : K_{\ell^{n_\ell}}]$ divides $[\tilde{K}_{\ell^{n_\ell}} : K_{\ell^{n_\ell}}]$, which in turn divides $[\tilde{K} : K]$, and since $[\tilde{K}_{\ell^{n_0}} : \tilde{K}_{\ell^{n_\ell}}] = [K_{\ell^{n_0}} : \tilde{K}_{\ell^{n_\ell}} \cap K_{\ell^{n_0}}]$, we have

$$\begin{aligned} v_\ell\left([K_{\ell^{n_0}} : K_{\ell^{n_\ell}}]\right) &= v_\ell\left([K_{\ell^{n_0}} : \tilde{K}_{\ell^{n_\ell}} \cap K_{\ell^{n_0}}]\right) + v_\ell\left([\tilde{K}_{\ell^{n_\ell}} \cap K_{\ell^{n_0}} : K_{\ell^{n_\ell}}]\right) \\ &\leqslant v_\ell\left([\tilde{K}_{\ell^{n_0}} : \tilde{K}_{\ell^{n_\ell}}]\right) + v_\ell\left([\tilde{K} : K]\right). \end{aligned}$$

By [17, Theorem 12] we have $v_\ell\left([K_{\ell^{n_0}} : K_{\ell^{n_\ell}}]\right) = \delta(n_0 - n_\ell) = \delta\left(v_\ell\left([\tilde{K} : K]\right) + 1\right)$, where δ is as in Proposition 3.4, and we get

$$v_\ell\left([\tilde{K}_{\ell^{n_0}} : \tilde{K}_{\ell^{n_\ell}}]\right) \geqslant \delta + (\delta - 1)v_\ell\left([\tilde{K} : K]\right) > (\delta - 1)(n_0 - n_\ell).$$

Consider now the tower of extensions

$$\tilde{K}_{\ell^{n_\ell}} \subseteq \tilde{K}_{\ell^{n_\ell+1}} \subseteq \cdots \subseteq \tilde{K}_{\ell^{n_0}}$$

and notice that by the pigeonhole principle for at least one $n \in \{n_\ell, n_\ell + 1, \ldots, n_0 - 1\}$ we must have $[\tilde{K}_{\ell^{n+1}} : \tilde{K}_{\ell^n}] \geqslant \delta$. But then by [17, Theorem 12] we have maximal growth over $\tilde{K}$ from $n < n_0$. Thus we get $\tilde{n}_\ell \leqslant n_\ell + v_\ell\left([\tilde{K} : K]\right)$ as claimed. □

3.2. **Uniform growth of ℓ-adic representations.** The results in this subsection and the next will be needed in Section 7. We start by recalling the following result, due to Arai:

Theorem 3.9 ([2, Theorem 1.2])**.** *Let K be a number field and let ℓ be a prime. Then there exists an integer $n \geqslant 0$, depending only on K and ℓ, such that for any elliptic curve E over K with no complex multiplication over $\overline{K}$ we have*

$$\tau_{\ell^\infty}(\mathrm{Gal}(\overline{K} \mid K)) \supseteq \{M \in \mathrm{GL}_2(\mathbb{Z}_\ell) : M \equiv \mathrm{Id} \pmod{\ell^n}\}.$$

For the next result we shall need a well-known Lemma about twists of elliptic curves:

Lemma 3.10. *Let E_1, E_2 be elliptic curves over K such that $(E_1)_{\overline{\mathbb{Q}}}$ is isomorphic to $(E_2)_{\overline{\mathbb{Q}}}$. There is an extension F of K, of degree dividing 12, such that E_1 and E_2 become isomorphic over F.*

Proof. Fixing a $\overline{\mathbb{Q}}$-isomorphism between E_1 and E_2 allows us to attach to E_2 a class in $H^1\left(\mathrm{Gal}(\overline{K} \mid K), \mathrm{Aut}(E_1)\right)$. Since $H^1\left(\mathrm{Gal}(\overline{K} \mid K), \mathrm{Aut}(E_1)\right) \cong K^\times/K^{\times n}$ for some $n \in \{2, 4, 6\}$ (see [31, Proposition X.5.4]), the class of E_2 corresponds to the class of a certain $[\alpha] \in K^\times/K^{\times n}$. Letting $F = K(\sqrt[n]{\alpha})$, whose degree over K divides 12, it is clear that $[\alpha] \in F^\times/F^{\times n}$ is the trivial class, so the same is true for $[E_2] \in H^1(\mathrm{Gal}(\overline{F} \mid F), \mathrm{Aut}(E_1))$, which means that E_2 is isomorphic to E_1 over F as desired. □

Corollary 3.11. *Let K be a number field and ℓ be a prime number. There exists an integer n_ℓ with the following property: for every elliptic curve E/K, the minimal parameter of maximal growth for the ℓ-adic representation attached to E is at most n_ℓ.*

Proof. Let n be the integer whose existence is guaranteed by Theorem 3.9. By the general theory of CM elliptic curves, we know that there are finitely many values $j_1, \ldots, j_k \in \overline{\mathbb{Q}}$ such that for every CM elliptic curve E/K we have $j(E) \in \{j_1, \ldots, j_k\}$. For each such j_i, fix an elliptic curve E_i/K with $j(E_i) = j_i$. To every E_i/K corresponds a minimal parameter of maximal growth for the ℓ-adic representation that we call m_i. Let $n_\ell = \max\{n, m_i + 2 \;\big|\; i = 1, \ldots, k\}$: we claim that this value of n_ℓ satisfies the conclusion of the Corollary. Indeed, let E/K be any elliptic curve. If E does not have CM, the minimal parameter of maximal growth for its ℓ-adic representation is at most $n \leqslant n_\ell$. If E has CM, then there exists i such that $j(E) = j_i = j(E_i)$, so E is a twist of E_i. By Lemma 3.10 the curves E and E_i become isomorphic over an extension F/K of degree dividing 12, so if m (resp. $\tilde{m}$, resp. $\tilde{m}_i$) denotes the minimal parameter of maximal growth for E/K (resp. for E/F, resp. for E_i/F) we have

$$m \leqslant \tilde{m} = \tilde{m}_i \leqslant m_i + 2 \leqslant n_\ell,$$

where the equality follows from the fact that E and E_i are isomorphic over F, while the inequality $\tilde{m}_i \leqslant m_i + 2$ follows from Lemma 3.8 and the fact that $v_\ell([F : K]) \leqslant v_\ell(12) \leqslant 2$ for every prime ℓ. □

3.3. **Possible images of $\mathrm{mod}\ \ell$ representations.** We recall several results concerning the images of the $\mathrm{mod}\ \ell$ representations attached to elliptic curves over $\mathbb{Q}$.

We begin with a famous Theorem of Mazur. Let $\mathcal{T}_0 := \{p \text{ prime } \mid p \leqslant 17\} \cup \{37\}$.

Theorem 3.12 ([20, Theorem 1])**.** *Let $E/\mathbb{Q}$ be an elliptic curve and assume that E has a $\mathbb{Q}$-rational subgroup of order p. Then $p \in \mathcal{T}_0 \cup \{19, 43, 67, 163\}$. If E does not have CM over $\overline{\mathbb{Q}}$, then $p \in \mathcal{T}_0$.*

Theorem 3.13 ([36, Proposition 1.13])**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p \notin \mathcal{T}_0$ be a prime. Let $C_{\mathrm{ns}}(p)$ be the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ consisting of all matrices of the form $\begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix}$ with $(a, b) \in \mathbb{F}_p^2 \setminus \{(0, 0)\}$ and ϵ a fixed element of $\mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$. Then H_p is conjugate to one of the following:*

(i) $\mathrm{GL}_2(\mathbb{F}_p)$*;*
(ii) the normaliser $N_{\mathrm{ns}}(p)$ of $C_{\mathrm{ns}}(p)$;
(iii) the index 3 subgroup

$$D(p) := \left\{a^3 \mid a \in C_{\mathrm{ns}}(p)\right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot a^3 \mid a \in C_{\mathrm{ns}}(p) \right\}$$

of $N_{\mathrm{ns}}(p)$.

Moreover, the last case can only occur if $p \equiv 2 \pmod 3$.

Corollary 3.14. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p \notin \mathcal{T}_0$ be a prime. The following hold:*

(1) The image H_p of the modulo-p representation attached to E contains $\{\lambda \mathrm{Id} \mid \lambda \in \mathbb{F}_p^\times\}$.
(2) Suppose $H_p \neq \mathrm{GL}_2(\mathbb{F}_p)$ and let $g_p \in \mathrm{GL}_2(\mathbb{F}_p)$ be an element that normalises H_p. Then there is $h \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $h^{-1} g_p h \in N_{\mathrm{ns}}(p)$ and $h^{-1} H_p h \subseteq N_{\mathrm{ns}}(p)$.

Proof. (1) We apply Theorem 3.13. If H_p is either $\mathrm{GL}_2(\mathbb{F}_p)$ or conjugate to $N_{\mathrm{ns}}(p)$, the conclusion follows trivially, since $C_{\mathrm{ns}}(p)$ contains all scalars. In case (iii) of Theorem 3.13, H_p contains the cubes of the scalars, hence all scalars since $p \equiv 2 \pmod 3$.

(2) We only have to consider cases (ii) and (iii) of Theorem 3.13. Up to conjugation, we may assume that $H_p \subseteq N_{\mathrm{ns}}(p)$ and the claim becomes $g_p \in N_{\mathrm{ns}}(p)$.

In case (ii) it suffices to check that the normaliser of $N_{\mathrm{ns}}(p)$ is $N_{\mathrm{ns}}(p)$ itself. This holds because $C_{\mathrm{ns}}(p)$, being the only cyclic subgroup of index 2 of $N_{\mathrm{ns}}(p)$, is characteristic in $N_{\mathrm{ns}}(p)$; hence any element that normalises $N_{\mathrm{ns}}(p)$ normalises $C_{\mathrm{ns}}(p)$ as well, so it must be in $N_{\mathrm{ns}}(p)$. In case (iii), one similarly sees that $\{a^3 \mid a \in C_{\mathrm{ns}}(p)\}$ is characteristic in $D(p)$ and that its normaliser is $N_{\mathrm{ns}}(p)$, and the conclusion follows as above.

□

Lemma 3.15. *Let ℓ be a prime number and let H be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Denote by H_ℓ the reduction of H modulo ℓ and suppose that H_ℓ contains a scalar matrix $\overline{\lambda}\,\mathrm{Id}$. Then H contains a scalar matrix $\lambda\,\mathrm{Id}$ for some $\lambda \in \mathbb{Z}_\ell^\times$ with $\lambda \equiv \overline{\lambda} \pmod \ell$.*

Proof. Let $h \in H$ be any element that is congruent modulo ℓ to $\overline{\lambda}\,\mathrm{Id}$. Let $\lambda \in \mathbb{Z}_\ell^\times$ be the Teichmüller lift of $\overline{\lambda}$ (that is, $\lambda^\ell = \ell$ and $\lambda \equiv \overline{\lambda} \pmod \ell$) and write $h = \lambda h_1$, where $h_1 = \mathrm{Id} + \ell A$ for some $A \in \mathrm{Mat}_2(\mathbb{Z}_\ell)$. The sequence $h^{\ell^n} = \lambda^{\ell^n} h_1^{\ell^n} = \lambda h_1^{\ell^n}$ converges to $\lambda\,\mathrm{Id}$, because for every n we have $h_1^{\ell^n} = (\mathrm{Id} + \ell A)^{\ell^n} \equiv \mathrm{Id} \pmod{\ell^n}$. As H is closed, the limit of this sequence, namely $\lambda\,\mathrm{Id}$, also belongs to H as claimed. □

4. The ℓ-adic failure

The aim of this section is to study the ℓ-adic failure $A_\ell(N)$ for a fixed prime ℓ. The divisibility properties of α in the group $E(K)$ play a crucial role in the study of this quantity, so we begin with the following definition:

Definition 4.1. Let $\alpha \in E(K)$ and let n be a positive integer. We say that α is *n-indivisible over K* if there is no $\beta \in E(K)$ such that $n\beta = \alpha$; otherwise we say that α is *n-divisible* or *divisible by n over K*. Let ℓ be a prime number. We say that α is *strongly ℓ-indivisible over K* if the point $\alpha + T$ is ℓ-indivisible over K for every torsion point $T \in E(K)$ of ℓ-power order. Finally, we say that α is *strongly indivisible over K* if its image in the free abelian group $E(K)/E(K)_{\mathrm{tors}}$ is not divisible by any $n > 1$, or equivalently if α is strongly ℓ-indivisible over K for every prime ℓ.

Our aim is to give an analogue of the following result, which bounds the index of the image of the Kummer representation, in those cases when the torsion representation is not surjective.

Theorem (Jones-Rouse, [12, Theorem 5.2])**.** *Assume that the ℓ-adic torsion representation $\tau_{\ell^\infty} : \mathrm{Gal}(K_{\ell^\infty} \mid K) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective. Assume that α is ℓ-indivisible in $E(K)$ and, if $\ell = 2$, that $K_{2,2} \not\subseteq K_4$. Then the ℓ-adic Kummer representation $\kappa_{\ell^\infty} : \mathrm{Gal}(K_{\ell^\infty, \ell^\infty} \mid K_{\ell^\infty}) \to \mathbb{Z}_\ell^2$ is surjective.*

4.1. **An exact sequence.** We shall need to understand the divisibility properties of α not only over the base field K, but also over the division fields of E. Thus we turn to studying how the divisibility of the point α by powers of ℓ changes when passing to a field extension. Our main tool will be the following Lemma.

Lemma 4.2. *Let L be a finite Galois extension of K with Galois group G. For every $m \geqslant 1$ there is an exact sequence of abelian groups*

$$0 \to mE(K) \to E(K) \cap mE(L) \to H^1(G, E[m](L)),$$

where the injective map on the left is the natural inclusion.

Proof. Consider the short exact sequence of G-modules

$$0 \to E[m](L) \to E(L) \xrightarrow{[m]} mE(L) \to 0$$

and the beginning of the long exact sequence in cohomology,

$$0 \to (E[m](L))^G \to (E(L))^G \to (mE(L))^G \to H^1(G, E[m](L)).$$

Noticing that

$$(E[m](L))^G = E[m](K), \qquad (E(L))^G = E(K), \qquad (mE(L))^G = E(K) \cap mE(L)$$

and that

$$E(K)/E[m](K) \cong mE(K)$$

the lemma follows. □

The quotient $(E(K) \cap mE(L))/mE(K)$ gives a measure of "how many" K-points of E are m-divisible in $E(L)$ but not m-divisible in $E(K)$. We shall often use this Lemma in the special case of $m = \ell^n$ being a power of ℓ: in this context, the quotient $(E(K) \cap \ell^n E(L))/\ell^n E(K)$ is a subgroup of $E(K)/\ell^n E(K)$, so it has exponent dividing ℓ^n. We conclude that if $\ell \nmid \#H^1(G, E[\ell^n](L))$ then no ℓ-indivisible K-point of E can become ℓ-divisible in $E(L)$. This applies in particular when $\ell \nmid \#G$, see [21, Proposition 1.6.2].

4.2. **Divisibility in the ℓ-torsion field.** As an example, we investigate the situation of Lemma 4.2 with $m = \ell$ and $L = K_\ell$. In this case the exact sequence becomes

$$0 \to \ell E(K) \to E(K) \cap \ell E(K_\ell) \to H^1(H_\ell, E[\ell]).$$

The following Lemma can also be found in [13, Section 3].

Lemma 4.3. *The cohomology group $H^1(H_\ell, E[\ell])$ is either trivial or cyclic of order ℓ. When $\ell = 2$ it is always trivial.*

Proof. Since $\ell E[\ell] = 0$, we have $\ell H^1(H_\ell, E[\ell]) = 0$. It follows from [28, Theorem IX.4] that we have an injective map $H^1(H_\ell, E[\ell]) \to H^1(S_\ell, E[\ell])$, where S_ℓ is an ℓ-Sylow subgroup of H_ℓ. This is either trivial, in which case $H^1(H_\ell, E[\ell]) = 0$, or cyclic of order ℓ. In the latter case, up to a change of basis for $E[\ell]$ we can assume that S_ℓ is generated by $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. One can conclude the proof by explicitly computing the cohomology of the cyclic group $\langle \sigma \rangle$ as in [13, Lemma 7]. □

In [13] the authors classify the cases when $H^1(H_\ell, E[\ell]) \neq 0$ for $K = \mathbb{Q}$ and they give rather complete results in case K is a number field with $K \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$. In particular, it turns out that, for $K = \mathbb{Q}$, the group $H^1(H_\ell, E[\ell])$ can be non-trivial only when $\ell = 3, 5, 11$, and only when additional conditions are satisfied (see [13, Theorem 1]).

The next Example shows that for $K = \mathbb{Q}$ a point in $E(\mathbb{Q})$ that is strongly 3-indivisible may become 3-divisible over the 3-torsion field.

Example 4.4. Consider the elliptic curve E over $\mathbb{Q}$ given by the equation

$$y^2 + y = x^3 - 216x - 1861$$

with Cremona label 17739g1 (see [32, label 17739g1]). We have $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, with a generator of the free part given by $P = \left(\frac{23769}{400}, \frac{3529853}{8000}\right)$. One can show that P is strongly 3-indivisible.

Since the $\mathbb{Q}$-isogeny class of E consists of exactly two curves, by [13, Theorem 1] we have $H^1(H_3, E[3]) = \mathbb{Z}/3\mathbb{Z}$. The 3-torsion field is given by $\mathbb{Q}(z)$, where z is any root of $x^6 + 3$. Over this field the point

$$Q = \left(\frac{803}{400}z^4 - \frac{416}{400}z^2 + \frac{507}{400}, \frac{89133}{8000}z^4 - \frac{199071}{8000}z^2 - \frac{95323}{8000}\right) \in E(\mathbb{Q}(z))$$

is such that $3Q = P$.

A computer search performed with the help of the LMFDB [32] and of Pari/GP [33] shows that there are only 20 elliptic curves with conductor less than 4×10^5 satisfying this property for $\ell = 3$, none of which has conductor less than 17739.

4.3. **Divisibility in the ℓ-adic torsion tower.** As we have seen in the previous Section, the ℓ-divisibility of a point can increase when we move along the ℓ-adic torsion field tower. We would now like to give a bound on the extent of this phenomenon.

Our purpose in this section is to prove Proposition 4.9 (essentially an application of Sah's lemma, see [26, Proposition 2.7 (b)] and [3, Lemma A.2]), which will allow us to give such a bound in terms of the image of the torsion representation.

Lemma 4.5. *Let L be a finite Galois extension of K containing K_{ℓ^n} and let $G := \mathrm{Gal}(L|K)$. Assume that $\ell^k H^1(G, E[\ell^n]) = 0$. If $\alpha \in E(K)$ is strongly ℓ-indivisible in $E(K)$, then α is not ℓ^{k+1}-divisible in $E(L)$.*

Proof. Applying Lemma 4.2 with $M = \ell^{k+1}$ we have that the quotient $\frac{E(K)\cap \ell^{k+1}E(L)}{\ell^{k+1}E(K)}$ embeds in $H^1(G, E[\ell^n])$, so it is killed by ℓ^k. Therefore $\ell^k \left(E(K) \cap \ell^{k+1}E(L)\right) \subseteq \ell^{k+1}E(K)$. Assuming by contradiction that $\alpha \in \ell^{k+1}E(L)$ we get $\ell^k\alpha = \ell^{k+1}\beta$ for some $\beta \in E(K)$. But then $T = \ell\beta - \alpha \in E[\ell^k](K)$ is such that $\alpha + T \in \ell E(K)$, contradicting our assumption that α is strongly ℓ-indivisible. □

Lemma 4.6. *Assume that for some $n_0 \geqslant 1$ we have $(1+\ell^{n_0})\,\mathrm{Id} \in H_{\ell^n}$ (if $n \leqslant n_0$ the condition is automatically satisfied). Then the exponent of $H^1(H_{\ell^n}, E[\ell^k])$ divides ℓ^{n_0} for every $k \leqslant n$.*

Proof. Let $\lambda = (1 + \ell^{n_0})\,\mathrm{Id}$ and let $\varphi : H_{\ell^n} \to E[\ell^k]$ be a cocycle. Using that λ is central in H_{ℓ^n} and that φ is a cocycle, for any $g \in H_{\ell^n}$ we have

$$g\varphi(\lambda) + \varphi(g) = \varphi(g\lambda) = \varphi(\lambda g) = \lambda\varphi(g) + \varphi(\lambda),$$

so

$$\ell^{n_0}\varphi(g) = (\lambda - 1)\varphi(g) = g\varphi(\lambda) - \varphi(\lambda),$$

that is, $\ell^{n_0}\varphi$ is a coboundary. This proves that $\ell^{n_0}H^1(H_{\ell^n}, E[\ell^k]) = 0$ as claimed. □

Lemma 4.7. *Assume that E does not have complex multiplication and let $n_\ell \geqslant 1$ be a parameter of maximal growth for the ℓ-adic torsion representation. Then for every $n \geqslant n_\ell$ and for every $g \in \mathrm{Mat}_2(\mathbb{Z}_\ell)$ we have that $(\mathrm{Id} + \ell^{n_\ell} g) \bmod \ell^n$ is an element of H_{ℓ^n}.*

Proof. We prove this by induction. For $n = n_\ell$ the statement is trivial, so suppose $(\mathrm{Id} + \ell^{n_\ell} g) \bmod \ell^n$ belongs to H_{ℓ^n} for some $n > n_\ell$. Since the map $H_{\ell^{n+1}} \to H_{\ell^n}$ is surjective we can lift this element to an element of the form $\mathrm{Id} + \ell^{n_\ell} g + \ell^n g' \in H_{\ell^{n+1}}$, where $g' \in \mathrm{Mat}_2(\mathbb{F}_\ell)$. Since

$$\ker(H_{\ell^{n+1}} \to H_{\ell^n}) = \{\mathrm{Id} + \ell^n h \mid h \in \mathrm{Mat}_2(\mathbb{F}_\ell)\}$$

we have that $\mathrm{Id} - \ell^n g'$ is in $H_{\ell^{n+1}}$, hence $H_{\ell^{n+1}}$ contains the product

$$(\mathrm{Id} - \ell^n g')(\mathrm{Id} + \ell^{n_\ell} g + \ell^n g') \equiv (\mathrm{Id} + \ell^{n_\ell} g) \pmod{\ell^{n+1}},$$

where we use the fact that $\ell^{2n}(g')^2 = \ell^{n+n_\ell} g'g = 0$ since we are working modulo ℓ^{n+1}. □

In the special case $g = \mathrm{Id}$, the same result also holds for elliptic curves with complex multiplication:

Lemma 4.8. *Let E be an arbitrary elliptic curve and let $n_\ell \geqslant 1$ be a parameter of maximal growth (in particular, $n_\ell \geqslant 2$ if $\ell = 2$). For every $n \geqslant n_\ell$ we have $(1 + \ell^{n_\ell})\,\mathrm{Id} \in H_{\ell^n}$.*

Proof. In the light of the previous lemma we may assume that E has complex multiplication, so that the image of the torsion representation is contained in the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. The equality $\#H_{\ell^{n+1}} = \ell^2 \# H_{\ell^n}$ for $n \geqslant n_\ell$ is equivalent to the fact that

$$\ker\left(H_{\ell^{n+1}} \to H_{\ell^n}\right) = \mathrm{Id} + \ell^n \mathbb{T} \subseteq \{M \in \mathrm{Mat}_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) : M \equiv \mathrm{Id} \pmod{\ell^n}\},$$

where $\mathbb{T}$ is the tangent space to the image of the Galois representation as introduced in [17, Definition 9] and further studied in [18, Definition 18]. We proceed by induction, the base case $n = n_\ell$ being trivial. By surjectivity of $H_{\ell^{n+1}} \to H_{\ell^n}$ and the inductive hypothesis, we know that $H_{\ell^{n+1}}$ contains an element reducing to $(1 + \ell^{n_\ell})\,\mathrm{Id}$ modulo ℓ^n, that is, an element of the form $M_{n+1} := (1 + \ell^{n_\ell})\,\mathrm{Id} + \ell^n t$. Here t is an element of $\mathbb{T}$: to see this, notice that M_{n+1} is congruent to the identity modulo ℓ^{n_ℓ}, so it cannot lie in the non-trivial coset of the normaliser of a Cartan subgroup ([18, Theorem 40]), and therefore belongs to the Cartan subgroup itself. But then M_{n+1} is of the form $\begin{pmatrix} x & \delta y \\ y & x + \gamma y \end{pmatrix}$ for appropriate parameters (γ, δ), hence

$$t = \frac{1}{\ell^n} \begin{pmatrix} x - 1 - \ell^{n_\ell} & \delta y \\ y & (x - 1 - \ell^{n_\ell}) + \gamma y \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{F}_\ell)$$

belongs to $\mathbb{T}$ by the explicit description given in [18, Definition 18]. Using the equality $\ker\left(H_{\ell^{n+1}} \to H_{\ell^n}\right) = \mathrm{Id} + \ell^n \mathbb{T}$ we see that $H_{\ell^{n+1}}$ also contains $\mathrm{Id} - \ell^n t$, so it contains

$$((1 + \ell^{n_\ell})\,\mathrm{Id} + \ell^n t)(\mathrm{Id} - \ell^n t) \equiv \mathrm{Id} - \ell^{2n} t^2 + \ell^{n_\ell}\,\mathrm{Id} - \ell^{n+n_\ell} t \equiv (1 + \ell^{n_\ell})\,\mathrm{Id} \pmod{\ell^{n+1}}$$

as claimed. □

Proposition 4.9. *Assume that α is strongly ℓ-indivisible in $E(K)$. Let n_ℓ be a parameter of maximal growth for the ℓ-adic torsion representation. Then for every n the point α is not $\ell^{n_\ell+1}$-divisible in K_{ℓ^n}; equivalently, α is not $\ell^{n_\ell+1}$-divisible in K_{ℓ^∞}.*

Proof. By Lemma 4.8 the group H_{ℓ^n} contains $(1 + \ell^{n_\ell})\,\mathrm{Id}$, so by Lemma 4.6 the exponent of $H^1(H_{\ell^n}, E[\ell^n])$ divides ℓ^{n_ℓ}. We conclude by Lemma 4.5. □

4.4. **The ℓ-adic failure is bounded.** In this section we establish some general results that will form the basis of all subsequent arguments (in particular Lemma 4.10 and Proposition 4.11) and use them to show that the ℓ-adic failure $A_\ell(N)$ can be effectively bounded (Theorem 4.15).

Lemma 4.10. *Assume that for some $d \geqslant 0$ the point $\alpha \in E(K)$ is not ℓ^{d+1}-divisible over K_{ℓ^∞}. Then V_{ℓ^∞} contains a vector of valuation at most d.*

Similarly, if $\alpha \in E(K)$ is not ℓ^{d+1}-divisible over K_∞ then W_{ℓ^∞} contains a vector of valuation at most d.

Proof. Assume by contradiction that every element of V_{ℓ^∞} has valuation at least $d+1$. Then the image of V_{ℓ^∞} in $E[\ell^{d+1}] = T_\ell(E)/\ell^{d+1}T_\ell(E)$ is zero. As this image is exactly $\mathrm{Gal}(K_{\ell^\infty,\ell^{d+1}} \mid K_{\ell^\infty})$, we obtain $K_{\ell^\infty,\ell^{d+1}} = K_{\ell^\infty}$, so α is ℓ^{d+1}-divisible in K_{ℓ^∞}, a contradiction.

The second part can be proved in exactly the same way. □

The following group-theoretic Proposition will be applied in this section and in Section 7. In all of our applications the group H will be the image of the ℓ-adic torsion representation associated with some elliptic curve.

Proposition 4.11. *Let ℓ be a prime number, d be a positive integer, H be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, and $A = \mathbb{Z}_\ell[H]$ be the sub-$\mathbb{Z}_\ell$-algebra of $\mathrm{Mat}_2(\mathbb{Z}_\ell)$ generated by the elements of H. Let $V \subseteq \mathbb{Z}_\ell^2$ be an A-submodule of $\mathbb{Z}_\ell^2$, and suppose that V contains at least one vector of ℓ-adic valuation at most d.*

1. *Suppose that H contains $\{M \in \mathrm{Mat}_2(\mathbb{Z}_\ell) : M \equiv \mathrm{Id} \pmod{\ell^n}\}$ for some $n \geqslant 1$. Then V contains $\ell^{d+n}\mathbb{Z}_\ell^2$.*
2. *Suppose that the reduction of H modulo ℓ acts irreducibly on $\mathbb{F}_\ell^2$. Then V contains $\ell^d\mathbb{Z}_\ell^2$.*
3. *Let C be a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with parameters (γ, δ) and let N be its normaliser. Suppose that H is an open subgroup of N not contained in C, and that H contains $\{M \in C : M \equiv \mathrm{Id} \pmod{\ell^n}\}$ for some $n \geqslant 1$. Then V contains $\ell^{3n+d+v_\ell(4\delta)}\mathbb{Z}_\ell^2$.*

Proof. The assumptions and the conclusions of the Proposition are invariant under changes of basis in $\mathbb{Z}_\ell^2$, so we may assume that $v = \ell^d e_1$ is in V, where $e_1 = \begin{pmatrix}1\\0\end{pmatrix}$.

(1) It is clear that A contains $\ell^n \mathrm{Mat}_2(\mathbb{Z}_\ell)$, so we have

$$V \supseteq A \cdot v \supseteq \ell^n \mathrm{Mat}_2(\mathbb{Z}_\ell) \cdot v = \ell^{n+d} \mathrm{Mat}_2(\mathbb{Z}_\ell) \cdot e_1 = \ell^{n+d}\mathbb{Z}_\ell^2.$$

Let H_ℓ denote the reduction of H modulo ℓ. The condition that H_ℓ acts irreducibly on $\mathbb{F}_\ell^2$ implies that there exists $\overline{M} \in \mathbb{F}_\ell[H_\ell]$ such that $\overline{M}e_1 \equiv \begin{pmatrix}0\\1\end{pmatrix} \pmod{\ell}$. Fix a lift $M \in A$ of $\overline{M}$, which exists because the natural reduction map $A = \mathbb{Z}_\ell[H] \to \mathbb{F}_\ell[H_\ell]$ is clearly surjective. Then $Mv = \ell^d M e_1$ is a vector whose second coordinate has valuation exactly d and whose first coordinate has valuation strictly larger than d. It is then immediate to see that v and Mv, that are contained in V, generate $\ell^d\mathbb{Z}_\ell^2$.

(2) It is enough to show that A contains $\ell^{3n+v_\ell(4\delta)} \mathrm{Mat}_2(\mathbb{Z}_\ell)$, and the conclusion follows as in (1) above.

Suppose first that $\gamma = 0$, and let $M_0 = \begin{pmatrix} x_0 & -\delta y_0 \\ y_0 & -x_0 \end{pmatrix} \in H \setminus C$ and $M_1 = \begin{pmatrix} 1+\ell^n x_0 & \delta\ell^n y_0 \\ \ell^n y_0 & 1+\ell^n x_0 \end{pmatrix} \in H$. The existence and the form of such matrices follow from the assumptions and from the description of Cartan subgroups and their normaliser given in Definition 2.8 and Lemma 2.10. Then A contains $M_2 = M_1 -$

$\mathrm{Id} + \ell^n M_0 = 2\ell^n \begin{pmatrix} x_0 & 0 \\ y_0 & 0 \end{pmatrix}$. Let moreover $M_3 = \ell^n \begin{pmatrix} 0 & \delta \\ 1 & 0 \end{pmatrix}$, which is in A since it can be written as $\begin{pmatrix} 1 & \ell^n\delta \\ \ell^n & 1 \end{pmatrix} - \mathrm{Id}$, where both matrices are in H by assumption. Then we have

$$4\ell^{2n} \begin{pmatrix} x_0^2 - \delta y_0^2 & 0 \\ 0 & 0 \end{pmatrix} = (M_2 - 2y_0 M_3) \cdot M_2 \in A$$

and $x_0^2 - \delta y_0^2 = -\det M_0 \in \mathbb{Z}_\ell^\times$. It follows that A contains $4\ell^{2n} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, and since $\mathrm{Id} \in A$ we have that all diagonal matrices of valuation at least $2n + v_\ell(4)$ are in A, which therefore also contains $\begin{pmatrix} 0 & 0 \\ \ell^{3n+v_\ell(4)} & 0 \end{pmatrix} = M_3 \begin{pmatrix} \ell^{2n+v_\ell(4)} & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & \ell^{3n+v_\ell(4)}\delta \\ 0 & 0 \end{pmatrix} = M_3 \begin{pmatrix} 0 & 0 \\ 0 & \ell^{2n+v_\ell(4)} \end{pmatrix}$. Together with the diagonal matrices found above, these elements clearly generate $\ell^{3n+v_\ell(4\delta)} \mathrm{Mat}_2(\mathbb{Z}_\ell)$, and we are done.

If $\gamma \neq 0$, by Remark 2.9 we may assume $\gamma = 1$ and $\ell = 2$. In this case let $M_0 = \begin{pmatrix} x_0 + y_0 & \delta y_0 + x_0 + y_0 \\ -y_0 & -x_0 - y_0 \end{pmatrix} \in H \setminus C$ and $M_1 = \mathrm{Id} + \ell^n \begin{pmatrix} x_0 & \delta y_0 \\ y_0 & x_0 + y_0 \end{pmatrix} \in H$. Then A contains $M_2 = M_1 - \mathrm{Id} + \ell^n M_0 = \ell^n \begin{pmatrix} 2x_0 + y_0 & 2\delta y_0 + x_0 + y_0 \\ 0 & 0 \end{pmatrix}$. Let moreover $M_3 = \ell^n \begin{pmatrix} -1 & \delta \\ 1 & 0 \end{pmatrix} \in A$. Then we have

$$M_2(\delta M_2 - (2\delta y_0 + x_0 + y_0)M_3) = -\ell^{2n} \det(M_0)(1 + 4\delta) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in A,$$

and using the fact that $\det(M_0) \in \mathbb{Z}_\ell^\times$ (since $M_0 \in H \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$) we obtain that A contains all diagonal matrices of valuation at least $2n$. We can then conclude as before.

□

Proposition 4.12. *Assume that α is strongly ℓ-indivisible in $E(K)$ and let n_ℓ be a parameter of maximal growth for the ℓ-adic torsion representation.*

(1) Assume that E does not have complex multiplication. Then for every $k \geqslant 1$ we have $E[\ell^k] \subseteq V_{\ell^{k+2n_\ell}}$.
(2) Assume that E has complex multiplication by $\mathcal{A} := \mathrm{End}_{\overline{K}}(E)$, and that K does not contain the imaginary quadratic field $\mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Q}$. Let (γ, δ) be parameters for the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathcal{A}$. Then for all $k \geqslant 1$ we have $E[\ell^k] \subseteq V_{\ell^{k+4n_\ell+v_\ell(4\delta)}}$.

Proof. By Remark 2.6, in order to show part (1) it is enough to prove $\ell^{2n_\ell} T_\ell(E) \subseteq V_{\ell^\infty}$. To see that this holds, notice that by Lemma 4.10 and Proposition 4.9 there is an element of valuation at most n_ℓ in V_{ℓ^∞}. Now we just need to apply Proposition 4.11(1) with $H = H_{\ell^\infty}$, $V = V_{\ell^\infty}$ and $d = n = n_\ell$. Part (2) can be proved in the same way using Proposition 4.11(3). □

In §6 we will show that a naïve analogue of Proposition 4.12 does not hold in case E has complex multiplication defined over K.

Remark 4.13. Write $\alpha = \ell^d\beta + T_h$, where $\beta \in E(K)$ is strongly ℓ-indivisible and $T_h \in E[\ell^h](K)$ is a point of order ℓ^h, for some $h, d \geqslant 0$. Notice that it is always possible to do so: first, let $\beta \in E(K)$ and d be such that $\alpha = \ell^d\beta + T$ for some $T \in E(K)$ of order a power of ℓ, with d maximal. Assume then by contradiction that β is not strongly ℓ-indivisible. This means that there are $\gamma, S \in E(K)$ with S of order a power of ℓ such that $\beta = \ell\gamma + S$. But then $\alpha = \ell^d(\ell\gamma + S) + T = \ell^{d+1}\gamma + (\ell^d S + T)$, contradicting the maximality of d.

Remark 4.14. Let $\hat{h}$ be the canonical (Néron-Tate) height on E, as described in [31, Section VIII.9]. Following [22], it is possible to bound the divisibility parameters d and h in terms of $\hat{h}(\alpha)$, the degree of K over $\mathbb{Q}$, the discriminant Δ_E of E over K and the Szpiro ratio

$$\sigma = \begin{cases} 1 & \text{if } E \text{ has everywhere good reduction} \\ \dfrac{\log|N_{K/\mathbb{Q}}(\Delta_E)|}{\log|N_{K/\mathbb{Q}}(N_E)|} & \text{otherwise} \end{cases}$$

where N_E denotes the conductor of E over K. In fact, [22, Theorem 1] gives the bound

$$h \leqslant v_\ell\left\lfloor c_1[K:\mathbb{Q}]\sigma^2 \log\left(c_2[K:\mathbb{Q}]\sigma^2\right)\right\rfloor$$

where $c_1 = 134861$ and $c_2 = 104613$.

For the parameter d we can reason as follows. For $\alpha = \ell^d\beta + T_h$, by [31, Theorem 9.3] we have

$$\hat{h}(\alpha) = \hat{h}(\ell^d\beta + T_h) = \hat{h}(\ell^d\beta) = \ell^{2d}\hat{h}(\beta)$$

so we get $d \leqslant \dfrac{1}{2\log\ell}\log\left(\dfrac{\hat{h}(\alpha)}{\hat{h}(\beta)}\right)$. Now in view of [22, Theorem 2] for any non-torsion point $\beta \in E(K)$ we have

$$\hat{h}(\beta) \geqslant B := \frac{\log|N_{K/\mathbb{Q}}(\Delta_E)|}{10^{15}[K:\mathbb{Q}]^3\sigma^6\log^2(c_2[K:\mathbb{Q}]\sigma^2)},$$

where again $c_2 = 104613$. We thus obtain the effective bound $d \leqslant \frac{1}{2\log\ell}\log\left(\frac{\hat{h}(\alpha)}{B}\right)$.

Theorem 4.15. *Let ℓ be a prime and assume that $\mathrm{End}_K(E) = \mathbb{Z}$ (i.e. either E does not have CM, or it has CM but the complex multiplication is not defined over K). There is an effectively computable constant a_ℓ, depending only on α and on the ℓ-adic torsion representation associated to E, such that $A_\ell(N)$ divides ℓ^{a_ℓ} for all positive integers N.*

Moreover, a_ℓ is zero for every odd prime ℓ such that α is ℓ-indivisible and for which the ℓ-adic torsion representation associated with E is maximal (see Definition 3.2). For the finitely many remaining primes ℓ we can take a_ℓ as follows: let n_ℓ be a parameter of maximal growth for the ℓ-adic torsion representation and let d be as in Remark 4.13. If E has CM over $\overline{K}$, let (γ, δ) be parameters for the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathrm{End}_{\overline{K}}(E)$. Then:

- *$a_\ell = 4n_\ell + 2d$ if E does not have CM over $\overline{K}$;*
- *$a_\ell = 8n_\ell + 2v_\ell(4\delta) + 2d$ if E has CM over $\overline{K}$.*

Proof. Let $\alpha = \ell^d\beta + T_h$ as described above. Notice that if α is strongly ℓ-indivisible we have $d = 0$, and the conclusion follows from Proposition 4.12. If the ℓ-adic torsion representation is

maximal, the fact that a_ℓ is zero in the cases stated follows from [12, Theorem 5.2 and Theorem 5.8].

We now study the ℓ-adic failure $A_\ell(N)$ in the general case. Let $n = v_\ell(N)$ and notice that the claim is trivial for $n \leqslant d$, so we may assume $n > d$. Since

$$[K_{\ell^{n+h}}(\ell^{-n}\alpha) : K_{\ell^{n+h}}] = [K_{\ell^n}(\ell^{-n}\alpha)K_{\ell^{n+h}} : K_{\ell^n}K_{\ell^{n+h}}] \quad \text{divides} \quad [K_{\ell^n}(\ell^{-n}\alpha) : K_{\ell^n}]$$

we have that $\dfrac{\ell^{2n}}{[K_{\ell^n}(\ell^{-n}\alpha) : K_{\ell^n}]}$ divides $\dfrac{\ell^{2n}}{[K_{\ell^{n+h}}(\ell^{-n}\alpha) : K_{\ell^{n+h}}]}$, and since we have

$$K_{\ell^{n+h}}(\ell^{-n}\alpha) = K_{\ell^{n+h}}(\ell^{-(n-d)}\beta)$$

we get

$$\frac{\ell^{2n}}{[K_{\ell^{n+h}}(\ell^{-n}\alpha) : K_{\ell^{n+h}}]} = \ell^{2d}\frac{\ell^{2(n-d)}}{[K_{\ell^{n+h}}(\ell^{-(n-d)}\beta) : K_{\ell^{n+h}}]}$$

so in view of Remark 2.1 we are reduced to proving the statement for β instead of α. Since β is strongly ℓ-indivisible, we can conclude as stated at the beginning of the proof.

The fact that a_ℓ is effective follows from the fact that one can effectively compute a parameter of maximal growth for the ℓ-adic torsion representation (Remark 3.7), an upper bound for the value of d (Remark 4.14), and the endomorphism ring $\mathrm{End}_{\overline{K}}(E)$ ([1], [8], [16]). □

5. THE ADELIC FAILURE

In this section we study the adelic failure $B_\ell(N)$, that is, the degree of the intersection $K_{\ell^n,\ell^n} \cap K_N$ over K_{ℓ^n}. Notice that this intersection is a finite Galois extension of K_{ℓ^n}.

5.1. **Intersection of torsion fields in the non-CM case.** We first aim to establish certain properties of the intersections of different torsion fields of E, assuming for this subsection that E does not have complex multiplication over $\overline{K}$. Our main tool (Theorem 5.3) is a refinement of [6, Theorem 3.3.1], and will appear in an upcoming paper of F. Campagna and P. Stevenhagen. The proof of the stronger version we need requires only minor changes with respect to that of [6, Theorem 3.3.1], and can be easily derived from it using the following well-known lemmas (see [27] and [29]).

Lemma 5.1. *Let p be a prime and let H be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Let S be a non-abelian simple group that occurs in H. Then S is isomorphic either to A_5 or to $\mathrm{PSL}_2(\mathbb{F}_p)$; the latter case is only possible if H contains $\mathrm{SL}_2(\mathbb{F}_p)$.*

Lemma 5.2 (Serre)**.** *Let $\ell \geqslant 5$ be a prime and let $G \subseteq \mathrm{SL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ be a subgroup. Let $\pi : \mathrm{SL}_2(\mathbb{Z}/\ell^k\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ be the reduction homomorphism and suppose that $\pi(G) = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$: then $G = \mathrm{SL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$.*

Theorem 5.3. *Assume that E does not have complex multiplication. Let S be the set consisting of the primes ℓ satisfying one or more of the following three conditions:*

(i) $\ell \mid 30\,\mathrm{disc}(K \mid \mathbb{Q})$;
(ii) *E has bad reduction at some prime of K above ℓ;*

(iii) the modulo ℓ torsion representation is not surjective.

For every $\ell \notin S$ we have $K_{\ell^n} \cap K_M = K$ for all $M, n \geqslant 1$ with $\ell \nmid M$.

Remark 5.4. The finite set S appearing in Theorem 5.3 can be computed explicitly. In fact, it is well known that one can compute the discriminant of K and the set of primes of bad reduction of E. An algorithm to compute the set of primes for which the $\bmod \ell$ representation is not surjective is described in [37].

As a corollary, we give a slightly more precise version of [29, §3.4, Lemma 6].

Corollary 5.5. *Assume that E does not have complex multiplication and let S be as in Theorem 5.3. Let M be a positive integer and write $M = M_1 M_2$, where*

$$M_1 = \prod_{p \notin S} p^{e_p} \qquad p \text{ prime, } e_p \geqslant 0,$$

$$M_2 = \prod_{q \in S} q^{e_q} \qquad q \text{ prime, } e_q \geqslant 0.$$

Then we have

$$\mathrm{Gal}(K_M \mid K) \cong \mathrm{GL}_2\left(\mathbb{Z}/M_1\mathbb{Z}\right) \times \mathrm{Gal}\left(K_{M_2} \mid K\right).$$

Proof. By Theorem 5.3 we have that, for any $p \notin S$ and any $e \geqslant 0$, the field K_{p^e} is linearly disjoint over K from K_{M_2} and from K_{q^f} for every $q \neq p$ and every $f \geqslant 1$. Moreover we have

$$\mathrm{GL}_2\left(\mathbb{Z}/M_1\mathbb{Z}\right) \cong \prod_{p \notin S} \mathrm{GL}_2(\mathbb{Z}/p^{e_p}\mathbb{Z}) \cong \prod_{p \notin S} \mathrm{Gal}(K_{p^{e_p}} \mid K),$$

and the Corollary follows by standard Galois theory. □

Remark 5.6. Let $\tilde{K}$ be the compositum of the fields K_p for all $p \in S$, where S is as in Theorem 5.3. In the following section it will be important to notice that S is stable under base change to $\tilde{K}$. More precisely, let $\tilde{S}$ be the set of all primes ℓ that satisfy one of the following:

(i') $\ell \mid 30 \operatorname{disc}(\tilde{K} \mid \mathbb{Q})$;
(ii') E has bad reduction at some prime of $\tilde{K}$ above ℓ;
(iii') the modulo ℓ torsion representation attached to $E/\tilde{K}$ is not surjective.

Then $\tilde{S} = S$.

Indeed, the inclusion $\tilde{S} \supseteq S$ is easy to see: clearly conditions (i) and (iii) imply (i') and (iii') respectively, so we only need to discuss (ii). Let $\mathfrak{p}$ be a prime of K (of characteristic ℓ) at which E has bad reduction, and let $\mathfrak{q}$ be a prime of $\tilde{K}$ lying over $\mathfrak{p}$. We need to show that $\ell \in \tilde{S}$. If E has bad reduction at $\mathfrak{q}$ we have $\ell \in \tilde{S}$ by (ii'), while if E has good reduction at $\mathfrak{q}$ then $\mathfrak{p}$ ramifies in $\tilde{K}$ by [31, Proposition VII.5.4 (a)], so we have $\ell \mid \operatorname{disc}(\tilde{K} \mid \mathbb{Q})$ and ℓ is in $\tilde{S}$ by (i').

Conversely, let $\ell \in \tilde{S}$. If (ii') holds, then clearly also (ii) holds, and ℓ is in S. Suppose that (i') holds. If ℓ divides 30, then it is in S by (1). Otherwise ℓ divides $\operatorname{disc}(\tilde{K} \mid \mathbb{Q})$, which by [28, III.§4, Proposition 8] is equal to $\operatorname{disc}(K \mid \mathbb{Q})^{[\tilde{K}:K]} N_{K/\mathbb{Q}} \operatorname{disc}(\tilde{K} \mid K)$; if ℓ divides $\operatorname{disc}(K \mid \mathbb{Q})$, then it is in S by (1), while if it divides $\operatorname{disc}(\tilde{K} \mid K)$ then we have $\ell \in S$ by

[31, Proposition VIII.1.5(b)]. We may therefore assume that (i') and (ii') do not hold. Since ℓ is in $\tilde{S}$, (iii') must hold, that is, the modulo-ℓ torsion representation attached to $E/\tilde{K}$ is not surjective. We claim that the same is true for E/K. Indeed, if ℓ is in S this is true by definition, while if $\ell \notin S$ the previous corollary shows that K_ℓ is linearly disjoint from $\tilde{K}$, so the images of the modulo-ℓ representations over K and over $\tilde{K}$ coincide.

5.2. **The adelic failure is bounded.** We now go back to the general case of E possibly admitting complex multiplication.

Fix an integer $N > 1$ and a prime number ℓ dividing N. Write $N = \ell^n R$ with $\ell \nmid R$ and recall that the adelic failure $B_\ell(N)$ is defined to be the degree $[K_{\ell^n,\ell^n} \cap K_N : K_{\ell^n}]$. In this section we study this failure for $N = \ell^n R$, starting with a simple Lemma in Galois theory.

Lemma 5.7. *Let L_1, L_2 and L_3 be Galois extensions of K with $L_1 \subseteq L_2$. Then the compositum $L_1(L_2 \cap L_3)$ is equal to the intersection $L_2 \cap (L_1 L_3)$.*

Proof. For $i = 1, 2, 3$ let $G_i := \mathrm{Gal}(\overline{K} \mid L_i)$. The claim is equivalent to $G_1 \cap (G_2 \cdot G_3) = G_2 \cdot (G_1 \cap G_3)$, where the inclusion "$\supseteq$" is obvious. Let then $g \in G_1 \cap (G_2 \cdot G_3)$, so that there are $g_1 \in G_1$, $g_2 \in G_2$ and $g_3 \in G_3$ such that $g = g_1 = g_2 g_3$. But then $g_2^{-1} g_1 = g_3 \in G_3$ and, since $G_2 \subseteq G_1$, also $g_2^{-1} g_1 \in G_1$, so that $g = g_2(g_2^{-1} g_1) \in G_2 \cdot (G_1 \cap G_3)$. □

We now establish some properties of certain subfields of $K_{\ell^n R,\ell^n}$.

Lemma 5.8. *Setting*

$$L := K_{\ell^n,\ell^n} \cap K_N, \quad F := L \cap K_R = K_{\ell^n,\ell^n} \cap K_R, \quad T := F \cap K_{\ell^n} = K_{\ell^n} \cap K_R$$

we have:

- *(a) The compositum FK_{ℓ^n} is L.*
- *(b) $\mathrm{Gal}(F \mid T) \cong \mathrm{Gal}(L \mid K_{\ell^n})$; in particular, $\mathrm{Gal}(F \mid T)$ is an abelian ℓ-group.*
- *(c) F is the intersection of the maximal abelian extension of T contained in K_{ℓ^n,ℓ^n} and the maximal abelian extension of T contained in K_R.*

Proof. (a) By Lemma 5.7 we have $FK_{\ell^n} = K_{\ell^n}(K_{\ell^n,\ell^n} \cap K_R) = K_{\ell^n,\ell^n} \cap K_{\ell^n R} = L$. (b) Follows from (a) and standard Galois theory. For (c), notice that F is abelian over T by (b), so it must be contained in the maximal abelian extension of T contained in K_{ℓ^n,ℓ^n} and in the maximal abelian extension of T contained in K_R. On the other hand, F cannot be smaller than the intersection of these abelian extensions, because by definition it is the intersection of K_{ℓ^n,ℓ^n} and K_R. □

Proposition 5.9. *The adelic failure $B_\ell(N)$ is equal to $[F : T]$, where $F = K_{\ell^n,\ell^n} \cap K_R$ and $T = K_{\ell^n} \cap K_R$.*

Proof. Let as above $L = K_{\ell^n,\ell^n} \cap K_{\ell^n R}$. We have $\mathrm{Gal}(K_{\ell^n,\ell^n} \mid L) \cong \mathrm{Gal}(K_{\ell^n R,\ell^n} \mid K_{\ell^n R})$, so we get

$$[K_{\ell^n,\ell^n} : K_{\ell^n}] = [K_{\ell^n,\ell^n} : L][L : K_{\ell^n}] = [K_{\ell^n R,\ell^n} : K_{\ell^n R}][L : K_{\ell^n}]$$

and we conclude by Lemma 5.8(b). □

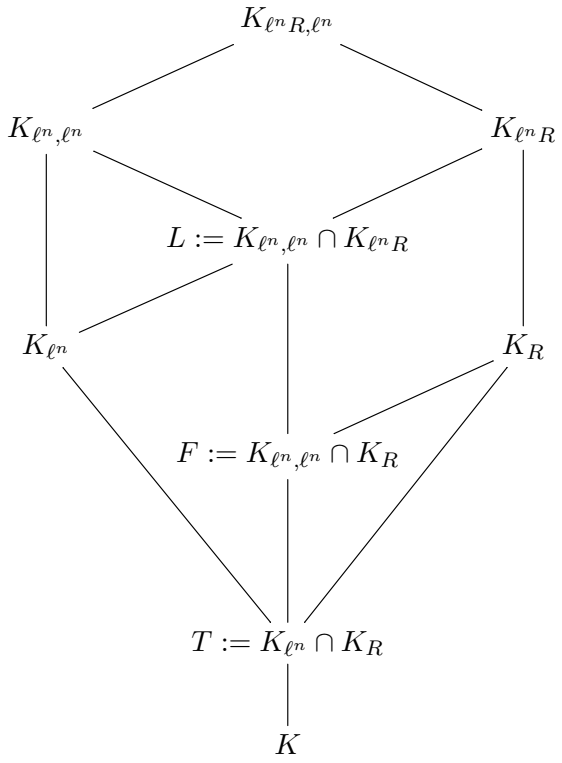


FIGURE 1. The situation described in Lemma 5.8 and Proposition 5.9.

In what follows we will need to work over a certain extension $\tilde{K}$ of K; this extension will depend on the prime ℓ. More precisely, we give the following definition.

Definition 5.10. Let $\tilde{K}$ be the finite extension of K defined as follows:

- If E has complex multiplication, we take $\tilde{K}$ to be the compositum of K with the CM field of E. This is an at most quadratic extension of K. Notice that in this case by [19, Lemma 2.2] we have $\tilde{K}_n = K_n$ for every $n \geqslant 3$.
- If E does not have CM and ℓ is not one of the primes in the set S of Theorem 5.3, we just let $\tilde{K} = K$. Notice that this happens for all but finitely many primes ℓ.
- If E does not have CM and ℓ is one of the primes in the set S of Theorem 5.3, we let $\tilde{K}$ be the compositum of all the K_p for $p \in S$. Notice that in this case $\tilde{K}_\ell = \tilde{K}$.

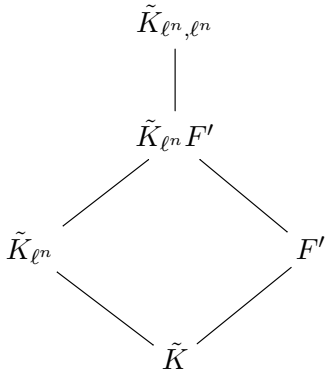
We shall use the notation $\tilde{K}_M$ (respectively $\tilde{K}_{M,N}$) for the torsion (resp. Kummer) extensions of $\tilde{K}$. We shall also write

$$\tilde{H}_{\ell^n} := \mathrm{Im}\left(\tau_{\ell^n} : \mathrm{Gal}(\overline{K} \mid \tilde{K}) \to \mathrm{Aut}(E[\ell^n])\right) \cong \mathrm{Gal}\left(\tilde{K}_{\ell^n} \mid \tilde{K}\right),$$
$$\tilde{V}_{\ell^n} := \mathrm{Im}\left(\kappa_{\ell^n} : \mathrm{Gal}(\overline{K} \mid \tilde{K}_{\ell^n}) \to E[\ell^n]\right) \cong \mathrm{Gal}\left(\tilde{K}_{\ell^n,\ell^n} \mid \tilde{K}_{\ell^n}\right)$$

for the images of the ℓ^n-torsion representation and of the (ℓ^n, ℓ^n)-Kummer map attached to $E/\tilde{K}$. Finally, we let $\tilde{n}_\ell$ be the minimal parameter of maximal growth for the ℓ-adic torsion representation over $\tilde{K}$. Notice that, thanks to Lemma 3.8, we have $\tilde{n}_\ell \leqslant n_\ell + v_\ell([\tilde{K} : K])$.

Proposition 5.11. *The extension $F' := \tilde{K}_{\ell^n,\ell^n} \cap \tilde{K}_R$ is abelian over $\tilde{K}$.*

Proof. This is well known if E has complex multiplication because then $\tilde{K}_R$ is itself abelian over $\tilde{K}$, see for example [30, Theorem II.2.3]. In case E does not have complex multiplication and ℓ is not in the set S of Theorem 5.3, this follows easily by considering the diagram



In fact, since $\tilde{K}_{\ell^n} \cap F' = \tilde{K}$ by Theorem 5.3 (notice that in this case $\tilde{K} = K$), we have that $\mathrm{Gal}(F' \mid \tilde{K}) \cong \mathrm{Gal}(\tilde{K}_{\ell^n} F' \mid \tilde{K}_{\ell^n})$ is a quotient of $\tilde{V}_{\ell^n}$, hence abelian. Thus we can assume that E does not have CM and that ℓ is in the set S of Theorem 5.3.

Notice that F' is a Galois extension of $\tilde{K}$ with degree a power of ℓ, since the same is true for $\tilde{K}_{\ell^n,\ell^n} \mid \tilde{K}$ and $F' \subseteq \tilde{K}_{\ell^n,\ell^n}$. Letting r denote the radical of R, the degree of $[F' : F' \cap \tilde{K}_r]$, which is still a power of ℓ, divides $[\tilde{K}_R : \tilde{K}_r]$, which is a product of primes dividing R. So since $\ell \nmid R$ we obtain $[F' : F' \cap \tilde{K}_r] = 1$, that is $\tilde{K}_{\ell^n,\ell^n} \cap \tilde{K}_R = \tilde{K}_{\ell^n,\ell^n} \cap \tilde{K}_r$, and we may assume that R is squarefree. Write now $R = R_1 R_2$, where R_1 is the product of the prime factors of R that are *not* in S and R_2 is the product of the prime factors of R that belong to S. By definition of $\tilde{K}$ we have $\tilde{K}_R = \tilde{K}_{R_1}$, so we may further assume that no prime $p \in S$ divides R. By Corollary 5.5 we then have $\mathrm{Gal}(\tilde{K}_R \,|\, \tilde{K}) \cong \mathrm{GL}_2(\mathbb{Z}/R\mathbb{Z})$.

Since $F' \subseteq \tilde{K}_R$, there must be a normal subgroup $D = \mathrm{Gal}(\tilde{K}_R \mid F') \trianglelefteq \mathrm{GL}_2(\mathbb{Z}/R\mathbb{Z})$ of index a power of ℓ. In order to conclude we just need to show that D contains $\mathrm{SL}_2(\mathbb{Z}/R\mathbb{Z})$, for then $\mathrm{Gal}(F' \mid \tilde{K}) \cong \mathrm{GL}_2(\mathbb{Z}/R\mathbb{Z})/D$ is abelian.

Since $\mathrm{SL}_2(\mathbb{Z}/R\mathbb{Z}) \cong \prod_{p|R} \mathrm{SL}_2(\mathbb{F}_p)$, we can consider the intersection $D_p := D \cap \mathrm{SL}_2(\mathbb{F}_p)$, which is a normal subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$. Here we identify $\mathrm{SL}_2(\mathbb{F}_p)$ with the corresponding direct factor of $\mathrm{SL}_2(\mathbb{Z}/R\mathbb{Z})$. The quotient $\mathrm{SL}_2(\mathbb{F}_p)/D_p$ cannot have order a power of ℓ unless it is trivial (recall that in our case $p \geqslant 5$), so we deduce that $D \supseteq \mathrm{SL}_2(\mathbb{F}_p)$. As this is true for every $p \mid R$, we have $D \supseteq \mathrm{SL}_2(\mathbb{Z}/R\mathbb{Z})$, and we are done. □

In what follows, whenever A is an abelian group and Q is a group acting on A, we denote by $[A, Q]$ the subgroup of A generated by elements of the form $gv - v$ for $v \in A$ and $g \in Q$. For example, we will consider the case $A = \tilde{V}_{\ell^n}$ and $Q = \tilde{H}_{\ell^n}$.

Lemma 5.12. *Let*

$$1 \to A \to G \to Q \to 1$$

be a short exact sequence of groups, with A abelian, so that Q acts naturally on A. Let G^{ab} and Q^{ab} be the maximal abelian quotients of G and Q respectively. Then $A/[A,Q]$ surjects onto $\ker(G^{\mathrm{ab}} \to Q^{\mathrm{ab}})$.

Proof. We have an injective map of short exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A \cap G' & \longrightarrow & G' & \longrightarrow & Q' & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & A & \longrightarrow & G & \longrightarrow & Q & \longrightarrow & 1 \end{array}$$

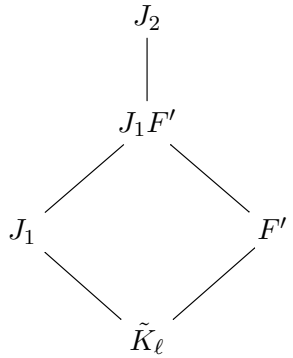
from which we get the exact sequence

$$1 \to \frac{A}{A \cap G'} \to G^{\mathrm{ab}} \to Q^{\mathrm{ab}} \to 1$$

and since $[A,Q] \subseteq A \cap G'$ we get that $A/[A,Q]$ surjects onto $A/A \cap G' = \ker(G^{\mathrm{ab}} \to Q^{\mathrm{ab}})$. □

Proposition 5.13. *The adelic failure $B_\ell(N)$ divides* $[\tilde{K} : K] \cdot \#\dfrac{\tilde{V}_{\ell^n}}{[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]}$.

Proof. Let J_1 and J_2 be the maximal abelian extensions of $\tilde{K}$ contained in $\tilde{K}_{\ell^n}$ and $\tilde{K}_{\ell^n,\ell^n}$ respectively. Then we have $\mathrm{Gal}(J_1 \,|\, \tilde{K}) = \tilde{H}_{\ell^n}^{\mathrm{ab}}$ and $\mathrm{Gal}(J_2 \,|\, \tilde{K}) = \tilde{G}_{\ell^n}^{\mathrm{ab}}$, where $\tilde{G}_{\ell^n} = \mathrm{Gal}(\tilde{K}_{\ell^n,\ell^n} \,|\, \tilde{K})$. Notice that $[J_2 : J_1] = \#W$, where $W = \ker(\tilde{G}_{\ell^n}^{\mathrm{ab}} \to \tilde{H}_{\ell^n}^{\mathrm{ab}})$ is a quotient of $\tilde{V}_{\ell^n}/[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$ by Lemma 5.12. Let moreover $F' := \tilde{K}_{\ell^n,\ell^n} \cap \tilde{K}_R$ and $T' := \tilde{K}_{\ell^n} \cap \tilde{K}_R$. By Proposition 5.11 we have $F' \subseteq J_2$ and clearly also $T' \subseteq J_1$ (indeed T' is abelian over $\tilde{K}$ since it is a sub-extension of F'). Consider the compositum J_1F' inside J_2.



It is easy to check that $F' \cap J_1 = T'$, so we have that $[F' : T'] = [J_1F' : J_1]$ divides $[J_2 : J_1]$, which in turn divides $\tilde{V}_{\ell^n}/[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$.

Now applying Proposition 5.9 with $\tilde{K}$ in place of K we get that

$$\frac{[\tilde{K}_{\ell^n,\ell^n} : \tilde{K}_{\ell^n}]}{[\tilde{K}_{\ell^n R,\ell^n} : \tilde{K}_{\ell^n R}]} \qquad \text{divides} \qquad [F' : T'],$$

and using that $[\tilde{K}_{\ell^n R,\ell^n} : \tilde{K}_{\ell^n R}]$ divides $[K_{\ell^n R,\ell^n} : K_{\ell^n R}]$ it is easy to see that

$$\frac{[K_{\ell^n,\ell^n} : K_{\ell^n}]}{[K_{\ell^n R,\ell^n} : K_{\ell^n R}]} \qquad \text{divides} \qquad [\tilde{K} : K] \cdot \frac{[\tilde{K}_{\ell^n,\ell^n} : \tilde{K}_{\ell^n}]}{[\tilde{K}_{\ell^n R,\ell^n} : \tilde{K}_{\ell^n R}]}.$$

We conclude that

$$B_\ell(N) = \frac{[K_{\ell^n,\ell^n} : K_{\ell^n}]}{[K_{\ell^n R,\ell^n} : K_{\ell^n R}]} \qquad \text{divides} \qquad [\tilde{K} : K] \cdot \#\frac{\tilde{V}_{\ell^n}}{[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]}.$$

□

So we are left with giving an upper bound on the ratio $\#\tilde{V}_{\ell^n}/\#[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$: this is achieved in the following Proposition.

Proposition 5.14. *For every n, the order of $\tilde{V}_{\ell^n}/[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$ divides $\ell^{2\tilde{n}_\ell}$, where $\tilde{n}_\ell$ is the minimal parameter of maximal growth for the ℓ-adic torsion representation of $E/\tilde{K}$.*

Proof. By Lemma 4.8, the group $\tilde{H}_{\ell^n}$ contains $(1+\ell^{\tilde{n}_\ell})\,\mathrm{Id}$. This implies that for every $v \in \tilde{V}_{\ell^n}$ the group $[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$ contains

$$\left[v, (1+\ell^{\tilde{n}_\ell})\,\mathrm{Id}\right] = (1+\ell^{\tilde{n}_\ell})\,\mathrm{Id}\cdot v - v = \ell^{\tilde{n}_\ell} v,$$

that is, $[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$ contains $\ell^{\tilde{n}_\ell}\tilde{V}_{\ell^n}$. The claim now follows from the fact that $\tilde{V}_{\ell^n}$ is generated over $\mathbb{Z}/\ell^n\mathbb{Z}$ by at most two elements. □

Lemma 5.15. *Assume that $\ell \geqslant 5$ is unramified in $K \mid \mathbb{Q}$ and that the image of the $\bmod \ell$ torsion representation is $\mathrm{GL}_2(\mathbb{F}_\ell)$ (so in particular E does not have CM over $\overline{K}$). Assume moreover that α is ℓ-indivisible. Then $V_{\ell^n} = [V_{\ell^n}, H_{\ell^n}]$.*

Proof. Since H'_{ℓ^∞} is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ whose reduction modulo ℓ contains $H'_\ell = \mathrm{GL}_2(\mathbb{F}_\ell)' = \mathrm{SL}_2(\mathbb{F}_\ell)$, by Lemma 5.2 the group H_{ℓ^∞} contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$. The assumption that ℓ is unramified in K implies that $\det(H_{\ell^\infty}) = \mathbb{Z}_\ell^\times$, which together with the inclusion $\mathrm{SL}_2(\mathbb{Z}_\ell) \subseteq H_{\ell^\infty}$ implies $H_{\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$, and in particular $H_{\ell^n} = \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. By [12, Theorem 5.2] we have $V_{\ell^n} = (\mathbb{Z}/\ell^n\mathbb{Z})^2$, so it is enough to consider

$$g_1 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in H_{\ell^n}, \quad g_2 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in H_{\ell^n}, \quad v := \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in V_{\ell^n}$$

to conclude that

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = g_1 v - v \in [V_{\ell^n}, H_{\ell^n}] \quad \text{and} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} = g_2 v - v \in [V_{\ell^n}, H_{\ell^n}],$$

so that $V_{\ell^n} \subseteq [V_{\ell^n}, H_{\ell^n}]$. □

Lemma 5.16. *Let E/K be an elliptic curve such that $\mathrm{End}_{\overline{K}}(E)$ is an order $\mathcal{A}$ in the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. Let $\ell \geqslant 3$ be a prime unramified both in K and in $\mathbb{Q}(\sqrt{-d})$, and suppose that E has good reduction at all places of K of characteristic ℓ. Then $V_{\ell^n} = [V_{\ell^n}, H_{\ell^n}]$ and $\tilde{V}_{\ell^n} = [\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]$.*

Proof. By [15, Theorem 1.5], the image of the ℓ-adic representations attached to both E/K and $E/\tilde{K}$ contains $(\mathcal{A} \otimes \mathbb{Z}_\ell)^\times$, hence in particular it contains an operator that acts as multiplication by 2 on $E[\ell^n]$ for every n. Let λ be such an operator: then $[V_{\ell^n}, H_{\ell^n}]$ contains $[V_{\ell^n}, \lambda] = \{\lambda v - v \;\big|\; v \in V_{\ell^n}\} = V_{\ell^n}$ as claimed. The case of $\tilde{V}_{\ell^n}$ is similar. □

Theorem 5.17. *Let ℓ be a prime. There is a constant b_ℓ, depending only on the p-adic torsion representations associated with E for all the primes p, such that $B_\ell(N)$ divides ℓ^{b_ℓ} for all positive integers N. Moreover,*

- *Suppose that E does not have complex multiplication over $\overline{\mathbb{Q}}$. Then b_ℓ is zero whenever the following conditions all hold: α is ℓ-indivisible, $\ell > 5$ is unramified in $K \mid \mathbb{Q}$, the $\bmod \ell$ torsion representation is surjective, and E has good reduction at all places of K of characteristic ℓ.*
- *Suppose that $\mathrm{End}_{\overline{K}}(E)$ is an order in the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. Then b_ℓ is zero whenever the following conditions all hold: $\ell \geqslant 3$ is a prime unramified both in K and in $\mathbb{Q}(\sqrt{-d})$, and E has good reduction at all places of K of characteristic ℓ.*

Both in the CM and non-CM cases, for the finitely many remaining primes ℓ we can take $b_\ell = 2n_\ell + 3v_\ell\left([\tilde{K} : K]\right)$, where $\tilde{K}$ is as in Definition 5.10 and n_ℓ is a parameter of maximal growth for the ℓ-adic torsion part.

Proof. Let n be the ℓ-adic valuation of N. By Proposition 5.13, the adelic failure $B_\ell(N)$ divides $[\tilde{K} : K] \cdot \#\dfrac{\tilde{V}_{\ell^n}}{[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]}$.

- Suppose that E does not have CM over $\overline{\mathbb{Q}}$, that α is ℓ-indivisible, that $\ell > 5$ is unramified in $K \mid \mathbb{Q}$, that the $\bmod \ell$ torsion representation is surjective, and that E has good reduction at all places of K of characteristic ℓ. Under these assumptions, the prime ℓ does not belong to the set S of Theorem 5.3, so we have $\tilde{K} = K$ and $[\tilde{K} : K] \cdot \#\dfrac{\tilde{V}_{\ell^n}}{[\tilde{V}_{\ell^n}, \tilde{H}_{\ell^n}]}$ is simply $\#\dfrac{V_{\ell^n}}{[V_{\ell^n}, H_{\ell^n}]}$. We conclude because this quotient is trivial by Lemma 5.15.
- In the CM case, the conclusion follows from Lemma 5.16 since $\ell \nmid [\tilde{K} : K] \leqslant 2$.

For all other primes, combining Proposition 5.13 and Proposition 5.14 we get that $B_\ell(N)$ divides $[\tilde{K} : K] \cdot \ell^{2\tilde{n}_\ell}$ and we conclude using Lemma 3.8. □

Remark 5.18. The proof shows that the inequality $v_\ell(B_\ell(N)) \leqslant 2n_\ell + 3v_\ell\left([\tilde{K} : K]\right)$ holds for every prime ℓ and for every rational point $\alpha \in E(K)$. In other words, for a fixed prime ℓ the adelic failure can be bounded independently of the rational point α.

We can finally prove our first Theorem from the introduction:

Proof of Theorem 1.1. By Remark 2.1, Theorem 1.1 follows from Theorems 4.15 and 5.17 by taking $C := \prod_\ell \ell^{a_\ell + b_\ell}$. □

Remark 5.19. Theorem 1.1 is completely effective, in the following sense: the quantities a_ℓ and b_ℓ can be computed in terms of $[\tilde{K} : K]$, n_ℓ, and the divisibility parameter d. The integer d can be bounded effectively in terms of the height of α and of standard invariants of the elliptic curve, as showed in Remark 4.14. The remaining quantities $[\tilde{K} : K]$ and n_ℓ can be bounded effectively in terms of $[K : \mathbb{Q}]$ and of the height of E, as shown in [14].

6. A COUNTEREXAMPLE IN THE CM CASE

We give an example showing that Proposition 4.12 does not hold in the CM case when ℓ is split in the field of complex multiplication, and that in fact in this case there can be no uniform lower bound on the image of the Kummer representation depending only on the image of the torsion representation, even when α is strongly ℓ-indivisible.

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication over $\overline{\mathbb{Q}}$ by the imaginary quadratic field F. Let $\alpha \in E(\mathbb{Q})$ be such that the ℓ^n-arboreal representation attached to (E, α) maps onto $(\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes N_{\ell^n}$ for every $n \geqslant 1$, where N_{ℓ^n} is the normaliser of a Cartan subgroup C_{ℓ^n} of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Suppose furthermore that ℓ is split in F and does not divide the conductor of the order $\mathrm{End}_{\overline{\mathbb{Q}}} E \subseteq \mathcal{O}_F$. Such triples (E, α, ℓ) exist: by [12, Example 5.11] we can take $E : y^2 = x^3 + 3x$ (which has CM by $\mathbb{Z}[i]$), $\alpha = (1, -2)$ and $\ell = 5$ (which splits in $\mathbb{Z}[i]$). Notice that for this elliptic curve and this α the same property holds for every $\ell \equiv 1 \pmod 4$: [15, Theorem 1.5 (2)] implies that for all $\ell \geqslant 5$ the image of the Galois representation is the full normaliser of a Cartan subgroup, at which point surjectivity of the Kummer representation follows from [12, Theorem 5.8].

Consider now the image of the arboreal representation associated with the triple $(E/F, \alpha, \ell)$. Base-changing E to F has the effect of replacing the normaliser of the Cartan subgroup with Cartan itself: more precisely we have $\omega_{\ell^n}\left(\mathrm{Gal}(F_{\ell^n, \ell^n} \mid F)\right) = (\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes C_{\ell^n}$ for every $n \geqslant 1$. As ℓ is split in the quadratic ring $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$, so is the Cartan subgroup C_{ℓ^n}, and therefore we can assume – choosing a different basis for $E[\ell^n]$ if necessary – that C_{ℓ^n} is the subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Fix now a large n and let

$$B_{\ell^n} = \left\{ (t, M) \in (\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes C_{\ell^n} : t \equiv (*, 0) \pmod{\ell^{n-1}} \right\}.$$

Using the explicit group law on $(\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes C_{\ell^n}$ one checks without difficulty that B_{ℓ^n} is a subgroup of $(\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes C_{\ell^n}$: indeed, given two elements $g_1 = (t_1, M_1)$ and $g_2 = (t_2, M_2)$ in B_{ℓ^n}, we have

$$g_1 \cdot g_2 = (t_1, M_1) \cdot (t_2, M_2) = (t_1 + M_1 t_2, M_1 M_2),$$

and (since M_1 is diagonal) the second coordinate of $t_1 + M_1 t_2$ is a linear combination (with $\mathbb{Z}/\ell^n\mathbb{Z}$-coefficients) of the second coordinates of t_1, t_2, hence is zero modulo ℓ^{n-1}. Finally, let $K \subset F_{\ell^n, \ell^n}$ be the field corresponding by Galois theory to the subgroup B_{ℓ^n} of $(\mathbb{Z}/\ell^n\mathbb{Z})^2 \rtimes C_{\ell^n} \cong \mathrm{Gal}(F_{\ell^n, \ell^n} \mid F)$.

We now study the situation of Proposition 4.12 for the elliptic curve E/K and the point α. By construction, the image of the ℓ^{n-1}-torsion representation attached to $(E/K, \ell)$ is $C_{\ell^{n-1}}$, so the parameter of maximal growth can be taken to be $n_\ell = 1$. We claim that $\alpha \in E(K)$ is strongly ℓ-indivisible. The modulo-ℓ torsion representation is surjective onto C_ℓ, so that in particular no ℓ-torsion point of E is defined over K, and strongly ℓ-indivisible is equivalent to ℓ-indivisible. To see that this last condition holds, notice that if α were ℓ-divisible then we would have $K_{\ell,\ell} = K_\ell$. However this is not the case, because by construction $\mathrm{Gal}(K_{\ell,\ell} \mid K_\ell) = \{t \in (\mathbb{Z}/\ell\mathbb{Z})^2 : t \equiv (*, 0) \pmod{\ell}\}$ has order ℓ. Finally, for $k = n - 3$ we have

$$V_{\ell^{k+2n_\ell}} = V_{\ell^{n-1}} = \{t \in (\mathbb{Z}/\ell^{n-1}\mathbb{Z})^2 : t \equiv (*, 0) \pmod{\ell^{n-1}}\},$$

which is very far from containing $E[\ell^k]$ – in fact, the index of $V_{\ell^{k+2n_\ell}}$ in $E[\ell^{k+2n_\ell}]$ can be made arbitrarily large by choosing larger and larger values of n. Notice that in any such example the ℓ-adic representation will be surjective onto a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

7. Uniform Bounds for the Adelic Kummer Representation

Our aim in this section is to show:

Theorem 7.1. *There is a positive integer C with the following property: for every elliptic curve $E/\mathbb{Q}$ and every strongly indivisible point $\alpha \in E(\mathbb{Q})$, the image $W_\infty \cong \mathrm{Gal}(K_{\infty,\infty} \mid K_\infty)$ of the Kummer map associated with $(E/\mathbb{Q}, \alpha)$ has index dividing C in $\prod_\ell T_\ell(E)$.*

This result immediately implies Theorem 1.2:

Proof of Theorem 1.2. By Remark 2.6, for every $N \mid M$ the ratio $\dfrac{N^2}{[\mathbb{Q}_{M,N} : \mathbb{Q}_M]}$ divides

$$\frac{N^2}{[\mathbb{Q}_{\infty,N} : \mathbb{Q}_\infty]} = \left[(\hat{\mathbb{Z}}/N\hat{\mathbb{Z}})^2 : W_\infty/NW_\infty\right],$$

which in turn divides $[\hat{\mathbb{Z}}^2 : W_\infty]$. □

As in Subsection 3.3, we will denote by $\mathcal{T}_0$ the finite set of primes

$$\mathcal{T}_0 := \{p \text{ prime } \mid p \leqslant 17\} \cup \{37\}.$$

7.1. **Bounds on Cohomology Groups.** Let $E/\mathbb{Q}$ be an elliptic curve and N_1, N_2 be positive integers with $N_1 \mid N_2$. The first step in the proof of Theorem 7.1 is to bound the exponent of the cohomology group $H^1(H_{N_2}, E[N_1])$. In the course of the proof we shall need the following technical result, which will be proved in Section 7.2.

Proposition 7.2. *There is a universal constant e satisfying the following property. Let $E/\mathbb{Q}$ be a non-CM elliptic curve, N a positive integer and ℓ a prime factor of N. Let ℓ^k be the largest power of ℓ dividing N and $J = \mathrm{Gal}(\mathbb{Q}_N \mid \mathbb{Q}_{\ell^k}) \triangleleft H_N$. Consider the action of H_N on $\mathrm{Hom}(J, E[\ell^k])$ defined by $(h\psi)(x) = h\psi(h^{-1}xh)$ for all $h \in H_N$, $\psi : J \to E[\ell^k]$ and $x \in J$. Then the exponent of $\mathrm{Hom}\left(J, E[\ell^k]\right)^{H_N}$ divides e.*

Proposition 7.3. *There is a positive integer C_1 with the following property. Let $E/\mathbb{Q}$ be an elliptic curve, N_1 and N_2 be positive integers with $N_1 \mid N_2$. Then the exponent of $H^1(H_{N_2}, E[N_1])$ divides C_1.*

Proof. We can prove the statement separately for CM and non-CM curves, and then conclude by taking the least common multiple of the two constants obtained in the two cases.

Assume first that $E/\mathbb{Q}$ has CM over $\overline{\mathbb{Q}}$. Let F be the CM field of E, $\mathcal{O}_F$ the ring of integers of F and $\mathcal{O}_\ell := \mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. By [15, Theorem 1.5] we have $d := \left[\prod_\ell \mathcal{O}_\ell^\times : H_\infty \cap \prod_\ell \mathcal{O}_\ell^\times\right] \leqslant 6$. In particular all the d-th powers of elements in $\prod_\ell \mathcal{O}_\ell^\times$ are in H_∞, hence we have $\hat{\mathbb{Z}}^{\times d} \subseteq H_\infty \subseteq \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$ and H_∞ contains the nontrivial homothety $\lambda = (\lambda_\ell)$, where $\lambda_2 = 3^d$ and $\lambda_\ell = 2^d$ for $\ell \neq 2$. By Sah's Lemma [3, Lemma A.2] we have $(\lambda - 1)H^1(H_{N_2}, E[N_1]) = 0$. Notice that the image of $\lambda - 1$ in $\mathbb{Z}_\ell$ is nonzero for all ℓ, and that it is invertible for almost all ℓ. The claim follows from the fact that d is bounded.

Assume now that E does not have complex multiplication over $\overline{\mathbb{Q}}$. As cohomology commutes with finite direct products we have

$$H^1(H_{N_2}, E[N_1]) \cong H^1\left(H_{N_2}, \bigoplus_{\ell^v \mid N_1} E[\ell^v]\right) \cong \bigoplus_{\ell^v \mid N_1} H^1\left(H_{N_2}, E[\ell^v]\right).$$

Fix an ℓ in this sum and let $J = \mathrm{Gal}(\mathbb{Q}_{N_2} \mid \mathbb{Q}_{\ell^k}) \triangleleft H_{N_2}$, where ℓ^k is the largest power of ℓ dividing N_2. By the inflation-restriction sequence we get

$$0 \to H^1(H_{N_2}/J, E[\ell^v]^J) \to H^1(H_{N_2}, E[\ell^v]) \to H^1(J, E[\ell^v])^{H_{N_2}};$$

since by definition J fixes $E[\ell^v]$, this is the same as

$$0 \to H^1(H_{\ell^k}, E[\ell^v]) \to H^1(H_{N_2}, E[\ell^v]) \to \mathrm{Hom}(J, E[\ell^v])^{H_{N_2}}.$$

It is clear that the exponent of $H^1(H_{N_2}, E[N_1])$ is the least common multiple of the exponents of the direct summands $H^1\left(H_{N_2}, E[\ell^v]\right)$ for $\ell \mid N_1$, so we can focus on one such summand at a time. Furthermore, the above inflation-restriction exact sequence shows that the exponent of $H^1(H_{N_2}, E[\ell^v])$ divides the product of the exponents of $H^1(H_{\ell^k}, E[\ell^v])$ and of $\mathrm{Hom}(J, E[\ell^v])^{H_{N_2}}$. It is enough to give a uniform bound for the exponents of these two cohomology groups.

- $\boxed{H^1(H_{\ell^k}, E[\ell^v])}$ Assume first that $\ell \notin \mathcal{T}_0$. By Theorem 3.12, H_ℓ is not contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, so by [13, Lemma 4] it contains a nontrivial homothety. By Lemma 3.15 the image H_{ℓ^∞} of the ℓ-adic representation contains a homothety that is non-trivial modulo ℓ, so by Sah's Lemma [3, Lemma A.2] we have $H^1(H_{\ell^k}, E[\ell^v]) = 0$. For $\ell \in \mathcal{T}_0$ let n_ℓ be a universal bound on the parameter of maximal growth of the ℓ-adic representation, as in Corollary 3.11. By Lemma 4.8 we have $(1 + \ell^{n_\ell})\,\mathrm{Id} \in H_{\ell^k}$, and from Lemma 4.6 we obtain that the exponent of $H^1(H_{\ell^k}, E[\ell^v])$ divides ℓ^{n_ℓ}.
- $\boxed{\mathrm{Hom}(J, E[\ell^v])^{H_{N_2}}}$ As $v \leqslant k$, this group is contained in $\mathrm{Hom}(J, E[\ell^k])^{H_{N_2}}$, whose exponent is uniformly bounded by Proposition 7.2. Notice that the action of H_{N_2} on $\mathrm{Hom}(J, E[\ell^k])$ is precisely the one considered in Proposition 7.2 by well-known

properties of the inflation-restriction exact sequence (see for example [24, Theorem 4.1.20]).

□

Corollary 7.4. *Let C_1 be as in Proposition 7.3. Let $E/\mathbb{Q}$ be an elliptic curve and let $\alpha \in E(\mathbb{Q})$ be a strongly indivisible point. If α is divisible by $n \geqslant 1$ over $\mathbb{Q}_\infty$, then $n \mid C_1$.*

Proof. Without loss of generality we can assume that $n = \ell^e$ is a power of a prime ℓ. Since $\mathbb{Q}_\infty$ is the union of the torsion fields $\mathbb{Q}_N$, there exists N such that α is divisible by ℓ^e over $\mathbb{Q}_N$, and we may assume that ℓ^e divides N. The claim then follows from Lemma 4.5, since by Proposition 7.3 the exponent of $H^1(\mathrm{Gal}(\mathbb{Q}_N \mid \mathbb{Q}), E[\ell^e])$ is a power of ℓ that divides C_1. □

Lemma 7.5. *Let C_1 be as in Proposition 7.3. The following hold for every prime ℓ:*

1. *The $\mathbb{Z}_\ell$-module W_{ℓ^∞}, considered as a submodule of $\mathbb{Z}_\ell^2$, contains a vector of valuation at most $v_\ell(C_1)$.*
2. *If E does not have CM over $\overline{\mathbb{Q}}$ and n_ℓ is a parameter of maximal growth for the ℓ-adic torsion representation, then W_{ℓ^∞} contains $\ell^{n_\ell + v_\ell(C_1)} T_\ell(E)$.*
3. *If $E[\ell]$ is an irreducible H_ℓ-module, then W_{ℓ^∞} contains $\ell^{v_\ell(C_1)} T_\ell(E)$.*
4. *If E has CM over $\overline{\mathbb{Q}}$, let (γ, δ) be parameters for the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$. If n_ℓ is a parameter of maximal growth for the ℓ-adic torsion representation, then W_{ℓ^∞} contains $\ell^{3n_\ell + v_\ell(4\delta C_1)} T_\ell(E)$.*

Proof. Part (1) follows from Lemma 4.10, since by Corollary 7.4 the point α is not divisible by $\ell^{v_\ell(C_1)+1}$ over $\mathbb{Q}_\infty$. Parts (2), (3) and (4) then follow from Proposition 4.11 (for part (4) observe that no elliptic curve over $\mathbb{Q}$ has CM defined over $\mathbb{Q}$). □

We can now prove the main Theorem of this section.

Proof of Theorem 7.1. As already explained, we have $W_\infty = \prod_\ell W_{\ell^\infty}$, so we obtain

$$\left[\prod_\ell T_\ell(E) : W_\infty\right] = \prod_\ell [T_\ell(E) : W_{\ell^\infty}].$$

Let

$$\mathcal{T}_1 = \mathcal{T}_0 \cup \{\ell \text{ prime} \mid \ell \text{ divides } C_1\} \cup \{19, 43, 67, 163\}.$$

Notice that by Theorem 3.12 for $\ell \notin \mathcal{T}_1$ there is no elliptic curve over $\mathbb{Q}$ with a rational subgroup of order ℓ. By Lemma 7.5 (3), for $\ell \notin \mathcal{T}_1$ we have $W_{\ell^\infty} = T_\ell(E)$, so

$$\left[\prod_\ell T_\ell(E) : W_\infty\right] = \prod_{\ell \in \mathcal{T}_1} [T_\ell(E) : W_{\ell^\infty}]. \tag{2}$$

Now it is enough to prove the Theorem separately in the CM and in the non-CM case, and then take the least common multiple of the two constants obtained.

Suppose first that E does not have CM over $\overline{\mathbb{Q}}$. Applying Lemma 7.5(2) we see that $[T_\ell(E) : W_{\ell^\infty}]$ divides $\ell^{2(n_\ell + v_\ell(C_1))}$, where n_ℓ is a parameter of maximal growth for the ℓ-adic torsion

for E. By Theorem 3.9 this can be bounded uniformly in E. Since C_1 does not depend on E, each factor of the right hand side of (2) is uniformly bounded.

Assume now that E has complex multiplication over $\overline{\mathbb{Q}}$ and let (γ, δ) be parameters for the Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ corresponding to $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$. Applying Lemma 7.5(4), we see that $[T_\ell(E) : W_{\ell^\infty}]$ divides $\ell^{2(3n_\ell + v_\ell(4\delta C_1))}$, where n_ℓ is a parameter of maximal growth for the ℓ-adic torsion representation for E, which is uniformly bounded by Corollary 3.11. It remains to show that $v_\ell(\delta)$ can be bounded uniformly as well. This follows from the fact that δ only depends on the $\overline{\mathbb{Q}}$-isomorphism class of E, and that there are only finitely many rational j-invariants corresponding to CM elliptic curves. □

7.2. **Proof of Proposition 7.2.** Recall the setting of Proposition 7.2: $E/\mathbb{Q}$ is a non-CM elliptic curve, N is a positive integer, and ℓ is a prime factor of N. Let ℓ^k be the largest power of ℓ dividing N and $J = \mathrm{Gal}(\mathbb{Q}_N \mid \mathbb{Q}_{\ell^k}) \triangleleft H_N$. The question is to study the exponent of the group $\mathrm{Hom}\left(J, E[\ell^k]\right)^{H_N}$. In order to do this, we shall study the conjugation action of $g \in H_N$ on the abelianisation of J. More generally, we shall also consider the conjugation action of elements in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that normalise J.

It will be useful to work with a certain subgroup $J(2)$ of J. More generally, we introduce the following notation.

Definition 7.6. Let G be a group and M a positive integer. We denote by $G(M)$ the subgroup of G generated by $\left\{g^M \mid g \in G\right\}$.

Lemma 7.7. *The subgroup $J(2)$ is normal in J, the quotient group $J/J(2)$ has exponent at most 2, $J(2)$ is stable under the conjugation action of H_N, and*

$$\exp \mathrm{Hom}\left(J, E[\ell^k]\right)^{H_N} \mid 2 \exp \mathrm{Hom}\left(J(2), E[\ell^k]\right)^{H_N}.$$

Proof. Clearly $J(2)$ is a characteristic subgroup of J, so it is normal in J and stable under the conjugation action of H_N on J. Given a coset $hJ(2) \in J/J(2)$ we have $(hJ(2))^2 = h^2 J(2) = J(2)$ since $h^2 \in J(2)$ by definition, so the quotient $J/J(2)$ is killed by 2. Finally, take a homomorphism $\psi : J \to E[\ell^k]$ stable under the conjugation action of H_N and denote by d the exponent of the abelian group $\mathrm{Hom}\left(J(2), E[\ell^k]\right)^{H_N}$. The restriction of ψ to $J(2)$ is an element of $\mathrm{Hom}\left(J(2), E[\ell^k]\right)^{H_N}$, so it satisfies $d\psi|_{J(2)} = 0$, and thus given any $h \in J$ we have $d\psi|_{J(2)}(h^2) = 0$. This implies that for every $h \in J$ we have $2d\psi(h) = 0$, hence ψ is killed by $2d$. Since this is true for all ψ, the claim follows. □

We will also need the following two simple lemmas:

Lemma 7.8. *Let $E/\mathbb{Q}$ be an elliptic curve and let $M \geqslant 37$ be an integer. If $\ell > M + 1$ is a prime number, then $H_{\ell^\infty}(M)$ contains a homothety $\lambda \,\mathrm{Id}$ with $\lambda \not\equiv 1 \pmod{\ell}$.*

Proof. By Corollary 3.14, since $\ell > M + 1 > 37$, the image of the modulo-ℓ representation contains all the homotheties. In particular, if $\overline{\mu} \in \mathbb{F}_\ell^\times$ is a generator of the multiplicative group $\mathbb{F}_\ell^\times$, then H_ℓ contains $\overline{\mu}\,\mathrm{Id}$, so by Lemma 3.15 H_{ℓ^∞} contains $\mu\,\mathrm{Id}$, where $\mu \in \mathbb{Z}_\ell^\times$ is congruent

to $\overline{\mu}$ modulo ℓ. So $H_{\ell^\infty}(M)$ contains $\mu^M \operatorname{Id}$, which is nontrivial modulo ℓ since $\overline{\mu}$ has order $\ell - 1 > M$. □

Lemma 7.9. *Let p be a prime and let n be a positive integer (with $n \geqslant 2$ if $p = 2$). For every positive integer k let $U_k = \left\{x \in \mathbb{Z}_p \mid x \equiv 1 \pmod{p^k}\right\}$. Let M be a positive integer. Then $\left\{x^M \mid x \in U_n\right\} \supseteq U_{n+v_p(M)}$.*

Proof. Let $y \in U_{n+v_p(M)}$ and let $a = y - 1$. By [7, Corollary 4.2.17 and Corollary 4.2.18(1)], the p-adic integer $x = \exp(M^{-1} \log y)$ is well defined and satisfies $v_p(x-1) \geqslant v_p(M^{-1}a) \geqslant n$. Therefore $x \in U_n$ and clearly $x^M = y$. □

We will derive Proposition 7.2 from the following statement:

Proposition 7.10. *There is a universal constant M with the following property. For every elliptic curve $E/\mathbb{Q}$, every positive integer N, every prime power ℓ^k dividing N, and every $g \in H_N$, the conjugation action of g^M on the abelianisation of $J(2)$ is trivial.*

Proof that Proposition 7.10 implies Proposition 7.2. By Lemma 7.7 it suffices to prove Proposition 7.2 with J replaced by $J(2)$. Let $\psi \in \operatorname{Hom}\left(J(2), E[\ell^k]\right)$: then as $E[\ell^k]$ is abelian ψ factors through $J(2)^{\mathrm{ab}}$.

For every $g \in H_N$, every $\psi \in \operatorname{Hom}\left(J(2), E[\ell^k]\right)^{H_N}$ and every $h \in J(2)$ we have

$$\psi(h) = g^M \cdot \psi(g^{-M} h g^M) = g^M \cdot \psi(h),$$

where the first equality holds because ψ is H_N-invariant and the second because the automorphism induced by g^M on $J(2)^{\mathrm{ab}}$ is trivial by Proposition 7.10. This means that the image of ψ is contained in $E[\ell^k]^{H_N(M)}$. Since the action of H_N on $E[\ell^k]$ factors via the canonical projection $H_N \to \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$, this is the same as saying that the image of ψ is contained in the subgroup of $E[\ell^k]$ fixed under $H_{\ell^k}(M)$. It remains to show that the exponent of $E[\ell^k]^{H_{\ell^k}(M)}$ is uniformly bounded, and trivial for ℓ sufficiently large.

To see this, recall that by Theorem 3.9 there exists an integer $n \geqslant 1$, independent of E, such that H_{ℓ^k} contains $\operatorname{Id} + \ell^n \operatorname{Mat}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ (and we have $n \geqslant 2$ if $\ell = 2$). By Lemma 7.9, for every $E/\mathbb{Q}$ the group $H_{\ell^k}(M)$ contains all scalar matrices in $\operatorname{Mat}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ that are congruent to the identity modulo $\ell^{n+v_\ell(M)}$. We claim that the exponent of $E[\ell^k]^{H_{\ell^k}(M)}$ divides $\ell^{n+v_\ell(M)}$. In fact, by what we have seen $H_{\ell^k}(M)$ contains $(1+\ell^{n+v_\ell(M)})\operatorname{Id}$, so $E[\ell^k]^{H_{\ell^k}(M)}$ is in particular fixed by $(1 + \ell^{n+v_\ell(M)})\operatorname{Id}$, hence it is contained $E[\ell^{n+v_\ell(M)}]$.

Finally, we show that $\operatorname{Hom}(J, E[\ell^k])^{H_N}$ is trivial for $\ell > M + 1$. Since $\ell > 2$, by Lemma 7.7 it is enough to show that $\operatorname{Hom}(J(2), E[\ell^k])^{H_N}$ is trivial. As above, the image of any H_N-stable homomorphism from $J(2)$ to $E[\ell^k]$ is contained in the $H_{\ell^k}(M)$-fixed points of $E[\ell^k]$. By Lemma 7.8, $H_{\ell^k}(M)$ contains a homothety which is nontrivial modulo ℓ, so we are done since the only fixed point of this homothety is 0. □

We now turn to the proof of Proposition 7.10. We start by showing that we may assume N to be of the form $\ell^k \cdot \prod_{p|N, p\neq\ell} p$. To see this, let $N = \ell^k \prod_{p|N,p\neq\ell} p^{e_p}$ be arbitrary and let $N' := \ell^k \prod_{p|N,p\neq\ell} p$. There is an obvious reduction map $J \to \mathrm{Gal}(\mathbb{Q}_{N'} \mid \mathbb{Q}_{\ell^k})$. The kernel

$\mathcal{K}$ of this map is a subgroup of J whose order is divisible only by primes $p \mid N, p \neq \ell$. Recall that we will be considering $\mathrm{Hom}(J, E[\ell^k])^{H_N}$. Let $\psi : J \to E[\ell^k]$ be a homomorphism: we claim that ψ factors via the quotient $\mathrm{Gal}(\mathbb{Q}_{N'} \mid \mathbb{Q}_{\ell^k})$. Indeed, all the elements in $\mathcal{K}$ have order prime to ℓ, hence they must go to zero in $E[\ell^k]$. Therefore we may assume $N = N'$, that is, $N = \ell^k \cdot \prod_{p|N, p\neq\ell} p$.

We identify H_N with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z}) \times \prod_{p|N,p\neq\ell} \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and J with the subgroup of H_N consisting of elements having trivial first coordinate, and for $g \in H_N$ we write $g = (g_\ell, g_{p_1}, \ldots, g_{p_r})$ with $g_\ell \in \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ and $g_{p_i} \in \mathrm{GL}_2(\mathbb{Z}/p_i\mathbb{Z})$. Finally, for $p \mid N$, $p \neq \ell$ we denote by $\pi_{p_i} : H_N \to \mathrm{GL}_2(\mathbb{Z}/p_i\mathbb{Z})$ the projection on the factor corresponding to p_i, and we denote by $\pi_\ell : H_N \to \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ the projection on the factor corresponding to ℓ.

Lemma 7.11. *Let p be a prime factor of N with $p \geqslant 7$, $p \neq \ell$. Suppose that the modulo-p representation attached to $E/\mathbb{Q}$ is surjective. Then $J(2)$ contains $\{1\} \times \cdots \times \{1\} \times \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \times \{1\} \times \cdots \times \{1\}$.*

Proof. Clearly $\mathrm{PSL}_2(\mathbb{F}_p)$ occurs in H_N. Hence it must occur either in J or in H_N/J, but the latter is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ with $\ell \neq p$, so it must occur in J. Consider the kernel of the projection $J \to \prod_{q|N,q\neq p} \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$: then $\mathrm{PSL}_2(\mathbb{F}_p)$ must occur either in this kernel or in $\prod_{q|N,q\neq p} \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$, but the latter case is impossible. Using Lemma 5.1, it follows immediately that J contains $\{1\} \times \cdots \times \{1\} \times \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \times \{1\} \times \cdots \times \{1\}$. We conclude by noting that $\mathrm{SL}_2(\mathbb{F}_p)$ is generated by its squares. □

Lemma 7.12. *Let $g \in H_N$ and $h \in J(2)$. Then $gh \in H_N$, and the automorphisms of $J(2)^{\mathrm{ab}}$ induced by g and by gh coincide.*

Proof. As $J(2)$ is a subgroup of H_N, the fact that $gh \in H_N$ is obvious. For the second statement, notice that for every $x \in J(2)$ the element $(gh)^{-1}x(gh)$ differs from $g^{-1}xg$ by multiplication by $h^{-1}(g^{-1}x^{-1}g)^{-1}h(g^{-1}x^{-1}g)$, which is a commutator in $J(2)$. Hence the classes of $(gh)^{-1}x(gh)$ and $g^{-1}xg$ are equal in $J(2)^{\mathrm{ab}}$. □

Lemma 7.13. *For each $p \mid N, p \neq \ell$, the component g_p of g along $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ normalises $\pi_p(J(2))$ in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.*

Proof. Since H_N normalises $J(2)$ by Lemma 7.7, we have $\pi_p(g^{-1}J(2)g) = \pi_p(J(2))$. On the other hand $\pi_p(g^{-1}J(2)g) = \pi_p(g)^{-1}\pi_p(J(2))\pi_p(g)$, so $g_p^{-1}\pi_p(J(2))g_p = \pi_p(J(2))$ as desired. □

Corollary 7.14. *Let $p_1, \ldots, p_s \geqslant 7$ be primes all different from ℓ and such that the mod-p_i representation attached to $E/\mathbb{Q}$ is surjective for each p_i. Let $g \in H_N$ and let $\hat{g}$ be the element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by replacing every p_i-component (for $i = 1, \ldots, s$) of g by Id. Then $\hat{g}^2$ normalises $J(2)$, and it induces on $J(2)^{\mathrm{ab}}$ the same conjugation action as g^2.*

Proof. By Lemma 7.12, if we multiply g^2 by any element of $J(2)$ the conjugation action on $J(2)^{\mathrm{ab}}$ does not change. By construction, the determinant of $\pi_{p_i}(g^2) = g_{p_i}^2$ is a square in $\mathbb{F}_{p_i}^\times$, say λ_i^2. It follows that the determinant of $g_{p_i}^2/\lambda_i$ is 1, so $g_{p_i}^2/\lambda_i \in \mathrm{SL}_2(\mathbb{Z}/p_i\mathbb{Z})$. By Lemma

7.11 we have that $J(2)$ contains $h_i = (1, 1, \dots, 1, g_{p_i}^2/\lambda_i, 1, \dots, 1)$. Letting $h = h_1 \cdots h_s$, we obtain that the action of $g^2 h^{-1}$ is the same as that of g^2. But the element

$$\mu = (1, \dots, 1, \lambda_1, 1, \dots, 1) \cdots (1, \dots, 1, \lambda_s, 1, \dots, 1)$$

is central in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, so $\hat{g}^2 = g^2 h^{-1} \mu^{-1}$ normalises $J(2)$ and it induces the same action as g^2 on $J(2)^{\mathrm{ab}}$. □

Let $M = \mathrm{lcm}\{\exp \mathrm{PGL}_2(\mathbb{F}_p) : p \in \mathcal{T}_0\}$, where $\exp \mathrm{PGL}_2(\mathbb{F}_p)$ denotes the exponent of the group $\mathrm{PGL}_2(\mathbb{F}_p)$.

Remark 7.15. Notice that M is even. Moreover, for any $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and any $p \in \mathcal{T}_0$ with $p \mid N$ and $p \neq \ell$ we have that $\pi_p(g^M)$ is a scalar in $\mathrm{GL}_2(\mathbb{F}_p)$, since it is trivial in $\mathrm{PGL}_2(\mathbb{F}_p)$.

We now prove Proposition 7.10, using the constant M just introduced.

Proof of Proposition 7.10. Write as before $g = (g_p)$. We divide the prime factors of N different from ℓ into three sets as follows:

$$\begin{aligned}
\mathcal{P}_0 &= \{p \mid N \text{ such that } p \in \mathcal{T}_0,\, p \neq \ell\}\,, \\
\mathcal{P}_1 &= \{p \mid N \text{ such that } H_p = \mathrm{GL}_2(\mathbb{F}_p),\, p \neq \ell\}\,, \\
\mathcal{P}_2 &= \{p \mid N \text{ such that } H_p \text{ is conjugate to a subgroup of } N_{\mathrm{ns}}(p),\, p \neq \ell\}\,.
\end{aligned}$$

Notice that by Theorem 3.13 each prime factor of N different from ℓ belongs to one of these three sets.

We now apply Corollary 7.14 with $\{p_1, \dots, p_s\} = \mathcal{P}_1$ to obtain an element $\hat{g} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\pi_p(\hat{g}) = \mathrm{Id}$ for every $p \in \mathcal{P}_1$ and such that $\hat{g}^2$ induces on $J(2)^{\mathrm{ab}}$ the same conjugation action as g^2. In particular, $\hat{g}^M$ induces on $J(2)^{\mathrm{ab}}$ the same conjugation as g^M (recall that M is even).

We now prove that this conjugation action is trivial by showing that $\hat{g}^M$ commutes with every element of $J(2)$. It suffices to show that for each $p \mid N$ the projection $\pi_p(\hat{g}^M)$ commutes with every element of $\pi_p(J(2))$.

- *Case $p \in \mathcal{P}_0$:* by Remark 7.15, $\pi_p(\hat{g}^M)$ is a scalar, thus it commutes with all of $\mathrm{GL}_2(\mathbb{F}_p)$.
- *Case $p \in \mathcal{P}_1$:* by construction $\pi_p(\hat{g}^M)$ is trivial.
- *Case $p \in \mathcal{P}_2$:* by Corollary 3.14 applied to $\pi_p(\hat{g})$, there is $h \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $\pi_p(\hat{g}) \in h N_{\mathrm{ns}}(p) h^{-1}$ and $H_p \subseteq h N_{\mathrm{ns}}(p) h^{-1}$. Since M is even and $C_{\mathrm{ns}}(p)$ has index 2 in $N_{\mathrm{ns}}(p)$, $\pi_p(\hat{g}^M) \in h C_{\mathrm{ns}}(p) h^{-1}$ and $\pi_p(J(2)) \subseteq \langle a^2 \mid a \in H_p \rangle \subseteq h C_{\mathrm{ns}}(p) h^{-1}$. Since $C_{\mathrm{ns}}(p)$ is abelian, $\pi_p(\hat{g}^M)$ commutes with every element of $\pi_p(J(2))$.
- *Case $p = \ell$:* by construction $\pi_p(J(2))$ is trivial.

□

REFERENCES

[1] ACHTER, J. D. Detecting complex multiplication. In *Computational aspects of algebraic curves*, vol. 13 of *Lecture Notes Ser. Comput.* World Sci. Publ., Hackensack, NJ, 2005, pp. 38–50.

[2] ARAI, K. On uniform lower bound of the Galois images associated to elliptic curves. *J. Théor. Nombres Bordeaux 20*, 1 (2008), 23–43.

[3] BAKER, M. H., AND RIBET, K. A. Galois theory and torsion points on curves. *J. Théor. Nombres Bordeaux 15*, 1 (2003), 11–32. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[4] BERTRAND, D. Galois representations and transcendental numbers. In *New advances in transcendence theory (Durham, 1986)*. Cambridge Univ. Press, Cambridge, 1988, pp. 37–55.

[5] BRUIN, P., AND PERUCCA, A. Reductions of points on algebraic groups, II. *arXiv e-prints* (Feb 2018), arXiv:1802.08527.

[6] CAMPAGNA, F. Cyclic reduction of elliptic curves. Master's thesis, Algant - Universiteit Leiden. Supervised by prof. Peter Stevenhagen.

[7] COHEN, H. *Number theory. Vol. I. Tools and Diophantine equations*, vol. 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[8] COSTA, E., MASCOT, N., SIJSLING, J., AND VOIGHT, J. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp. 88*, 317 (2019), 1303–1339.

[9] DEURING, M. Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. Math.-Phys.-Chem. Abt. 1953* (1953), 85–94.

[10] DEURING, M. *Die Klassenkörper der komplexen Multiplikation*, vol. 23 of *Enzyklopädie der mathematischen Wissenschaften: Mit Einschluss ihrer Anwendungen, Band I 2, Heft 10, Teil II (Article I 2*. B. G. Teubner Verlagsgesellschaft, Stuttgart, 1958.

[11] HINDRY, M. Autour d'une conjecture de Serge Lang. *Invent. Math. 94*, 3 (1988), 575–603.

[12] JONES, R., AND ROUSE, J. Galois theory of iterated endomorphisms. *Proc. Lond. Math. Soc. (3) 100*, 3 (2010), 763–794. Appendix A by Jeffrey D. Achter.

[13] LAWSON, T., AND WUTHRICH, C. Vanishing of some Galois cohomology groups for elliptic curves. In *Elliptic curves, modular forms and Iwasawa theory*, vol. 188 of *Springer Proc. Math. Stat.* Springer, Cham, 2016, pp. 373–399.

[14] LOMBARDO, D. Bounds for Serre's open image theorem for elliptic curves over number fields. *Algebra Number Theory 9*, 10 (2015), 2347–2395.

[15] LOMBARDO, D. Galois representations attached to abelian varieties of CM type. *Bull. Soc. Math. France 145*, 3 (2017), 469–501.

[16] LOMBARDO, D. Computing the geometric endomorphism ring of a genus-2 Jacobian. *Math. Comp. 88*, 316 (2019), 889–929.

[17] LOMBARDO, D., AND PERUCCA, A. Reductions of points on algebraic groups. *arXiv e-prints* (Dec 2016), arXiv:1612.02847.

[18] LOMBARDO, D., AND PERUCCA, A. The 1-eigenspace for matrices in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. *New York J. Math. 23* (2017), 897–925.

[19] LOZANO-ROBLEDO, Á. Galois representations attached to elliptic curves with complex multiplication. *arXiv e-prints* (Sep 2018), arXiv:1809.02584.

[20] MAZUR, B. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math. 44*, 2 (1978), 129–162.

[21] NEUKIRCH, J., SCHMIDT, A., AND WINGBERG, K. *Cohomology of number fields*, second ed., vol. 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2008.

[22] PETSCHE, C. Small rational points on elliptic curves over number fields. *New York J. Math. 12* (2006), 257–268.

[23] RIBET, K. A. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J. 46*, 4 (1979), 745–761.

[24] ROSENBERG, J. *Algebraic K-theory and its applications*, vol. 147 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[25] ROUSE, J., AND ZUREICK-BROWN, D. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Res. Number Theory 1* (2015), Art. 12, 34.

[26] SAH, C.-H. Automorphisms of finite groups. *J. Algebra 10* (1968), 47–68.
[27] SERRE, J.-P. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math. 15*, 4 (1972), 259–331.
[28] SERRE, J.-P. *Local fields*, vol. 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.
[29] SERRE, J.-P. *Abelian l-adic representations and elliptic curves*, vol. 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.
[30] SILVERMAN, J. H. *Advanced topics in the arithmetic of elliptic curves*, vol. 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.
[31] SILVERMAN, J. H. *The arithmetic of elliptic curves*, second ed., vol. 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2009.
[32] THE LMFDB COLLABORATION. The l-functions and modular forms database. `http://www.lmfdb.org`, 2019. [Online; accessed 11 June 2019].
[33] THE PARI GROUP. *PARI/GP version* `2.12.0 (development 23147-6f9379e35)`. Univ. Bordeaux, 2019. Available from `http://pari.math.u-bordeaux.fr/`.
[34] THE SAGE DEVELOPERS. *SageMath, the Sage Mathematics Software System (Version 8.3)*, 2018. `https://www.sagemath.org`.
[35] YELTON, J. Dyadic torsion of elliptic curves. *Eur. J. Math. 1*, 4 (2015), 704–716.
[36] ZYWINA, D. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. Preprint. Available at `http://pi.math.cornell.edu/~zywina/papers/PossibleImages/PossibleImages.pdf`.
[37] ZYWINA, D. On the surjectivity of mod ℓ representations associated to elliptic curves. Preprint. Available at `http://pi.math.cornell.edu/~zywina/papers/EffectiveModl.pdf`.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI PISA, LARGO BRUNO PONTECORVO 5, 56127 PISA, ITALY

Email address: `davide.lombardo@unipi.it`

MATHEMATICS RESEARCH UNIT, UNIVERSITY OF LUXEMBOURG, 6 AV. DE LA FONTE, 4364 ESCH-SUR-ALZETTE, LUXEMBOURG

Email address: `sebastiano.tronto@uni.lu`