On the vanishing of almost all primary components of the Shafarevich-Tate group of elliptic curves over the rationals

François Destrempes  Dmitry Malinin
fdestrempes@bell.net  dmalinin@gmail.com

July 16, 2018

Abstract
The Shafarevich-Tate and Selmer groups arise in the context of Kummer theory for elliptic curves. The finiteness of the Shafarevich-Tate group of an elliptic curve $E$ over the field of rational numbers is included in the Birch and Swinnerton-Dyer conjectures, and is still an open question.

We present an overview of the Shafarevich-Tate and Selmer groups of an elliptic curve in the framework of Galois cohomology. Known results on the finiteness of the Shafarevich-Tate group are mentioned, including results of Coates and Wiles, Rubin, Gross and Zagier, and Kolyvagin.

We then prove the vanishing of the $\ell$-primary component of the Shafarevich-Tate group for almost all primes $\ell$, for any elliptic curve $E$ over the rationals without complex multiplication.

1 Introduction

1.1 Statement of the problem
We recall Kummer theory for elliptic curves [43 pp. 331–332] to introduce the Shafarevich-Tate groups and the related Selmer groups.

Let $K$ be an algebraic number field with absolute Galois group $G = \text{Gal}(\overline{K}/K)$, where $\overline{K}$ denotes the algebraic closure of $K$. Given an elliptic curve $E$ over $K$ and a prime number $\ell$, one has the short exact sequence (isogeny property) of $G$-modules:

$$0 \to E[\ell] \to E(\overline{K}) \xrightarrow{\ell} E(\overline{K}) \to 0,$$

where $E[\ell]$ denotes the group of $\ell$-torsion points in $E(\overline{K})$. This yields, from the long exact sequence of Galois cohomology, the following exact sequence of Abelian groups:

$$0 \to E(K)/[\ell](E(K)) \xrightarrow{\partial} H^1(G, E[\ell]) \to H^1(G, E(\overline{K}))[\ell] \to 0.$$
Recall that Galois cohomology (see [11] and [43, pp. 333-335]) is based on the profinite group structure of Galois groups (see [11] and [26, pp. 4-6]). In particular, 1-cocycles are continuous maps with respect to the Krull topology on Galois groups [26, p. 2] and the discrete topology on Galois modules. When the Galois group is finite, Galois cohomology coincides with group cohomology.

Given a place $v$ of $K$, let $K_v$ be the completion of $K$ at $v$, and denote $G_v$ the absolute Galois group of $K_v$. Then, $G_v$ may be viewed as a subgroup of $G$ upon considering an embedding $\xi$ of $K$ into $K_v$. Moreover, the resulting embedding is continuous with respect to the Krull topology on Galois groups. One then has a commutative diagram:

\[
\begin{array}{cccc}
0 & \longrightarrow & E(K)/[\ell](E(K)) & \longrightarrow & H^1(G, E[\ell]) & \longrightarrow & H^1(G, E(K))/[\ell] & \longrightarrow & 0 \\
0 & \longrightarrow & E(K_v)/[\ell](E(K_v)) & \longrightarrow & H^1(G_v, E[\ell]) & \longrightarrow & H^1(G_v, E(K_v))/[\ell] & \longrightarrow & 0,
\end{array}
\]

where $\text{Res}_{G_v}^G$ denotes the restriction map of Galois cohomology [43, pp. 331–332]. At this point, recall that the Shafarevich-Tate group of $E$ over $K$ is defined as [43, p. 332]:

\[
\text{III}(E/K) = \text{Ker}\left\{H^1(G, E(\overline{K})) \rightarrow \bigoplus_v H^1(G_v, E(\overline{K}_v))\right\}.
\]

Also, the $[\ell]$-Selmer group is defined as [43, pp. 331–334]:

\[
S^{[\ell]}(E/K) = \text{Ker}\left\{H^1(G, E[\ell]) \rightarrow \bigoplus_v H^1(G_v, E(\overline{K}_v))\right\}.
\]

In both equations (11) and (12), $v$ covers the set at all places of $K$. Note that each homomorphism $H^1(G, E[\ell]) \rightarrow H^1(G_v, E(\overline{K}_v))$ maps into the $\ell$-torsion group $H^1(G_v, E(\overline{K}_v))/[\ell]$. The above commutative diagram then yields a short exact sequence of the form [43, p. 333]:

\[
0 \rightarrow E(K)/[\ell](E(K)) \xrightarrow{\partial} S^{[\ell]}(E/K) \rightarrow \text{III}(E/K)/[\ell] \rightarrow 0.
\]

One can show that the Selmer group $S^{[\ell]}(E/K)$ is finite [43, pp. 333–334], from which follows the finiteness of $E(K)/[\ell](E(K))$ (Weak Mordell-Weil Theorem). A descent argument based on the notion of height function then shows the following result [43, Theorem 6.7, p. 239].

**Theorem 1** (Mordell-Weil Theorem). For any elliptic curve over an algebraic number field $K$, the group $E(K)$ is finitely generated.

From the Mordell-Weil Theorem, one can define the rank of an elliptic curve:

\[
\text{rank}(E/K) = \text{rank}_\mathbb{Z} E(K).
\]

Given a prime number $\ell$, the Mordell-Weil Theorem implies that:

\[
\text{dim}_{\mathbb{F}_\ell} E(K)/[\ell](E(K)) = \text{rank}(E/K) + \text{dim}_{\mathbb{F}_\ell} E[\ell](K),
\]

(8)
where $E[\ell](K)$ is the group of $\ell$-torsion points of $E(K)$. Considering the special case where $K = \mathbb{Q}$, a Theorem of Mazur implies that $\#E_{\text{tor}}(\mathbb{Q}) \leq 16$ [43 Theorem 7.5, p. 242], so that $\text{dim}_{K_\ell} E[\ell](\mathbb{Q}) = 0$ for almost all prime numbers $\ell$. Then, $\text{rank}(E/\mathbb{Q}) = \text{dim}_{K_\ell} E(\mathbb{Q})/\ell(E(\mathbb{Q}))$.

Next, we recall the following results on the $L$-series attached to elliptic curves. Given an elliptic curve $E$ over a global field $K$, one defines the auxiliary function [43, p. 450]:

$$
\Lambda(E,s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s),
$$

(9)

where $N_E$ denotes the conductor of $E/K$, $\Gamma$ denotes the Euler gamma function, and $L(E,s)$ is the $L$-series attached to $E$ [43 pp. 449–452].

A construction of Eichler and Shimura associates to special functions, called modular forms [43 Section C.12], a type of elliptic curves, called modular elliptic curves [43 Section C.13], for which analytic continuation of the auxiliary function $\Lambda(E,s)$ to the entire complex plane can be demonstrated [43 Section C.16]. See [25] for a brief introduction.

Now, the Taniyama-Shimura-Weil conjecture states that any elliptic curve over $\mathbb{Q}$ is modular. This conjecture was proved in 1995 for semi-stable elliptic curves over $\mathbb{Q}$ [51, 48] and then, the proof was extended to cover all elliptic curves over $\mathbb{Q}$ [3]. From there, one can conclude that $L(E,s)$ has an analytic continuation on the entire complex plane.

**Theorem 2** (Wiles 1995, Taylor and Wiles 1995, Breuil et al. 2001). **Modularity Theorem:** Any elliptic curve $E$ over $\mathbb{Q}$ is modular.

Based on Theorem 2 one can define the analytic rank of an elliptic curve over $\mathbb{Q}$:

$$
\text{rank}_{an}(E/\mathbb{Q}) = \text{ord}_{s=1} L(E,s).
$$

(10)

The Birch and Swinnerton-Dyer conjectures include the following statement [43 Conjecture 16.5, part a), p. 452]:

**BSD-1:** $\text{rank}(E/\mathbb{Q}) = \text{rank}_{an}(E/\mathbb{Q})$, for any elliptic curve $E$ over $\mathbb{Q}$.

The Birch and Swinnerton-Dyer conjectures assume also the following conjecture [43 p. 341] formulated independently by Shafarevich and Tate [33]:

**S-T:** the Shafarevich-Tate group $\text{III}(E/\mathbb{Q})$ is finite, for any elliptic curve $E$ over $\mathbb{Q}$.

From S-T, one would have:

$$
\text{rank}(E/\mathbb{Q}) = \text{dim}_{\mathbb{Q}_\ell} E(\mathbb{Q})/\ell(E(\mathbb{Q})) = \text{dim}_{\mathbb{Q}_\ell} S^{[\ell]}(E/\mathbb{Q}),
$$

(11)

for all but finitely many prime numbers $\ell$, based on Mazur’s Theorem on torsion points.

Conjecture S-T is assumed in the second part of the BSD conjectures (BSD-2) on the value of the leading coefficient in the Taylor expansion of $L(E,s)$ at $s = 1$. See [43 Conjecture 16.5, part b), p. 452].
A result of Coates and Wiles [7] states that BSD-1 holds in the case of an elliptic curve over \( \mathbb{Q} \) with complex multiplication (CM), if the analytic rank is equal to 0. Rubin [31] proved that conjecture S-T holds under the same conditions.

**Theorem 3** (Coates and Wiles 1977, Rubin 1987). *Let \( E \) be an elliptic curve over \( \mathbb{Q} \) with CM. Assume that\( \text{rank}_{\text{an}}(E/\mathbb{Q}) = 0 \). Then, conjectures BSD-1 and S-T hold.*

Kolyvagin extended Rubin’s result to any elliptic curve of analytic rank at most 1 [14, 15, 17], building on a result of Gross and Zagier [10]; see also [16, Theorem 1, p. 430].

**Theorem 4** (Gross and Zagier 1986, Kolyvagin 1988–1991). *Let \( E \) be an elliptic curve over \( \mathbb{Q} \). Assume that\( \text{rank}_{\text{an}}(E/\mathbb{Q}) \leq 1 \). Then, conjectures BSD-1 and S-T hold.*

The reader may consult [32] and [33] for further reading on the Birch and Swinnerton-Dyer conjectures and the rank of elliptic curves. In particular, the notions of Heegner points and Euler systems are explained. In this work, these notions do not intervene.

Results on the finiteness of the Shafarevich-Tate group have been obtained by Kolyvagin and Logachev in the case of Abelian varieties [18, 19].

The finiteness of \( \Sha(E/\mathbb{Q}) \) implies that its order is a perfect square, based on Cassels’ pairing for elliptic curves [43, p. 341]. Poonen and Stoll have studied the Cassels-Tate pairing in the case of Abelian varieties [29].

### 1.2 Main theorem of this work and consequences

Firstly, as mentioned in [28, Section 3], the Shafarevich-Tate group is a torsion group, for the simple reason that it is a subgroup of the torsion group \( H^1(G,E(\overline{\mathbb{K}})) \), having considered Galois cohomology.

The following proposition states equivalent formulations.

**Proposition 1.** *Let \( E \) be an elliptic curve over an algebraic number field \( K \). Let \( \ell \) be a prime number. Then, the following conditions are equivalent:*

\( \text{a) } \Sha(E/K)_{\ell} = 0, \quad (12) \)  

\( \text{where } \Sha(E/K)_{\ell} \text{ denotes the } \ell\text{-primary component of } \Sha(E/K). \)

\( \text{b) } \Sha(E/K)[\ell] = 0. \quad (13) \)

\( \text{c) } \quad \partial : E(K)/[\ell](E(K)) \to S^{[\ell]}(E/K). \quad (14) \)

\( \text{d) } \quad S^{[\ell]}(E/K) = \ker\{H^1(G,E[\ell]) \to H^1(G,E(\overline{K}))\}. \quad (15) \)
Proof. a) ⇒ b). This is clear since \( \text{III}(E/K)[\ell] \subseteq \text{III}(E/K)_\ell \).

b) ⇒ a). Assume that \( \text{III}(E/K)[\ell] = 0 \). Let \( A \) be any finite subgroup of \( \text{III}(E/K)_\ell \). Then, \( A \) is of the form \( \bigoplus_{i=1}^m \mathbb{Z}/\ell^m \mathbb{Z} \), where \( m_i \in \mathbb{N} \). Now, one must have \( n \leq \dim_{\mathbb{F}_\ell} \text{III}(E/K)[\ell] \). Thus, \( n = 0 \) and \( \text{III}(E/K)_\ell = 0 \).

c) ⇔ d). From the short exact sequence:

\[
0 \to E(K)/[\ell](E(K)) \to S^{[\ell]}(E/K) \to \text{III}(E/K)[\ell] \to 0. \tag{16}
\]

\( \partial : E(K)/[\ell](E(K)) \cong \text{Ker}\{H^1(G, E[\ell]) \to H^1(G, E(\bar{K}))\}. \tag{17} \]

From the compositum of homomorphisms at any place \( v \) of \( K \):

\[
H^1(G, E[\ell]) \to H^1(G, E(\bar{K})) \xrightarrow{\text{Res}^G_{S_v}} H^1(G_v, E(\bar{K}_v)), \tag{18}
\]

one obtains

\[
\partial : E(K)/[\ell](E(K)) \cong \text{Ker}\{H^1(G, E[\ell]) \to H^1(G, E(\bar{K}))\} \subseteq S^{[\ell]}(E/K). \tag{19}
\]

The equivalence is now clear. \( \square \)

**Remark 1.** Part d) of the proposition expresses a local-global principle: \( f \in H^1(G, E[\ell]) \) splits in \( E(\bar{K}_v) \) for all places \( v \) if and only if it does in \( E(\bar{K}) \). The obstruction to this principle is thus \( \text{III}(E/K)_\ell \) in view of part a) of the proposition.

We now state the main results of this paper. As in \[39][IV-2.1\), we say that an elliptic curve has complex multiplication (CM), if it does over some finite extension \( F_{\text{CM}}/\mathbb{Q} \); i.e., \( \text{End}_{F_{\text{CM}}}(E) \) is an order in an imaginary quadratic field \( K_{\text{CM}} \) \[22][Section 5\).

Given a prime number \( \ell \), one has a Galois representation \( \rho_\ell : G \to \text{GL}_2(T_\ell) \), obtained by Galois action on the Tate module \( T_\ell \) of \( E \). This representation identifies \( \text{Gal}(L_\infty/\mathbb{Q}) \) with \( \rho_\ell(G) \), where \( L_\infty \) denotes the field obtained by adjoining to \( \mathbb{Q} \) the affine coordinates of all \( \ell^n \)-torsion points of \( E \), with \( n \geq 1 \).

**Theorem 5.** Let \( E \) be an elliptic curve over \( \mathbb{Q} \) without CM, and consider a Weierstrass equation of the form \( y^2 = x^3 + Ax + B \), with \( A, B \in \mathbb{Z} \).

Let \( \ell \neq 2, 3, 5, 7, 13 \) be a prime number. Assume that: i) \( \rho_\ell(G) \) is the full linear group \( \text{GL}_2(\mathbb{Z}_\ell) \); and ii) \( \ell \nmid \Delta' := 4A^3 + 27B^2 \).

Then, one has:

\[
S^{[\ell]}(E/\mathbb{Q}) = \text{Ker}\{H^1(G, E[\ell]) \to H^1(G, E(\bar{Q}))\}. \tag{20}
\]

Note that from Serre’s Theorems \[10][Théorème 2, p. 294\] and \[40][Théorème 4', p. 300\], it follows that the Galois group \( \rho_\ell(G) \) is the full linear group for
almost all primes, whenever $E$ has no CM. Furthermore, in the case $E$ is semi-stable (i.e., with no additive reduction) without CM, Mazur’s Theorem [23, Theorem 4, p. 131] implies that $\rho_\ell(G)$ is the full linear group for $\ell \geq 11$. It follows that $\text{III}(E/\mathbb{Q})_\ell = 0$, for any $\ell \geq 17$ not dividing $\Delta'$, whenever $E$ is semi-stable.

Proposition 1 states that Theorem 5 implies the following consequences.

**Corollary 1.** Let $E$ be any elliptic curve over $\mathbb{Q}$ without CM. Then, for almost all prime numbers $\ell$, one has:

a) $\text{III}(E/\mathbb{Q})_\ell = 0$,

where $\text{III}(E/\mathbb{Q})_\ell$ denotes the $\ell$-primary component of $\text{III}(E/\mathbb{Q})$;

b) $\text{III}(E/\mathbb{Q})[\ell] = 0$;

c) $\partial : E(\mathbb{Q})/\ell(E(\mathbb{Q})) \xrightarrow{\cong} S^{[\ell]}(E/\mathbb{Q})$.

Mazur’s Theorem on torsion points [43, Theorem 7.5, p. 242] then implies the following result.

**Corollary 2.** Let $E$ be any elliptic curve over $\mathbb{Q}$ without CM. Then, for almost all prime numbers $\ell$, one has:

$$\text{rank}(E/\mathbb{Q}) = \dim_{\mathbb{F}_\ell} S^{[\ell]}(E/\mathbb{Q}).$$

Since $\text{III}(E/\mathbb{Q})[\ell]$ is finite for any prime $\ell$, as it is a quotient group of the finite group $S^{[\ell]}(E/\mathbb{Q})$, it follows that the $\ell$-primary component of $\text{III}(E/\mathbb{Q})$ is of the form:

$$\text{III}(E/\mathbb{Q})_\ell = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{n_\ell} \oplus T_\ell,$$

where $n_\ell \geq 0$ and $T_\ell$ is a finite $\ell$-group [28, Section 12].

Thus, based on Theorem 5, the only missing piece to proving that $\text{III}(E/\mathbb{Q})$ is finite in the non-CM case, is a proof that $\text{III}(E/\mathbb{Q})$ has no infinitely divisible element. See also [43, p. 341] on this issue.

Examples of CM elliptic curves of rank 2 or 3 with endomorphism ring $\mathbb{Z}[i]$ are studied in [6]. The statement of [6, Theorems 1.2] assumes the condition $\ell \equiv 1 \mod 4$, and the very strong condition $\ell < 30,000$ (and $\ell \neq 41$), in the case of a specific curve. In the case of [6, Theorems 1.3], the condition $\ell \equiv 1 \mod 4$ is also assumed, and the extra restriction that $\ell < 30,000$ (except for finitely many exceptions), and the statement is valid for 5 specific elliptic curves. In contrast, Theorem 5 is valid for any elliptic curve without CM, and all primes $\ell$, but finitely many. However, we have not succeeded in carrying out the strategy of our proof to the CM case, as of now.

In Section 5, an example from [27] of an elliptic curve $E$ over the rationals without CM of rank at least 7 is mentioned. Furthermore, we show that, in this example, $\ell = 41$ is the smallest prime (i.e., based on the conditions of Theorem
for which Corollary 2 applies. Therefore, one can in principle find out the exact rank of \( E/\mathbb{Q} \) from a computation of \( \dim_{\mathbb{F}_2} S^{[41]}(E/\mathbb{Q}) \).

It can be noticed that this example solves the open problem mentioned in [44, Problem 2.16, p. 27] in the non-CM case.

An example that was communicated to us by Professor C. Wuthrich is also mentioned in Section 5. This example shows that the condition \( \rho_\ell(G) = \text{GL}_2(\mathbb{Z}_\ell) \) is not sufficient to conclude that \( X(E/\mathbb{Q})_\ell = 0 \), if ever \( \ell \) is one of the exceptional ones (i.e., 2, 3, 5, 7, or 13). This issue is crucial, in view of BSD-2.

We end this paper with a complement to Proposition 2 that clarifies its proof, but that is not needed as such for the proof of Theorem 5 that is presented here.

2 Background on elliptic curves

2.1 Basic notions

Let \( K \) be a field and \( E \) be an elliptic curve over \( K \); i.e., a smooth projective curve of genus 1, together with a base point \( O \). The elliptic curve admits a Weierstrass equation [43, p. 42]:

\[
y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \tag{26}
\]

with coefficients \( a_i \in K, i = 1, 2, 3, 4, 6 \). One defines the quantities:

\[
\begin{align*}
 b_2 &= a_1^2 + 4a_2; \\
 b_4 &= 2a_4 + a_1 a_3; \\
 b_6 &= a_3^2 + 4a_6; \\
 b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2.
\end{align*} \tag{27}
\]

We also set:

\[
\begin{align*}
 c_4 &= b_2^2 - 24b_4; \\
 c_6 &= -b_2^3 + 36b_2 b_4 - 216b_6.
\end{align*} \tag{28}
\]

Then, the discriminant \( \Delta \) of \( E \) corresponding to a given Weierstrass equation is equal to:

\[
\Delta(E) := -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6, \tag{29}
\]

and its \( j \)-invariant (independent of the Weierstrass equation) is equal to:

\[
j(E) := c_4^3 / \Delta. \tag{30}
\]

Given the cubic curve defined by a Weierstrass equation (26), there are three cases [43, p. 45]:

1. The curve is non-singular if \( \Delta \neq 0 \).
2. The curve has a node if \( \Delta = 0 \) and \( c_4 \neq 0 \).
3. The curve has a cusp if \( \Delta = 0 \) and \( c_4 = 0 \).

In cases (2) and (3), there is only one singular point. In case (1), the curve is an elliptic curve with base point \( O = [0, 1, 0] \).
The elliptic curve has also Weierstrass equation \( y^2 = x^3 + Ax + B \). Two elliptic curves are isomorphic over \( \overline{K} \) if and only if they have the same \( j \)-invariant [43, p. 45]. If \( K \) has characteristic different from 2 and 3, the proof of that result [43, pp. 46–47] shows that an isomorphism holds over a base extension obtained by adjoining \( (\frac{A}{A'} \frac{B}{B'})^{1/4} \) (case \( j = 1728 \)) or \( (\frac{A}{A'} \frac{B}{B'})^{1/6} \) (other cases) to \( K \), where the two curves have equations \( y^2 = x^3 + Ax + B \) and \( y^2 = x^3 + A'x + B' \) over \( K \), respectively. So, unless \( j = 0 \) or 1728, the base field extension has degree dividing 2 (the g.c.d. of 4 and 6).

There is a group law defined on \( E(K) \) that is a consequence of a special case of Bezout’s Theorem, but that can also be defined explicitly. See [43, Chapter II, Section §2].

Now, let \( \ell \) be a prime number. If the characteristic of \( K \) is different from \( \ell \), then the group \( E[\ell] = E[\ell](\overline{K}) \) of \( \ell \)-torsion points of \( E \) is isomorphic to \( \mathbb{Z}/\ell \mathbb{Z} \oplus \mathbb{Z}/\ell \mathbb{Z} \). If \( K \) has characteristic \( \ell \), then \( E[\ell] \) is isomorphic to 0 or \( \mathbb{Z}/\ell \mathbb{Z} \). See [43, p. 86].

If \( m \) is a positive integer coprime with the characteristic of \( K \), then there is the Weil pairing \( e_m : E[m] \times E[m] \to \mu_m \), which is bilinear, alternating, non-degenerate, Galois invariant, and compatible [43, Proposition 8.1, p. 94]. As a consequence, one deduces that \( \mu_m \subset K \), if \( E[m] \subset E(K) \), under the condition \( \text{char}(K) \nmid m \) [43, Corollary 8.1.1, p. 96].

Given an elliptic curve over a field \( K \), one constructs its formal group \( F \) as in [43, pp. 115-120]. If \( K \) has characteristic \( \ell \), multiplication by \( \ell \) in \( F \) (denoted \( \ell[X] \in K[[X]] \)) is either 0 or else is of the form \( g(X^{\ell^h}) \), where \( g'(0) \neq 0 \) [13]. In the latter case, \( h \) is called the height of \( F \).

Let \( k \) be a finite field of characteristic \( \ell \) and \( \tilde{E} \) be an elliptic curve over \( k \). Then, either [43, p. 144–145]:

1. The formal group of \( \tilde{E} \) has height \( h = 2 \) and \( \tilde{E}[\ell] = 0 \) (the Hasse invariant is 0, or the curve is supersingular); or

2. The formal group of \( \tilde{E} \) has height 1 and \( \tilde{E}[\ell] = \mathbb{Z}/\ell \mathbb{Z} \) (the Hasse invariant is 1, or the curve is ordinary).

The first case occurs if and only if \( j(\tilde{E}) \in \mathbb{F}_{\ell^2} \) and the map \( [\ell] \) is purely inseparable.

### 2.2 Elliptic curves over local fields

Let \( K \) be a finite extension of \( \mathbb{Q}_p \) and let \( \overline{K} \) be its algebraic closure. Let \( v \) be the discrete valuation of \( K \). Given an elliptic curve \( E \) over \( K \), we consider its minimal Weierstrass equation [43, pp. 185–187]. That is a Weierstrass equation with coefficients in the integer ring \( \mathcal{O}_v \) of \( K \) with minimal value of \( v(\Delta) \) among all such equations. Therefore, one can look at its reduction \( \tilde{E} \) modulo a uniformizer \( \pi_v \) of \( K \) [43, p. 187–188], defined over the residue field \( k_v \) of \( K \). One says [43, pp. 196–197]:
1) $E$ has good reduction if $\bar{E}$ is non-singular ($v(\Delta) = 0$).

2) $E$ has multiplicative reduction if $\bar{E}$ has a node ($v(\Delta) > 0$ and $v(c_4) = 0$).

3) $E$ has additive reduction if $\bar{E}$ has a cusp ($v(\Delta) > 0$ and $v(c_4) > 0$).

The set of non-singular points $\bar{E}_{ns}(\bar{k}_v)$ of the reduced curve forms a group $[43$, p. 56]. In the case of good reduction $\bar{E}_{ns}(\bar{k}_v) = \bar{E}(\bar{k}_v)$ is an elliptic curve defined over $k_v$. In the case of multiplicative reduction, $\bar{E}_{ns}(\bar{k}_v) \approx \bar{k}_v^+$. In the case of additive reduction, $\bar{E}_{ns}(\bar{k}_v) \approx \bar{k}_v^\times$. See also $[43$, Exercise 3.5, p. 105].

A sufficient condition for a Weierstrass equation to be minimal is that $v(\Delta) < 12$ or that $v(c_4) < 4$ $[43$, Remark 1.1, p. 186]. Therefore, in the case of good reduction ($v(\Delta) = 0$) or multiplicative reduction ($v(c_4) = 0$), a minimal Weierstrass equation remains minimal after base field extension $[43$, Proposition 5.4.(b), p. 197]. In the case of additive reduction, after a suitable finite base field extension (see below), the reduction turns either good or multiplicative. For an example of the former case, see $[43$, Example 5.2, p. 196–197]. For an example of the latter case, let $p$ be a prime number greater than 3 and consider $E : y^2 = x^3 + \sqrt{p}x^2 + p^2$ over $K = \mathbb{Q}_p(\sqrt{p})$; then, over $K(\sqrt{p})$, $E$ has Weierstrass equation $y^2 = x^3 + x^2 + p$, as can be seen with the change of variable $y' = \sqrt{p}y$ and $x = \sqrt{p}x'$.

Next, recall that $E$ has good reduction after a base extension (potential good reduction) if and only if its $j$-invariant is an integer of $K$ $[43$, p. 197]. The proof of this result in the case $\text{char}(k_v) \neq 2$ $[43$, p. 199] relies on a Weierstrass equation in Legendre form $y^2 = x(x - 1)(x - \lambda)$, $\lambda \neq 0, 1, 4$ $[43$, p. 49]. Such an equation can be obtained after adjoining the roots of the cubic polynomial $x^3 + (b_2/4)x^2 + (b_4/2)x + b_6/4 = (x - e_1)(x - e_2)(x - e_3)$ and then adjoining the square root of $e_2 - e_1$. Thus, the base field extension $K'/K$ can be taken of degree dividing 12. If $\text{char}(k_v) = 2$, the proof relies on a Weierstrass equation in Deuring normal form $y^2 + axy + y = x^3$, $\alpha^3 \neq 27$. Such an equation is obtained after adjoining a root $\alpha$ of the polynomial $x^3((x^3 - 24)^3 - (x^3 - 27))j(E)$, yielding a base field extension of degree dividing $3d'$ with $1 \leq d' \leq 4$, and then over an extra base field extension of degree 2, 4 or 6 to obtain an isomorphism with the initial elliptic curve $[43$, Proposition 1.3, p. 412, and p. 47]. In all cases, the base field extension $K'/K$ has degree divisible only by powers of 2 and 3.

If $\text{char}(k_v) \neq 2$, consideration of a Weierstrass equation in Legendre form over a field extension $K'$ of degree dividing 12 shows that $E$ has either good or multiplicative reduction over $K'$ $[43$, p. 198]. If $\text{char}(k_v) = 2$, one considers a Weierstrass equation in Deuring normal form over a field extension $K'/K$ of degree $d$ with only 2 or 3 as prime factors $[43$, p. 413].

There is a well-defined reduction map $E(K) \to \bar{E}(k_v)$ $[43$, p. 188]. Let $E_0(K)$ denote the pre-image of $\bar{E}_{ns}(k_v)$ under the reduction map. Then, there is an exact sequence

$$0 \to E_1(K) \to E_0(K) \to \bar{E}_{ns}(k_v) \to 0,$$

where the second map is the reduction map, the first map is inclusion, and $E_1(K)$ consists of all points that reduce to the point $\bar{O}$ of $\bar{E}(k_v)$ $[43$, pp. 187–188]. From the above remark, in the case of good reduction or multiplicative
reduction, the above sequence extends to a short exact sequence of Galois modules:

$$0 \rightarrow E_1(K) \rightarrow E_0(K) \rightarrow \tilde{E}_{ns}(k_v) \rightarrow 0,$$

(32)

where $E_{ns}(k_v) \approx \mathbb{k}_v^*$ in the case of multiplicative reduction.

Moreover, there is an isomorphism

$$F_{\nu}(\mathcal{M}_v) \approx E_1(K),$$

(33)

where $F_{\nu}$ is the formal group of $E$ over $\mathcal{O}_v$, and $\mathcal{M}_v$ is the maximal ideal of $\mathcal{O}_v$.\footnote{[43], p. 191].}

Now, let $\ell$ be a prime number (possibly different from $p$) and consider a finite extension $L/K$ with valuation $w$. Based on the above facts, we obtain an exact sequence of Abelian groups:

$$0 \rightarrow W_1 \approx E_1[\ell] \rightarrow E_0[\ell] \rightarrow \tilde{E}_{ns}[\ell].$$

(34)

Here, $W_1$ is the group of $\ell$-torsion points of $F_{\nu}(\mathcal{M}_w)$, and $E_1[\ell]$, $E_0[\ell]$ and $\tilde{E}_{ns}[\ell]$ are the groups of $\ell$-torsion points of $E_1(L)$, $E_0(L)$ and $\tilde{E}_{ns}(k_w)$, respectively.

Also, reduction is with respect to a minimal Weierstrass equation for $E$ over $L$ (not necessarily the same one as over $K$ in the case of additive reduction over $K$).

We also have an exact sequence of Abelian groups:

$$0 \rightarrow E_0[\ell] \rightarrow E[\ell] \approx \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \rightarrow E[\ell]/E_0[\ell] \rightarrow 0.$$

(35)

The Kodaira-Néron Theorem\footnote{[43], Theorem 6.1, p. 200] states that the Abelian group $E[\ell]/E_0[\ell]$ has order at most 4 except possibly in the case of split multiplicative reduction, in which case $E[\ell]/E_0[\ell]$ is cyclic of order $v(\Delta) = -v(j)$.}

**Lemma 1.** Let $E$ be an elliptic curve defined over a local field $K$, with bad reduction. Let $\ell > 3$ be a prime number different from the characteristic $p$ of the residue field $k_w$ of $K$. If $E$ has potential good reduction, then $E$ has good reduction over $L = K(E[\ell])$. If $E$ has potential multiplicative reduction, then $E$ has multiplicative reduction over $L$.

**Proof.** By way of contradiction, assume that $E$ has additive reduction over $L$. Then, there is a short exact sequence of Abelian groups:

$$0 \rightarrow E_1(L) \rightarrow E_0(L) \rightarrow \tilde{E}_{ns}(k_w) \approx k_w^+ \rightarrow 0,$$

(36)

where $k_w$ denotes the residue field of $L$. This yields a short exact sequence:

$$0 \rightarrow E_1[\ell] \rightarrow E_0[\ell] \rightarrow k_w^+[\ell],$$

(37)

since $E_1[\ell], E_0[\ell] \subseteq E[\ell]$, as $L = K(E[\ell])$. But since $\ell \neq p$, it follows that $E_1[\ell] = 0$ and that $k_w^+[\ell] = 0$. Therefore, one obtains that $E_0[\ell] = 0$. Now, let $o$ be the order of $E(L)/E_0(L)$. Then, an element $P$ of $E[\ell]$ satisfies both conditions $[\ell]P = o \in E_0(L)$ and $[o]P \in E_0(L)$. Therefore, since $(o, \ell) = 1$, as $\ell > 3$, one
concludes that \( P \in E_0[\ell] \). This means that \( E[\ell] \subseteq E_0[\ell] = 0 \). However, this conclusion contradicts the fact that \( E[\ell] \approx \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z} \), as \( L = K(E[\ell]) \).

So, if \( E \) has bad potentially good reduction (i.e., potential good reduction), then \( E \) must have good reduction over \( L \). If \( E \) has bad and no potential good reduction (i.e., potential multiplicative reduction), then \( E \) must have multiplicative reduction over \( L \).

**Lemma 2.** Let \( E \) be an elliptic curve defined over a local field \( K \), with good reduction. Let \( m \) be a positive integer coprime with the characteristic \( p \) of the residue field \( k_v \) of \( K \). Then, one has an isomorphism:

\[
E[m](K) \cong \bar{E}[m](k_v).
\]

**Proof.** Firstly, there is a well-defined map \( E[m](K) \to \bar{E}[m](k_v) \) obtained by restriction of the reduction map \( E(K) \to \bar{E}(k_v) \). Next, this map is one-to-one, having assumed that \( (m, p) = 1 \) and that \( \bar{E} \) is non-singular [43, Proposition 3.1, p. 192]. Lastly, the Criterion of \( \text{Néron-Ogg-Shafarevich} \) implies that the extension \( K(E[m])/K \) is unramified, having assumed good reduction and \( (m, p) = 1 \) [43, Theorem 7.1, p. 201]. It follows that, for any \( Q \in E[m](K) \), the degree of the extension \( K(Q)/K \) is equal to its residue degree. Thus, a torsion point in \( \bar{E}[m](k_v) \) can be lifted to a torsion point in \( E[m](K) \).

2.3 Elliptic curves over an algebraic number field

Let \( E \) be an elliptic curve over an algebraic number field \( K \). Then, \( E \) admits a Weierstrass equation of the form \( y^2 = x^3 + Ax + B \), with \( A, B \in \mathcal{O}_K \), where \( \mathcal{O}_K \) denotes the integer ring of \( K \). Indeed, \( E \) has a Weierstrass equation over \( K \) of the form \( y^2 = x^3 - 27c_4x - 54c_6 \), with \( c_4, c_6 \in K \) [43, pp. 42–43]. Writing \( c_4 = C_4/d \) and \( c_6 = C_6/d \), with \( C_4, C_6, d \in \mathcal{O}_K \), one obtains the Weierstrass equation \( y^2 = x^3 - 27C_4d^5x - 54C_6d^5 \), upon replacing \( (x, y) \) by \( (x/d^2, y/d^3) \).

Thus, \( E \) has a Weierstrass equation of the form \( y^2 = x^3 + Ax + B \), upon taking \( A = -27C_4d^3, B = -54C_6d^5 \in \mathcal{O}_K \).

The elliptic curve \( E \) admits a global minimal Weierstrass equation with coefficients in the integer ring of the Hilbert class field of \( K \) [43, Corollary 8.3, p. 245].

We denote \( \Sigma_E \) the set of places at which \( E \) has bad reduction. The set \( \Sigma_E \) is finite [43, Remark 1.3, p. 211]. We let \( \Sigma_{E,\text{add}} (\Sigma_{E,\text{mult}}) \) denote the (finite) sets of places \( v \) such that \( E \) has additive (respectively, multiplicative) reduction at \( v \). We denote \( \Sigma_{E,\text{p.g}} \), the set of places at which \( E \) has potential good reduction and \( \Sigma_{E,\text{p.m}} \), the set of primes at which \( E \) has potential multiplicative reduction. Thus, there is a decomposition of \( \Sigma_E \) into a disjoint union \( \Sigma_{E,\text{p.g}} \cup \Sigma_{E,\text{p.m}} \), with \( \Sigma_{E,\text{p.g}} \subseteq \Sigma_{E,\text{add}} \) and \( \Sigma_{E,\text{mult}} \subseteq \Sigma_{E,\text{p.m}} \) (both inclusions are a consequence of the other one). A place \( v \) of \( \Sigma_{E,\text{add}} \) is in \( \Sigma_{E,\text{p.g}} \) if and only if \( v(j(E)) \geq 0 \). Here, the place \( v \) is identified with the discrete valuation on the completion of \( K \) at \( v, K_v \), that maps \( K_v^* \) onto \( \mathbb{Z} \).

The following cases will be considered in Section [4,2]
2.4 Elliptic curves over $\mathbb{Q}$

Let $E$ be an elliptic curve over $\mathbb{Q}$. Then, $E$ admits a global minimal Weierstrass equation (with coefficients in $\mathbb{Z}$) [43] Corollary 8.3, p. 245. It is also convenient to consider a Weierstrass equation of the form $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$; for instance, see [33 Corollary 9.4, p. 102].

One says [39, IV-2.1] that $E/K$ has CM if for some finite extension $F_{CM}/K$, the endomorphism ring $\text{End}_{F_{CM}}(E)$ is an order $\mathcal{O}$ of an imaginary quadratic extension $K_{CM}/\mathbb{Q}$ [32, Section 5]. One may assume that $F_{CM} \supseteq K_{CM}$. Indeed, if $F'$ is a subfield of $F$, then $\text{End}_{F'}(E) \subseteq \text{End}_{F}(E)$, so that one may replace $F_{CM}$ with the compositum $K_{CM}F_{CM}$, if necessary. In the case of a curve without CM, the endomorphism ring $\text{End}_{\mathbb{C}}(E)$ is minimal; i.e., it is isomorphic to $\mathbb{Z}$ [43, Corollary 9.4, p. 102].

Let $E$ be an elliptic curve over $\mathbb{Q}$ with CM. Then, $\text{End}_{F_{CM}}(E)$ is of the form $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_{CM}$ over some finite base field extension $F_{CM}/K_{CM}$, where $\mathcal{O}_{CM}$ is the integer ring of the imaginary quadratic field $K_{CM}$, and $c = 1, 2,$ or $3$ [30].

Let $\ell$ be a prime number, and set $L = \mathbb{Q}(E[\ell])$. Based on [32 Corollary 5.13], there exists an elliptic curve $E'$ defined over $K_{CM}$, such that $\text{End}_{K_{CM}}(E') = \mathcal{O}_{CM}$. From [32 Proposition 5.3], one has $\text{End}_{F_{CM}}(E') = \mathcal{O}_{CM}$ and $E[\ell] \cong E'[\ell]$ as Galois modules for any prime $\ell$ coprime with $c$, a condition satisfied if $\ell > 3$. This relation is obtained from a short exact sequence based on an isogeny:

$$0 \rightarrow E[c] \rightarrow E(K_{CM}) \rightarrow E'(K_{CM}) \rightarrow 0,$$

where $E[c]$ denotes the group of $c$-torsion points of $E$. In particular, one deduces the identities $LF_{CM} = F_{CM}(E[\ell]) = F_{CM}(E'[\ell])$. Then, using [32 Corollary 5.5], one obtains an embedding of groups:

$$\varphi : \text{Gal}(LF_{CM}/F_{CM}) = \text{Gal}(F_{CM}(E'[\ell])/F_{CM}) \rightarrow (\mathcal{O}_{CM}/(\ell))^*, \quad (40)$$

From [40], it follows that $\ell \nmid \vert \text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})\vert$ in the CM case, unless possibly if $\ell$ ramifies in $K_{CM}$ or $\ell$ divides $[F_{CM} : \mathbb{Q}]$. In particular, $\text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ is not the full linear group for almost all primes $\ell$, as $|\text{GL}_2(\mathbb{F}_\ell)|$ is divisible by $\ell$.

In contrast, in the non-CM case, the Galois group $\text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ is the full linear group for almost all primes $\ell$ [40 Théorème 2, p. 294]; i.e., the representation $\hat{\rho}_\ell : \mathcal{G} \rightarrow \text{GL}_2(\mathbb{F}_\ell)$ obtained by Galois action on $\ell$-torsion points

\[12\]
is surjective for almost all primes $\ell$. Moreover, sufficient conditions for the isomorphism $\tilde{\rho}_\ell : \text{Gal}(\mathbb{Q}(E[\ell]) / \mathbb{Q}) \xrightarrow{\sim} \text{GL}_2(\mathbb{F}_\ell)$ to hold at a specific prime $\ell$ are presented in Serre’s work, together with several examples, in the case of semistable curves [40, §5.6 to 5.10, p. 311–323]. See also [23] for further results.

Note that from [39, Proposition, IV-19] and [40] Théorème 2, p. 294, one has for almost all primes $\ell$, an isomorphism $\text{Gal}(\mathbb{Q}(E[\ell^n]) / \mathbb{Q}) \xrightarrow{\sim} \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ induced by $\rho_\ell$, for any $n \geq 1$. Indeed, from [39, p. IV-18], the representation $\rho_\ell : G \to \text{GL}_2(\mathbb{Z}_\ell)$, obtained by Galois action on the Tate module $T_\ell$, composed with the determinant map yields the cyclotomic character $\psi_\ell$, whose image is $\mathbb{Z}_\ell^\times$ (since the base field is $\mathbb{Q}$). Setting $X = \text{SL}_2(\mathbb{Z}_\ell) \cap \text{Im}(\rho_\ell)$, one obtains a closed subgroup of $\text{SL}_2(\mathbb{Z}_\ell)$. Then, assuming that the image of $X$ into $\text{SL}_2(\mathbb{F}_\ell)$ is equal to $\text{SL}_2(\mathbb{F}_\ell)$, one concludes that $\text{Im}(\rho_\ell) = \text{SL}_2(\mathbb{Z}_\ell)$ whenever $\ell \geq 5$ [39, Lemma 3, p. IV-23]. Altogether, one has:

$$\ell \geq 5 \quad \mathbf{and} \quad \text{Im}(\tilde{\rho}_\ell) = \text{GL}_2(\mathbb{F}_\ell) \implies \text{Im}(\rho_\ell) = \text{GL}_2(\mathbb{Z}_\ell). \quad (41)$$

See [40], pp. 299–301.

We denote $\Sigma_E$ the set of primes at which $E$ has bad reduction. The set $\Sigma_E$ is finite [43, Remark 1.3, p. 211] and is non-empty [43, Exerc. 8.15, p. 264]. In the case of curves without CM, Serre proved that the set of primes $\ell$ at which $E$ has ordinary good reduction has density 1 (c.f. [42, Corollaire 1, p. 189], using [43, Exerc. 5.10, p. 154]). See also [43, Exerc. 5.11, p. 154] for a weaker statement in the case of an arbitrary elliptic curve over $\mathbb{Q}$. On the other hand, Elkies proved that any elliptic curve over $\mathbb{Q}$ has infinitely many primes $\ell$ at which $E$ has supersingular good reduction [8].

If $p$ is a prime of $\mathbb{Z}$, $\text{ord}_p$ denotes the valuation on $\mathbb{Q}_p$ such that $\text{ord}_p(p) = 1$.

3 Liftings of points on reduced elliptic curves to points with coordinates in specific algebraic number fields

We collect in this section results on torsion points of elliptic curves that will be useful in the sequel.

3.1 Torsion points over algebraic number fields

First of all, the following result on torsion points of elliptic curves over algebraic number fields expresses [43] Theorem 7.1, p. 240 in a context relevant to this work. Equation (42) follows from a result of Cassels; see [43] Theorem 3.4, p. 193. Part b) is due to Lutz and Nagell independently in the case where $K = \mathbb{Q}$; see [43, Corollary 7.2, p. 240].

**Lemma 3.** Let $E$ be an elliptic over an algebraic number field $K$, with Weierstrass equation of the form $y^2 = x^3 + Ax + B$, where $A, B \in \mathcal{O}_K$. Let $\ell$ be a prime number.
a) Assume that \( \ell > 3 \). Then, any non-trivial \( \ell^n \)-torsion point \( P \) of \( E \) over \( \mathbb{Q} \), where \( n \geq 1 \), satisfies the conditions:

\[
\begin{align*}
  x(P), y(P) &\in (\ell)^{-1}; \\
  (\ell y(P))^2 &\mid \Delta' \ell^5,
\end{align*}
\]

where \((x(P), y(P))\) are the affine coordinates of \( P \), \( \Delta' = 4A^3 + 27B^2 \), so that \( \Delta = -16\Delta' \) is the discriminant of the Weierstrass equation, and the divisibility condition holds in the integer ring \( \mathcal{O}_n \) of \( L_n := K(E[\ell^n]) \).

b) If \( \ell \) is unramified in \( K \), any non-trivial \( \ell^n \)-torsion point \( P \) of \( E \) over \( K \), where \( n \geq 1 \), satisfies the conditions:

\[
\begin{align*}
  x(P), y(P) &\in \mathcal{O}_K; \\
  y(P)^2 &\mid \Delta',
\end{align*}
\]

where the divisibility condition holds in the integer ring \( \mathcal{O}_K \) of \( K \).

Proof. Part a). The proof follows closely [43, pp. 240-241], but with some modifications.

From [43, Theorem 7.1, p. 240], \( x(P) \) and \( y(P) \) are \( v \)-integral for any place \( v \nmid \ell \) of \( L_n \). Moreover, from that result, if \( v \mid \ell \), then one has \( v(y(P)) \geq -3v(\ell)/v(\ell-1) > -v(\ell) \) and \( v(x(P)) \geq -2v(\ell)/v(\ell-1) > -v(\ell) \), having assumed that \( \ell \geq 5 \). Therefore, \( x(P), y(P) \in (\ell)^{-1} \).

Next, from [43, Sublemma 4.3, p. 222], one deduces the identity:

\[
    f(x(P)) \phi(x(P)) - g(x(P)) \psi(x(P)) = \Delta',
\]

where

\[
\begin{align*}
  f(X) &= 3X^2 + 4A; \\
  \phi(X) &= X^4 - 2AX^2 - 8BX + A^2; \\
  g(X) &= 3X^3 - 5AX - 27B; \\
  \psi(X) &= X^3 + AX + B; \\
  \Delta' &= 4A^3 + 27B^2.
\end{align*}
\]

Note here that \(-16\Delta'\) is the discriminant of the Weierstrass equation \( y^2 = x^3 + Ax + B \) [43, p. 45]. But, one has the duplication identity, which can be deduced from [43, p. 54], as \( \ell \neq 2 \):

\[
    x([2]P) = \frac{\phi(x(P))}{4\psi(x(P))}.
\]

It follows that:

\[
    y(P)^2 \left[ 4f(x(P))x([2]P) - g(x(P)) \right] = \Delta',
\]

since \( y(P)^2 = \psi(x(P)) \). Now, multiplying by \( \ell^5 \), one obtains:

\[
    (\ell y(P))^2 \ell^5 \left[ 4f(x(P))x([2]P) - g(x(P)) \right] = \Delta' \ell^5.
\]
But, \( \ell^4 [4f(x(P)) x([2]P) - g(x(P))] \) is an integral element of \( L_n \) because both \( \ell x(P) \) and \( \ell x([2]P) \) are integral elements. This proves part a).

Part b). If \( \ell \) is unramified in \( K \), then \( v(\ell) = 1 \). Thus, the above conditions \( v(y(P)) \geq -3v(\ell)/(\ell - 1) > -v(\ell) \) and \( v(x(P)) \geq -2v(\ell)/(\ell - 1) > -v(\ell) \) mean that \( x(P), y(P) \in \mathcal{O}_K \). This yields:

\[
(y(P))^2 [4f(x(P)) x([2]P) - g(x(P))] = \Delta',
\]

where \([4f(x(P)) x([2]P) - g(x(P))] \in \mathcal{O}_K \). This proves part b). \( \square \)

**Lemma 4.** Let \( E \) be an elliptic curve over an algebraic number field \( K \). Given a prime number \( \ell \) and a positive integer \( n \), let \( L_n \) denote the field extension over \( K \) obtained by adjoining the affine coordinates of all \( \ell^n \)-torsion points of \( E \).

a) Then, there is a group embedding:

\[
0 \rightarrow \text{Gal}(L_n/K) \rightarrow \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}).
\]

b) The latter group has order dividing \( \ell(\ell - 1)^2(\ell + 1)\ell^{4(n-1)} \). In particular, \([L_n : K]\) divides \( \ell(\ell - 1)^2(\ell + 1)\ell^{4(n-1)} \).

c) Let \( \ell_i, i = 1, \ldots, \nu \), be distinct prime numbers, and let \( n_i \) be positive integers, \( i = 1, \ldots, \nu \). Set \( m = \prod_{i=1}^\nu n_i \). Let \( K(E[m]) \) be the field obtained by adjoining over \( K \) the affine coordinates of all \( m \)-torsion points of \( E \) (so, \( L_n \) means \( K(E[\ell^n]) \)). Then, there is a group embedding:

\[
0 \rightarrow \text{Gal}(K(E[m])/K) \rightarrow \prod_{i=1}^\nu \text{GL}_2(\mathbb{Z}/\ell_i^n\mathbb{Z}).
\]

In particular, \([K(E[m]): K]\) divides the integer:

\[
\prod_{i=1}^\nu \ell_i(\ell_i - 1)^2(\ell_i + 1)\ell_i^{4(n_i-1)}.
\]

**Proof.** Part a). Since \( \text{Gal}(L_n/K) \) acts faithfully on the finite group of \( \ell^n \)-torsion points \( E[\ell^n] \), one has a group embedding:

\[
0 \rightarrow \text{Gal}(L_n/K) \rightarrow \text{Aut}(E[\ell^n]).
\]

Since \( E[\ell^n] \) is isomorphic to \( \mathbb{Z}/\ell^n\mathbb{Z} \oplus \mathbb{Z}/\ell^n\mathbb{Z} \) [43 Corollary 6.4, p. 86], it follows that

\[
\text{Aut}(E[\ell^n]) \cong \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}).
\]

Part b). One has an exact sequence of groups:

\[
0 \rightarrow I + \ell \text{Mat}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \xrightarrow{\pi} \text{GL}_2(\mathbb{F}_\ell),
\]

where \( I \) denotes the \( 2 \times 2 \) identity matrix over \( \mathbb{Z}/\ell^n\mathbb{Z} \), and the map \( \pi \) is induced by the projection of rings \( \pi : \mathbb{Z}/\ell^n\mathbb{Z} \rightarrow \mathbb{Z}/\ell\mathbb{Z} \approx \mathbb{F}_\ell \). But the rightmost factor \( \text{GL}_2(\mathbb{F}_\ell) \) has order \( (\ell^2 - 1)(\ell^2 - \ell) = \ell(\ell - 1)^2(\ell + 1) \), whereas the left most
factor $I + \ell \text{Mat}_2(\mathbb{Z}/\ell^m\mathbb{Z})$ has order $(\ell^n-1)^4$. Thus, the order of $\text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ divides $\ell(\ell-1)^2(\ell+1)^{\ell(n-1)}$. Lastly, part a) implies that $[L_n : K]$ divides the order of $\text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

Part c). Generalizing the proof of part a), one has a group embedding:

$$0 \to \text{Gal}(K[E[m]]/K) \to \text{Aut}(E[m])/\mathbb{Z} \to \text{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

(58)

since $\text{Gal}(K[E[m]]/K)$ acts faithfully on $E[m]$, which is isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ [43 Corollary 6.4, p. 86]. But then, the isomorphism of rings $\mathbb{Z}/m\mathbb{Z} \approx \prod_{i=1}^\nu \mathbb{Z}/\ell_i^n\mathbb{Z}$ (from the Chinese Remainder Theorem) yields an isomorphism:

$$\text{GL}_2(\mathbb{Z}/m\mathbb{Z}) \approx \prod_{i=1}^\nu \text{GL}_2(\mathbb{Z}/\ell_i^n\mathbb{Z}).$$

(59)

Now, use part b) on each factor of the right-hand side of this equation. \qed

**Remark 2.** Recall from [42, §4.2, pp. 151–152] that the Galois group of the infinite extension $L_\infty/\mathbb{Q}$ obtained by adjoining over $\mathbb{Q}$ the affine coordinates of all $\ell^n$-torsion points of $E$, where $n \geq 1$, is an $\ell$-adic Lie group. Indeed, one has an embedding $\rho_\ell : \text{Gal}(L_\infty/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}_\ell)$ obtained by Galois action on the Tate module $\text{lim}_n E[\ell^n]$. Its dimension $N$ is at least 2 and at most 4, since $E[\ell^n] \approx \mathbb{Z}/\ell^n\mathbb{Z} \oplus \mathbb{Z}/\ell^n\mathbb{Z}$ for all $n \geq 1$. Then, Lemma 4 shows that $[L_n : \mathbb{Q}]$ is of the form $b\ell^{nN}$, for some integer $b$ dividing $(\ell - 1)^2(\ell + 1)^\beta$, with $\beta \geq 0$. See Appendix A for an expression of the different of the extension $L_n/\mathbb{Q}$ based on a theorem of Sen [45] that was conjectured by Serre [48].

### 3.2 Multiplication by positive integers in elliptic curves

We consider an elliptic curve $E$ over a field $K$, with Weierstrass equation $y^2 = x^3 + Ax + B$.

We consider multiplication by a positive integer $n$ in $E(K)$, where $K$ is a field. For this purpose, we recall from [20, 34] the polynomials over $\mathbb{Z}[A,B]$ (note that in [34], these polynomials are considered over a finite field):

$$\begin{cases}
\Psi_1(X,Y) = -1; \\
\Psi_0(X,Y) = 0; \\
\Psi_2(X,Y) = 2Y; \\
\Psi_3(X,Y) = 3X^4 + 6AX^2 + 12BX - A^2; \\
\Psi_4(X,Y) = 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3).
\end{cases}$$

(60)

Then, one has the recursion formulae for $n \geq 1$:

$$\begin{cases}
\Psi_{2n+1}(X,Y) = \Psi_{2n}(X,Y)(\Psi_{n+2}(X,Y)\Psi_{n-1}(X,Y) - \Psi_{n-2}(X,Y)\Psi_{n+1}(X,Y))/2Y; \\
\Psi_{2n+2}(X,Y) = \Psi_{n+2}(X,Y)\Psi_{n+1}(X,Y) - \Psi_{n+1}(X,Y)\Psi_{n-1}(X,Y).
\end{cases}$$

(61)
As in [34], we denote $\Psi'_n(X,Y)$ the polynomial obtained from $\Psi_n(X,Y)$ by replacing $Y^2$ with $X^3 + AX + B$. Then, it turns out that:

$$
\begin{cases}
  f_n(X) = \Psi'_n(X,Y), & \text{n odd;}
  f_n(X) = \Psi'_n(X,Y)/Y, & \text{n even,}
\end{cases}
$$

(62)

are polynomials in $X$. From [20, pp. 37–38], $f_n(X) \in 2\mathbb{Z}[X]$ for $n$ even. Moreover, from [34, p. 486], it follows that for any $n \geq 1$, one has:

$$
\begin{cases}
  f_n(X) = cX^{(n^2-1)/2} + \cdots, & \text{n odd;}
  f_n(X) = cX^{(n^2-4)/2} + \cdots, & \text{n even,}
\end{cases}
$$

(63)

for some element $c \neq 0$ in $K$.

One can also show, with $P = (x, y)$, that:

$$[n]P = O \iff f_n(x) = 0,$n

(64)

assuming that $[2]P \neq O$ [34, Proposition (2.1)]. One also has [20, Chapter II]:

$$[n]P = O \iff (\Psi'_n(x,y))^2 = 0,$n

(65)

for $P \neq O$.

Then, one has:

$$x([n]P) = x - \frac{\Psi'_{n-1}(x,y)\Psi'_{n+1}(x,y)}{(\Psi'_n(x,y))^2};$$

(66)

and

$$y([n]P) = \frac{\Psi'_{n+2}(x,y) (\Psi'_{n-1}(x,y))^2 - \Psi'_{n-2}(x,y) (\Psi'_{n+1}(x,y))^2}{4g (\Psi'_n(x,y))^3},$$

(67)

where $P = (x, y)$, assuming that $[n]P \neq O$; see [20, Theorem 2.1, p. 38] and [34, Proposition (2.2)].

The following result refines Eq. (63) (i.e., [34, p. 486]) and [20, Theorem 2.1, p. 38].

**Lemma 5.** For any $n \geq 1$, one has:

$$
\begin{cases}
  f_n(X) = nX^{(n^2-1)/2} + cX^{(n^2-1)/2-2} + \cdots, & \text{n odd;}
  f_n(X) = nX^{(n^2-4)/2} + cX^{(n^2-4)/2-2} + \cdots, & \text{n even.}
\end{cases}
$$

(68)

for some $c \in \mathbb{Z}[A,B]$ depending on $n$.

**Proof.** The proof is by induction on $n \geq 1$.

The result is obviously true for $n = 1, 2$, since $f_1(X) = 1$ and $f_2(X)$ is equal to 2. It is also true for $n = 3$, since $f_3(X) = 3X^4 + 6AX^2 + 12BX - A^2$. For $n = 4$, one has:

$$f_4(X) = 4(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3),$$

(69)
so that the result is true.

Assume by induction hypothesis that the result is true for any $1 \leq n' < n$, for some integer $n \geq 5$.

Case 1: $n = 2m$, with $m \geq 4$ even. Then, one computes:

\[
\begin{align*}
  f_n(X) &= \Psi_{2m}'(X,Y)/Y \\
  &= \Psi_m'(X,Y) (\Psi_{m+2}'(X,Y)(\Psi_{m-1}'(X,Y))^2 - \Psi_{m-2}'(X,Y)(\Psi_{m+1}'(X,Y))^2)/2Y^2 \\
  &= f_m(X)(f_{m+2}(X)Y f_{m-1}(X) - f_{m-2}(X)f_{m+1}(X))/2Y^2 \\
  &= f_m(X)(f_{m+2}(X)f_{m-1}(X) - f_{m-2}(X)f_{m+1}(X))/2.
\end{align*}
\]

We have:

\[
\begin{cases}
  \deg(f_{m+2}(X)f_{m-1}(X)) = \frac{1}{2}((m + 2)^2 - 4) + ((m - 1)^2 - 1) = \frac{3}{2}m^2; \\
  \lc(f_{m+2}(X)f_{m-1}(X)) = (m + 2)(m - 1)^2 = m^3 - 3m + 2,
\end{cases}
\]

and

\[
\begin{cases}
  \deg(f_{m-2}(X)f_{m+1}(X)) = \frac{1}{2}((m - 2)^2 - 4) + ((m + 1)^2 - 1) = \frac{3}{2}m^2; \\
  \lc(f_{m-2}(X)f_{m+1}(X)) = (m - 2)(m + 1)^2 = m^3 - 3m - 2,
\end{cases}
\]

where $\lc(f(X))$ denotes the leading coefficient of polynomial $f(X)$. We also let $\lc_-(f(X))$ denote the next coefficient. So, if $\deg(f(X)) = d$, one has $f(X) = \lc(f(X))X^d + \lc_-(f(X))X^{d-1} + \cdots$. Thus, one has $\lc(f_n(X)) = 2m = n$, $\lc_-(f_n(X)) = 0$, and $\deg(f_n(X)) = (n^2 - 4)/2$.

Case 2: $n = 2m$, with $m \geq 3$ odd. Then, one computes:

\[
\begin{align*}
  f_n(X) &= \Psi_{2m}'(X,Y)/Y \\
  &= \Psi_m'(X,Y) (\Psi_{m+2}'(X,Y)(\Psi_{m-1}'(X,Y))^2 - \Psi_{m-2}'(X,Y)(\Psi_{m+1}'(X,Y))^2)/2Y^2 \\
  &= f_m(X)(f_{m+2}(X)f_{m-1}(X)Y^2 - f_{m-2}(X)f_{m+1}(X)Y^2)/2Y^2 \\
  &= f_m(X)(f_{m+2}(X)f_{m-1}(X) - f_{m-2}(X)f_{m+1}(X))/2.
\end{align*}
\]

We have:

\[
\deg(f_{m+2}(X)f_{m-1}(X)) = \frac{1}{2}((m + 2)^2 - 1) + ((m - 1)^2 - 4) = \frac{3}{2}(m^2 - 1),
\]

and

\[
\deg(f_{m-2}(X)f_{m+1}(X)) = \frac{1}{2}((m - 2)^2 - 1) + ((m + 1)^2 - 4) = \frac{3}{2}(m^2 - 1),
\]

with leading coefficients as in Case 1. Thus, $\lc(f_n(X)) = 2m = n$, $\lc_-(f_n(X)) = 0$, and $\deg(f_n(X)) = (n^2 - 4)/2$.

Case 3: $n = 2m + 1$, with $m \geq 2$ even. Then, one computes:

\[
\begin{align*}
  f_n(X) &= \Psi_{2m+1}'(X,Y) \\
  &= \Psi_{m+2}'(X,Y)(\Psi_m'(X,Y))^3 - (\Psi_{m+1}'(X,Y))^3\Psi_{m-1}'(X,Y) \\
  &= f_{m+2}(X)Y(f_m(X)Y)^3 - f_{m+1}(X)^3f_{m-1}(X) \\
  &= f_{m+2}(X)f_{m-1}^3(AX + B)^2 - f_{m+1}(X)f_{m-1}(X).
\end{align*}
\]
We have:
\[
\begin{cases}
\deg(f_{m+2}(X)f_m^3(X)(X^3 + AX + B)^2) = \frac{1}{2}((m + 2)^2 - 4) + \frac{3}{2}(m^2 - 4) + 6 = 2m^2 + 2m; \\
\lc(f_{m+2}(X)f_m^3(X)(X^3 + AX + B)^2) = (m + 2)m^3 = m^4 + 2m^3.
\end{cases}
\]
\[
\text{(77)}
\]
and
\[
\begin{cases}
\deg(f_{m+1}^3(X)f_{m-1}(X)) = \frac{3}{2}((m + 1)^2 - 1) + \frac{3}{2}((m - 1)^2 - 1) = 2m^2 + 2m; \\
\lc(f_{m+1}^3(X)f_{m-1}(X)) = (m + 1)^3(m - 1) = m^4 + 2m^3 - 2m - 1.
\end{cases}
\]
\[
\text{(78)}
\]
So, one has \(\lc(f_n(X)) = 2m + 1 = n\), \(\lc_-(f_n(X)) = 0\), and \(\deg(f_n(X)) = (n^2 - 1)/2\).

**Case 4:** \(n = 2m + 1\), with \(m \geq 3\) odd. Then, one computes:
\[
\begin{align*}
\Psi_2(X,Y) &= \Psi_{m+2}(X,Y)(\Psi_m(X,Y))^3 - (\Psi_{m+1}(X,Y))^3(\Psi_{m-1}(X,Y)) \\
&= f_{m+2}(X)f_m^3(X) - (f_{m+1}(X)f_m^3(X)f_{m-1}(X)Y \\
&= f_{m+2}(X)f_m^3(X) - f_{m+1}^3(X)f_{m-1}(X)(X^3 + AX + B)^2.
\end{align*}
\]
\[
\text{(79)}
\]
We have:
\[
\deg(f_{m+2}(X)f_m^3(X)) = \frac{1}{2}((m + 2)^2 - 1) + \frac{3}{2}(m^2 - 1) = 2m^2 + 2m,
\]
\[
\text{(80)}
\]
and
\[
\deg(f_{m+1}^3(X)f_{m-1}(X)(X^3 + AX + B)^2)
= \frac{3}{2}((m + 1)^2 - 4) + \frac{1}{2}((m - 1)^2 - 4) + 6 = 2m^2 + 2m,
\]
\[
\text{(81)}
\]
with the same leading coefficients as in Case 3. So, one has \(\lc(f_n(X)) = 2m + 1 = n\), \(\lc_-(f_n(X)) = 0\), and \(\deg(f_n(X)) = (n^2 - 1)/2\).

We obtain the following refinement of [20] Theorem 2.1, ii, p. 38].

**Corollary 3.** Let \(E\) be an elliptic curve with Weierstrass equation of the form \(y^2 = x^3 + Ax + B\). For any \(n \geq 1\), one has in \(\mathbb{Z}[X,A,B]\):
\[
(\Psi_n'(X,Y))^2 = n^2 X^{n^2-1} + cX^{n^2-3} + \cdots.
\]
\[
\text{(82)}
\]
for some \(c \in \mathbb{Z}[A,B]\) depending on \(n\).

**Proof.** For \(n\) odd, one has directly from Lemma 3:
\[
(\Psi_n'(X,Y))^2 = f_n^2(X) = n^2 X^{n^2-1} + cX^{n^2-3} + \cdots,
\]
\[
\text{(83)}
\]
For \(n\) even, one has:
\[
(\Psi_n'(X,Y))^2 = f_n^2(X)Y^2 = (n^2 X^{n^2-4} + c' X^{n^2-6} + \cdots)(X^3 + AX + B) \\
= n^2 X^{n^2-1} + (c' + n^2 A)X^{n^2-3} + \cdots,
\]
\[
\text{(84)}
\]
as was to be shown, taking \(c = c' + n^2 A\).
Corollary 4. For any prime $\ell > 2$ and integer $n > 1$, one has in $\mathbb{Z}[X, A, B]$:
\[
\frac{(\Psi_{m}^\ell(X, Y))^2}{(\Psi_{m-1}^\ell(X, Y))^2} = \ell^2 X^2 X^2 + (X^2 X^2 + \cdots),
\]
for some $c \in \mathbb{Z}[A, B]$ depending on $\ell^n$.

Proof. Any $\ell^{n-1}$-torsion point is also an $\ell^n$-torsion point. Therefore, the polynomial $(\Psi_{m-1}^\ell(X, Y))^2$ divides $(\Psi_{m}^\ell(X, Y))^2$. From [20, Theorem 2.2-iii, p. 39], the quotient of these two polynomials is actually in $\mathbb{Z}[X, A, B]$. One then computes directly from Corollary 4:
\[
\frac{(\Psi_{m}^\ell(X, Y))^2}{(\Psi_{m-1}^\ell(X, Y))^2} = \frac{\ell^2 X^{2} + \cdots}{\ell^{n-1} X^{2} + \cdots} = \ell^2 X^{2} + \cdots,
\]
as was to be shown. \hfill \Box

Corollary 5. For any $m \geq 1$ and any element $\lambda$ in a field $K$ containing $A$ and $B$, one has in $K[X]$:
\[
\Phi_m(X, \lambda) := (X - \lambda)(\Psi_m^\ell(X, Y))^2 - \Psi_{m-1}^\ell(X, Y)\Psi_{m+1}^\ell(X, Y) = X^{m^2} - \lambda m^2 X^{m^2-1} + \cdots.
\]

Proof. For $m$ odd, one has:
\[
(X - \lambda)(\Psi_m^\ell(X, Y))^2 - \Psi_{m-1}^\ell(X, Y)\Psi_{m+1}^\ell(X, Y) = (X - \lambda)f_m^\ell(X) - f_{m-1}(X) Y f_{m+1}(X) Y = (X - \lambda)f_m^\ell(X) - f_{m-1}(X) f_{m+1}(X) (X^3 + AX + B),
\]
which shows the result using Lemma 3. For $m$ even, one has:
\[
(X - \lambda)(\Psi_m^\ell(X, Y))^2 - \Psi_{m-1}^\ell(X, Y)\Psi_{m+1}^\ell(X, Y) = (X - \lambda)f_m^\ell(X) Y^2 - f_{m-1}(X) f_{m+1}(X) = (X - \lambda)f_m^\ell(X) (X^3 + AX + B) - f_{m-1}(X) f_{m+1}(X),
\]
which implies the result in that case. \hfill \Box

3.3 Torsion points over $\mathbb{Q}$ in the non-CM case

In this section, we consider non-CM elliptic curves $E$ over $\mathbb{Q}$, with Weierstrass equation $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$.

Under these assumptions, the next results can be applied to almost all primes $\ell$, based on results of Serre. Namely, from [39, Proposition, IV-19] and [40, Théorème 2, p. 294], one has for almost all prime numbers $\ell$, the isomorphism $\rho_\ell : \text{Gal}(L_{\infty}/\mathbb{Q}) \cong \text{GL}_2(\mathbb{Z}_\ell)$. The condition $\text{Gal}(L_{\infty}/\mathbb{Q}) \approx \text{GL}_2(\mathbb{Z}_n)$, for a given $\ell$, is clearly equivalent to the condition $\text{Gal}(L_{n}/\mathbb{Q}) \approx \text{GL}_2(\mathbb{Z}/\ell^n \mathbb{Z})$ for any $n > 1$. Moreover, the latter condition for a given $n > 1$ implies the condition for all $1 \leq n' < n$. 20
Proof. From the assumption on \( \ell \), all primitive \( \ell^n \)-torsion points of \( E \) are conjugates. But there are \( 2^n - 2(n-1)/2 \) distinct \( x \)-coordinates. Now, the polynomial appearing in Corollary 4 is of the form \((g_{\ell^n}(X))^2\), where \( g_{\ell^n}(X):= f_{\ell^n}(X)/f_{\ell^{n-1}}(X) \) has degree \( d \). Thus, the polynomial \( g_{\ell^n}(X) \) is the irreducible polynomial of \( x_n \). As the coefficient of \( X^{d-1} \) in this polynomial is equal to 0 (using Corollary 4), it follows that \( \text{tr}_{K/Q}(x_n) = 0 \), where \( K \) is the splitting field of \( x_n \). Then, one computes: 

\[ \text{tr}_n(x_n) = [L_n : K] \text{tr}_{K/Q}(x_n) = 0. \]  

Corollary 7. Let \( E \) be an elliptic curve over \( \mathbb{Q} \) without CM. Let \( y^2 = x^3 + Ax + B \) be a Weierstrass equation for \( E \), with \( A, B \in \mathbb{Z} \). Given a prime number \( \ell > 2 \) and an integer \( n \geq 1 \), let \( L_n = \mathbb{Q}(E[\ell^n]) \) and \( \text{tr}_n = \text{tr}_{L_n/Q} \), the trace map of \( L_n \) over \( \mathbb{Q} \). Assume that \( \rho_\ell \) induces an isomorphism \( \text{Gal}(L_n/Q) \cong \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \).

Then, one has \([L_n : L_{n-1}] = \ell^4\), and the following identity holds:

\[ \frac{\text{tr}_{n,n-1}(x_n)}{[L_n : L_{n-1}]} = x_{n-1}, \]  

for any primitive \( \ell^n \)-torsion point \( P_n \) of \( E \), \( x_n \) and \( x_{n-1} \) denoting the \( x \)-coordinate of \( P_n \) and \([\ell]P_n \), respectively. In particular, \( x_n - x_{n-1} \in \text{Ker} \text{tr}_{n,n-1} \).

Proof. Given \( n > 1 \), let \( P_n \) be a primitive \( \ell^n \)-torsion point of \( E \), and set \( P_{n-1} := [\ell]P_{n-1} = x(P_{n-1}). \) The roots of the polynomial \( \Phi_\ell(X, x_{n-1}) \) appearing in Corollary 5 where we take \( \lambda = x_{n-1} \in L_{n-1} \) and \( m = \ell \), are the \( x \)-coordinates of the solutions \( P \) to the equation \([\ell]P = \pm P_{n-1}\). Since \( P \) and \(-P\) have the same \( x \)-coordinate, we may restrict to the solutions of \([\ell]P = P_{n-1}\). There are \( \ell^2 \) solutions to this equation; namely \( P = P_n + Q \), where \( Q \) is an \( \ell \)-torsion point. This yields \( \ell^2 \) distinct \( x \)-coordinates, since \( P_n + Q = \pm (P_n + Q') \) yields \( Q = Q' \), or else \( 2P_n = -Q - Q' \), which is excluded since \( \ell \neq 2 \) and \( n > 1 \). Now, \( \ell^2 \) is the degree of the polynomial \( \Phi_\ell(X, x_{n-1}) \). From the assumption on the Galois group, it follows that the solutions to \([\ell]P = P_{n-1}\) are conjugates, and hence that the roots of \( \Phi_\ell(X, x_{n-1}) \) are conjugates. Therefore, \( \Phi_\ell(X, x_{n-1}) \) is the minimal polynomial of \( x_n \) over \( L_{n-1} \). We conclude that \( \text{tr}_{K/L_{n-1}}(x_n) = \ell^2 x_{n-1} \), where \( K \) is the splitting field of \( x_n \) over \( L_{n-1} \). Thus, one obtains \( \text{tr}_{n,n-1}(x_n) = [L_n : K]\ell^2 x_{n-1} \). But then, \([L_n : L_{n-1}] = \ell^4\) from the assumption on the Galois group, whereas \([K : L_{n-1}] = \ell^2\) from above. Thus, \([L_n : K] = \ell^2\) and the result is shown.
In the next result, we consider a place \( v \) of \( \mathbb{Q} \), either \( p \)-adic or Archimedean, and pick the canonical norm \( | \cdot |_v \) such that \( |p|_v = p^{-1} \) if \( v \) is the non-Archimedean place associated to a prime \( p \), or \( | \cdot |_v \) is the absolute value of a real number, if \( v \) is the Archimedean place. See [21, pp. 34–35]. One then has the product formula [21 p. 99]:

\[
\prod_v |x|_v = 1, \tag{92}
\]

for any rational number \( x \), where the product covers all canonical places of \( \mathbb{Q} \).

If \( K \) is an algebraic field, we consider for each place \( w \) lying above a place \( v \) of \( \mathbb{Q} \), the unique norm that extends \( | \cdot |_v \). Namely, if \( w \) is non-Archimedean, one defines:

\[
|x|_w = p^{-w(x)/e_w}, \tag{93}
\]

where \( w \) is viewed as the discrete valuation associated to the place \( w \), \( p \) is the prime number lying below \( w \), and \( e_w \) denotes the absolute ramification index of \( p \) in \( K_w \). If \( w \) is Archimedean, \( | \cdot |_w \) denotes the absolute value if \( K_w = \mathbb{R} \), or the complex modulus if \( K_w = \mathbb{C} \). See [21 p. 35 and p. 99] for the alternative norm \( \|x\|_w = |x|_{K_w}^{2n/3} \) and the corresponding product formula, which is not used here.

We now introduce a topology on \( E(\mathbb{C}) \) as follows. Adapting [43, Exerc. 7.6, pp. 203–204], we consider the Euclidean topology on \( \mathbb{C} \) defined by the complex modulus \( | \cdot | \). Then, we consider the product topology on the affine space \( \mathbb{A}^2(\mathbb{C}) \). Next, for each \( 0 \leq i \leq 2 \), there is an inclusion \( \phi_i : \mathbb{A}^2(\mathbb{C}) \to \mathbb{P}^2(\mathbb{C}) \) [43 p. 9]. This allows gluing together the product spaces \( \phi_i(\mathbb{A}^2(\mathbb{C})) \), \( i = 0, 1, 2 \). In this manner, we obtain a topology naturally defined on \( \mathbb{P}^2(\mathbb{C}) \), and hence on \( E(\mathbb{C}) \) based on a homogeneous equation \( y^2z = x^3 + Axz^2 + Bz^3 \) for \( E \). Note that \( E(\mathbb{C}) \) is a Hausdorff space, so that a sequence of points in this topological space has at most one limit.

In the following result, we use the fact that the polynomial \( X^3 + AX + B \) has three distinct roots, since an elliptic curve is non-singular; equivalently, since its discriminant \( \Delta \) does not vanish.

**Proposition 2.** Let \( E \) be an elliptic curve over \( \mathbb{Q} \), having Weierstrass equation \( y^2 = x^3 + Ax + B \), with \( A, B \in \mathbb{Z} \). Given a prime number \( \ell \), set \( L_n = \mathbb{Q}(E[\ell^n]/) \) and \( \text{tr}_n = \text{tr}_{L_n/\mathbb{Q}} \).

a) Then, for all prime numbers \( \ell > 3 \) not dividing \( \Delta' \), and for any integer \( n \geq 1 \), one has:

\[
\left| \frac{\text{tr}_n(\alpha_n)}{[L_n : \mathbb{Q}]} \right|_v \leq C_{s,v}, \tag{94}
\]

for any primitive \( \ell^n \)-torsion point \( P_n \) of \( E \), where \( \alpha_n = \ell^3 \Delta'/y^2(P_n) \), and any place \( v \neq \ell \) of \( \mathbb{Q} \), for some constant \( C_{s,v} > 0 \) depending only on \( A \) and \( B \), the prime \( \ell \) and the place \( v \). Namely, one has explicitly:

\[
i): \quad C_{s,q} = |(\ell - 1)^{-2}(\ell + 1)^{-1}|_q, \quad \text{if} \quad q \neq \ell; \tag{95}
i): \quad C_{s,\infty} = |\Delta'|\ell^3 \max \left(2, 1/\delta^3\right), \tag{96}
\]
where the constant $\delta > 0$ is the minimal distance between $x$-coordinates $x_n$ and $e_1$ of any primitive $\ell^n$- and $2$-torsion points, respectively, of $E(\mathbb{C})$, such that $|x_n| < \sqrt{2(|A| + |B|)}$.

b) Let $E$ be a non-CM curve, and assume that $p_{\ell}$ induces an isomorphism $\text{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q}) \xrightarrow{\cong} \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for any $n \geq 1$, where $\ell > 3$ is a prime number. Then, $\text{tr}_n(\alpha_n)/[L_n : \mathbb{Q}]$ has only finitely many values for all $n \geq 1$ ($\ell$ being fixed). Moreover, (94) then also holds for the $\ell$-adic norm, taking:

$$iii: \quad C_{n, \ell} = \max_{n=1,2; \alpha_n} \frac{|\text{tr}_n(\alpha_n)|}{[L_n : \mathbb{Q}]} < \infty. \quad (97)$$

Similar estimates also hold for the other norms.

**Proof.** Step 1. Let us fix the prime $\ell > 3$, the integer $n \geq 1$, and the primitive $\ell^n$-torsion point $P_n$ with $x$ and $y$-coordinates $x_n = x(P_n)$ and $y_n = y(P_n)$, respectively. We set $\alpha_n = \ell^3\Delta'/q_{\ell}^2$. We assume that $\ell \nmid \Delta'$.

Step 2. We consider first the case where $v$ is a non-Archimedean place of $\mathbb{Q}$ corresponding to a prime number $q \neq \ell$. Since $\alpha_n$ is a divisor of $\ell^3\Delta'$, it follows that $\text{tr}_n(\alpha_n)$ is an integer. Therefore, one obtains:

$$\left| \frac{\text{tr}_n(\alpha_n)}{[L_n : \mathbb{Q}]} \right| < |(\ell - 1)^{-2}(\ell + 1)^{-1}|_q, \quad (98)$$

using Lemma 4, which proves inequality i).

Step 3. Next, fix a place $w$ of $L_n$ lying above the Archimedean place $v = \infty$ of $\mathbb{Q}$; equivalently, $w$ corresponds to an embedding $\xi : \mathbb{Q} \hookrightarrow \mathbb{C}$, with $|x|_w = |\xi(x)|$. We set $C_1 := \max \left(1, \frac{1}{2}\sqrt{2(|A|_w + |B|_w)} = \sqrt{2(|A| + |B|)}\right)$. Then, one has for $|x_n|_w \geq 1$:

$$|x_n^3 + Ax_n + B| \geq |x_n^3| - |A|_w x_n |w| - |B|_w \geq |x_n^3| - (|A|_w + |B|_w)|x_n|_w. \quad (99)$$

Assuming also that $|x_n|_w \geq \sqrt{2(|A|_w + |B|_w)}$, one obtains $|x_n|^3_2/2 \geq (|A|_w + |B|_w)$, which yields:

$$|x_n|^3_2 - (|A|_w + |B|_w)|x_n|_w \geq |x_n|^3_2/2. \quad (100)$$

Altogether, the lower bound $|x_n|_w \geq C_1$ implies the inequality:

$$\frac{\Delta'\ell^3}{(x_n^3 + Ax_n + B)} \leq \frac{\Delta'\ell^3}{|x_n|^3_2/2} \leq 2|\Delta'|\ell^3. \quad (101)$$

Step 4. We are left with the case where the norm $|x_n|_w$ corresponding to an Archimedean place $w$ of $L_n$, is within the bound $C_1$. Let $S$ denote the set of elements $x_n$ such that $|x_n|_w < C_1$. We then need a lower bound for $|x_n^3 + Ax_n + B|_w$, whenever $x_n \in S$.

Step 5. Assume that the set $S$ of step 4 is finite.

Then, if any element $x_n$ of $S$ is equal to a root of $X^3 + AX + B$, the point $(x_n, 0)$ is a $2$-torsion point of $E(\mathbb{Q})$, which contradicts the assumption that $x_n$
is the $x$-coordinate of a primitive $\ell^n$-torsion point, as $\ell \neq 2$. Therefore, these elements $x_n$ are away from the roots of $X^3 + AX + B$, say by a distance $\delta > 0$, which implies that $1/(x_n^3 + AX + B)$ remains bounded on $S$. Therefore, one obtains:

$$\left| \frac{\Delta' \ell^3}{(x_n^3 + AX + B)} \right|_w \leq |\Delta'| \ell^3 / \delta^3,$$

(102)

for all elements $x_n \in S$. In that case, one concludes that:

$$\left| \frac{\text{tr}_n(\alpha_n)}{[L_n : \mathbb{Q}]} \right| \leq |\Delta'| \ell^3 \max \left(2, 1/\delta^3\right),$$

(103)

making use of step 3.

**Step 6.** Next, we consider the case where the set $S$ of step 4 is infinite. At this point, we make use of the topology defined above on $E(\mathbb{C}) \hookrightarrow \mathbb{P}^2(\mathbb{C})$, and we identify $E(\mathbb{Q})$ with its image under the embedding $\xi : E(\mathbb{Q}) \hookrightarrow E(\mathbb{C})$.

As $S$ is bounded, there exists an accumulation point $x_* \in \mathbb{C}$ of $S$ such that $|x_*| \leq C_1$. Thus, $\lim_{x \to \infty} \xi(x_n) = x_*$ for some sequence $(x_n)$.

If the point $x_*$ is of the form $\xi(x_*)$, where $x_* := e_1$ is a root of $X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3)$, then $P_* = (x_*, 0)$ is a 2-torsion point of $E(\mathbb{Q})$. Since $\ell \neq 2$, one has $|\ell| P_* = P_*$. But, from (66), one has:

$$x([\ell] P_*) = x_* - \frac{\Psi'_{\ell-1}(x_*, 0) \Psi'_{\ell+1}(x_*, 0)}{\Psi'(x_*, 0)^2},$$

(104)

knowing that the denominator $(\Psi'(x_*, 0))^2$ does not vanish, since $\ell \neq 2$. Thus, one concludes that $\Psi'_{\ell-1}(x_*, 0) \Psi'_{\ell+1}(x_*, 0) = 0.$

We also have:

$$x([\ell] P_n) = x_n - \frac{\Psi'_{\ell-1}(x_n, y_n) \Psi'_{\ell+1}(x_n, y_n)}{\Psi'(x_n, y_n)^2},$$

(105)

assuming that $n > 1$. This yields:

$$|\Psi'_{\ell-1}(x_n, y_n) \Psi'_{\ell+1}(x_n, y_n)|_w = |\Psi'_{\ell-1}(x_n, y_n) \Psi'_{\ell+1}(x_n, y_n) - \Psi'_{\ell-1}(x_*, 0) \Psi'_{\ell+1}(x_*, 0)|_w \leq C|x_n - x_*|_w,$$

(106)

for some constant $C > 0$, since $|x_n|_w \leq C_1$. We thus conclude that:

$$|x_n - x([\ell] P_n)|_w = \left| \frac{\Psi'_{\ell-1}(x_n, y_n) \Psi'_{\ell+1}(x_n, y_n)}{\Psi'(x_n, y_n)^2} \right|_w \leq C'|x_n - x_*|_w,$$

(107)

for some constant $C' > 0$. In particular, one has $\lim_{x \to \infty} x([1 - \ell] P_n) = 0$. Therefore, for some infinite sequence $\{P_{n_k}\}$ of primitive $\ell^{n_k}$-torsion points, one has both $\lim_{n_k \to \infty} P_{n_k} = P_*$, and $\lim_{n_k \to \infty} [1 - \ell] P_{n_k} = (0, \sqrt{B}, 1)$ or $\lim_{n_k \to \infty} [1 - \ell] P_{n_k} = (0, -\sqrt{B}, 1).$
We now show that \( \lim_{k \to \infty} [1 - \ell] P_{n_k} = O \), based on the assumption that \( \lim_{k \to \infty} P_{n_k} \) is the 2-torsion point \( P_* \), which will yield a contradiction. For this purpose, we compute the \((x,y)\)-coordinates of \( Q_n := P_n[-] P_* = P_+[+] P_n \) [43 pp. 53–54]. Since \( P_n \neq P_* \), and \( a_1 = a_2 = a_3 = 0 \), one has:

\[
\begin{align*}
&\left\{ \begin{array}{l}
P_* = (e_1, 0); \quad P_{n_k} = (x_{n_k}, y_{n_k}); \\
\lambda_{n_k} = \frac{y_{n_k}}{(x_{n_k} - e_1)}; \\
\mu_{n_k} = \frac{-y_{n_k}}{(x_{n_k} - e_1)} = -\lambda_{n_k} e_1; \\
x(Q_{n_k}) = \lambda_{n_k}^2 - x_{n_k} - e_1; \\
y(Q_{n_k}) = -\lambda_{n_k} x(Q_{n_k}) - \mu_{n_k} = -\lambda_{n_k} (\lambda_{n_k}^2 - x_{n_k} - 2e_1). \\
\end{array} \right.
\end{align*}
\] (108)

One develops:

\[
\lambda_{n_k}^2 = \frac{x_{n_k}^3 + Ax_{n_k} + B}{(x_{n_k} - e_1)^2} = \frac{(x_{n_k} - e_2)(x_{n_k} - e_3)}{(x_{n_k} - e_1)},
\] (109)

where \( e_2 \) and \( e_3 \) are the two other roots of \( X^3 + AX + B \). Since \( e_2, e_3 \neq e_1 \) by non-singularity of \( E \), one obtains \( \lim_{k \to \infty} |\lambda_{n_k}|_w = \infty \), and henceforth:

\[
\begin{align*}
\frac{x(Q_{n_k})}{y(Q_{n_k})} = \frac{\lambda_{n_k}^2 - x_{n_k} - e_1}{-\lambda_{n_k}(\lambda_{n_k}^2 - x_{n_k} - 2e_1)} \to 0, \quad \text{as} \quad k \to \infty; \\
\frac{1}{y(Q_{n_k})} = -\frac{1}{\lambda_{n_k}(\lambda_{n_k}^2 - x_{n_k} - 2e_1)} \to 0, \quad \text{as} \quad k \to \infty.
\end{align*}
\] (110)

Thus, \( \lim_{k \to \infty} Q_{n_k} = O \), as expected. Here, we have thus used the \((x,z)\)-coordinates of \( Q_{n_k} \).

Next, based on (66) and (67), one has:

\[
\begin{align*}
&\left\{ \begin{array}{l}
x([a] Q_{n_k}) = \frac{x([a] Q_{n_k})^2 - \Psi_{a-1} \Psi_{a+1}}{\Psi_{a+2} - \Psi_{a-2}}; \\
y([a] Q_{n_k}) = \frac{-\Psi_{a+2}^2 (\Psi_{a-1})^2 - \Psi_{a-2} \Psi_{a+1}^2}{4y(\Psi_{a})^3}, \\
\end{array} \right.
\end{align*}
\] (111)

where \( y \) stands for \( y(Q_{n_k}) \) and \( a = \ell - 1 \), which is an even integer since \( \ell \neq 2 \).

Now, one computes, based on Lemma [5]

\[
(\Psi_{a+2}^2 (\Psi_{a-1})^2 - \Psi_{a-2} \Psi_{a+1}^2) / (4y) = \left( f_{a+2}(f_{a-1})^2 - f_{a-2}(f_{a+1})^2 \right) / 4 = \left( 4x^3 a^2 / 2 + \text{terms of lower degree} \right) / 4.
\] (112)

One also has:

\[
(\Psi_{a})^3 = (f_a)^3 / y^3 = (a^3 x^3 a^2 / 2 - 6 + \text{terms of lower degree}) y^3.
\] (113)

This yields:

\[
y([a] Q_{n_k}) = \frac{\left( x^3 / 2 + \text{terms of lower degree} \right)}{a^3 x^3 (a^2 / 2 - 6 + \text{terms of lower degree}) y^3} \sim \frac{1}{a^3 y^3},
\] (114)

25
where \( x \) stands for \( x(Q_n) \). It follows that:

\[
\frac{1}{y([a]Q_n)} \sim a^3y^3 \sim -a^3\frac{\lambda_n^9}{\lambda_n^{12}},
\]

which yields:

\[
\lim_{k \to \infty} \frac{1}{y([a]Q_n)} = 0,
\]

since \( \lim_{k \to \infty} |\lambda_n|_w = \infty \).

One shows similarly that:

\[
\lim_{k \to \infty} \frac{x([a]Q_n)}{y([a]Q_n)} = 0.
\]

Namely, one has from Lemma 5:

\[
x(\Psi'_a)^2 - \Psi'_{a+1}\Psi'_{a-1} = x(x^3 + Ax + B)(f_a)^2 - f_{a+1}f_{a-1} = \left(x^{a^2} + \text{terms of lower degree}\right).
\]

One also has:

\[
(\Psi'_a)^2 = (f_a)^2y^2 = \left(a^2x^{a^2-4} + \text{terms of lower degree}\right)y^2.
\]

This yields:

\[
x([a]Q_n) = \frac{\left(x^{a^2} + \text{terms of lower degree}\right)}{\left(a^2x^{a^2-4} + \text{terms of lower degree}\right)y^2} \sim \frac{1}{a^2y^2},
\]

so that:

\[
\frac{x([a]Q_n)}{y([a]Q_n)} \sim a\frac{y}{x^2} \sim -a\frac{\lambda_n^3}{\lambda_n^4}.
\]

One concludes that \( \lim_{k \to \infty} |a|Q_n = O \); i.e., \( \lim_{k \to \infty} [a]P_n = O \), since \( a \) is an even integer, as \( \ell \neq 2 \), and \( P \) is a 2-torsion point. Henceforth, one obtains \( \lim_{k \to \infty} |1 - \ell|P_n = O \) because \( [1 - \ell]P_n = (x(\ell - 1)P_n) - y((\ell - 1)P_n) \) as \( a_1 = a_3 = 0 \) [43, p. 53]. But on the other hand, from above, one has \( \lim_{k \to \infty} |1 - \ell|P_n = (0, \pm \sqrt{B}, 1) \neq O \), a contradiction.

Therefore, no root of \( X^3 + AX + B \) can be an accumulation point of the set \( S \). This means that \( |x_n - c_1| \geq \delta \), for some constant \( \delta > 0 \), for any \( n \geq 1 \) and any root \( c_1 \) of \( X^3 + AX + B \). This completes the proof of inequality ii), since [103] is then valid.
Step 7. Part a) being proved, we now show part b) under the assumptions on $E$ and $\ell$ stated in the proposition.

Let $F/\mathbb{Q}$ be the normal closure of the extension obtained by adjoining the roots $e_i$, $i = 1, 2, 3$, of $X^3 + AX + B$. Thus, $[F : \mathbb{Q}] = 6$. Consider $L'_n = L_n F$, and let $\text{tr}'_{n,n-1}$ denote the trace map of the relative extension $L'_n/L_{n-1}'$. Note that $L_n$ and $L'_{n-1}$ are linearly disjoint over $L_{n-1}$, since $[L_n : L_{n-1}] = \ell^3$ and $[L'_{n-1} : L_{n-1}] = 6$, as $\ell > 3$ by assumption.

Since $x_n$ is a root of the polynomial $f_{\ell^n}(X)$, whereas any root $e_i$ of $X^3 + AX + B$ is not, as $\ell \neq 2$, it follows that $x_n - e_i \neq 0$. One then computes:

$$\frac{1}{x_n^3 + AXn + B} = \frac{1}{(x_n - e_1)(x_n - e_2)(x_n - e_3)} = \sum_{i=1}^{3} \frac{A_i}{(x_n - e_i)},$$

where the coefficients $A_i = A_i(e_1, e_2, e_3)$, $i = 1, 2, 3$, belong to $F$. Concretely, one has:

$$\begin{align*}
A_1 &= -\frac{1}{(e_1 - e_3)(e_2 - e_3)}; \\
A_2 &= -\frac{1}{(e_3 - e_2)(e_3 - e_1)}; \\
A_3 &= -\frac{1}{(e_3 - e_2)(e_3 - e_1)}.
\end{align*}$$

Thus, one obtains:

$$\text{tr}'_{n,n-1}(\alpha_n) = \Delta' \epsilon^3 \left\{ \sum_{i=1}^{3} A_i \text{tr}'_{n,n-1} \left( \frac{1}{(x_n - e_i)} \right) \right\}. \quad (124)$$

Step 8. We consider the polynomial of Corollary 5, taking $m = \ell$ and $\lambda = x_{n-1}$:

$$\Phi_{\ell}(X, x_{n-1}) = (X - x_{n-1}) f_{\ell}^2(X) - f_{\ell-1}(X) f_{\ell+1}(X) (X^3 + AX + B)$$

$$:= \sum_{j=0}^{\ell^2} a_j X^j. \quad (125)$$

We observe that $\Phi_{\ell}(X + e_i, x_{n-1})$ is the minimal polynomial of $x_n - e_i$ over $L'_{n-1}$. Furthermore, dividing $\Phi_{\ell}(X + e_i, x_{n-1})$ by $X^{\ell^2}$ and making the change of variable $Y := 1/X$, one obtains the polynomial:

$$\sum_{j=0}^{\ell^2} a_j (X + e_i)^j X^{-j} X^{-\ell^2-j} = \sum_{j=0}^{\ell^2} a_j (1 + e_i Y)^j Y^{\ell^2-j},$$

which is the minimal polynomial of $1/(x_n - e_i)$ over $L'_{n-1}$.

We then obtain the trace $\text{tr}'_{n,n-1}$ of $1/(x_n - e_i)$ as the coefficient of the monomial $-Y^{\ell^2-1}$, which is:

$$- \sum_{j=1}^{\ell^2} a_j e_i^{j-1} = - \frac{d}{dX} \Phi_{\ell}'(X, x_{n-1}) \bigg|_{X=e_i}. \quad (127)$$
But then, one computes:

\[
\frac{d}{dX} \Phi'(X, x_{n-1}) \bigg|_{X=e_i} = f_\ell'(e_i) + (e_i - x_{n-1}) 2 f_\ell(e_i) \frac{d}{dX} f_\ell(X) \bigg|_{X=e_i} - f_{\ell-1}(e_i) f_{\ell+1}(e_i)(3e_i^2 + A),
\]

(128)
since \(e_i^3 + Ae_i + B = 0\). Therefore, one obtains:

\[
\text{tr}'_{n,n-1}(\alpha_n) = -\Delta'f^3 \left\{ \sum_{i=1}^{3} A_i \left( f_\ell'^2(e_i) + 2e_i f_\ell(e_i) \frac{d}{dX} f_\ell(X) \bigg|_{X=e_i} - f_{\ell-1}(e_i) f_{\ell+1}(e_i)(3e_i^2 + A) \right) \right\}
\]

\[
+ \Delta'f^3 \left\{ \sum_{i=1}^{3} A_i \left( 2x_{n-1} f_\ell(e_i) \frac{d}{dX} f_\ell(X) \bigg|_{X=e_i} \right) \right\}.
\]

(129)

Applying Corollary 7 iteratively, one then computes:

\[
\text{tr}_{L'_n/L'_1}(\alpha_n) = -\frac{\Delta'}{\ell} \left\{ \sum_{i=1}^{3} A_i \left( f_\ell'^2(e_i) + 2e_i f_\ell(e_i) \frac{d}{dX} f_\ell(X) \bigg|_{X=e_i} - f_{\ell-1}(e_i) f_{\ell+1}(e_i)(3e_i^2 + A) \right) \right\}
\]

\[
+ \frac{\Delta'}{\ell} \left\{ \sum_{i=1}^{3} A_i 2x_1 f_\ell(e_i) \frac{d}{dX} f_\ell(X) \bigg|_{X=e_i} \right\}.
\]

(130)

Altogether, we have reached the identity:

\[
\frac{\text{tr}_n(\alpha_n)}{|L_n : Q|} = \frac{\text{tr}'_n(\alpha_n)}{|L'_n : Q|} = -\frac{\Delta'}{\ell[F : Q]} \text{tr}_{F/Q} \left\{ \sum_{i=1}^{3} A_i \left( f_\ell'^2(e_i) + 2e_i f_\ell(e_i) \frac{d}{dX} f_\ell(X) \bigg|_{X=e_i} \right) \right\}
\]

\[
+ \frac{\Delta'}{\ell[F : Q]} \text{tr}_{F/Q} \left\{ \sum_{i=1}^{3} A_i f_{\ell-1}(e_i) f_{\ell+1}(e_i)(3e_i^2 + A) \right\}
\]

\[
+ \frac{\Delta'}{\ell[F : Q]} \text{tr}_{L'_n/Q} \left\{ \sum_{i=1}^{3} A_i 2x_1 f_\ell(e_i) \frac{d}{dX} f_\ell(X) \bigg|_{X=e_i} \right\}.
\]

(131)

Therefore, the rational number \(\text{tr}_n(\alpha_n)/|L_n : Q|\) has only finitely many values for \(n > 1\), namely the values reached when taking \(n = 2\). As for \(n = 1\), there are only finitely many values for \(\alpha_1\). This completes the proof of part b). \(\square\)
3.4 Liftings of points on reduced elliptic curves

In this section, we continue to specialize results to the case where \( E \) is an elliptic curve over \( \mathbb{Q} \) without CM.

**Theorem 6.** Let \( E \) be an elliptic over \( \mathbb{Q} \) without CM, with Weierstrass equation \( y^2 = x^3 + Ax + B \), where \( A, B \in \mathbb{Z} \). Set \( \Delta' = 4A^3 + 27B^2 \). Let \( \ell > 3 \) be a fixed prime number that does not divide \( \Delta' \). Assume that the isomorphism \( \rho_\ell : \text{Gal}(L_\infty/\mathbb{Q}) \cong \text{GL}_2(\mathbb{Z}_\ell) \) holds.

Let \( p \) be a prime number such that \( p \nmid \Delta'(\ell - 1)(\ell + 1) \). Let \( \tilde{P} \) be any non-trivial point of the \( \ell \)-component of the reduced curve \( \tilde{E}(\mathbb{F}_p) \). Let the prime power \( ℓ^n \), with \( n \geq 1 \), be the order of the point \( \tilde{P} \).

Then, the point \( P \) can be lifted to a point \( P \) of \( E(\mathbb{Q}) \) with affine coordinates satisfying:

\[
y(P) = \left( \frac{a}{b} \right)^{1/2},
\]

where \( a \) and \( b \) are integers such that \( 1 \leq |a|, |b| \leq C \), for some constant \( C \) independent of \( n \), and where both \( a \) and \( b \) are coprime with \( p \).

**Proof.** Step 1. Let \( \ell \) be a fixed prime number other than 2 and 3. Let \( \ell \nmid \Delta'(\ell - 1)(\ell + 1) \) be a prime number. In particular, since \( \text{ord}_p(\Delta) = 0 \), the reduced curve \( \tilde{E}(\mathbb{F}_p) \) is non-singular.

Let \( \tilde{P} \) be a non-trivial point of the \( \ell \)-component of the reduced curve \( \tilde{E}(\mathbb{F}_p) \). Let \((\bar{x}, \bar{y})\) be the affine coordinates of \( \tilde{P} \) and set \( \ell^n = \text{ord}_\ell(\tilde{P}) \) with \( n \geq 1 \).

Let \( \xi : \mathbb{Q} \to \mathbb{Q}_p \) be a fixed embedding of fields. From Lemma 2 applied to \( m = \ell^n \), \( \tilde{P} \) can be lifted to a point \( P' \) in \( E(\mathbb{Q}_p) \), since \( (\ell^n, p) = 1 \). Since \( \xi \) induces an isomorphism \( E[\ell^n](\mathbb{Q}) \cong E[\ell^n](\mathbb{Q}_p) \) [33 Corollary 6.4, part b), p. 86], it follows that there is an element \( P_n \in E[\ell^n](\mathbb{Q}) \) such that \( \xi(P_n) = P' \).

Step 2. We denote \( \mathbb{Q}(E[\ell^n]) \) by \( L_n \), and its integer ring by \( \mathcal{O}_n \). From part a) of Lemma 3 one has \( \ell x(P_n), \ell y(P_n) \in \mathcal{O}_n \), and \( (\ell y(P_n))^2 \alpha_n = \Delta' \ell^5 \), where \( \alpha_n \) is given by (50):

\[
\alpha_n = \ell^3[4f(x_n)x'_n - g(x_n)] = \ell^3 \left( 12x_n^2x'_n + 16Ax'_n - 3x_n^3 + 5Ax + 27B \right),
\]

with \( x_n = x(P_n) \) and \( x'_n = x([2]P_n) \). From step 1, there exists \( y \in \mathbb{Z} \) such that:

\[
y \equiv \ell y(P_n) \mod \mathfrak{P},
\]

where \( \mathfrak{P} \mid p \) is the prime ideal of \( L_n \) that induces the embedding \( \xi : (L_n)_{\mathfrak{P}} \to \mathbb{Q}_p \).

Taking \( y \in \mathbb{Z} \) as above, we then have:

\[
\ell^2y^2(P_n)\alpha_n = \Delta' \ell^5 \Rightarrow y^2\alpha_n = \Delta' \ell^5 + \alpha_0 \\
\Rightarrow y^2 \text{tr}_n(\alpha_n) = \Delta' \ell^5 |L_n : \mathbb{Q}| + \text{tr}_n(\alpha_0) \in \mathbb{Z},
\]

for some \( \alpha_0 \in \mathfrak{P} \), where \( \text{tr}_n \) denotes the trace map from \( L_n \) onto \( \mathbb{Q} \) and \( |L_n : \mathbb{Q}| \) denotes the degree of \( L_n/\mathbb{Q} \).
Now, $\operatorname{tr}_n(\alpha_0) \in (p)$, since $\alpha_0 \in \mathfrak{P}$. Indeed, one has a commutative diagram:

\[
\begin{array}{ccc}
L_n \otimes_{\mathbb{Q}} \mathbb{Q}_p & \xrightarrow{\Delta} & \prod_{\mathfrak{P}'|p} (L_n)_{\mathfrak{P}'} \\
\downarrow \operatorname{tr}_n & & \downarrow \sum_{\mathfrak{P}'|p} \operatorname{tr}(L_n)_{\mathfrak{P}'}/\mathbb{Q}_p \\
\mathbb{Q}_p & \xrightarrow{\Delta} & \mathbb{Q}_p.
\end{array}
\]

(136)

Moreover, from [50, Corollary 1, p. 142], one has $\operatorname{tr}_n(L_n)_{\mathfrak{P}'}/\mathbb{Q}_p(\alpha_0) \in (p)$, for each $\mathfrak{P}'|p$.

This yields:

\[
y^2 \operatorname{tr}_n(\alpha_n) \equiv \Delta' \ell^5 [L_n : \mathbb{Q}] \mod p.
\]

(137)

But $[L_n : \mathbb{Q}]$ divides $\ell(\ell - 1)^2(\ell + 1)^{\ell(n-1)}$, as follows from Lemma [applied to $m = \ell^n$. Henceforth, having assumed that $p \nmid \Delta' \ell(\ell - 1)(\ell + 1)$, one obtains:

\[
y^2 \equiv \frac{\Delta' \ell^5}{\operatorname{tr}_n(\alpha_n)/[L_n : \mathbb{Q}]} \mod p.
\]

(138)

Indeed, we see that $\operatorname{tr}_n(\alpha_n) \not\equiv 0 \mod p$, for otherwise we obtain the contradiction $\Delta' \ell^5 [L_n : \mathbb{Q}] \equiv 0 \mod p$, using (137). A similar argument shows that $y \not\equiv 0 \mod p$.

**Step 3.** It then follows that:

\[
y(P_n) \equiv y/\ell \mod \mathfrak{P},
\]

(139)

and

\[
y/\ell \equiv y(P) \mod p,
\]

(140)

where

\[
y(P) := \left(\frac{\Delta' \ell^3}{\operatorname{tr}_n(\alpha_n)/[L_n : \mathbb{Q}]}ight)^{1/2},
\]

(141)

and $p$ is the prime ideal of $K := \mathbb{Q}(y(P))$ that induces the embedding $\xi : K_p \hookrightarrow \mathbb{Q}_p$.

**Step 4.** At this point, we consider the dependency of $\alpha_n$ on $n$. Under the assumptions stated in the theorem, Proposition [implies that:

\[
\frac{\operatorname{tr}_n(\alpha_n)}{[L_n : \mathbb{Q}]} = \frac{b}{c},
\]

(142)

where $c \neq 0$ and $b$ are integers that are bounded independently of $n$, and which we may assume relatively prime. Moreover, we observe that $b$ has to be different from 0 and actually coprime with $p$, since $\operatorname{tr}_n(\alpha_n) \not\equiv 0 \mod p$ from step 2. Furthermore, $c$ is coprime with $p$ since $[L_n : \mathbb{Q}] \neq 0 \mod p$. The theorem follows using (141), upon setting $a = \Delta' \ell^3 c$. 

**Remark 3.** The lifting $P$ considered in Theorem [ might not be a $\ell^n$-torsion point of $E$, but it projects down to a $\ell^n$-torsion point $P$ of the reduced curve.
Remark 4. One observes that there are only finitely many admissible possibilities for the $y$-coordinate $y(P) = \left(\frac{b}{a}\right)^{1/2}$ of the lifting $P$ considered in the statement of Theorem 6. Note that both $a$ and $b$ are units of $\mathbb{Z}_p$ in the statement of Theorem 6. If one chooses to express $b^{-1}$ as an integer modulo $p$, there might be infinitely many such resulting integers as $p$ varies. But this is unnecessary. The point here, is to have finitely many possibilities for $y^2(P)$, rather than expressing $y^2(P)$ as an integer modulo $p$.

To appreciate Theorem 6 let us observe that, from [12, Corollary 2], it follows directly that the reduced curve $\tilde{E}(\mathbb{F}_p)$ of an elliptic curve $E$ over $\mathbb{Q}$ admits a set of generators $\tilde{P}_i$ with $y$-coordinates satisfying the condition:

$$0 \leq y(\tilde{P}_i) \leq \left\lceil 20(1 + \log p)p^{\nu/2} \right\rceil,$$

upon taking the rational function $f = y$ of degree 3 in this result. This implies in turn that any $\ell^n$-torsion point $P$ of the reduced curve $\tilde{E}$ can be lifted to a point $P$ of $E$ with $x$-coordinate belonging to the compositum of all field extensions over $\mathbb{Q}$ generated by the roots of cubic equations of the form

$$X^3 + AX + B = y^2,$$

for some $y \in \mathbb{Z}$ such that $0 \leq y \leq \left\lceil 20(1 + \log p)p^{\nu/2} \right\rceil$. In particular, there are infinitely many such extensions to consider as prime $p$ varies.

On the other hand, Theorem 6 restricts to $\ell^n$-torsion points $\tilde{P}$ of the reduced curve $\tilde{E}$, and states that a lifting $P$ of $\tilde{P}$ can be chosen so as to satisfy $[132]$. Most importantly, there are only finitely many possibilities for the right-hand side of this equation.

### 3.5 Properties of the specific algebraic number fields used for liftings

It will be convenient to define a field $K'$ step by step as follows.

First, we consider the cyclotomic field:

$$K_1 = \mathbb{Q}(\mu_4) = \mathbb{Q}(\sqrt{-1});$$

then, the field obtained by adjoining radicals:

$$K_2 := K_1(p_1^{1/2}, \ldots, p_\nu^{1/2}),$$

where $p_1, \ldots, p_\nu$ are the $\nu$ distinct prime numbers other than $\ell$ that are bounded by the constant $C$ appearing in Theorem 6. $C$ is a positive constant depending on $E$ and $\ell$. Next, we consider the field obtained by adjoining the remaining radical:

$$K_3 := K_2(\ell^{1/2}).$$
Lastly, one adjoins over \( K_3 \) the roots \( x_1, x_2, x_3 \) of cubic equations of the form:

\[
X^3 + AX + B = y^2,
\]

as \( y^2 \) covers the set \( \mathcal{U} \) of rational numbers of the form \( \frac{a}{b} \), where \( a \) and \( b \) are integers satisfying \( 1 \leq |a|, |b| \leq C \). The resulting field extension is denoted \( K_3^{(y)} \).

This yields the compositum of fields:

\[
K' := \prod_{y^2 \in \mathcal{U}} K_3^{(y)}.
\]

Proposition 3. The extension \( K'/\mathbb{Q} \) defined in (149) is a normal extension that contains all affine coordinates of liftings \( P \) appearing in Theorem 6. Moreover, the degree \( [K' : \mathbb{Q}] \) is of the form \( 2^s 3^t \), for some non-negative integers \( s \) and \( t \). In particular, \( [K' : \mathbb{Q}] \) is coprime with \( \ell > 3 \).

Proof. We proceed step by step as follows.

Firstly, the cyclotomic field \( K_1 := \mathbb{Q}(\mu_4) \) has degree 2 over \( \mathbb{Q} \).

Next, consider a Kummer extension of the form \( K_1(p^{1/2})/K_1 \), where \( p \) is the prime \( \ell \) or one of the prime numbers bounded by \( C \). This Kummer extension has relative degree dividing 2. Moreover, since the prime \( p \) is fixed under Galois action of \( \text{Gal}(K_1/\mathbb{Q}) \), it follows that \( K_1(p^{1/2}) \) is normal over \( \mathbb{Q} \). Hence, both \( K_2/\mathbb{Q} \) and \( K_3/\mathbb{Q} \) are normal extensions.

It is clear that a Kummer extension of the form \( K_1(y)/K_1 \), where \( y^2 = \frac{a}{b} \) with \( 1 \leq |a|, |b| \leq C \), is contained in \( K_3 \).

Next, fixing a rational number \( y \) as above, one obtains a cubic equation:

\[
X^3 + AX + B = y^2,
\]

whose roots are in \( K' \), by construction. The relative normal closure of this equation over \( K_3 \) has relative degree dividing 6.

Lastly, Galois action on the roots of such a cubic equation yields roots of another such cubic equation. Thus, \( K' \) is normal over \( \mathbb{Q} \).

Proposition 4. Assume that \( p \not\equiv 1 \mod \ell \). Then, the \( \ell \)-component of the reduced curve \( \tilde{E}(\mathbb{F}_p) \) is cyclic.

Proof. If \( \tilde{E}(\mathbb{F}_p) \ell \) is not cyclic, then it contains \( \tilde{E}[\ell] \), from which it follows that \( \mu_\ell \subset \mathbb{F}_p \) [38 Corollary 8.1.1, p. 96] (consequence of the Weil pairing). Thus, one would have \( \ell \mid (p - 1) \), contrary to the assumption that \( p \not\equiv 1 \mod \ell \).

The following results will be crucial in the proof of Lemma 9.

Proposition 5. Let \( \ell \) be a prime number. Let \( n \) be a positive integer coprime with \( \ell \). Define \( K_1 = \mathbb{Q}(\mu_n) \), and consider a field of the form

\[
K_2 = K_1(p_1^{1/n}, ..., p_\nu^{1/n}),
\]

where \( p_1, ..., p_\nu \) are \( \nu \) distinct prime numbers, each coprime with \( \ell \). Then, \( \ell \) is unramified in \( K_2 \).
Proof. Firstly, \( \ell \) is unramified in the cyclotomic field \( K_1 \) [21 Theorem 2, p. 74].

Next, let us consider the extension \( K_{(p_1)} := K_1(p_1^{1/n}) \). This is a Kummer extension over \( K_1 \) of degree \( d_1 \) dividing \( n \). Then, setting \( y_1 = p_1^{1/n} \), one deduces from Kummer theory that \( y_1^{d_1} \) belongs to \( K_1 \). In particular, \( f_1(x) = x^{d_1} - y_1^{d_1} \) is the minimal polynomial of \( y_1 \) over \( K_1 \). It follows that \( \ell \) is coprime with the discriminant of the relative Kummer extension \( K_{(p_1)}/K_1 \), because the different of this extension divides the ideal generated by \( f_1(y_1) = d_1y_1^{d_1-1} \) [21 Corollary 2, p. 56], as \( y_1 \) belongs to the integer ring of \( K_1(y_1) \), and both \( d_1 \) and \( y_1 \) are coprime with \( \ell \).

Proceeding by induction, one considers the Kummer extension \( K_{(p_1, \ldots, p_r, p_{r+1})} \) over \( K(p_1, \ldots, p_r) \), defined as \( K_{(p_1, \ldots, p_r)}(p_{r+1}^{1/n}) \), where \( 1 \leq r < \nu \). The same argument as above shows that the relative different of this extension divides the ideal generated by \( f_{r+1}(y_{r+1}) = d_{r+1}y_{r+1}^{d_{r+1}-1} \), where \( y_{r+1} = p_{r+1}^{1/n} \), \( d_{r+1} \) is the degree of the relative extension, and \( f_{r+1}(x) = x^{d_{r+1}} - y_{r+1}^{d_{r+1}} \) is the minimal polynomial of \( y_{r+1} \) over \( K_{(p_1, \ldots, p_r)} \).

One concludes that \( \ell \) is coprime with the different of the relative extension \( K_2/K_1 \), from the transitivity property [11 Proposition 8, p. 51]. Altogether, it follows that \( \ell \) is unramified in \( K_2 \), applying [11 Proposition 6, p. 50] and [21 Corollary 1, p. 53].

**Corollary 8.** Let \( \ell > 2 \) be a prime number. Let \( K' \) be the field defined in (149).

Then,

1. \( \ell \) is unramified in \( K_2 \), and hence, \( \mathbb{Q}(\mu_{\ell}) \cap K_2 = \mathbb{Q} \).
2. \( \mathbb{Q}(\mu_{\ell}) \cap K_3 \) is equal to the unique quadratic subfield \( K_0 \) of \( \mathbb{Q}(\mu_{\ell}) \) (i.e., \( \mathbb{Q}(\sqrt{\ell}) \) if \( \ell \equiv 1 \mod 4 \), or \( \mathbb{Q}(\sqrt{-\ell}) \) if \( \ell \equiv 2,3 \mod 4 \));
3. the extension \( (\mathbb{Q}(\mu_{\ell}) \cap K')/\mathbb{Q} \) has degree dividing 12.

**Proof.** Part a). The first statement follows from Proposition 5 applied to \( n = 4 \) and the distinct prime factors \( p_1, \ldots, p_\nu \) other than \( \ell \) that are bounded by \( C \), having assumed that \( \ell > 2 \).

Thus, the prime \( \ell \) is unramified in \( K_2 \subset K_1(p_1^{1/4}, \ldots, p_\nu^{1/4}) \). See (146). On the other hand, \( \ell \) is totally ramified in \( \mathbb{Q}(\mu_{\ell}) \) [11 Proposition 17, p. 78]. This yields the equality \( \mathbb{Q}(\mu_{\ell}) \cap K_2 = \mathbb{Q} \).

Part b). The extension \( K_3/K_2 \) has degree dividing 2, and hence the same property holds true for \( (\mathbb{Q}(\mu_{\ell}) \cap K_3)/(\mathbb{Q}(\mu_{\ell}) \cap K_2) \). But \( \mathbb{Q}(\mu_{\ell}) \cap K_2 = \mathbb{Q} \) from part a). Furthermore, \( \mathbb{Q}(\mu_{\ell}) \cap K_3 \) contains both quadratic fields \( \mathbb{Q}(\sqrt{\ell}) \) and \( \mathbb{Q}(\sqrt{-\ell}) \). Thus, it contains the unique quadratic subfield of \( \mathbb{Q}(\mu_{\ell}) \).

Part c). The field \( K' \) is obtained by adjoining to \( K_3 \) various roots of cubic equations. For each of these cubic equations, the splitting field has Galois group a quotient of the permutation group \( S_3 \), so that its Galois group has cardinality dividing 6. Therefore, the normal extension \( K'/K_3 \) has Galois group of exponent dividing 6.

Now, we have an isomorphism of groups:

\[
\text{Gal}((\mathbb{Q}(\mu_{\ell}) \cap K') \cdot K_3/K_3) \cong \text{Gal}((\mathbb{Q}(\mu_{\ell}) \cap K')/(\mathbb{Q}(\mu_{\ell}) \cap K') \cap K_3).
\] (152)
But since, \( K_3 \subseteq K' \), it follows that
\[
\text{Gal}((\mathbb{Q}(\mu_\ell) \cap K') \cdot K_3/K_3) \xrightarrow{\approx} \text{Gal}((\mathbb{Q}(\mu_\ell) \cap K')/(\mathbb{Q}(\mu_\ell) \cap K_3)). \tag{153}
\]
Then, since \((\mathbb{Q}(\mu_\ell) \cap K') \cdot K_3 \subseteq K'\), we obtain a surjective group homomorphism:
\[
\text{Gal}(K'/K_3) \twoheadrightarrow \text{Gal}((\mathbb{Q}(\mu_\ell) \cap K')/(\mathbb{Q}(\mu_\ell) \cap K_3)). \tag{154}
\]
Therefore, \( \text{Gal}((\mathbb{Q}(\mu_\ell) \cap K')/(\mathbb{Q}(\mu_\ell) \cap K_3)) \) is annihilated by 6, and henceforth, \( \text{Gal}((\mathbb{Q}(\mu_\ell) \cap K')/\mathbb{Q}) \) has exponent dividing 12. Since \( \text{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \) is a cyclic group, we conclude that \((\mathbb{Q}(\mu_\ell) \cap K')/\mathbb{Q}\) has degree dividing 12. \( \square \)

\section{Proof of the Main Theorem}

Let \( E \) be an elliptic curve over an algebraic number field \( K \) and \( \ell \) be a prime number. We denote the group of \( \ell \)-torsion points \( E[\ell](\overline{K}) \) by \( E[\ell] \). We set \( G = \text{Gal}(L/K) \), where \( L = K(E[\ell]) \). The absolute Galois groups \( \text{Gal}(\overline{K}/K) \) and \( \text{Gal}(\overline{L}/L) \) are denoted \( \mathcal{G} \) and \( \mathcal{H} \), respectively.

For each places \( v_0 \mid p \) and \( v \mid v_0 \) of \( K \) and \( L \), respectively, where \( p \) is a prime number, we set \( \mathcal{G}_{v_0} = \text{Gal}(\overline{K}_p/K_{v_0}) \) and \( \mathcal{H}_v = \text{Gal}(\overline{L}_p/L_v) \). We consider the \([\ell]\)-Selmer groups:

\[
S^{[\ell]}(E/L) = \ker \left\{ \text{Hom}(\mathcal{H}, E[\ell]) \xrightarrow{\oplus_v \text{Res}^\mathcal{H}_{E[\ell]}} \oplus_v H^1(\mathcal{H}_v, E(\overline{K}_p)) \right\}; \tag{155}
\]

\[
S^{[\ell]}(E/K) = \ker \left\{ \text{Hom}(\mathcal{G}, E[\ell]) \xrightarrow{\oplus_{v_0} \text{Res}^\mathcal{G}_{E[\ell]}} \oplus_{v_0} H^1(\mathcal{G}_{v_0}, E(\overline{K}_p)) \right\}. \tag{156}
\]

Here, \( v \) and \( v_0 \) cover all places of \( L \) and \( K \), respectively.

We are interested in computing the groups \( S^{[\ell]}(E/K) \) and \( S^{[\ell]}(E/L) \). Note that the \([\ell]\)-Selmer groups are finite \cite[Theorem 4.2, part b), p. 333]{Serre} and, in fact, are finite vector spaces over \( \mathbb{F}_\ell \). In Sections \ref{sec:infres} and \ref{sec:finres} we specialize to the case where \( K = \mathbb{Q} \).

\subsection{Map from \( S^{[\ell]}(E/K) \) into \( S^{[\ell]}(E/L) \)}

We recall the exact inflation-restriction sequence of Galois cohomology.

\textbf{Lemma 6} \textit{(Inflation-restriction exact sequence).} Let \( G \) be a (possibly infinite) profinite group with closed normal subgroup \( N \). Let \( A \) be a \( G \)-module. Then, there is an exact (inflation-restriction) sequence:

\[
0 \rightarrow H^1(G/N, A^N) \xrightarrow{\text{Inf}^G_{G/N}} H^1(G, A) \xrightarrow{\text{Res}^G_N} H^1(N, A)^{G/N}, \tag{157}
\]

where \( g \in G \) acts on a 1-cocycle \( f : N \rightarrow A \) as \((g \cdot f)(n) = g f(g^{-1}ng)\) for \( n \in N \).
Proof. As in [43, p. 420], one has an exact sequence:

$$0 \to H^1(G/N, A) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(N, A). \quad (158)$$

Then, one computes directly, assuming that $f$ is defined at $g$:

$$g f(g^{-1}ng) = g\{f(g^{-1}) + g^{-1}(f(n) + nf(g))\}$$

$$= g(f(g^{-1}) + f(n) + nf(g)) = -f(g) + f(n) + nf(g)$$

$$= f(n) + (n-1)f(g). \quad (159)$$

So, taking $g \in N$, one sees that the action of $G$ on $H^1(N, A)$ factors through $G/N$. Moreover, if $f$ is defined on all of $G$, one deduces that $\text{Res}^G_N(f) \in H^1(N, A)^{G/N}$.

**Proposition 6.** Let $\ell$ be a prime number and $E$ an elliptic curve over an algebraic number field $K$. Set $L = K(E[\ell])$. Then, one has a homomorphism of groups:

$$\text{Res}^G_N : S[\ell](E/K) \to S[\ell](E/L)^{G/H}, \quad (160)$$

where $G$ and $H$ denote the absolute Galois groups of $K$ and $L$, respectively.

Proof. From the inflation-restriction sequence, we obtain a commutative diagram for any places $v_0 \mid p$ of $K$ and $v \mid v_0$ of $L$:

$$
\begin{array}{ccc}
H^1(G, E[\ell]) & \xrightarrow{\text{Res}^G_N} & H^1(H, E[\ell])^{G/H} \\
\downarrow \text{Res}^{G_{v_0}} & & \downarrow \text{Res}^H_{v_0} \\
H^1(G_{v_0}, E((\bar{\mathbb{Q}}_p))[\ell]) & \xrightarrow{\text{Res}^{G_{v_0}}_{v_0}} & H^1(H_{v_0}, E((\bar{\mathbb{Q}}_p))[\ell]).
\end{array} \quad (161)
$$

where $G_{v_0}$ and $H_{v_0}$ are the absolute Galois groups of $K_{v_0}$ and $L_{v_0}$, respectively. The result now follows from an easy diagram chasing.

4.2 The group $S^{[\ell]}(E/L)$

In this section, $E$ is an elliptic curve over an algebraic number field $K$.

Motivated by Proposition 6, we consider the $[\ell]$-Selmer group of $E$ over $L = K(E[\ell])$.

Now, by construction, the Galois group $H$ acts trivially on $E[\ell]$, so that one has:

$$H^1(H, E[\ell]) = \text{Hom}(H, E[\ell]) \approx \oplus_{i=1}^2 \text{Hom}(H, \mathbb{F}_\ell). \quad (162)$$

Moreover, $L$ contains necessarily $\mu_\ell$ because $\Lambda^2 T_\ell(E) \approx T_\ell(\mu)$, where $\mu$ denotes here the multiplicative group. See [43, p. 99].

Thus, any non-trivial character $\chi$ in $\text{Hom}(H, \mathbb{F}_\ell)$ factors through the Galois group of a Kummer extension of degree $\ell$. In particular, one has an isomorphism:

$$L^*/(L^*)^\ell \cong \text{Hom}(H, \mathbb{F}_\ell) = \text{Hom}(H/H^\ell, \mathbb{F}_\ell). \quad (163)$$
Since the group \( L^*/(L^*)^\ell \) is infinite, we want to specify those group homomorphisms in \( \text{Hom}(H, E[\ell]) \) that belong to the \([\ell]-\text{Selmer group of } E \) over \( L \).

Thus, we consider a group homomorphism \( \Psi \in \text{Hom}(H, E[\ell]) \) such that the following condition holds:

\[
(*) \quad \text{Res}_{H_v}^N(\Psi) \mapsto 0 \in H^1(H_v, E(\overline{\mathbb{Q}_p})),
\]

(164)

for a given finite place \( v | p \) of \( L \).

Let \( L' = \mathbb{Q}^{\text{Ker} \Psi} \), \( N = \text{Gal}(L'/L) \) and \( N_{v'} = N_v \) (\( N \) is Abelian) be its decomposition group at \( v' | v \). Thus, \( N \) can be viewed as a subgroup of \( \mathbb{F}_\ell \oplus \mathbb{F}_\ell \).

We have a commutative diagram with exact rows:

\[
\begin{array}{ccc}
0 & \longrightarrow & \text{Hom}(N, E[\ell]) \\
& & \text{Inf}_{N_v}^N \\
0 & \longrightarrow & H^1(N_v, E(L'_{v'})) \quad \text{Inf}_{N_v}^N \quad H^1(H_v, E(\overline{\mathbb{Q}_p})).
\end{array}
\]

(165)

Therefore, given \( \Psi' \in \text{Hom}(N, E[\ell]) \), \( \text{Res}_{N_v}^N(\Psi') \) splits in \( E(L'_{v'}) \) if and only if \( \text{Res}_{N_v}^N \circ \text{Inf}_{N_v}^N(\Psi') \) does in \( E(\overline{\mathbb{Q}_p}) \). Henceforth, condition \((*)\) – applied to \( \Psi = \text{Inf}_{N_v}^N(\Psi') \) – is equivalent to:

\[
(**) \quad \text{Res}_{N_v}^N(\Psi') \mapsto 0 \in H^1(N_v, E(L'_{v'})).
\]

(166)

In particular, if \( N_v = 0 \), condition \((**)\) holds trivially. Note also that \( \Psi' \) is not identically 0 on any non-trivial subgroup of \( N \).

**Proposition 7.** Let \( \ell > 3 \) be a prime number.

a) In cases B and C, condition \((**)\) holds at a place \( v \) of \( L \) if only if \( v \) is unramified in \( L'_{v'} \) and \( \text{Res}_{N_v}^N(\Psi') \) maps to 0 in \( H^1(N_v, E_v(k_{v'})) \), where \( k_{v'} \) denotes the residue field of \( L'_{v'} \).

b) In Case D, \( v \) is at most tamely ramified in \( L'_{v'} \).

**Proof.** Part a). Case B: \( v | v_0 | p \neq \ell \) and \( v_0 \notin \Sigma_E \). Assume that condition \((*)\) holds. Let \( I_v \) be the inertia subgroup of \( L'_{v'}/L_v \). Then, there is an exact sequence:

\[
0 \rightarrow E_1(L'_{v'}) \rightarrow E(L'_{v'}) \rightarrow E_v(k_{v'}) \rightarrow 0,
\]

(167)

where \( k_{v'} \) denotes the residue field of \( L'_{v'} \). Condition \((**)\) then implies that \( \text{Res}_{N_v}^N(\Psi') \) splits in \( E_v(k_{v'}) \). Since \( I_v \) acts trivially on \( E_v(k_{v'}) \) and \( E[\ell] \approx E_v[\ell] \subset E_v(k_{v'}) \), this implies that \( \Psi' \) is trivial on \( I_v \). Therefore, \( I_v = 0 \), which means that \( v \) is unramified in \( L'_{v'} \). Furthermore, we obviously have that \( \text{Res}_{N_v}^N(\Psi') \) maps to 0 in \( H^1(N_v, E_v(k_{v'})) \).

For the converse, it is sufficient to prove that

\[
H^1(N_v, E_1(L'_{v'})) = 0,
\]

(168)
where $L_v$ is the largest Abelian extension of the form $F/L_v$ for then one obtains a commutative diagram:

\[
\begin{array}{ccc}
\text{Hom}(N, E[\ell]) & \xrightarrow{\cong} & \text{Hom}(N, \bar{E}_v[\ell]) \\
\downarrow \text{Res}^N_{L_v} & & \downarrow \text{Res}^N_{L_v} \\
0 & \longrightarrow & H^1(N_v, E(L'_v)) \xrightarrow{\text{reduction}} H^1(N_v, \bar{E}_v(k_v')).
\end{array}
\]

(169)

Now, $E_1(L'_v) \approx F_v(M_{v'})$, where $F_v$ is the formal group of $E$ over $O_v$, the integer ring of $L_v$, and $M_{v'}$ is the maximal ideal of the integer ring $O_v'$ of $L'_v$. Moreover, from [43, Proposition 6.3, p. 200], one has a short exact sequence:

\[
0 \rightarrow \pi_v'O_v' \rightarrow F_v(M_{v'}) \rightarrow M \rightarrow 0
\]

(170)

for some positive integer $r$, where $\pi_v$ is a uniformizer of $L_v$, and $M$ is a finite $\mathbb{Z}_p$-representation of $N_v$ that is annihilated by a power of $p$ (recall that $v \mid p \neq \ell$).

Since $N_v$ has order $\ell$ (recall that $N_v$ is a cyclic subgroup of $\mathbb{F}_\ell \oplus \mathbb{F}_{\ell}$), it follows that $H^1(N_v, M) = 0$. Thus, it is sufficient to show that:

\[
H^1(N_v, O_v') = 0,
\]

(171)

whenever $L'_v/L_v$ is unramified. This result is well-known and can be proved by using the facts that $H^1(N_v, k_v') = 0$ and that $O_v'$ is complete.

Case C: $v \mid v_0 \mid p \neq \ell$ and $p \in \Sigma_E$, with additive reduction of $E$ at $v_0$ and $v_0(j(E)) \geq 0$. From Lemma 1 (by assumption, $\ell > 3$), it follows that $E$ has good reduction over $L$. Therefore, the argument in case B applies.

Part b). Case D: This is clear since $\ell$ is coprime with the characteristic of the residue field of $L_v$.

\[\square\]

At this point, we make use of class field theory. One may consult reference [21] for the classical approach, close to Takagi-Artin’s treatment. One may also consult [146] for global class field theory, and [37] for local class field theory, with a treatment based extensively on homological algebra, including the notion of invariant class. A treatment based on the notion of henselian valuation with respect to a degree map can be found in [26]. Reference [9] should be consulted for a development of local class field theory, including explicit reciprocity laws, that does not rely on homological algebra. In this work, we found convenient to refer to [21, 26, 41].

We now recall the notion of conductor of a finite Abelian extension of local fields $F/L_v$ [26, p. 44]. Let $\pi_v$ be a uniformizer of $L_v$ and denote the prime ideal $(\pi_v)$ by $p_v$. Set $U_v^{(0)} = U_v$ the group of units of the ring of integers $O_v$ of $L_v$, and $U_v^{(n)} = 1 + p_v^n$ for $n \geq 1$. The conductor of $F/L_v$ is equal to $f_v = p_v^n$, where $n$ is the smallest integer such that $U_v^{(n)} \subset N_{F/L_v}(F^*)$.

Next, assume that $\mu_\ell \subset L_v^*$. Let $(L_v^{ab}/L_v) : L_v^* \rightarrow \text{Gal}(L_v^{ab}/L_v)$ be the local reciprocity map, where $L_v^{ab}$ denotes the maximal Abelian extension over $L_v$ [41, pp. 168–171]. Let $\chi_a$ be the Kummer character associated to an element.
Proposition 7 (since \( \ell > 3 \)). Assume that condition (***) holds at a place \( v \) of \( L \). Let \( \mathfrak{f}_v \) be the conductor of \( L^{1/\ell}_v/L_v \). Then,

a) Case A: \( \mathfrak{f}_v \mid p_v^{1+e_v/\ell} \), where \( e_v \) is the absolute ramification index of \( L_v \).

b) Cases B and C: \( \mathfrak{f}_v = 1 \).

c) Case D: \( \mathfrak{f}_v \mid p_v e_v/(\ell-1) \).

\[ \text{Proof.} \] Part a). Case A: The prime number \( \ell \) is equal to the characteristic of the residue field of \( L_v \). Moreover, one has \( \mu_\ell \subset L^*_v \). It is sufficient to consider the case where \( F'/L \) is a cyclic sub-extension of \( L_v'/L_v \) of degree \( \ell \). Indeed, \( L_v'/L_v \) is either the trivial extension, a cyclic extension of degree \( \ell \) or the compositum of two cyclic extensions \( F' \) and \( F'' \) of degree \( \ell \). In the first case, there is nothing to prove. In the third case, the inclusions \( 1 + p_v^{\alpha} \subset N_{F'/L_v}((F')^\ast) \) and \( 1 + p_v^{\beta} \subset N_{F'/L_v}((F'')^\ast) \) imply that \( 1 + p_v^{\max(m,n)} \subset N_{F'/L_v}((F')^\ast) \cap N_{F'/L_v}((F'')^\ast) = N_{F'/L_v}((F')^\ast) \). Thus, we consider the case where \( F'/L_v \) is a Kummer extension of degree \( \ell \), say \( F' = L_v(x^{1/\ell}) \), that might be wildly ramified. From 21 p. 186, one has the inclusion \( U^{1+e_v/\ell}(U_v, L_v) \subset U_v^{1+e_v/\ell} \). But, one obviously has \( (x, b) \mid p_v^{1+e_v/\ell} \) if and only if \( L_v'/L_v \) is unramified 26 Proposition (3,4), p. 44], which holds from Proposition 1 (since \( \ell > 3 \)).

Part b). Cases B and C: From local class field theory, one has \( \mathfrak{f}_v = 1 \) if and only if \( L_v'/L_v \) is unramified 26 Proposition 1 (since \( \ell > 3 \)).

Part c). Case D: The prime number \( \ell \) is coprime with the characteristic \( p \) of the residue field of \( L_v \). Moreover, one has \( \mu_\ell \subset L^*_v \). As above, it is sufficient to consider the case where \( F'/L_v \) is a cyclic sub-extension of \( L_v'/L_v \) of degree \( \ell \). Then, \( F'/L_v \) is tamely ramified and it is sufficient to consider the case where it is totally tamely ramified. Thus, we consider the case where \( F'/L_v \) is a Kummer extension of the form \( L_v(\pi_v^{1/\ell})/L_v \) for some uniformizer \( \pi_v \) of \( L_v \) 21 Proposition 12, p. 52]. In the case where \( \ell \) is coprime with \( p \), Hilbert’s local symbol can be computed explicitly as in [16 pp. 210–211]. Namely, let \( \alpha = (\pi_v)^\alpha \) and \( \beta = (\pi_v)^\beta \). Set \( e = (-1)^\alpha \beta^{\delta} / b^\alpha \). Then, \( (a, b) = (\bar{c}q^{-1}/\ell) \), where \( \bar{c} \) is the image of \( c \) in the residue field of \( L_v \) and \( q \) is the cardinality of the residue field. In our case, \( a = \pi_v \), so that \( \alpha = 1 \). Now, let \( b \in U_v \), so that \( \beta = 0 \). Then, \( c = 1/b \), so that \( (a, b) = (\bar{c})^{-1}/\ell \). It follows that \( (a, b) = 1 \) for all \( b \in U_v \) (i.e., the group of units that map to 1 in the residue field). On the other hand, the extension \( L_v(\pi_v^{1/\ell})/L_v \) is ramified, so that \( \mathfrak{f}_v \neq 1 \). Therefore, in the totally tamely ramified case, one concludes that \( \mathfrak{f}_v = p_v \).
Let \( m \) be the cycle \([26\text{ p. 97}]\) defined as:

\[
m = \prod_{v | \ell} p_v^{1+e_v/\ell} \prod_{v | v_0 \in \Sigma_{E, p, m.}} p_v,
\]

where \( e_v \) is the absolute ramification index of \( L_v \). One considers the subgroup \( I^m_L \) of the idele group \( I_L \) \([26\text{ p. 98}]\):

\[
I^m_L = \prod_{v | \ell} U_v^{(1+e_v/\ell)} \times \prod_{v | v_0 \in \Sigma_{E, p, m.}} U_v \times \prod_{v \notin T} U_v,
\]

where \( T = \{ v : v | \ell \} \cup \{ v : v_0 \in \Sigma_{E, p, m.} \} \). Here, \( \{ v \} \) includes the set \( S_\infty \) of infinite places of \( L \). Since \( \mu_\ell \subset L^* \), assuming that \( \ell \neq 2 \), it follows that the infinite places of \( L \) are all complex. In that case, one sets \( U_v = \mathbb{C}^* \). From global class field theory \([26\text{ Chapter IV, \S 7}]\), there exists a unique finite Abelian extension \( L^m/L \) such that:

\[
( \mathbb{L}^m/L ) : C_L/C^m_L \xrightarrow{\cong} \text{Gal}(L^m/L),
\]

where \( C_L = (L^* \cdot I_L)/L^* \) and \( C^m_L = (L^* \cdot I^m_L)/L^* \).

In the next result, we let \( I^S_L \) denote \( \prod_{v \in S} L_v^* \times \prod_{v \notin S} U_v \) \([26\text{ p. 76}]\). Now, let \( T \) be any finite set of prime ideals of an algebraic number field \( L \). Then, there exists a finite set of primes \( S \), disjoint from \( T \), such that the classes of the elements of \( S \) generate the ideal class group of \( L \) \([21\text{ pp. 124–125}]\). Next, let \( S \) be an arbitrary set of primes of an algebraic number field \( L \), such that: 1) \( S \) includes the set \( S_\infty \) of infinite places of \( L \); 2) the classes of the elements of \( S \setminus S_\infty \) generate the ideal class group of \( L \). Then, \( L^* \cdot I^S_L = L^* \cdot I_L \) \([26\text{ pp. 77–78}]\).

Thus, given a finite set \( T \) of non-Archimedean places, there exists a finite set of places \( S \supset S_\infty \) disjoint from \( T \) such that \( L^* \cdot I^S_L = L^* \cdot I_L \).

**Lemma 7.** Let \( E \) be an elliptic curve over \( K \) and \( \ell > 2 \) be a prime number. Set \( L = K(E[\ell]) \). Let \( T = \{ v : v | \ell \} \cup \{ v : v_0 \in \Sigma_{E, p, m.} \} \). Let \( S \supset S_\infty \) be a finite set of places of \( L \), disjoint from \( T \), such that \( L^* \cdot I^S_L = L^* \cdot I_L \). Take \( S \) sufficiently large, so that \( S \) is closed under Galois action of \( \text{Gal}(L/K) \). Let \( \mathcal{N} \) be the subgroup of \( I_L \) defined as:

\[
\mathcal{N} = \prod_{v \in T} U_v^\ell \times \prod_{v \in S} U_v \cdot (L_v^*)^\ell \times \prod_{v \notin S \setminus T} U_v.
\]

Then, \( \overline{\mathcal{N}} = (L^* \cdot \mathcal{N})/L^* \) is the class group of the maximal sub-extension \( \overline{L}/L \) of \( L^m/L \) whose Galois group is annihilated by \( \ell \). In particular, \( \text{Gal}(\overline{L}/L) \) is a direct product of cyclic groups of order \( \ell \) such that:

\[
\text{Hom}(\text{Gal}(\overline{L}/L), E[\ell]) = \text{Hom}(\text{Gal}(L^m/L), E[\ell]).
\]

Moreover, \( \overline{L}/K \) is a Galois extension.
Proof. Let $\bar{L}/L$ be the maximal sub-extension of $L^m/L$ with Galois group annihilated by $\ell$. Then, one has:

$$\text{Hom}(\text{Gal}(\bar{L}/L), E[\ell]) = \text{Hom}(\text{Gal}(L^m/L), E[\ell]),$$

(177)

and $\text{Gal}(\bar{L}/L)$ is a direct product of cyclic groups of order $\ell$. We show that $\mathcal{N}$ is its class group; i.e., the class field $\bar{L}/L$ is equal to $\bar{L}$.

First, we observe that $\mathcal{L}_L/\mathcal{N} \cong (L^* \cdot I_L)/(L^* \cdot \mathcal{N})$ is annihilated by $\ell$, since $L^* \cdot I_L = L^* \cdot \mathcal{I}_L$ and $(\mathcal{I}_L)_{\ell} \subseteq \mathcal{N}$. Thus, $\mathcal{L}_L/\mathcal{N} \subseteq \bar{L}$.

Conversely, the Galois group $\text{Gal}(\bar{L}/L)$ is the maximal quotient group of $\text{Gal}(L^m/L) \cong \mathcal{C}_L \cong (L^* \cdot \mathcal{I}_L)/(L^* \cdot \mathcal{I}_L)$ that is annihilated by $\ell$. But $\prod_{v \in S} U_v^\ell \times \prod_{v \in S} (\mathcal{I}_L)_{\ell} \subset (\mathcal{I}_L)_{\ell}$, and $\prod_{v \in S} U_v \times \prod_{v \notin S} U_v \subset I_L^m$. Since both $(\mathcal{I}_L)_{\ell}$ and $I_L^m$ map to 0 under the natural projection $I_L \rightarrow \mathcal{C}_L/\langle \mathcal{C}_L \rangle$, $\mathcal{N}$ is contained in the class group of $\bar{L}/L$, which means that $\bar{L} \subseteq L/\mathcal{N}$.

Since $S$ is taken closed under Galois action of $\text{Gal}(L/K)$, the same holds true for the class group $\mathcal{N}$. It follows that $L/\mathcal{N}$ is closed under any element of $\mathcal{G} = \text{Gal}(K/K)$.

Having assumed that $\ell > 2$, the group $U_v \cdot (L_v^*)^\ell$ is actually equal to $U_v = L_v^* = \mathbb{C}^*$, for any $v \in S_\infty$.

Combining Propositions 7 and 8 and Lemma 7 we have reached the following result.

**Proposition 9.** Let $\ell > 3$ be a prime number. Let $\mathcal{N}$ be the class group defined in Lemma 7. Let $\bar{L} = L/\mathcal{N}$ be the corresponding class field. Set $\bar{H} = \text{Gal}(\bar{L}/L)$. Then, one has:

$$S^{[\ell]}(E/L) = \inf_H^H \ker \left\{ \text{Hom}(\bar{H}, E[\ell]) \rightarrow \oplus_w \text{H}^1(\bar{H}_w, E(\bar{L}_w)) \right\},$$

(178)

where $w$ covers all places of $\bar{L}$.

### 4.3 Returning to the group $S^{[\ell]}(E/K)$

In this section, $E$ is an elliptic curve over an algebraic number field $K$.

Given a prime number $\ell > 3$, we set $L = K(E[\ell])$. Let $\mathcal{N}$ be the class group defined in Lemma 7 and let $\bar{L} = L/\mathcal{N}$ be the corresponding class field. We set $\bar{G} = \text{Gal}(\bar{L}/K)$ and $\bar{H} = \text{Gal}(\bar{L}/L)$.

Combining Propositions 6 and 9 we have obtained the following result.

**Corollary 9.** Let $E$ be an elliptic curve over $K$. Let $\ell > 3$ be a prime number. Then, one has:

$$S^{[\ell]}(E/K) = \inf_G^G \ker \left\{ \text{H}^1(\bar{G}, E[\ell]) \rightarrow \oplus_w \text{H}^1(\bar{G}_w, E(\bar{L}_w)) \right\},$$

(179)

where $w$ covers the places of $\bar{L}$ and $\bar{G}_w$ is the decomposition group of $w$ in $\bar{L}/K$. 

40
\textbf{Proof.} Let \( w \mid v \mid v_0 \mid p \) be places of \( \bar{L}, L, K, \) and \( \mathbb{Q}_p, \) respectively.

We show the inclusion:
\[
S^{[\ell]}(E/K) \subseteq \text{Inf} \mathcal{G}_w \mathcal{Ker}\left\{ H^1(\bar{G}, E[\ell]) \to \bigoplus_w H^1(\bar{G}_w, E(\bar{L}_w)) \right\}. \quad (180)
\]
Let \( f \in S^{[\ell]}(E/K). \) Then, \( \text{Res}^\mathcal{G}_w(f) = \text{Inf} g \mathcal{H}(g), \) for some group homomorphism \( g \in \text{Hom}(\overline{H}, E[\ell]) \) satisfying the property of Proposition 9. Then, for \( \sigma_1 \in \mathcal{G} \) and \( \sigma_2 \in \text{Gal}(\mathbb{Q}/\bar{L}), \) one computes:
\[
f(\sigma_1 \sigma_2) = f(\sigma_1) + \sigma_1 f(\sigma_2) = f(\sigma_1) + \sigma_1 g(\sigma_2) = f(\sigma_1). \quad (181)
\]
Thus, \( f = \text{Inf} \mathcal{G}_w(\bar{f}), \) for some \( \bar{f} \in H^1(\bar{G}, E[\ell]), \) and satisfies the stated property, as follows from the following diagram with exact bottom row:
\[
\begin{array}{ccc}
H^1(\bar{G}, E[\ell]) & \xrightarrow{\text{Inf} \mathcal{G}_w} & H^1(\mathcal{G}, E[\ell]) \\
\downarrow \text{Res}^\mathcal{G}_w & & \downarrow \text{Res}^\mathcal{G}_w \\
0 & \to & H^1(\bar{G}_w, E(\bar{L}_w))[\ell] \xrightarrow{\text{Inf} \mathcal{G}_w} H^1(\mathcal{G}_w, E(\mathbb{Q}_p))[\ell],
\end{array} \quad (182)
\]
where \( \mathcal{G}_w \) denotes the absolute Galois group of \( K_w. \)

The other inclusion is clear. \( \square \)

\subsection{The group \( S^{[\ell]}(E/\mathbb{Q}) \)}

We now specialize to the case where \( E \) is an elliptic curve over \( \mathbb{Q}, \) of Weierstrass equation of the form \( y^2 = x^3 + Ax + B, \) where \( A, B \in \mathbb{Z}. \) Let \( \Delta' := 4A^3 + 27B^2. \)

We consider a prime number \( \ell > 3, \) and set \( L = \mathbb{Q}(E[\ell]). \) We let \( \bar{L} \) denote the class field corresponding to the subgroup \( \mathcal{N} \) of \( C_L \) as in Lemma 3 when taking the base field \( K = \mathbb{Q}. \) We set \( \overline{H} = \text{Gal}(\bar{L}/L). \)

Next, we consider the field \( K' \) defined in (139), and we denote:
\[
L' := LK'. \quad (183)
\]
In addition to the field \( \bar{L}, \) we also consider \( \bar{L}' \) the class field corresponding to the subgroup \( \mathcal{N} \) of \( C_L', \) as in Lemma 3 when taking the base field \( K = K'. \)

The motivation for Theorem 3 and Proposition 5 was to reach the following result, which is useful for passing from \( p \)-adic rational points to algebraic ones.

\textbf{Proposition 10.} Let \( E \) be an elliptic curve over \( \mathbb{Q} \) without CM, with Weierstrass equation of the form \( y^2 = x^3 + Ax + B, \) where \( A, B \in \mathbb{Z}. \) Set \( \Delta' = 4A^3 + 27B^2. \)

Let \( \ell > 3 \) be a prime number such that \( p_\ell(\mathcal{G}) = \text{GL}_2(\mathbb{Z}_\ell). \) Let \( p \) be any prime number such that \( p \nmid \Delta'(\ell - 1)(\ell + 1). \) Let \( \xi \) be a fixed embedding of \( \mathbb{Q} \) into \( \mathbb{Q}_p, \) inducing an embedding of Galois groups \( \mathcal{G}_p = \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \mathcal{G} = \text{Gal}(\mathbb{Q}/\mathbb{Q}). \)

Then, one can write any point \( P_0 \in E(\mathbb{Q}_p) \) in the form:
\[
P_0 = \xi(P) + [\ell]Q', \quad (184)
\]
for some point \( P \in E(K') \), where \( K' \) is the field defined in [13,4], and \( Q' \in E(\mathbb{Q}_p) \).

More precisely, let \( \mathfrak{p} \) be the prime ideal of \( K' \) lying above \( p \) such that \( \xi \) induces \( K'_\mathfrak{p} \rightarrow \overline{\mathbb{Q}}_p \). Let \( F \) be the subfield of \( K' \) fixed by the decomposition group \( \text{Gal}(K'/\mathbb{Q})_\mathfrak{p} \). Then, in fact, one may take \( P \in E(F) \).

**Proof.** Since \( \text{ord}_p(\Delta) = 0 \), the reduced curve \( \tilde{E} \) of \( E \) over the residue field \( \mathbb{F}_p \) is non-singular. Let \( \# \tilde{E}(\mathbb{F}_p) = \ell^n m \), where \( n \geq 0 \) and \( (m, \ell) = 1 \).

Let \( P_0 \in E(\mathbb{Q}_p) \). Then, \( [m]P_0 \) projects to a point \( \tilde{P} \) of \( \tilde{E} \). We first consider the non-trivial case where \( n > 0 \). From Theorem 6, there is a lifting \( P' \) of \( P \) with affine coordinates in the field \( K' \) that projects to \( \tilde{P} \). If \( n = 0 \), then one may take \( P' = O \), so that \( P' \in E(\mathbb{Q}) \subset K' \) and \( P' \) is trivially a lifting of \( [m]P_0 = O \).

Then, \( [m]P_0 - \xi(P') \in E_1(K'_\mathfrak{p}) \), where \( \mathfrak{p} \) is the maximal ideal of \( K' \) lying above \( p \) that is compatible with the embedding \( \xi \). Now, one has a commutative diagram:

\[
\begin{array}{ccc}
E(K') & \xrightarrow{\xi} & E(K'_{\mathfrak{p}}) \\
\downarrow \text{tr}_{K'/F} & & \downarrow \text{tr}_{K'_{\mathfrak{p}}/\mathbb{Q}_p} \\
E(F) & \xrightarrow{\xi} & E(\mathbb{Q}_p),
\end{array}
\]

where \( F \) is the fixed field of \( K' \) by the decomposition group \( \text{Gal}(K'/\mathbb{Q})_\mathfrak{p} \). Here, we have used the fact that \( F'_{\mathfrak{p}} = \mathbb{Q}_p \), where \( \mathfrak{p}' \) is the prime ideal of \( F \) lying below \( \mathfrak{p} \), as well as [13 Exerc. 1.12 b), p.16]. This yields \( [m] \text{tr}_{K'/\mathbb{Q}_p}(P_0) - \xi(\text{tr}_{K'/F}(P')) \in E_1(\mathbb{Q}_p) \). We set \( P'' := \text{tr}_{K'/F}(P') \in E(F) \). Moreover, one has \( \text{tr}_{K'/\mathbb{Q}_p}(P_0) = [m']P_0 \), where \( m' = \frac{\text{ord}_{\mathfrak{p}}(\text{Gal}(K'/\mathbb{Q})_\mathfrak{p})}{\text{ord}_{\mathfrak{p}}(\text{Gal}(K'/\mathbb{Q})_\mathfrak{p})} \) is coprime with \( \ell \), based on Proposition 3.

Now, \( E_1(\mathbb{Q}_p) \approx F(\mathcal{M}_p) \), where \( F_p \) is the formal group of \( E \) over \( \mathbb{Q}_p \). From [13], \( F_p \) is necessarily a formal \( \mathbb{Z}_p \)-module. Since \( \ell \in \mathbb{Z}_p^* \) by assumption, it follows that \( [m'']P_0 - \xi(P'') = [\ell]Q'' \in [\ell](E_1(\mathbb{Q}_p)), \) for some point \( Q'' \in E_1(\mathbb{Q}_p) \).

Writing \( 1 = m''a + b\ell \), with \( a, b \in \mathbb{Z} \), one deduces that

\[
P_0 = [a][m'']P_0 + [\ell][b]P_0 = [a](\xi(P'') + [\ell]Q'') + [\ell][b]P_0,
\]

where \( P := [a]P'' \in E(F) \) and \( Q' := [a]Q'' + [b]P_0 \in E(\mathbb{Q}_p) \). \( \square \)

Proposition 11 allows proving the following result.

**Proposition 11.** Let \( E \) be an elliptic curve over \( \mathbb{Q} \) without CM, with Weierstrass equation \( y^2 = x^3 + Ax + B \), where \( A, B \in \mathbb{Z} \). Set \( \Delta' = 4A^3 + 27B^2 \).

Let \( \ell > 3 \) be a prime number such that \( \rho_\ell(G) = \text{GL}_2(\mathbb{Z}_\ell) \). Let \( p \) be a prime number such that \( p \nmid \Delta' \ell(\ell - 1)(\ell + 1) \). Consider \( \bar{L}, K' \), and \( \bar{L}' \) as above. Let \( w' \) be a place of \( \bar{L}' \) that lies above \( p \), and consider the place \( w \) of \( \bar{L} \) that lies below \( w' \). Assume that the decomposition group \( \bar{H}'_{w'} \), where \( \bar{H}' = \text{Gal}(\bar{L}'/\bar{L}') \), maps onto
the decomposition group $\tilde{H}_w$, where $\tilde{H} = \text{Gal}(\tilde{L}/L)$, under the natural projection $\text{Res}_L^{\tilde{L}} : H' \to H$ (defined by restriction of automorphisms to $L$).

Consider $\tilde{f}$ in $\text{Ker}\left\{ \text{H}^1(\tilde{G}, E[\ell]) \to \text{H}^1(\tilde{G}_w, E(\tilde{L}_w)) \right\}$.

Then, there exists an element $\tilde{Q} \in E(\mathbb{Q})$ such that $[\ell]\tilde{Q} \in E(K')$, and $\tilde{f}(\text{Res}_L^{\tilde{L}}(\sigma)) = [\sigma - 1]\tilde{Q}$, for all $\sigma \in \tilde{H}_w$.

Proof. Firstly, consider a place $w'$ of $\tilde{L}'$, as in the statement of the proposition. Let us fix an embedding $\xi : \mathbb{Q} \to \mathbb{Q}_p$ that yields the embedding $(\tilde{L}')_w \hookrightarrow \mathbb{Q}_p$.

Let $\tilde{f} : \tilde{G} \to E[\ell]$ be a 1-cocycle such that $\tilde{f}(\sigma) = [\sigma - 1]Q_0$ for all $\sigma \in G_w$, for some $Q_0 \in E(\tilde{L}_w)$. Then, one has $P_0 := [\ell]Q_0 \in E(\tilde{L}_w) = E(\mathbb{Q}_p)$. Now, Proposition$^{10}$ applies to $P_0$, having assumed that $\ell > 3$, and $p \nmid \Delta'(\ell - 1)(\ell + 1)$. Thus, one may write $P_0$ in the form $\xi(P) + [\ell]Q'$, where $P \in E(K')$, and $Q' \in E(\mathbb{Q}_p)$, based on Proposition$^{10}$.

Let $Q \in E(\mathbb{Q})$ such that $[\ell]Q = P$. The extension $L'(Q)/L'$ is an Abelian extension with Galois group embedded into $E[\ell]$, since $E[\ell] \subseteq L$. Indeed, the function $\text{Gal}(L'(Q)/L') \to E[\ell]$ that maps $\sigma \in \text{Gal}(L'(Q)/L')$ to $[\sigma - 1]Q$ is a group homomorphism (it is a “Kummer character” of the elliptic curve). Moreover, it is injective. Furthermore, one computes in $E(\mathbb{Q}_p)$:

$$[\ell](Q_0 - \xi(Q) - Q') = P_0 - \xi(P) - [\ell]Q' = 0. \quad (187)$$

Thus, one has $Q_0 = \xi(Q) + Q' + \xi(Q'')$, with $Q'' \in E[\ell] \subseteq E(L)$. We set

$$\tilde{Q} = Q + Q''. \quad (188)$$

Let us define $\tilde{g}(\sigma) := [\sigma - 1]\tilde{Q}$, for $\sigma \in G$. Let $w$ be the place of $\tilde{L}$ lying below $w'$, and consider the case where $\tilde{H}_w = \text{Res}_L^{\tilde{L}}(\tilde{H}_w)$, as in the statement of the proposition. Let $\sigma \in \tilde{H}_w$. One then computes:

$$\xi \left( \tilde{f}(\text{Res}_L^{\tilde{L}}(\sigma)) \right) = [\sigma - 1]Q_0 = [\sigma - 1](Q_0 - Q')$$

$$= [\sigma - 1](\xi(Q + Q'')) = [\sigma - 1]\xi(\tilde{Q}) = [\sigma - 1]\xi(\tilde{g}(\sigma)) = \xi(\tilde{g}(\sigma)), \quad (189)$$

since $Q' \in E(\mathbb{Q}_p)$, and the embedding $\xi$ was chosen to be compatible with localization of $\tilde{L}'$ at $w'$. Thus, one obtains $\tilde{f}(\text{Res}_L^{\tilde{L}}(\sigma)) = g(\sigma)$ for any $\sigma \in \tilde{H}_w$.

The hypotheses of Proposition$^{11}$ comprise a condition on the characteristic $p$ of the finite field intervening in the reduced curve, as well as condition $\text{Res}_L^{\tilde{L}}(\tilde{H}_w) = \tilde{H}_w$. Using Chebotarev’s Density Theorem, one can show that these conditions can be met, in a form relevant to Proposition$^{12}$ Namely, we have the following result.

43
Lemma 8. Let $E$ be an elliptic curve over $\mathbb{Q}$, of Weierstrass equation $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$. Let $\ell \neq 2, 3, 5, 7, 13$ be a prime number such that $\ell \nmid \Delta' := 4A^3 + 27B^2$. Set $L = \mathbb{Q}(E[\ell])$, and let $d_0$ be a prime factor of $(\ell - 1)/\gcd(\ell - 1, 12)$.

Let $K'$ and $L'$ be the fields defined in (149) and (183), respectively. Let $H_1$ be a subspace of $\tilde{H}' = \text{Gal}(\tilde{L}'/L')$, of dimension $n_1$, that is a normal subgroup of $\text{Gal}(\tilde{L}'/(L')^{\sigma_0})$, for some element $\sigma_0'$ of order $d_0$ in $\text{Gal}(L'/K')$.

Then, $H_1$ admits a decomposition $\oplus_{\nu=1}^{n_1} C_\nu$, where each $C_\nu$ is a cyclic group (of order $\ell$) that is closed under conjugation by elements of $\text{Gal}(L'/K')$. In particular, $\langle \sigma_0' \rangle$ acts on each group $C_\nu$ through some character $\chi_\nu$.

Then, in the case where $\chi_\nu$ is the trivial character, the group $C_\nu$ is equal to the decomposition group $H_{w_0}'$ of some place $w'$ of $L'$ (depending on $C_\nu$) that lies above a prime $p$ satisfying the condition $p \nmid \Delta'(\ell - 1)(\ell + 1)$.

Moreover, assume that $\text{Res}_{\tilde{L}_L}(C_\nu) \neq 0$, where $\text{Res}_{\tilde{L}_L}$ denotes the natural projection $\tilde{H}' \to \tilde{H}$, with $\tilde{H} = \text{Gal}(\tilde{L}/L)$. Then, one has $\text{Res}_{\tilde{L}_L}(C_\nu) = \tilde{H}_w$, where $w$ is the place of $L$ lying below $w'$.

Proof. Step 1. We consider the fields $K'$ and $L'$ as in (149) and (183), respectively. We view the Galois group $\text{Gal}(L'/K')$ as the subgroup $\tilde{\rho}_\ell(Gal(L/(L \cap K'))) < \text{GL}_d(F_{\ell})$, under the Galois embedding $\tilde{\rho}_\ell$.

We denote $\text{Res}_{\tilde{L}_L}$ the projection of Galois groups $\text{Gal}(\tilde{L}'/(L')^{\sigma_0'}) \to \text{Gal}(L'/K')$.

Step 2. Let $\sigma_0'$ be an element of $\text{Gal}(L'/K')$ of order $d_0$. Thus, one has:

1) $\text{ord}(\sigma_0') = d_0$ is coprime with $\ell$.

Let then $\sigma_0''$ be any lifting of $\sigma_0'$ in $\text{Gal}(\tilde{L}'/K')$. Set $\tilde{\sigma}_0 := (\sigma_0'')^0_\ell$. Then, $(\tilde{\sigma}_0')^{d_0} = ((\sigma_0'')^{d_0})^0_\ell = 1$, since $(\sigma_0'')^{d_0} \in \tilde{H}'$, as $(\sigma_0'')^{d_0} = 1$, and $\tilde{H}'$ is a vector space over $F_{\ell}$. Therefore, one has $d'' := \text{ord}(\tilde{\sigma}_0') < d_0$.

Moreover, the projection $\text{Res}_{\tilde{L}_L}(\tilde{\sigma}_0') \in \text{Gal}(L'/K')$ is equal to $\langle \sigma_0' \rangle$. Thus, one has $(\sigma_0')^{d''} = 1$, which combined with $(\sigma_0'')^{d_0} = 1$, yields $d_0 = \text{ord}(\sigma_0') < \text{gcd}(d'' \ell, d_0) = d''$ (since $d'' \mid d_0$ is coprime with $\ell$). Thus, one has ii) $\text{ord}(\tilde{\sigma}_0') = d_0$.

Step 3. Assume that $h'$ is a non-trivial element of $\tilde{H}'$ that is in the centralizer of $\tilde{\sigma}_0'$. Consider the cyclic group $\langle h' \tilde{\sigma}_0' \rangle$, where $\tilde{\sigma}_0'$ is as in step 2. Then, this cyclic group has order $d_0 \ell$, since $d_0$ is coprime with $\ell$. It follows that iii) $h' \tilde{\sigma}_0' = (h')^{d_0}$ is a generator of the cyclic group $\langle h' \rangle$.

Step 4. Assume now that $p$ is a prime that does not ramify in $\tilde{L}'$, and that $w' \mid p$ is a place of $\tilde{L}'$ such that $\text{Frob}_{\tilde{L}'\mathbb{Q}}(w') = h' \tilde{\sigma}_0'$, with $h'$ as in step 3, and $\tilde{\sigma}_0'$ as in step 2.

Then, except for finitely many such primes, one may assume that $p \nmid \Delta'\ell(\ell - 1)(\ell + 1)$.

Step 5. Since the element $\text{Res}_{\tilde{L}_L}(\tilde{\sigma}_0')$ considered in step 2 has order $d_0$, it follows that a prime $p$ as in step 4 would have residue degree $f_{L'/\mathbb{Q}}$ equal to $d_0$. Then, this means that any place $w'$ of $L'$ lying above $p$ would have Frobenius element equal to $\text{Frob}_{\tilde{L}'\mathbb{Q}}(w') = \text{Frob}_{\tilde{L}'\mathbb{Q}}(w')^{d_0}$, from property iii) of step 3. Therefore, $\text{Frob}_{\tilde{L}'\mathbb{Q}}(w')$ generates the cyclic group $\langle h' \rangle$. 

44
Therefore, all desired properties for \( p \) would be met, provided \( \sigma'_0 \) satisfies condition i) – step 2 –, and \( h' \) is in the centralizer of \( \sigma'_0 \) – step 3.

**Step 6.** Now, the cyclic group \( \langle \sigma'_0 \rangle < \text{Gal}(L'/K') \) acts by Galois conjugation on the \( \mathbb{F}_p \)-vector space \( H_1 \), which yields a representation \( \langle \sigma'_0 \rangle \hookrightarrow \text{Aut}(H_1) \). Since \( \#(\sigma'_0) = d_0 \mid (\ell - 1) \), the eigenvalues of this representation belong to \( \mathbb{F}^*_p \). Therefore, one obtains a decomposition of representations of the finite group \( \langle \sigma'_0 \rangle \) over \( \mathbb{F}_p \):

\[
H_1 = \bigoplus_{\nu=1}^{n_1} C_{\nu},
\]

where \( n_1 := \dim_{\mathbb{F}_p}(H_1) \), and \( C_{\nu} \cong \mathbb{F}_p(\chi_{\nu}) \), for some character \( \chi_{\nu} \) of the group \( \langle \sigma'_0 \rangle \).

If every \( \chi_{\nu} \) is the trivial character, then the element \( \sigma'_0 \) satisfies condition i), and \( C_{\nu} \) is in the centralizer of \( \sigma'_0 \).

An application of Chebotarev’s Density Theorem [49] to \( \widetilde{L}'/\mathbb{Q} \) and the conjugacy class of \( h' \sigma'_0 \), then yields \( \text{Frob}_{\widetilde{L}'/\mathbb{Q}}(w'_0) = \tau h' \sigma'_0 \tau^{-1} \), for some place \( w'_0 \) of \( \widetilde{L}' \) and element \( \tau \) of the Galois group \( \text{Gal}(\widetilde{L}'/\mathbb{Q}) \). But then, \( \text{Frob}_{\widetilde{L}'/\mathbb{Q}}(\tau^{-1}w'_0) = h' \sigma'_0 \), so that one may take \( w' = \tau^{-1}w'_0 \). Then, the prime \( p \) lying below \( w' \) satisfies all the desired properties: \( p \) is unramified in \( L' \); \( p \nmid \Delta' \), \( (\ell - 1)(\ell + 1) \); and \( \text{Frob}_{\tilde{L}'/\mathbb{Q}}(w') \) generates \( C_{\nu} \).

**Step 7.** One has \( \text{Frob}_{\tilde{L}'/\mathbb{Q}}(w) = \text{Res}_{\tilde{L}'/\mathbb{Q}}(\text{Frob}_{\tilde{L}'/\mathbb{Q}}(w')) \), where \( w \) is the place of \( \tilde{L} \) lying below \( w' \). Let \( v \) be the place of \( L \) lying below \( w \), and \( v' \) be the place of \( L' \) lying below \( w' \). One computes:

\[
\text{Frob}_{\tilde{L}'/\mathbb{Q}}(v) = \text{Res}_{\tilde{L}'/\mathbb{Q}}(\text{Frob}_{\tilde{L}'/\mathbb{Q}}(w)) = \text{Res}_{\tilde{L}'/\mathbb{Q}}(\text{Frob}_{\tilde{L}'/\mathbb{Q}}(w')) = \text{Res}_{\tilde{L}'/\mathbb{Q}}(\text{Frob}_{\tilde{L}'/\mathbb{Q}}(v')), \tag{191}
\]

which shows that \( f_{\tilde{L}'/\mathbb{Q}} = f_{\tilde{L}'/\mathbb{Q}} \), as \( \sigma_0 = \text{Frob}_{\tilde{L}'/\mathbb{Q}}(v) \) has same order as \( \sigma'_0 = \text{Frob}_{\tilde{L}'/\mathbb{Q}}(v') \) under the isomorphism \( \text{Res}_{\tilde{L}'/\mathbb{Q}} : \text{Gal}(L'/K') \xrightarrow{\cong} \text{Gal}(L/(L \cap K')) \).

One then obtains:

\[
\text{Frob}_{\tilde{L}'/\mathbb{Q}}(w) = \text{Frob}_{\tilde{L}'/\mathbb{Q}}(w)^{\tilde{L}'/\mathbb{Q}} = \text{Res}_{\tilde{L}'/\mathbb{Q}}(\text{Frob}_{\tilde{L}'/\mathbb{Q}}(w'))^{\tilde{L}'/\mathbb{Q}} = \text{Res}_{\tilde{L}'/\mathbb{Q}}(\text{Frob}_{\tilde{L}'/\mathbb{Q}}(w'))^{\tilde{L}'/\mathbb{Q}} = \text{Res}_{\tilde{L}'/\mathbb{Q}}(\text{Frob}_{\tilde{L}'/\mathbb{Q}}(w')), \tag{192}
\]

since \( f_{\tilde{L}'/\mathbb{Q}} = f_{\tilde{L}'/\mathbb{Q}} \). It then follows that \( \text{Frob}_{\tilde{L}'/\mathbb{Q}}(w) \) generates \( \text{Res}^{\tilde{L}'}_{\tilde{L}'}(C_{\nu}) = \langle \text{Res}^{\tilde{L}'}_{\tilde{L}'}(\text{Frob}_{\tilde{L}'/\mathbb{Q}}(w')) \rangle \). One then concludes that \( \text{Res}^{\tilde{L}'}_{\tilde{L}'}(C_{\nu}) = \tilde{H}_w \) since \( p \) is unramified in \( \tilde{L} \), and \( \tilde{H} \) is an Abelian group of exponent \( \ell \), which implies that any of its non-trivial cyclic subgroups has order \( \ell \). \( \square \)
Combining Lemma 8 and Proposition 11, we have reached the following result.

**Corollary 10.** Let $E$ be an elliptic curve over $\mathbb{Q}$, of Weierstrass equation $y^2 = x^3 + Ax + B$ without CM, where $A, B \in \mathbb{Z}$. Let $\ell \neq 2, 3, 5, 7, 13$ be a prime number such that i) $p_1(\mathcal{G}) = \text{GL}_2(\mathbb{Z}_\ell)$; and ii) $\ell \nmid \Delta' := 4A^3 + 27B^2$. Set $L = \mathbb{Q}(E[\ell])$, and let $d_0$ be a prime factor of $(\ell - 1)/\gcd(\ell - 1, 12)$.

Let $K'$ and $L'$ be the fields defined in (149) and (158), respectively (depending on $A, B$ and $\ell$). Let $H_1$ be a subspace of $\mathcal{H} = \text{Gal}(L'/L')$, of dimension $n_1$, that is a normal subgroup of $\text{Gal}(\overline{L}/(L')^{\nu_0})$, for some element $\sigma'_0$ of order $d_0$ in $\text{Gal}(L'/K')$.

Let $H_1 = \oplus_{v=1}^{n_1} C_v$ be the decomposition of representations of $(\sigma'_0)$ over $\mathbb{F}_\ell$, as in Lemma 8.

Let $f = \inf_{\mathcal{G}}(\overline{f})$ be a 1-cocycle in the Selmer group $\mathcal{S}[1](E/\mathbb{Q})$, where $\mathcal{G} = \text{Gal}((\overline{L}/\mathbb{Q})$ and $f \in H^1(\mathcal{G}, E[\ell])$.

Then, in the case where $\chi_v$ is the trivial character and $\text{Res}_{\mathcal{G}}^\overline{L}(C_v) \neq 0$, one has $\overline{f}(\text{Res}_{\mathcal{G}}^\overline{L}(\sigma)) = [\sigma - 1]\overline{Q}$, for any $\sigma \in C_v$, for some $\overline{Q} \in \mathcal{S}[1](E/\mathbb{Q})$ such that $[\ell]\overline{Q} \in E(K')$. The point $\overline{Q}$ depends on $\overline{f}$ and $C_v$.

**Proof.** Let $E$ have Weierstrass equation $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$. Set $\Delta' = 4A^3 + 27B^2$. Assume that $C_v$ has conjugacy action defined by the trivial character of $(\sigma'_0)$. Then, using Lemma 8 one can take a place $w'$ of $L'$ such that $\overline{H}'_w = C_v$, where $w'$ lies above a prime $p$ such that $p \nmid \Delta'\ell(\ell - 1)(\ell + 1)$. The condition $\text{Res}_{\mathcal{G}}^\overline{L}(C_v) \neq 0$ implies that $\overline{H}_w = \text{Res}_{\mathcal{G}}^\overline{L}(C_v)$, where $w$ is the place of $\overline{L}$ lying below $w'$.

The corollary now follows from Proposition 11. \[\square\]

**4.5 Proof of Theorem 5**

The following lemma will be crucial in the proof of the important intermediate result, Proposition 12, and the proof of Theorem 5.

**Lemma 9.** Let $E$ be an elliptic curve over $\mathbb{Q}$ without CM, of Weierstrass equation $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$. Given a prime number $\ell \neq 2, 3, 5, 7, 13$, set $L = \mathbb{Q}(E[\ell])$. Assume that: i) $\text{Gal}(L/\mathbb{Q}) \approx \text{GL}_2(\mathbb{F}_\ell)$; and ii) $\ell \nmid \Delta' := 4A^3 + 27B^2$. Let $K'$ and $K_2$ be the fields defined in (149) and (146), respectively (depending on $A, B$ and $\ell$). Then, one has:

- a) $\mathbb{Q}(\mu_\ell)/\mathbb{Q}$ is the maximal Abelian subextension of $L/\mathbb{Q}$, and $\text{Gal}(L/\mathbb{Q}(\mu_\ell))$ corresponds to $\text{SL}_2(\mathbb{F}_\ell)$ under $\overline{\rho}_\ell$;
- b) $L \cap K_2 = \mathbb{Q}$, and $(L \cap K_3)/\mathbb{Q}$ has degree 2;
- c) $L \cap K' \subseteq \mathbb{Q}(\mu_\ell)$;
- d) $L \cap K' = \mathbb{Q}(\mu_\ell) \cap K'$ has degree over $\mathbb{Q}$ dividing 12;
- e) let $d_0$ be a prime divisor of $(\ell - 1)/\gcd(\ell - 1, 12)$; then, there exists an element $\sigma_0 \in \text{Gal}(L/(L \cap K'))$, of order $d_0$, such that $\overline{\rho}_\ell(\sigma_0) = \begin{pmatrix} \lambda_0 & 0 \\ 0 & 1 \end{pmatrix}$, with
\( \lambda_0 \in \mathbb{F}_\ell^* \) (of order \( d_0 \)); in particular, \( \sigma_0 \) acts on \( X_{(\chi)} := \langle \frac{1}{0} \rangle \) through the character defined by \( \chi(\sigma_0) = \lambda_0 \), and acts on \( X_{(\chi)} := \langle \frac{0}{1} \rangle \) through the trivial character;

f) the element \( \tau \in \text{Gal}(L/\mathbb{Q}) \) defined by \( \tilde{\rho}_\ell(\tau) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \) belongs to the subgroup \( \text{Gal}(L/(L \cap K')) \); in particular, \( X_{(\chi)} \) is not stable under the action of \( \tau \);

g) the element \( \beta \in \text{Gal}(L/\mathbb{Q}) \) defined by \( \tilde{\rho}_\ell(\beta) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \), where \( \lambda \) has order \( \ell - 1 \) \( \text{gcd}(\ell - 1, 12) \), belongs to the subgroup \( \text{Gal}(L/(L \cap K')) \), and \( \beta - 1 \) defines an automorphism of \( E[\ell] \).

**Proof.** Step 1. Firstly, we claim that the maximal Abelian sub-extension of \( L/\mathbb{Q} \) is \( \mathbb{Q}(\mu_\ell) \).

Indeed, \( \mathbb{Q}(\mu_\ell)/\mathbb{Q} \) is an Abelian sub-extension of \( L/\mathbb{Q} \). Let \( \tilde{\rho}_\ell \) be the Galois representation of \( \text{Gal}(L/\mathbb{Q}) \) on \( E[\ell] \). Having assumed that \( \text{Gal}(L/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_\ell) \), it follows that \( \text{SL}_2(\mathbb{F}_\ell) = \text{Ker} \text{det}(\tilde{\rho}_\ell) \). But from the Weil pairing, one has \( \text{det}(\tilde{\rho}_\ell) = \psi_\ell \), where \( \psi_\ell \) is the cyclotomic character \([39, 1.2, \text{Example 2, pp. I-3-4}] \). Therefore, \( \text{Gal}(L/\mathbb{Q}(\mu_\ell)) = \text{Ker} \psi_\ell = \text{SL}_2(\mathbb{F}_\ell) \).

Now, let \( K/\mathbb{Q} \) be an Abelian extension, with \( L \supseteq K \supseteq \mathbb{Q}(\mu_\ell) \). Then, \( \text{Gal}(K/\mathbb{Q}(\mu_\ell)) \) corresponds to an Abelian quotient of \( \text{SL}_2(\mathbb{F}_\ell) \). Since this special linear group is a perfect group for \( \ell > 3 \) \([30, \text{p. 61}] \), it follows that \( \text{Gal}(K/\mathbb{Q}(\mu_\ell)) \) is trivial. Thus, \( K \) is equal to \( \mathbb{Q}(\mu_\ell) \), which completes the proof of part a).

**Step 2.** Let \( K_1 := \mathbb{Q}(\mu_4) \) as in equation \((\text{145})\). Also, as in equation \((\text{140})\), let \( K_2 = K_1(p_1^{1/2}, \ldots, p_\nu^{1/2}) \), where \( p_1, \ldots, p_\nu \) are the distinct prime factors other than \( \ell \) that are bounded by the constant \( C \) of Theorem \([6] \).

Then, the extension \( L \cap K_1 \) is an Abelian sub-extension of \( L/\mathbb{Q} \), and hence is contained in \( \mathbb{Q}(\mu_\ell) \), from step 1. From part a) of Corollary \([8] \) it follows that \( L \cap K_1 \subseteq \mathbb{Q}(\mu_\ell) \cap K_2 = \mathbb{Q} \).

**Step 3.** Next, the extension \((L \cap K_2)/\mathbb{Q}\) is an Abelian sub-extension of \( L \), since \( K_2/K_1 \) is Abelian, and \( L \cap K_1 = \mathbb{Q} \) from step 2. From steps 1 and 2, one must have \( L \cap K_2 \subseteq \mathbb{Q}(\mu_\ell) \cap K_2 = \mathbb{Q} \), which proves the first statement of part b).

**Step 4.** Since the Kummer extension \( K_3/K_2 \) has degree dividing 2, it follows that the extension \((L \cap K_3)/(L \cap K_2)\) has degree dividing 2. But \( L \cap K_2 = \mathbb{Q} \) from step 3. Thus, \((L \cap K_3)/\mathbb{Q}\) has degree 1 or 2. But \( L \cap K_3 \) contains the unique quadratic subextension of \( \mathbb{Q}(\mu_\ell) \). This proves the second statement of part b).

**Step 5.** The field \( K' \) is obtained by adjoining to \( K_3 \) various roots of cubic equations, as in equation \((\text{148})\). Since \( K'/\mathbb{Q} \) is a normal extension of degree dividing a power of 6, it follows that the extension \((L \cap K')/\mathbb{Q}\) has degree dividing a power of 6.

Since both \( K'/\mathbb{Q} \) and \( L/\mathbb{Q} \) are normal extensions, the extension \( L \cap K' \) is...
also normal over \( \mathbb{Q} \). We consider the compositum \( K'' := (L \cap K') \cdot \mathbb{Q}(\mu_\ell) \subseteq L \). Then, \( K'' \) is normal over \( \mathbb{Q} \), and hence over \( \mathbb{Q}(\mu_\ell) \). We set \( N := \text{Gal}(L/K'') \), which is a normal subgroup of \( \text{SL}_2(\mathbb{F}_\ell) \), using part a). From [135, Theorem 2, p. 62], there are only three cases if \( \ell \geq 5 \): \( N = 1, N = \{ \pm I \} \), or \( N = \text{SL}_2(\mathbb{F}_\ell) \), where \( J \) denotes the \( 2 \times 2 \) matrix over \( \mathbb{F}_\ell \). But the first two cases are ruled out, since the order of \( \text{SL}_2(\mathbb{F}_\ell)/\mathbb{N} \) would then be divisible by \( \ell \), whereas \( K''/\mathbb{Q}(\mu_\ell) \) has degree dividing a power of \( 6 \). It follows that \( K'' = \mathbb{Q}(\mu_\ell) \). This means that \( L \cap K' \subseteq \mathbb{Q}(\mu_\ell) \), which proves part c).

**Step 6.** From part c) of Corollary 8 having assumed that \( \ell > 2 \), the extension \( (\mathbb{Q}(\mu_\ell) \cap K')/\mathbb{Q} \) has degree dividing 12, which proves part d), making use of part c).

**Step 7.** Part e) is a consequence of part d) and the assumption that \( \text{Gal}(L/\mathbb{Q}) \) is the full linear group. Indeed, consider \( \sigma \in \text{Gal}(L/\mathbb{Q}) \) such that \( \overline{\rho}_\ell(\sigma) = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \), where \( \lambda \) is a generator of \( \mathbb{F}_\ell^* \). Let \( d_0 \) be a divisor of \( (\ell - 1)/\gcd(\ell - 1, 12) \). Then, one has \( \sigma_0 := \sigma^{(\ell - 1)/d_0} \in \text{Gal}(L/(L \cap K')) \), using part d), since \( \gcd(\ell - 1, 12) | (\ell - 1)/d_0 \). Then, the element \( \sigma_0 \) has order \( d_0 \), and \( \overline{\rho}_\ell(\sigma_0) \) is of the form \( \begin{pmatrix} \lambda_0 & 0 \\ 0 & 1 \end{pmatrix} \), where \( \lambda_0 \) has same order as \( \sigma_0 \).

**Step 8.** The element \( \tau \) has order \( \ell \), so \( \tau^\ell = 1 \in \text{Gal}(L/(L \cap K')) \). But, from part d), one has \( \tau^{12} \in \text{Gal}(L/(L \cap K')) \). As \( \gcd(\ell, 12) = 1 \), one concludes that \( \tau \in \text{Gal}(L/(L \cap K')) \), which proves part f).

**Step 9.** Let \( \lambda_1 \) have order \( \ell - 1 \) in \( \mathbb{F}_\ell^* \), and set \( \beta_1 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1 \end{pmatrix} \). Then, the element \( \beta := \beta_1^{\gcd(\ell - 1, 12)} \) belongs to \( \text{Gal}(L/(L \cap K')) \), using part d). Furthermore, since \( \ell \neq 2, 3, 5, 7, 13 \), the element \( \beta \) is non-trivial, and it then follows that \( \beta - 1 \) is an automorphism of \( E[\ell] \). Lastly, \( \overline{\rho}_\ell(\beta) \) is equal to \( \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \), where \( \lambda := \lambda_1^{\gcd(\ell - 1, 12)} \) has order \( (\ell - 1)/\gcd(\ell - 1, 12) \). This proves part g).

Lemma 19 and Corollary 10 play an important role in our proof of the following intermediate result.

**Proposition 12.** Let \( E \) be an elliptic curve over \( \mathbb{Q} \) without CM, of Weierstrass equation \( y^2 = x^3 + Ax + B \), where \( A, B \in \mathbb{Z} \). Let \( \ell \neq 2, 3, 5, 7, 13 \) be a prime number such that: i) \( \text{Res}(\mathcal{G}) = \text{GL}_2(\mathbb{Z}_\ell) \); and ii) \( \ell : \Delta' := 4A^3 + 27B^2 \). Set \( L = \mathbb{Q}(E[\ell]) \), and let \( K' \) and \( L' \) be the fields defined in \([149] \) and \([183] \), respectively.

Then, for any element of \( S^\ell(E/\mathbb{Q}) \) represented by 1-cocycle \( f \), one has a decomposition of the form:

\[
\text{Res}_{E'/E}^\ell(f) = g + \text{Inf}_{E'/E}^\ell(\tilde{h}),
\]

where \( E' := \text{Gal}(\overline{\mathbb{Q}}/K') \) and \( G' := \text{Gal}(L'/K') \approx \text{Gal}(L/(L \cap K')) \), \( g \in H^1(G', E(\overline{\mathbb{Q}})) \) splits in \( E(\overline{\mathbb{Q}}) \), and \( \tilde{h} \in H^1(G', E[\ell]) \).

**Proof. Step 1.** From Corollary 9 (assuming that \( \ell > 3 \)), \( f \in S^\ell(E/\mathbb{Q}) \) is of
the form $\text{Inf}^G_{\mathcal{O}}(f)$, for some $f \in H^1(\tilde{G}, E[\ell])$, where $\tilde{L} = L_{\mathcal{O}}$ is the class field defined in Lemma 17 (with $K = \mathbb{Q}$) and $\tilde{G} = \text{Gal}(\tilde{L}/\mathbb{Q})$.

Step 2. Let $y^2 = x^3 + Ax + B$ be a Weierstrass equation for $E$, with $A, B \in \mathbb{Z}$. We assume the non-CM case, with $\rho(\mathcal{O}) = \text{GL}_2(\mathbb{Z}_\ell)$, $\ell \nmid \Delta' := 4A^3 + 27B^2$, and $\ell \neq 2, 3, 5, 7, 13$. We consider the field $K'$ defined in (149). From part d) of Lemma 9 the extension $(L \cap K')/\mathbb{Q}$ has degree dividing 12.

Having assumed that $\ell \neq 2, 3, 5, 7, 13$, let $d_0$ be a prime factor of $(\ell - 1)/\text{gcd}(\ell - 1, 12)$. Applying part e) of Lemma 9, consider the element $\sigma_0' \in \text{Gal}(L'/K') \approx \text{Gal}(L/(L \cap K'))$ defined by $\tilde{\rho} \sigma_0' = \left( \begin{array}{cc} \lambda_0 & 0 \\ 0 & 1 \end{array} \right)$, where $\lambda_0$ is an element of order $d_0$ in the multiplicative group $\mathbb{F}_\ell^*$. Let $X_{(\chi)} = \langle \chi \rangle$ be the one-dimensional $\mathbb{F}_\ell$-subspace of $E[\ell]$ on which the automorphism $\sigma_0'$ acts through the character defined by $\chi(\sigma_0') = \lambda_0$. Let $X_{(1)} = \langle 1 \rangle$, be the one-dimensional $\mathbb{F}_\ell$-subspace of $E[\ell]$ on which $\sigma_0'$ acts through the trivial character.

One has the decomposition $E[\ell] = X_{(\chi)} \oplus X_{(1)}$.

Step 3. Given $\tilde{Q} \in E(\mathbb{Q})$ such that $[\ell]\tilde{Q} = P \in E(K')$, the 1-cocycle defined by $\tilde{g}(\sigma) := [\sigma - 1]\tilde{Q}$ belongs to $S^{[\ell]}(E/K')$. Furthermore, by construction, any such element of this Selmer group splits in $E(L')$. Let $S^{[\ell]}(E/K')_{\text{split}}$ be the subgroup of $S^{[\ell]}(E/K')$ consisting of such elements.

We define (with $L' = LK'$):

$$
\begin{align*}
G' &= \text{Gal}(\mathbb{Q}/K'); \\
H' &= \text{Gal}(\mathbb{Q}/L'); \\
\bar{G}' &= \text{Gal}(\bar{L}'/K'); \\
\bar{H}' &= \text{Gal}(\bar{L}'/L'); \\
G'' &= \text{Gal}(L'/K').
\end{align*}
$$

(194)

The $\mathbb{F}_\ell\langle \sigma_0' \rangle$-module $\bar{H}'$ admits a decomposition:

$$
\bar{H}' = \oplus_{i=0}^{d_0-1} \bar{H}'_{(\chi^i)},
$$

(195)

where $\langle \sigma_0' \rangle$ acts on $\bar{H}'_{(\chi^i)}$ through the character $\chi^i$ of the cyclic group $\langle \sigma_0' \rangle$, for $i = 0, 1, ..., d_0 - 1$.

Let then $T'$ be the image of the map:

$$
\begin{align*}
\phi' : S^{[\ell]}(E/K')_{\text{split}} \quad &\xrightarrow{\text{Rec}_{\mathbb{F}_\ell}(\bar{G}')} \quad S^{[\ell]}(E/L')^{\bar{G}'} \quad \xrightarrow{\text{Hom}(\bar{H}', E(\ell)/X_{(\chi)})} \quad S^{[\ell]}(E/L')^{\bar{G}'} \quad \xrightarrow{\approx} \quad \text{Hom}(\bar{H}'/(\oplus_{i=0}^{d_0-1} \bar{H}'_{(\chi^i)}), E(\ell)/X_{(\chi)}),
\end{align*}
$$

(196)

where the first map is the one of Proposition 6 (applied to $K = K'$), and the second map is induced by restriction of $G'$ to $\langle \sigma_0' \rangle$ and the projection $E(\ell) \to E(\ell)/X_{(\chi)}$. We have used the isomorphism $E(\ell)/X_{(\chi)} \approx X_{(1)}$ in the third map.

Then, from Pontryagin duality, one has an isomorphism:

$$
T' \approx \text{Hom}(\bar{H}'/H_1, E(\ell)/X_{(\chi)}),
$$

(197)
for some closed subspace $H_1 \supset \oplus_{i=1}^{d_0-1} \tilde{H}'(\chi^i)$ of $\tilde{H}'$.

**Step 4.** Since $X_{(\chi)}$ is stable under $\sigma_0^*$, it follows that $H_1$ is stable under conjugation by a lifting $\tilde{\sigma}_0'$ of $\sigma_0'$ in $\text{Gal}(\tilde{L}'/K')$. Indeed, with notation as above, the equality $[h-1]Q \in X_{(\chi)}$ for all $\tilde{Q}$ such that $[\ell]Q = \overline{P} \in E(K')$, implies that $[h-1](\overline{\sigma}_0)^{\ell}(\tilde{Q}) \in X_{(\chi)}$ for all such point $\tilde{Q}$, because $K'$ is normal over $Q$. But then, this implies that $\overline{\sigma}_0' h(\overline{\sigma}_0')^{-1} - 1 \tilde{Q} = \overline{\sigma}_0'[h-1](\overline{\sigma}_0')^{-1}(\tilde{Q}) \in \overline{\sigma}_0'(X_{(\chi)}) = X_{(\chi)}$ for all such point $\tilde{Q}$. Therefore, $\overline{\sigma}_0' h(\overline{\sigma}_0')^{-1} \in H_1$.

**Step 5.** We define:

$$
\begin{cases}
G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}); & \quad H = \text{Gal}(\overline{\mathbb{Q}}/L); \\
\widetilde{G} = \text{Gal}(L/\mathbb{Q}); & \quad \widetilde{H} = \text{Gal}(L/L); \quad \text{and} \\
G = \text{Gal}(L/Q).
\end{cases}
$$

(198)

Let then $I$ denote the image of the map

$$
\rho : S[\ell](E/Q) \overset{\text{Res}_{\ell}^G}{\longrightarrow} S[\ell](E/L)^G \overset{\text{Hom}(\tilde{H}, E[\ell]/X_{(\chi)})^{\sigma_0}}{\longrightarrow} \text{Hom}(\tilde{H}', E[\ell]/X_{(\chi)})^{\sigma_0}
$$

(199)

where the first map is the one of Proposition 6 (applied to $K = \mathbb{Q}$), and $\text{Res}_{\ell}^G$ denotes the natural projection $\tilde{H}' \to \tilde{H}$ of Galois groups. We have used the isomorphism $E[\ell]/X_{(\chi)} \approx X_{(\chi)}$ in the fourth map.

Then, from Pontryagin duality, one has an isomorphism:

$$
I \approx \text{Hom}(\tilde{H}'/H_2, E[\ell]/X_{(\chi)}),
$$

(200)

for some closed subspace $H_2 \supset \oplus_{i=1}^{d_0-1} \tilde{H}'(\chi^i)$ of $\tilde{H}'$.

**Step 6.** We claim that $I \subseteq I'$, equivalently $H_1 \subseteq H_2$.

Based on step 4, the subgroup $H_1$ is normal in the Galois group $\text{Gal}(\tilde{L}'/(L')^{\sigma_0})$, where $\sigma_0^*$ is constructed in step 2. From Lemma 8 one obtains a decomposition $H_1 = \oplus_{\nu=1}^{n_1} C_{\nu}$ of representations of $\langle \sigma_0^* \rangle$ over $\mathbb{F}_\ell$.

If the one-dimensional representation $C_{\nu}$ maps to 0 under the Galois projection $\text{Res}_{\ell}^{\tilde{L}'} : \tilde{H}' \to \tilde{H}$, then $C_{\nu}$ is contained in $H_2$, and there is nothing to prove.

If the one-dimensional representation $C_{\nu}$ is defined by the trivial character $\chi_{\nu}$ of $\langle \sigma_0^* \rangle$, and $\text{Res}_{\ell}^{\tilde{L}'}(C_{\nu}) \neq 0$, then Corollary 10 implies that $\tilde{f}(\text{Res}_{\ell}^{\tilde{L}'}(\sigma)) = [\sigma - 1]Q$, for any $\tilde{f} \in S[\ell](E/Q)$ and any $\sigma \in C_{\nu}$, for some $\tilde{Q} \in E(\overline{\mathbb{Q}})$ such that $[\ell]Q \in E(K')$, depending on $\tilde{f}$ and $C_{\nu}$. But then, the inclusion $C_{\nu} \subset H_1$ implies that $\tilde{f}(\text{Res}_{\ell}^{\tilde{L}'}(\sigma)) = 0$, for any $\tilde{f} \in S[\ell](E/Q)$ and any $\sigma \in C_{\nu}$. This means that $C_{\nu} \subset H_2$.  

50
If the one-dimensional representation $C_\nu$ is defined by a non-trivial character of $\langle \sigma_0' \rangle$, then $C_\nu < \oplus_{i=1}^{d_0} H'_{\chi(i)}$. But from step 5, one has the inclusion
\[ \oplus_{i=1}^{d_0} H'_{\chi(i)} \subseteq H_2, \]
which means that $C_\nu < H_2$.

Altogether, we conclude that $H_1 \subseteq H_2$.

Step 7. From Step 6, we have $I \subseteq I'$. So, let $f$ be in the Selmer group $S^{[\ell]}(E/Q)$. Then, $\varrho(f)$ satisfies:
\[ \varrho(f)(\sigma) = \varrho'(g)(\sigma) \mod X(\chi), \] 
valid for any $\sigma \in H'$, for some 1-coboundary $g$ of the form:
\[ \tilde{g}(\sigma) := [\sigma - 1]\tilde{Q}, \]
where $\tilde{Q} \in E(\overline{Q})$ such that $[\ell]\tilde{Q} = P \in E(K')$.

Define:
\[ h := \text{Res}_{G'}^G(f) - g. \] 
Thus, $\text{Res}_{H'}^G(h)$ maps to $0 \in \text{Hom}(H', E[\ell]/X(\chi))$. This means that $h$ maps the Galois group $H'$ into $X(\chi)$.

Step 8. Now, from Proposition 6 applied to $K'$, one has:
\[ \text{Res}_{H'}^G(h) \in \text{Hom}(H', E[\ell])^{G'}. \]
Therefore, for any $\sigma \in G'$ and $\tau \in H'$, one has:
\[ \sigma(h(\tau)) = h(\sigma\tau\sigma^{-1}) \in X(\chi), \] 
since $H'$ is a normal subgroup of $G'$. Thus, one must have $h(\tau) = 0$ for any $\tau \in H'$, since the one-dimensional subspace $X(\chi)$ is not stable under Galois action of $G'$. Indeed, one may take the element $\tau$ corresponding to the matrix
\[ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \]
of order $\ell$, as in part f) of Lemma 9.

It follows that $\text{Res}_{H'}^G(f) - g = 0$ on $H'$, so that
\[ \text{Res}_{H'}^G(f) - g = \text{Inf}_{G'}^G(h), \] 
for some $\tilde{h} \in H^1(G', E[\ell])$, as was to be shown.

Equipped with Lemma 9 and Proposition 12, we are now ready to prove Theorem 5.

Proof of Theorem 5. We show the inclusion:
\[ S^{[\ell]}(E/Q) \subseteq \text{Ker}\left\{ H^1(G, E[\ell]) \to H^1(G, E(\overline{Q})) \right\}. \] 

Let $\ell \neq 2, 3, 5, 7, 13$ be a prime number. Assuming that: i) $\rho_\ell(G) = \text{GL}_2(\mathbb{Z}_\ell)$, as well as the condition: ii) $\ell \nmid \Delta'$, Proposition 12 applies. Set $L := \mathbb{Q}(E[\ell])$ and $G := \text{Gal}(L/Q)$. Thus, for any $f \in S^{[\ell]}(E/Q)$, $\text{Res}_{H'}^G(f)$ is of the form
$g + \text{Inf}_{\mathbb{Q}}(h)$ on $G'$, for some $g \in H^1(G', E(\overline{Q}))$ that splits in $E(\overline{Q})$, and $h \in H^1(G', E[\ell])$.

Now, consider the element $\beta = \left( \begin{array}{cc} \lambda & 0 \\ 0 & \lambda \end{array} \right)$, where $\lambda \in \mathbb{F}_p^*$ has order $(\ell - 1)/\gcd(\ell - 1, 12)$. Then, from part g) of Lemma 9, $\beta$ is in the center of $\text{Gal}(L/(L \cap K')) \approx G'$, and $\beta - 1$ defines an automorphism of $E[\ell]$. Thus, from Sah’s Theorem [20, Theorem 5.1, p. 118], one has:

$$H^1(G', E[\ell]) = 0. \quad (208)$$

See [2] Proposition 19, p. 51] in the context of Abelian varieties. Note that [22, Theorem 11] on vanishing of Galois cohomology groups defined on torsion points does not apply here, since $\mathbb{Q}(\mu_\ell) \cap K'$ might be larger than $\mathbb{Q}$ (c.f. part d) of Lemma 9. On the other hand, Coates’ result [5, Lemma 10, p. 179] does apply, since $G' = \text{Gal}(L'/K')$ contains $\text{SL}_2(\mathbb{F}_\ell)$, as follows from parts a) and d) of Lemma 9.

Thus, one has for any $\sigma \in G'$:

$$f(\sigma) = [\sigma - 1](\overline{Q} + R), \quad (209)$$

where $\overline{Q} \in E(\overline{Q})$ and $R \in E[\ell]$. Lastly, one has for any $\sigma \in G$:

$$f(\sigma) - [\sigma - 1](\overline{Q} + R) = \text{Inf}_{\mathbb{Q}}(h'), \quad (210)$$

for some $h' \in H^1(\text{Gal}(K'/\mathbb{Q}), E(K'))$. But then, from [4, Corollary 10.2, p. 84], $H^1(\text{Gal}(K'/\mathbb{Q}), E(K'))$ is annihilated by $|\text{Gal}(K'/\mathbb{Q})| = n$. Therefore, one has for any $\sigma \in G$:

$$[n] \left( f(\sigma) - [\sigma - 1](\overline{Q} + R) \right) = [\sigma - 1]R', \quad (211)$$

for some $R' \in E(K')$. Thus, $[n]f$ maps to 0 in $H^1(G, E(\overline{Q}))$. Since, on the other hand, $f$ maps into $H^1(G, E(\overline{Q}))/\ell F$, the inclusion (207) is proved, as $\gcd(n, \ell) = 1$ by Proposition 3.

The other inclusion is clear since, for any place $v_0$ of $\mathbb{Q}$, the homomorphism $\text{Res}_{G_{v_0}}^G : H^1(G, E[\ell]) \to H^1(G_{v_0}, E(\overline{Q}_{v_0}))$ is the composition of homomorphisms $H^1(G, E[\ell]) \to H^1(G, E(\overline{Q})) \xrightarrow{\text{Res}_{G_{v_0}}^G} H^1(G_{v_0}, E(\overline{Q}_{v_0}))$. \qed

5 Examples

Recall that, given an elliptic curve $E$ over the rationals, there is, for each prime $\ell$, a Galois representation $\overline{\rho}_\ell : G \to \text{GL}_2(\mathbb{F}_\ell)$, where $G$ is the absolute Galois group of $\mathbb{Q}$, through Galois action on the $\ell$-torsion points of $E$. Then, one has an isomorphism $\text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \approx \overline{\rho}_\ell(G)$. In [40], the notation is $\phi_\ell(G)$.

Example 1. From [43] Proposition 1.4, p. 45], to each $j \in \mathbb{Q}$ corresponds a unique class of elliptic curves over $\mathbb{Q}$ up to isomorphism over $\mathbb{Q}$. For each
\( j_0 \in \mathbb{Q} \), the class of elliptic curves having \( j_0 \) as \( j \)-invariant is in one-to-one correspondence with \( \mathbb{Q}^*/(\mathbb{Q}^*)^{n(j)} \), where \( n(j) = 2, 4, 6 \) according to the cases \( j \neq 0, 1738, j = 1728 \), or \( j = 0 \), respectively [43, Corollary 5.4.1, p. 343]. From [43, p. 427], there are exactly 13 elliptic curves over \( \mathbb{Q} \), up to isomorphism over \( \mathbb{Q} \), having CM. Then, for each corresponding \( j \)-invariant (see [43, p. 295] for a list), there are infinitely many elliptic curves over \( \mathbb{Q} \) having CM (i.e., over a finite base field extension). Moreover, except for these 13 \( j \)-invariants, to any \( j \in \mathbb{Q} \) corresponds a class of elliptic curves without CM.

**Example 2.** Consulting [33 Table 1], we consider the elliptic curve from [27]:

\[
E : y^2 = x^3 + ax^2 + bx,
\]

with \( a = 1,692,602 = 2 \cdot 37 \cdot 89 \cdot 257 \) and \( b = -3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \). This equation corresponds to [43 p. 42]

\[
\begin{align*}
  a_1 &= a_3 = a_6 = 0; \\
  a_2 &= a; \quad a_4 = b; \\
  b_2 &= 4a; \quad b_4 = 2b; \quad b_6 = 0; \\
  b_8 &= -b^2; \\
  c_4 &= 16a^2 - 48b; \\
  c_6 &= -64a^3 + 36 \cdot 8ab. 
\end{align*}
\]

One computes the discriminant:

\[
\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = 16a^2b^2 - 64b^3 \\
= 16b^2(a^2 - 4b),
\]

and the \( j \)-invariant:

\[
j(E) = \frac{c_4^3}{\Delta} = \frac{(16)^2(a^2 - 3b)^3}{b^2(a^2 - 4b)}. \tag{215}\]

Furthermore, one has:

\[
\begin{align*}
  \Delta(E) &= 2^8 \cdot 3^2 \cdot 5^2 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29^2 \cdot 31^2 \cdot 37^3 \cdot p'; \\
  j(E) &= \frac{2^4 \cdot 3^3 \cdot 7^3 \cdot 61^3 \cdot 347^3 \cdot (p'')^3}{3^3 \cdot 5^3 \cdot 11^3 \cdot 13^3 \cdot 17^3 \cdot 19^3 \cdot 23^3 \cdot 29^3 \cdot 31^3 \cdot p''}, \tag{216}
\end{align*}
\]

where \( p' \) and \( p'' \) are the prime numbers 8, 420, 798, 017 and 812, 633, respectively. In particular, \( E \) is not semi-stable.

Thus, this elliptic curve has potential multiplicative reduction at \( p_0 = 3 \). Therefore, \( E \) has no CM. Moreover, from [27], \( E \) has rank at least 7 over \( \mathbb{Q} \). Therefore, Theorem 4 does not apply, whereas Theorem 5 does.

Moreover, \( p = 7 \) is the smallest prime number at which \( E \) has good reduction. From [44, Proposition 24, p. 314], one concludes that \( \hat{\rho}_\ell(G) = \text{GL}_2(F_\ell) \), whenever \( \ell \nmid \Delta(E), \ell \nmid \text{ord}_{p_0}(j(E)) = -2 \), and \( \ell > (\sqrt{\ell} + 1)^8 \). This means that Theorem 5 applies to \( E \) with \( \ell > 31, 210 \) other than \( p' \).
Pushing further these computations, let us consider the corresponding Tate’s curve [43, Theorem 14.1, p. 445] at \( p_0 = 3 \). One obtains an isomorphism \( \phi : \mathbb{Q}_{p_0}/(\mathbb{Z}/p_0\mathbb{Z}) \to \mathcal{E}(\mathbb{Q}_{p_0}) \), as \( \text{Gal}(\mathbb{Q}_{p_0}/K') \)-modules, for some unramified quadratic extension \( K'/\mathbb{Q}_{p_0} \). Here, \( q \) is defined in [43, p. 444]. One can easily check that \( \text{ord}_{p_0}(q) = 2 \), from the fact that \( \text{ord}_{p_0}(\Delta) = 2 \). Therefore, one obtains an isomorphism \( \phi : ((q^{1/\ell}) \times \mu_\ell)/(q) \to \mathcal{E}(\mathbb{Q}_{p_0}) \), as \( \text{Gal}(\mathbb{Q}_{p_0}/K') \)-modules. This implies that \( \tilde{\rho}_\ell(G) \) has a cyclic subgroup of order \( \ell \), for any prime \( \ell \neq 2 \).

Now, from [23, Theorem 3], if \( G = \tilde{\rho}_\ell(G) \neq \text{GL}_2(\mathbb{F}_\ell) \), then either \( G \) is in the normalizer \( N \) of a Cartan subgroup \( C \), or \( \ell \) is one of the exceptional primes \( 2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163 \). But \( C \) has index 2 in \( N \) [40, §2.2, p. 279], so that \( N \) has order coprime with \( \ell \). Therefore, one concludes that \( \ell \) is one of the exceptional primes.

Furthermore, note that \( E \) has potential good reduction at 2, since \( \text{ord}_2(\Delta(E)) = 8 \) and \( \text{ord}_2(\ell(E)) = 4 \). It follows from [40, a3], that the group \( \Phi_2 \) defined in [40, pp. 311–312], has cardinality 2, 3, 4, 6, 8, or 24. Recall that \( \Phi_2 \) is a quotient group of the inertia group \( I_2 \), and that it embeds into \( \text{GL}_2(\mathbb{F}_\ell) \), if \( \ell \geq 5 \) [40, pp. 311–312]. Now, the Weierstrass equation \( y^2 = x^3 + ax^2 + bx \) is minimal over \( \mathbb{Q}_2 \) since \( \text{ord}_2(\Delta) = 8 < 12 \). From Section 2.2 the curve \( E \) has good reduction over a finite extension \( K'/\mathbb{Q}_2 \) of degree with only 2 or 3 as prime factors. Moreover, one can make a change of variable of the form \( x = u^2x' + r \) and \( y = u^3y' + u^2sx' + t \), where \( u \in \mathcal{O}_K^*, r, s, t \in \mathcal{O}_K \) [43, Proposition 1.3, part a], p. 186, and obtain the discriminant \( u^{-12}\Delta \). Remark 1.1, p. 186]. It follows that \( v(u^{-12}\Delta) = -12v(u) + 8v(2) = 0 \), where \( v \) is the discrete valuation of \( K' \). This in turn implies that \( 3 | v(2) \), so that the ramification index of the extension \( K'/\mathbb{Q}_2 \) is divisible by 3. One concludes that \( \Phi_2 \) has order 3, 6, or 24 (see [40, p. 312]).

Thus, for \( \ell \neq 2 \), if \( \tilde{\rho}_\ell(G) \) is not the full linear group, then it is contained in a Borel subgroup of the linear group. Indeed, [40, Corollaire, p. 277] implies that \( \tilde{\rho}_\ell(G) \) contains a split Cartan semi-subgroup of the form \( \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix} \). Then, the condition \( \ell | \# \tilde{\rho}_\ell(G) \) for \( \ell \neq 2 \) implies that \( \tilde{\rho}_\ell(G) \) is either the full linear group, or else is contained in a Borel subgroup. See [40, Proposition 17 and remark a], p. 282. But then, assuming \( \ell \geq 5 \), [40, Proposition 23, part b], p. 313] implies that the divisor 3 of \( [\Phi_2] \) divides the order of \( (\mathbb{Z}/2^n\mathbb{Z})^* \), for some \( n \geq 1 \), which is not the case. So, actually, \( \tilde{\rho}_\ell(G) = \text{GL}_2(\mathbb{Z}_\ell) \), for all \( \ell \geq 5 \). See [40, 5.7.1, p. 315] for this argument. It follows from [41] that \( \rho_\ell(G) = \text{GL}_2(\mathbb{Z}_\ell) \), for all \( \ell \geq 5 \).

Next, we consider the Weierstrass equation of \( E \):

\[
E : y^2 = x^3 + Ax + B;
A = -27c_4 = -27(16a^2 - 48b);
B = -54c_6 = -54(-64a^3 + 36 \cdot 8ab);
\Delta'(E) = -2^{20} \cdot 3^{12} \cdot b^2(a^2 - 4b).
\]

We conclude from Theorem [5] that \( \text{III}(E/\mathbb{Q})_\ell \) vanishes at all primes \( \ell \), other
than the ones in the set:

\[ P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, p'\}. \]  

(218)

In particular, the smallest prime number for which Corollary 2 applies is \( \ell = 41 \). Thus, one has:

\[ \text{rank}(E/\mathbb{Q}) = \dim_{\mathbb{F}_4} S^{[41]}(E/\mathbb{Q}), \]  

(219)

since \( \text{III}(E/\mathbb{Q})[41] = 0 \), from Theorem 5, and \( E[41](\mathbb{Q}) = 0 \) from Mazur’s Theorem on torsion points.

Remark 5. The previous example solves the open problem mentioned in [44, Problem 2.16, p. 27] in the non-CM case.

Example 3. The following example was communicated to us by Professor C. Wuthrich. The non-CM elliptic curve of rank 0 defined by the cubic equation [52]:

\[ E : y^2 + xy = x^3 - x^2 - 332,311x - 73,733,731; \]
\[ \Delta(E) = -5,302,593,435,347,072 = -2^7 \cdot 23^{10}; \]
\[ c_4 = 15,950,937 = 3 \cdot 19 \cdot 23^3; \]
\[ j(E) = -\left(\frac{3 \cdot 19 \cdot 23^4}{2^7 \cdot 23^{10}}\right)^3 = -2^{-7} \cdot 3^3 \cdot 19^3 \cdot 23^2, \]  

(220)

has Shafarevich-Tate group of analytic order 25, which is denoted as \( \#\text{III}(E/\mathbb{Q})_{an} = 25 \). From [24], one concludes that \( \#\text{III}(E/\mathbb{Q}) = 25 \), as \( E \) has conductor \( N = 1058 < 5000 \), and rank \( r \leq 1 \).

Recall that \( \#\text{III}(E/\mathbb{Q})_{an} \) is based on BSD-2, and is computed as follows:

\[ \#\text{III}(E/\mathbb{Q})_{an} = \lim_{s \to 1} \frac{(s - 1)^{-r} L(E, s) (\#E_{tor}(\mathbb{Q}))^2}{\Omega 2^r R \prod_p c_p}, \]  

(221)

where \( L(E, s) \) denotes the \( L \)-series of \( E \), \( r \) is the rank of \( E/\mathbb{Q} \), \( \Omega \) is defined from the invariant differential, \( R \) is the elliptic regulator of \( E(\mathbb{Q})/E_{tor}(\mathbb{Q}) \), and \( c_p \) denotes \( \#E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p) \). See [43] pp. 451–452. In the example, based on the information available on the Website [52], this expression simplifies to:

\[ \#\text{III}(E/\mathbb{Q})_{an} = \frac{L(E, 1)}{\Omega} = 25, \]  

(222)

which is consistent with Cassels’ result [43, Theorem 4.14, p. 341].

Since \( E \) has multiplicative reduction at \( p_0 = 2 \), it follows that \( \tilde{\rho}_\ell(G) \) has a cyclic subgroup of order \( \ell \), for any prime \( \ell \neq 7 \). Indeed, the Tate’s curve \( E_q \), with \( \text{ord}_{p_0}(q) = 7 \), yields an isomorphism \( \phi : ((q^{1/\ell}) \times \mu_\ell) / (q) \tilde{\to} E[\ell](\mathbb{Q}_{p_0}) \), as \( \text{Gal}(\mathbb{Q}_{p_0}/K') \)-modules (where \( K' \) is the unramified extension of degree 2 over \( \mathbb{Q}_{p_0} \), since \( E \) has non-split multiplicative reduction at \( p_0 = 2 \)).
Thus, unless \( \ell \) is one of the exceptional primes 2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, or 163, one has \( \bar{\rho}_\ell(\mathcal{G}) = \text{GL}_2(\mathbb{F}_\ell) \) [24 Theorem 3].

Pushing further this example, observe that \( E \) has potential good reduction at 23. It follows from [40] a1), p. 312], that the group \( \Phi_{23} \) has cardinality 6, since \( 23 > 3 \) and \( \text{ord}_{23}(\Delta) = 10 \). Thus, for \( \ell \neq 7 \), if \( \bar{\rho}_\ell(\mathcal{G}) \) is not the full linear group, then it is contained in a Borel subgroup of the linear group. But then, it is reported that \( \bar{\rho}_\ell(\mathcal{G}) = \text{GL}_2(\mathbb{F}_\ell) \), for all \( \ell \neq 2, 3, 7 \), and hence, in particular for \( \ell = 5 \). It follows from [41] that \( \rho_\ell(\mathcal{G}) = \text{GL}_2(\mathbb{Z}_\ell) \), for all \( \ell \) except possibly 2, 3 and 7.

Actually, it is reported that \( \bar{\rho}_\ell(\mathcal{G}) = \text{GL}_2(\mathbb{F}_\ell) \) holds for any prime \( \ell \) [52].

Next, we consider the Weierstrass equation of \( E \):

\[
E : y^2 = x^3 + Ax + B; \\
A = -430675299 = -3^4 \cdot 19 \cdot 23^4; \\
B = -3,443,997,030,498 = -2 \cdot 3^6 \cdot 23^5 \cdot 367; \\
\Delta'(E) = 2^{15} \cdot 3^{12} \cdot 23^{10}. \tag{223}
\]

This yields the following Weierstrass equation, under the change of variable \((x, y) \mapsto (3^2x', 3^3y')\):

\[
E : y^2 = x^3 + A_1 x + B_1; \\
A_1 = -5,316,979 = -19 \cdot 23^4; \\
B_1 = -4724275762 = -2 \cdot 23^5 \cdot 367; \\
\Delta'_1(E) = 2^{15} \cdot 23^{10}. \tag{224}
\]

Thus, one has to discard the prime \( \ell = 23 \) \( \Delta'_1(E) \) in addition to the exceptional primes 2, 3, 5, 7, 13 (to avoid the exceptional condition \( (\ell-1)/\gcd(\ell-1, 12) = 1 \)). So, although \( \rho_\ell(\mathcal{G}) = \text{GL}_2(\mathbb{Z}_\ell) \) at \( \ell = 5 \) in this example, Theorem [5] does not predict the vanishing of \( \text{III}(E/\mathbb{Q})_\ell \) due to the exceptional condition \( (\ell-1) | 12 \).

Altogether, Theorem [5] predicts that \( \text{III}(E/\mathbb{Q})_\ell \) vanishes at any prime \( \ell \) other than 2, 3, 5, 7, 13, 23. In particular, the conclusion is consistent with BSD-2 in this example (i.e., \#\( \text{III}(E/\mathbb{Q}) = 25 \)).

**Example 4.** Consider the elliptic curve presented in Example 3:

\[
E : y^2 = x^3 + A_1 x + B_1; \\
A_1 = -5,316,979 = -19 \cdot 23^4; \\
B_1 = -4724275762 = -2 \cdot 23^5 \cdot 367; \\
\Delta'_1(E) = 2^{15} \cdot 23^{10}. \tag{225}
\]

This curve has no rational points over \( \mathbb{Q} \) [52].

Let us consider the prime \( p = 7 \). The reduced curve has Weierstrass equation:

\[
\bar{E}_p : y^2 = x^3 + 4x + 4, \tag{226}
\]
since \( y^2 = x^3 + A_1x + B_1 \) is a minimal Weierstrass equation for \( E \) at \( p \). The non-trivial points of the reduced curve modulo \( p \) are: \((0, \pm 2), (1, \pm 3), (3, \pm 1), (-3, 0), (-2, \pm 3)\). Thus, \( \tilde{E}(\mathbb{F}_p) \) has order \( 2 \cdot 5 \). We take \( \ell = 5 \), so that \( \ell \nmid \Delta' \).

Since \( p \nmid \Delta'(\ell-1)(\ell+1)\ell \), it follows that Theorem 6 applies.

The non-trivial points that have order \( \ell = 5 \) are the ones of the form \([2]P\) with \([2]P \neq O\): \((1, \pm 3), (-2, \pm 3)\). One may take the generator \((1, 3)\) of \( \tilde{E}(\mathbb{F}_p)_\ell \), so that \( \frac{\xi}{\ell} = 9 \) in Theorem 6. We may choose the radical \( y = \left(\frac{\xi}{\ell}\right)^{1/2} = 3 \), in this simple situation. Let then \( x \) be a root of \( X^3 + A_1X + B_1 = 3^2 \) in \( \mathbb{F}_p \) that maps to 1 in the residue field \( \mathbb{F}_p \), under an embedding \( \xi : \mathbb{Q}(x) \to \mathbb{F}_p \) followed by projection into the residue field of \( \mathbb{Q}(x) \) at some prime \( p \mid p \). By Hensel’s Lemma [21, p. 43], one has \( \mathbb{Q}(x)_p = \mathbb{Q}_p \). Any point of \( \tilde{E}[\ell](\mathbb{F}_p) \) can be lifted to a point of \( \mathbb{Q}(x) \), which is contained in the field \( K' \) defined in (149).

Then, for any point \( P_0 \in E(\mathbb{Q}_p) \), the point \([m]P_0\), where \( m = 2 \), projects to a point \( \tilde{P} \in \tilde{E}(\mathbb{F}_p) \) that can be lifted to a point \( P' \) with affine coordinates in \( K' \) (in fact, in \( \mathbb{Q}(x) \)). Thus, \([m]P_0 - \xi(P') \in E_1(\mathbb{Q}_p) \subset [\ell]E(\mathbb{Q}_p) \), so that \([m]P_0 - \xi(P') = [\ell]Q'' \), for some \( Q'' \in E(\mathbb{Q}_p) \). Since \( 3m - \ell = 1 \), one obtains: 

\[
P_0 = \xi(3P') + [\ell](3Q'' - P_0),
\]

and we set \( P = [3]P' \) and \( Q' = [3]Q'' - P_0 \).

Now, assume that \( P_0 \notin [\ell]E(\mathbb{Q}_p) \). Such a point exists since \( \#E(\mathbb{F}_p) = 2 \cdot \ell \) and \( E(\mathbb{Q}_p) \) projects onto \( \tilde{E}(\mathbb{F}_p) \). Then, one must have \( P \in E(\mathbb{Q}(x)) \setminus E(\mathbb{Q}) \). Indeed, since \( E(\mathbb{Q}) = 0 \) in this example, the case \( P \in E(\mathbb{Q}) \) would imply that \( P_0 \in [\ell]E(\mathbb{Q}_p) \). This issue was pointed out to us by Professor K. Rubin in an early draft of this paper. This motivated us to develop the results of Section 3. As the field \( K' \) is a finite extension over \( \mathbb{Q} \), our approach in Section 4 was then sufficient to prove Theorem 5.

A Ramification of the extension \( L_{\infty}/\mathbb{Q} \)

The following result is a consequence of a theorem of Sen [35] that was conjectured by Serre [33].

Proposition 13. Let \( E \) be an elliptic curve over the rationals. Let \( \ell \geq 3 \) be a prime number at which \( E \) has good reduction. Let \( L_n \) be the number field obtained by adjoining the affine coordinates of the \( \ell^n \)-torsion points of \( E \). Then, the different \( \mathfrak{D}_n \) of \( L_n/\mathbb{Q} \) satisfies the estimate:

\[
(\ell^n a) \subseteq \mathfrak{D}_n \subseteq (\ell^n a^{-1}),
\]

for all \( n \geq 1 \), for some integer \( a \).

Proof. We consider the following four cases, in view of [41] Proposition 10, p. 52.

Case A: \( p = \ell > 3 \) (and \( p \notin \Sigma_E \)). Consider the Galois group \( G \) of the infinite extension obtained by adjoining over \( \mathbb{Q} \) the affine coordinates of all \( \ell^n \)-torsion points of \( E \), where \( n \geq 1 \), as an \( \ell \)-adic Lie group. Let \( \{G_n\} \) be a Lie filtration
on $G$. For instance, one may take $G_n := \rho^{-1}_\ell(I + \ell^n \text{Mat}_{2 \times 2}(\mathbb{Z}_\ell))$. On the other hand, let $\{G(n)\}$ denote the upper numbering filtration on the Galois group $G$ corresponding to an embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{Q}_\ell$. Sen’s Theorem [35, Theorem, p. 48] gives the estimate:

$$G(ne - c) \subseteq G_n \subseteq G(ne + c),$$

(228)

valid for all $n$, for some constant $c$ (depending only on $G$, and hence on $E$ and $\ell$), where $e$ is the absolute ramification index of the ground field (so, $\mathbb{Q}_\ell$ here, and $e = 1$).

Now, let $\mathfrak{p}$ denote a prime ideal of $L_n$ lying above $\ell$. Then, using [41, Proposition 4, p. 64], one has:

$$\text{val}_{\mathfrak{p}}(\mathfrak{D}_n) = \sum_{u=0}^{u_0} (|G[u]| - 1),$$

(229)

where $G[u]$ denotes the lower numbering ramification groups, and $u_0$ is the largest integer $u$ such that $G[u]$ is non-trivial. One has:

$$\sum_{u=0}^{u_0} |G[u]| = |G[0]| \int_{u=0}^{u_0+1} \frac{1}{(G[0] : G[u])} \, du = |G[0]| \varphi(u_0 + 1),$$

(230)

where $\varphi$ denotes Herbrand’s function [41, p. 73]. From Sen’s Theorem, one has $n - c \leq \varphi(u_0 + 1) \leq n + c$.

Moreover, from [41, Exerc. 3 c), pp. 71-72], one has $u_0 \leq e_{\mathfrak{p}}/(\ell - 1)$, and hence $u_0 + 1 \leq e_{\mathfrak{p}}/\ell - 1$. Thus, we obtain:

$$\prod_{\mathfrak{p} | \ell} \mathfrak{p}^{e_{\mathfrak{p}}(n+c)} \subseteq \prod_{\mathfrak{p} | \ell} (\mathfrak{D}_n)_{\mathfrak{p}} \subseteq \prod_{\mathfrak{p} | \ell} \mathfrak{p}^{e_{\mathfrak{p}}(n-c-\ell/(\ell-1))},$$

(231)

that is:

$$(\ell^{n+c}) \subseteq \prod_{\mathfrak{p} | \ell} (\mathfrak{D}_n)_{\mathfrak{p}} \subseteq (\ell^{n-c-\ell/(\ell-1)}).$$

(232)

**Case B:** $p \neq \ell$ and $p \notin \Sigma_E$. Then, from the Criterion of Néron-Ogg-Shafarevich, the extension $L_n/\mathbb{Q}$ is unramified. Hence, using [41, Theorem 1, p. 53], one obtains:

$$\prod_{\mathfrak{p} | \ell} (\mathfrak{D}_n)_{\mathfrak{p}} = (1),$$

(233)

where $\mathfrak{p}$ stands for prime ideals of $L_n$.

**Case C:** $p \neq \ell$ and $p \in \Sigma_{E,p,g}$. Then, from Lemma [having assumed that $\ell > 3$], $E$ has good reduction over $L_1$. From the Criterion of Néron-Ogg-Shafarevich, the extension $L_n/L_1$ is unramified. Therefore, using [41] Proposition 8, p. 51, one has:

$$\prod_{\mathfrak{p} | \ell} (\mathfrak{D}_n)_{\mathfrak{p}} = \prod_{\mathfrak{p} | \ell} (\mathfrak{D}_1)_{\mathfrak{p}},$$

(234)

58
where \( p \) denotes prime ideals of \( L_1 \).

**Case D:** \( p \neq \ell \) and \( p \in \Sigma_{E,p,m} \). From Lemma \( \mathbf{1} \) (having assumed that \( \ell > 3 \)), \( E \) has multiplicative reduction over \( L_1 \). Considering Tate’s curves, the extension \( L_n/L_1 \) is at most tamely ramified. Therefore, one obtains:

\[
\prod_{p'|p} (\mathfrak{D}_1)_{p'} \leq \prod_{p'|p} (\mathfrak{D}_1)_{p'} \mathfrak{P}_{p'/(L_n/L_1)^{-1}} \leq \prod_{p'|p} (\mathfrak{D}_n)_{p'} \leq (1),
\]

(235)

using \([41] \) Proposition 13, p. 58]. Here, \( e_p(L_n/L_1) \) denotes the relative ramification index of \( \mathfrak{P} \) in \( L_n/L_1 \). Since \( e_p(L_n/L_1) \) is bounded by (in fact, divides) the ramification index \( e_p \) of \( \mathfrak{P} \) in \( L_n/Q \), the first inclusion holds, as \( (p) = \prod_{p'|p} \mathfrak{P}_{p'} \).

**Remark 6.** Let \( L_\infty \) be the infinite Galois extension obtained by adjoining the affine coordinates of all \( \ell^n \)-torsion points of \( E \), with \( n \geq 1 \). Consider the cyclotomic fields \( K_n = \mathbb{Q}(\mu_{\ell^n}) \), for \( n \geq 1 \). From the Weil pairing, one has the inclusions \( K_n \subset L_n \), for \( n \geq 1 \). From [21] Theorem 3, p. 75], one has:

\[
\mathfrak{D}_{K_n/Q} = (\ell^n \ell^{1/(\ell-1)}).
\]

(236)

This is consistent with the general results of Tate [47] §3.1, pp. 170–172. Based on Sen’s Theorem, one deduces that:

\[
\begin{align*}
(1) & \supseteq \mathfrak{D}_{L_n/K_n} = \mathfrak{D}_{L_n/Q} \mathfrak{D}_{K_n/Q}^{-1} \supseteq (\ell^n a)(\ell^{1/(\ell-1)}) \\
& = (a\ell^{1/(\ell-1)}) \supseteq (c),
\end{align*}
\]

(237)

for all \( n \geq 1 \), where \( c = a\ell \). See also [42] Remarque, p. 152] for a consequence of Sen’s Theorem.

Now, consider \( \alpha_n \) as in Proposition \( \mathbf{2} \) an element of the integer ring \( \mathfrak{O}_n \) of \( L_n = \mathbb{Q}(E[\ell^n]) \), with \( n \geq 1 \). Then, using Proposition \( \mathbf{2} \) and Remark 2, one has:

\[
\left| \frac{\text{tr}_n(\alpha_n)}{[L_n:Q]} \right|_{\ell} = \left| \frac{\text{tr}_n(\alpha_n)}{b\ell^n N} \right|_{\ell} \sim C_0 \ell^{n(N-1)} \left| \frac{\text{tr}_n(\alpha_n)}{\ell^n} \right|_{\ell} \leq 1,
\]

(238)

for some positive constant \( C_0 \). On the other hand, Proposition \( \mathbf{13} \) implies that:

\[
\left| a \left| \frac{\text{tr}_n(\alpha_n)}{\ell^n} \right|_{\ell} \right|_{\ell} \leq \left| \text{tr}_n(\alpha_n \mathfrak{D}_{L_n/Q}^{-1}) \right|_{\ell} \leq 1.
\]

(239)

But \( \lim_{n \to \infty} C_0 \ell^{n(N-1)} = \infty \), as \( N \geq 2 \), whereas \( |a|_{\ell} < \infty \). Thus, the precise form of \( \alpha_n \) in Proposition \( \mathbf{2} \) i.e., \( \alpha_n = \Delta'\ell^3/g^2(P) \), is at stake in this proposition concerning the \( \ell \)-adic norm, in addition to the strong condition \( \rho_\ell(\mathcal{G}) = \mathbf{GL}_2(\mathbb{Z}_\ell) \). For the Archimedean norm, one also needs the precise form of \( \alpha_n \), but not the condition on \( \rho_\ell(\mathcal{G}) \). But for the other non-Archimedean norms, the mere fact that \( \alpha_n \) is an integral element is sufficient, and this is the only trivial case. Thus, the result of Sen indicates that Proposition \( \mathbf{2} \) is by no
means elementary, as it seems. In particular, Serre’s Theorems on the Galois group of $L_{\infty}/\mathbb{Q}$, in the case of non-CM elliptic curves over the rationals, played an essential role in our proof of Theorems 5 and 6.

Acknowledgments

We are grateful to Professors Karl Rubin and Christian Wuthrich for their helpful comments on the first version of this article. Moreover, we acknowledge the helpful comments of Professor Rubin on drafts of the second version. The elliptic curve in Example 3 that was mentioned to us by Professor Wuthrich was very helpful in developing the second version of this work.

References

[1] E. Artin and J. T. Tate. *Class field theory*. New York: WA Benjamin, 1967.

[2] M. I. Bashmakov. The cohomology of Abelian varieties over a number field. *Uspekhi Mat. Nauk*, 27(6):25–66, 1972.

[3] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises. *J. Am. Math. Soc.*, 14(4):843–939, 2001.

[4] K. S. Brown. *Cohomology of groups*. Springer-Verlag New-York, 1982.

[5] J. Coates. An application of the division theory of elliptic functions to diophantine approximation. *Invent. Math.*, 11(2):167–182, 1970.

[6] J. Coates, Z. Liang, and R. Sujatha. The Tate-Shafarevich group for elliptic curves with complex multiplication II. *Milan J. Math.*, 78(2):395–416, 2010.

[7] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[8] N. D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. *Invent. Math.*, 89:561–568, 1987.

[9] I. B. Fesenko and S. V. Vostokov. *Local Fields and Their Extensions, 2nd edition*. American Mathematical Soc., 2002.

[10] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[11] K. Gruenberg. Profinite groups. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*, pages 116–127. Academic Press, 1967.
[12] D. R. Kohel and I. E. Shparlinski. On exponential sums and group generators for elliptic curves over finite fields. In *International Algorithmic Number Theory Symposium*, pages 395–404. Springer Berlin Heidelberg, 2000.

[13] V. A. Kolyvagin. Formal groups and the norm residue symbol. *Math. USSR Izvestija*, 15(2):289–348, 1980.

[14] V. A. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $\text{SH}(E, \mathbb{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR, Ser. Mat.*, 52:522–540, 1988.

[15] V. A. Kolyvagin. On the Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves. *Izv. Akad. Nauk SSSR, Ser. Mat.*, 52:1154–1180, 1988.

[16] V. A. Kolyvagin. On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves. *Proceedings of the International Congress of Mathematicians, Kyoto, Japan, 1990*, pages 429–436, 1990.

[17] V. A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. in Math.*, pages 435–483. Boston: Birkhäuser, 1991.

[18] V. A. Kolyvagin and D. Y. Logachev. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[19] V. A. Kolyvagin and D. Y. E. Logachev. Finiteness of sh over totally real fields. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 55(4):851–876, 1991.

[20] S. Lang. *Elliptic curves: Diophantine analysis*. Springer-Verlag Berlin, 1978.

[21] S. Lang. *Algebraic Number Theory*. Springer-Verlag New-York Berlin Heidelberg London Paris Tokyo, 1986.

[22] T. Lawson and C. Wuthrich. Vanishing of some Galois cohomology groups for elliptic curves. In D. Loeffler and S. Zerbes, editors, *Elliptic Curves, Modular Forms and Iwasawa Theory – Conference in honour of the 70th birthday of John Coates, 2015*, volume 188 of *Proceedings in Mathematics & Statistics*, pages 373–399. Springer, Cham, 2016.

[23] B. Mazur. Rational isogenies of prime degrees. *Invent. Math.*, 44(2):129–162, 1978.

[24] R. L. Miller. Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one. *LMS J. Comput. Math.*, 14:327–350, 2011.

[25] V. K. Murty. Modular elliptic curves. In V. K. Murty, editor, *Seminar on Fermat’s Last Theorem*, volume 17, pages 1–38. CMS Conference Proceedings, 1995.
[26] J. Neukirch. *Class Field Theory*. Springer-Verlag Berlin Heidelberg NewYork Tokyo, 1986.

[27] D. E. Penney and C. Pomerance. Three elliptic curves with rank at least seven. *Math. Comp.*, 39(131):965–967, 1975.

[28] B. Poonen. The Selmer group, the Shafarevich-Tate group, and the weak Mordell-Weil Theorem. [http://math.univ-lyon1.fr/~roblot/ihp/weakmw.pdf](http://math.univ-lyon1.fr/~roblot/ihp/weakmw.pdf) 1999.

[29] B. Poonen and M. Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. Math.*, 150(3):1109–1149, 1999.

[30] J. S. Rose. *A Course in Group Theory*. New York: Dover, 1994.

[31] K. Rubin. Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. *Invent. Math.*, 89(3):527–559, 1987.

[32] K. Rubin. Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. In *Arithmetic theory of elliptic curves*, pages 167–234. Springer Berlin Heidelberg, 1999.

[33] K. Rubin and A. Silverberg. Ranks of elliptic curves. *Bull. (New Series) of the AMS*, 39(4):455–474, 2002.

[34] R. Schoof. Elliptic curves over finite field and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–494, 1985.

[35] S. Sen. Ramification in p-adic Lie extensions. *Invent. math.*, 17:44–50, 1972.

[36] J.-P. Serre. Complex multiplication. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*, pages 292–296. Academic Press, 1967.

[37] J.-P. Serre. Local class field theory. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*, pages 128–161. Academic Press, 1967.

[38] J.-P. Serre. Sur les groupes de Galois attachés aux groupes p-divisibles. In *Proceedings of Conference on Local Fields, Driebergen, 1966*, pages 118–131. Springer Berlin Heidelberg, 1967.

[39] J.-P. Serre. *Abelian l-adic Representations and Elliptic Curves*. Benjamin, 1968.

[40] J.-P. Serre. Propriétés galoisienes des points d’ordre fini des courbes elliptiques. *Invent. math.*, 15:259–331, 1972.

[41] J.-P. Serre. *Local fields*. Springer-Verlag New-York, 1979.

[42] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, 54:323–401, 1981.
[43] J. H. Silverman. *The arithmetic of elliptic curves, 2nd edition*. Springer-Verlag New-York, 2009.

[44] W. A. Stein. The Birch and Swinnerton-Dyer Conjecture, a Computational Approach. [http://www.wstein.org/edu/2007/spring/bsd/bsd.pdf](http://www.wstein.org/edu/2007/spring/bsd/bsd.pdf), 2007.

[45] D. A. Suprunenko. *Matrix groups*, volume 45 of *Translation of Mathematical Monographs*. American Mathematical Society, 1976.

[46] J. T. Tate. Global class field theory. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*, pages 162–203. Academic Press, 1967.

[47] J. T. Tate. p-divisible groups. In *Proceedings of Conference on Local Fields, Driebergen, 1966*, pages 158–183. Springer Berlin Heidelberg, 1967.

[48] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. Math.*, 141(3):553–572, 1995.

[49] N. Tschebotareff. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Math. Ann.*, 95(1):191–228, 1926.

[50] A. Weil. *Basic Number Theory, Third edition*. Grundlehren der mathematischen Wissenschaften. Springer-Verlag New York Heidelberg Berlin, 1974.

[51] A. Wiles. Modular elliptic curves and Fermat’s Last Theorem. *Ann. Math.*, 141(3):443–551, 1995.

[52] C. Wuthrich. LMFDB - Elliptic Curve 1058.e1 (Cremona label 1058d1). [http://www.lmfdb.org/EllipticCurve/Q/1058/e/1](http://www.lmfdb.org/EllipticCurve/Q/1058/e/1) Last accessed: 2017-11-04.