Morrow *Res. Number Theory*
DOI 10.1007/s40993-016-0059-1

Research in Number Theory

RESEARCH Open Access

Selmer groups of twists of elliptic curves over K with K-rational torsion points

Jackson Salvatore Morrow*

*Correspondence: jmorrow4692@gmail.com
Department of Mathematics and Computer Science, Emory University, Atlanta, GA 30322, USA

Abstract

We generalize a result of Frey on Selmer groups of twists of elliptic curves over $\mathbf{Q}$ with $\mathbf{Q}$-rational torsion points to elliptic curves defined over number fields of small degree K with a K-rational torsion point. We also provide examples of elliptic curves coming from Zywina that satisfy the conditions of our Corollary D.

Keywords: Selmer groups, Quadratic twists of elliptic curves

1 Introduction

Let ℓ be an odd, rational prime and let E/K be an elliptic curve defined over a number field K. The K-rational points $E(K)$ form a finitely generated group by the Mordell-Weil theorem. Recall from [1, Section X.4] that we have the following exact sequence

$$0 \to E(K)/\ell E(K) \to \mathrm{Sel}_\ell(E,K) \to \text{Ш}(E,K)[\ell] \to 0,$$

where $\mathrm{Sel}_\ell(E,K)$ denotes the ℓ-Selmer group and $\text{Ш}(E,K)[\ell]$ is the ℓ-Shafarevich-Tate group. If $K = \mathbf{Q}$, then Frey [2] provides explicit examples of quadratic twist of elliptic curves over $\mathbf{Q}$ with $\mathbf{Q}$-rational points of odd, prime order ℓ whose ℓ-Selmer groups are non-trivial; a theorem of Mazur [3] implies that $\ell \in \{3,5,7\}$.

Theorem 1.1 ([2], Corollary) *Suppose that $E/\mathbf{Q}$ is an elliptic curve with a $\mathbf{Q}$-rational torsion point P of odd prime order ℓ, and suppose that P is not contained in the kernel of reduction modulo ℓ; in particular, this means that E is not supersingular modulo ℓ if* $\mathrm{ord}_\ell(j_E) \geq 0$. *Let $\widetilde{S}_E$ be the subset of odd primes dividing the conductor $N(E)$ of E defined by*

$$\widetilde{S}_E := \left\{p | N(E) : p \equiv -1 \pmod{\ell},\ \ell \nmid \mathrm{ord}_p(\Delta_E)\right\},$$

where j_E is the j-invariant of E and Δ_E is the discriminant of E. Suppose that $\widetilde{S}_E = \varnothing$. Suppose that $d \equiv 3 \pmod 4$ is a negative, square-free integer coprime to $\ell N(E)$ satisfying:

Springer Open

1. *if* $\mathrm{ord}_\ell(j_E) < 0$, *then* $\left(\frac{d}{\ell}\right) = -1$;
2. *if* $p|N(E)$ *is an odd prime, then*

$$\left(\frac{d}{p}\right) = \begin{cases} -1 & \text{if } \mathrm{ord}_p(j_E) \geq 0; \\ -1 & \text{if } \mathrm{ord}_p(j_E) < 0 \text{ and } E/\mathbf{Q}_p \text{ is a Tate curve}; \\ 1 & \text{otherwise.} \end{cases}$$

Then we have that $\mathrm{Sel}_\ell(E^d, \mathbf{Q})$ *is non-trivial if and only if the* ℓ*-torsion of the class group of* $\mathbf{Q}(\sqrt{d})$ *is non-trivial.*

Remark 1.2 Frey actually proved a more explicit double divisibility statement [2, Theorem] concerning the ℓ-Selmer group of E^d and ℓ-torsion of ray class groups, when $\widetilde{S}_E \neq \varnothing$.

In this paper, we generalize Frey's results [2, Theorem, Corollary] to number fields K of small degree. We show that for specific quadratic twists E^d, the order of the ℓ-torsion of some ray class group of $K(\sqrt{d})$ divides the order of $\mathrm{Sel}_\ell(E^d, K)$, and the order of $\mathrm{Sel}_\ell(E^d, K)$ divides the order of the ℓ-torsion of a different ray class group of $K(\sqrt{d})$ times the degree of some maximal abelian extension of exponent ℓ with prescribed ramification and Galois conditions (cf. Theorems A, B for precise statements and Remark 3.1 for a colloquial statement). These results allow us to give explicit applications to elliptic curves defined over $\mathbf{Q}$ (cf. Corollaries C, D), and we provide explicit examples of elliptic curves over $\mathbf{Q}$ satisfying Corollary D in Sect. 6. Finally, in Corollary E, we generalize Theorem 1.1 to number fields of small degree.

Remark 1.3 Frey's result [2, Theorem] has been used to produce twists of elliptic curves E^d over $\mathbf{Q}$ such that $Ш(E^d, \mathbf{Q})[\ell]$ is non-trivial. Most notably, Ono [4] utilized Frey's result to prove that for a large class of $E/\mathbf{Q}$ with torsion subgroup over $\mathbf{Q}$ isomorphic to $\mathbf{Z}/\ell\mathbf{Z}$ where $\ell \in \{3, 5, 7\}$, there are infinitely many negative square-free integers d for which

$$\mathrm{rk}(E^d, \mathbf{Q}) = 0 \quad \text{and} \quad \mathbf{Z}/\ell\mathbf{Z} \times \mathbf{Z}/\ell\mathbf{Z} \subset Ш(E^d, \mathbf{Q}).$$

Later, Balog and Ono [5] used a new type of result concerning the non-triviality of class groups of imaginary quadratic fields (cf. [5, Theorem 1]) and Frey's result to prove that for such $E/\mathbf{Q}$,

$$\#\left\{-X < D < 0 : L(E^d, 1) \neq 0,\ \mathrm{rk}(E^d, \mathbf{Q}) = 0,\ \text{and } \ell \mid \#Ш(E^d, \mathbf{Q})\right\} \gg_E \frac{X^{\frac{1}{2}+\frac{1}{2\ell}}}{\log^2 X}.$$

Frey's idea was to obtain information about $\mathrm{Sel}_\ell(E^d, \mathbf{Q})$ when $E(\mathbf{Q})$ contains an element of order ℓ. In particular, he studied the behavior of E over local fields $\mathbf{Q}_\ell$ and their algebraic closures $\overline{\mathbf{Q}}_\ell$. His work illustrated a deep relationship between ℓ-ranks of Selmer groups and class groups of finite Galois extensions of exponent ℓ. In this paper, we investigate the ℓ-Selmer rank in families of quadratic twists of elliptic curves E/K with K-rational points of odd prime order ℓ. We use Frey's proof as a blueprint for our own, but the techniques we utilize come from class field theory. That being said, many of his arguments go through *mutatis mutandis*.

In order to state our results, we first need to recall some facts concerning prime torsion of elliptic curves defined over number fields of small degree. We give a succinct summary of these results and refer the reader to [6] for a more detailed synopsis. Let $S(n)$ denote the set of primes that can arise as the order of a rational point on an elliptic curve defined over a number field of degree n and let $\mathsf{Primes}(n)$ denote the set of primes bounded by n. By Merel-Oesterlé's bound, we know that

$$S(n) \subseteq \mathsf{Primes}((3^{n/2}+1)^2).$$

The exact value of the set $S(n)$ is currently known for $n \le 5$, but reasonable good bounds on $S(6)$ and $S(7)$ are given in [7].

n	$S(n)$	References
1	$\mathsf{Primes}(7)$	[3]
2	$\mathsf{Primes}(13)$	[8]
3	$\mathsf{Primes}(13)$	[9]
4	$\mathsf{Primes}(17)$	[10]
5	$\mathsf{Primes}(19)$	[11]
6	$\subseteq \mathsf{Primes}(19) \cup \{37, 73\}$	[7]

One can also consider the subset $S_{\mathbf{Q}}(n) \subseteq S(n)$ corresponding to primes that can arise as the order of a rational point on an elliptic curve $E_K = E \times_{\mathbf{Q}} K$ where E is defined over $\mathbf{Q}$ and K is a number field of degree n. From [12], it is known that

$$S_{\mathbf{Q}}(n) \subseteq \mathsf{Primes}(13) \cup \{37\} \cup \mathsf{Primes}(2n+1),$$

and [12, Corollary 1.1] states that for $1 \le n \le 20$,

$$S_{\mathbf{Q}}(n) = \begin{cases} \mathsf{Primes}(7) & \text{for } n = 1, 2 \\ \{2, 3, 5, 7, 13\} & \text{for } n = 3, 4 \\ \mathsf{Primes}(13) & \text{for } n = 5, 6, 7 \\ \mathsf{Primes}(17) & \text{for } n = 8 \\ \mathsf{Primes}(19) & \text{for } n = 9, 10, 11 \\ \mathsf{Primes}(19) \cup 37 & \text{for } 12 \le n \le 20. \end{cases}$$

In this paper, we generalize the full double divisibility statement of [2, Theorem] to elliptic curves defined over small degree number fields K. We state explicit versions of our results, Theorems A, B and Corollary E, in Sect. 3 once we have established some notation.

1.1 Some remarks about the proofs

The problem of constructing elements in the Selmer group is a classical question with many avenues of approach. Frey's condition that the elliptic curve E/K have a K-rational point of odd prime power order $\ell > 3$ has two immediate consequences. First, the image of Galois under the mod ℓ representation is conjugate to

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \subset \mathrm{GL}_2(\mathbf{F}_\ell),$$

which will assist in our explicit description the Galois structure of splitting fields of ℓ-covers of E/K and the splitting fields of elements in $\mathrm{Sel}_\ell(E^d, K)$. The second is that we can immediately identify a quotient of $H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})[\ell])$, namely $H^1(\mathrm{Gal}(\overline{K}/K), \mu_\ell)$. Frey's (and our) proof relies on an analysis of cocyles in $H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})[\ell])$ and this fact will allow us to deduce local triviality in certain cases using Hilbert's Theorem 90. A laborious aspect of our proofs is the case by case analysis of how primes $\mathfrak{p}$ dividing $N(E)$ behave in the field $K(\sqrt{d}) \cdot K(E[\ell])$ where $d \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ yields the quadratic twist E^d of E and $K(E[\ell])$ is the ℓ-division field of E/K.

1.2 Organization of paper

In Sect. 2, we recall some classical facts from class field theory and algebraic number theory. In Sect. 3, we state our main results, Theorems A, B and Corollary E. In Sect. 4, we prove Theorem A, which yields a single divisibility statement. In Sect. 5, we prove the double divisibility statement of Theorem B by investigating the Galois structure of splitting fields of ℓ-covers of E/K and the splitting fields of elements $\mathrm{Sel}_\ell(E^d, K)$. Finally in Sect. 6, we provide explicit examples of elliptic curves over $\mathbf{Q}$ coming from [13] that satisfy the Corollary D.

2 Background and notation

Let L/K be a Galois extension of K, with ring of integers $\mathcal{O}_L$ and $\mathcal{O}_K$. For any finite prime $\mathfrak{P} \in \mathcal{O}_L$ lying over a prime $\mathfrak{p} \in \mathcal{O}_K$, let $D(\mathfrak{P})$ denote the decomposition group of $\mathfrak{P}$, let $I(\mathfrak{P})$ denote the inertia group of $\mathfrak{P}$ and let $\kappa' := \mathcal{O}_L/\mathfrak{P}$ and $\kappa = \mathcal{O}_K/\mathfrak{p}$ be the residue fields of characteristic $q = p^n$. In this note, we need a specific result concerning the Artin symbol and ramification theory for quadratic extensions L/K. For the definition of the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$, we refer the reader to [14, Chapter IV].

Lemma 2.1 *Let L/K be a quadratic extension, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, let $\mathfrak{P}$ denote some prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$, and let $\langle\delta\rangle = \mathrm{Gal}(L/K)$. Then:*

1. *$\mathfrak{p}$ is unramified and splits completely in $L \iff \left(\frac{L/K}{\mathfrak{p}}\right) = \mathrm{id}$,*
2. *$\mathfrak{p}$ is unramified and non-split in $L \iff \left(\frac{L/K}{\mathfrak{p}}\right) = \delta$,*
3. *$\mathfrak{p}$ is ramified in $L \iff \mathfrak{p}|\Delta_{L/K}$ where $\Delta_{L/K}$ denotes the relative discriminant of L/K.*

Proof Part (3) follows directly from the definition of the Artin symbol. Since $\mathfrak{p}$ is unramified, we know that $|D(\mathfrak{P})| = f$ where f is the inertia degree of $\mathfrak{P}$ over $\mathfrak{p}$. A prime $\mathfrak{p}$ splits completely in L if and only if the ramification index e of $\mathfrak{P}$ above $\mathfrak{p}$ and the inertia degree f of $\mathfrak{P}$ above $\mathfrak{p}$ are equal to 1. Hence,

$$|D(\mathfrak{P})| = [\kappa' : \kappa] = 1 \iff \mathrm{ord}\left(\frac{L/K}{\mathfrak{p}}\right) = 1 \iff \left(\frac{L/K}{\mathfrak{p}}\right) = \mathrm{id},$$

which proves (1). For (2), our assumptions and the fundamental identity tell us that $e = 1$ and $g = 1$ if and only if $f = 2$. Thus,

$$|D(\mathfrak{P})| = [\kappa' : \kappa] = 2 \iff \mathrm{ord}\left(\frac{L/K}{\mathfrak{p}}\right) = 2 \iff \left(\frac{L/K}{\mathfrak{p}}\right) = \delta.$$

□

In Theorem A, we use primitive Hecke characters to describe a subset of primes $\mathfrak{p}|N(E)$; we refer the reader to [14, Chapter VII, Section 6] for the definition of these characters.

Remark 2.2 Recall that there is a conductor-preserving correspondence between primitive Dirichlet characters of order ℓ and cyclic, degree ℓ number fields $F/\mathbf{Q}$. From [15, Theorem 3.7], the Dirichlet character χ corresponds to the fixed field F of $\ker\chi \subseteq \left(\mathbf{Z}/f_\chi\mathbf{Z}\right)^\times = \mathrm{Gal}(\mathbf{Q}(\zeta_{f_\chi})/\mathbf{Q})$. For any prime q,

$$\chi(q) = 0 \iff q \text{ ramifies in } F \quad \text{and} \quad \chi(q) = 1 \iff q \text{ splits in } F.$$

By class field theory, any primitive Hecke character χ_H of K of order ℓ determines a cyclic extension N/K of degree ℓ. Moreover, the set of primitive Hecke characters determining this cyclic extension equals $\{\chi_H, \chi_H^2, \dots, \chi_H^{\ell-1}\}$. These $\ell - 1$ Hecke characters have the same conductor $\mathfrak{f}$, and the determinant of L/K equals their product $\mathfrak{f}^{\ell-1}$ by the Hasse conductor-discriminant theorem. Thus for any prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$, we have that

$$\chi_H(\mathfrak{q}) = 0 \iff \mathfrak{q} \text{ ramifies in } N \quad \text{and} \quad \chi_H(\mathfrak{q}) = 1 \iff \mathfrak{q} \text{ splits in } N.$$

2.1 Notation

We set the following notation:

$$\begin{aligned}
K &:= \text{Galois number field,}\\
\ell &:= \text{odd, rational prime in } S(n)\setminus\{2,3\} \text{ such that } \ell \nmid \mathrm{cl}(K) \text{ and } \zeta_\ell \notin K,\\
L/K &:= \text{algebraic extension of } K,\\
\mathfrak{p} &:= \text{prime divisor of the rational prime } p \text{ in } \mathcal{O}_K,\\
\mathfrak{P} &:= \text{prime divisor of } \mathfrak{p} \text{ in } \mathcal{O}_L,\\
K_\mathfrak{p} &:= \text{completion of } K \text{ with respect to } \mathfrak{p},\\
L_\mathfrak{P} &:= \text{completion of } L \text{ with respect to } \mathfrak{P},\\
S &:= \text{finite set of primes of } \mathcal{O}_K,\\
M/L &:= \text{Galois extension with abelian Galois group of exponent } \ell.
\end{aligned}$$

More generally, lower case gothic font will denote a divisor of a rational prime of $\mathbf{Q}$, and similarly, upper case gothic font will denote a divisor of a prime of K.

Definition 2.3 M/L is said to be little ramified outside S if for primes $\mathfrak{p} \notin S$ and all $\mathfrak{P}_L|\mathfrak{p}$ one has

$$M \cdot L_\mathfrak{P}(\zeta_\ell) = L_\mathfrak{P}(\zeta_\ell)(\sqrt[\ell]{u_1}, \dots, \sqrt[\ell]{u_k})$$

with $k \in \mathbf{N}$ and $\mathrm{ord}_{\mathfrak{P}_L}(u_i) = 0$. Here ζ_ℓ is a ℓth root of unity, $u_1, \dots, u_k$ are elements in $L_\mathfrak{P}(\zeta_\ell)$, and $\mathrm{ord}_{\mathfrak{P}_L}$ is the normed valuation belonging to $\mathfrak{P}_L$.

If M/L little ramified outside S, then M/L is unramified at all divisors of primes $\mathfrak{p} \notin S \cup \{\mathfrak{l}\}$.

2.2 Notation

We set the following notation, which comes directly from [2]:

$$\begin{aligned}
L_S &:= \text{maximal abelian extension of exponent } \ell \text{of L which is}\\
&\quad\ \text{little ramified outside } S,\\
L_{S,u} &:= \text{maximal subfield of } L_S \text{ which is unramified outside of } S,\\
H_S(L) &:= \text{Galois group of } L_S/L,\\
H_{S,u}(L) &:= \text{Galois group of } L_{S,u}/L,\\
\mathrm{cl}_S(L)[\ell] &:= \text{order of } H_S(L),\\
\mathrm{cl}_{S,u}(L)[\ell] &:= \text{order of } H_{S,u}(L).
\end{aligned}$$

Remark 2.4 If $S = \emptyset$, we see that $\mathrm{cl}_{\emptyset,u}(L)$ is equal to the order of the subgroup of the divisor class group of L consisting of elements of order ℓ which we denote by $\mathrm{cl}(L)[\ell]$.

Now assume that L/K is normal with cyclic Galois group generated by an element γ of order $\ell - 1$. Take an extension $\widetilde{\gamma}$ to $L(\zeta_\ell)$. Let χ_ℓ be the cyclotomic character induced by the action of $\mathrm{Gal}(L(\zeta_\ell)/K)$ on $\langle\zeta_\ell\rangle$. Then $\chi_\ell(\widetilde{\gamma})$ is determined by

$$\widetilde{\gamma}(\zeta_\ell) = \zeta_\ell^{\chi_\ell(\widetilde{\gamma})}.$$

Let M be normal over K containing L such that $\mathrm{Gal}(M/L)$ is abelian of exponent ℓ. Then $\widetilde{\gamma}$ operates by conjugation on

$$\mathrm{Gal}(M(\zeta_\ell)/L(\zeta_\ell)) \cong \mathrm{Gal}(M/L),$$

and this operation does not depend on choice of $\widetilde{\gamma}$. Hence the subgroup

$$H(\chi_\ell) := \left\{\alpha \in \mathrm{Gal}(M/L) : \widetilde{\gamma}\alpha\widetilde{\gamma}^{-1} = \alpha^{\chi_\ell(\widetilde{\gamma})}\right\} \subseteq \mathrm{Gal}(M/L)$$

is well-defined. In the special case that $M = L_S$, we denote the order of $H_S(L)(\chi_\ell)$ by $\mathrm{cl}_S(L)_\ell(\chi_\ell)$.

Now we shall consider an elliptic curve E/K given by a Weierstrass equation $F(x, y) = 0$ with coefficients in $\mathcal{O}_K$ and minimal discriminant Δ_E. For any extension L/K, we denote the L-rational points of E (including ∞) by $E(L)$. Let χ_H be a primitive Hecke character of order ℓ and let

$$\widetilde{S}_E := \left\{\mathfrak{p}|N(E) : \chi_H(\mathfrak{p}) \neq 0, \mathrm{ord}_\mathfrak{p}(\Delta_E) \not\equiv 0 \pmod{\ell}\right\}$$
$$S_E := \{\mathfrak{p} \in \widetilde{S}_E : \mathrm{ord}_\mathfrak{p}(j_E) < 0\}.$$

Let $d \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ and denote the twist of E/K by E^d/K. Via the general theory of twists [1, Section X.2], we know that E^d is isomorphic to E over $K(\sqrt{d})$ but not over K. Let $G_K := \mathrm{Gal}(\overline{K}, K)$ denote the absolute Galois group. Let $\mathfrak{W}(E^d, K)[\ell]$ be the set of elements of order ℓ in the kernel of

$$\rho : H^1(G_K, E^d(\overline{K})) \longrightarrow \bigoplus_{\mathfrak{p}\text{ prime}} H^1(\mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p}), E^d(\overline{K_\mathfrak{p}})).$$

The group of elements of order ℓ in the Selmer group of E^d, denoted by $\mathrm{Sel}_\ell(E^d, K)$ is given as the pre-image of $\mathfrak{W}(E^d, K)[\ell]$ by the map

$$\alpha : H^1(G_K, E^d(\overline{K})[\ell]) \longrightarrow H^1(G_K, E^d(\overline{K})).$$

There are two main cases we need to consider:

Case 1 Assume that $\mathrm{ord}_\mathfrak{p}(j_E) \geq 0$. Then there is a finite extension N/K such that E has good reduction modulo all $\mathfrak{P}_N|\mathfrak{p}$ i.e., we find an elliptic curve $\widetilde{E}$ such that $\tilde{E}$ modulo $\mathfrak{P}_N$ is an elliptic curve over the residue field of $\mathfrak{P}_N$. $\widetilde{E}(\overline{N_\mathfrak{P}})$ contains a subgroup $\widetilde{E}_-(N_\mathfrak{P})$ consisting of points $(\widetilde{x}, \widetilde{y})$ with $\mathrm{ord}_{\mathfrak{P}_N}(\widetilde{x}) < 0$. $\widetilde{E}_-$ is the kernel of reduction modulo $\mathfrak{P}_N$, and $\mathrm{ord}_{\mathfrak{P}_N}(\widetilde{x}/\widetilde{y})$ is the level of $(\widetilde{x}, \widetilde{y})$. For ease of notation, we say that a point $(x, y) \in E(\overline{N_\mathfrak{P}})$ is in the kernel of the reduction modulo $\mathfrak{P}_N$ if its image $(\widetilde{x}, \widetilde{y}) \in \widetilde{E}_-(\overline{N_\mathfrak{P}})$.

Case 2 Assume that $\mathrm{ord}_\mathfrak{p}(j_E) < 0$. Then after an extension $L/K_\mathfrak{p}$ of degree ≤ 2, E becomes a Tate curve (via a theorem of Tate [1, Theorem C.14.1]); in particular, one has a Tate parametrization

$$\tau : \overline{L}^\times/\langle q\rangle \longrightarrow E(\overline{L})$$

where q is the $\mathfrak{p}$-adic period of E. One also has that

$$j_E = \frac{1}{q} + \sum_{i=0}^{\infty} a_i q^i \quad \text{with } a_i \in \mathbf{Z}$$

and the points of order ℓ in $E(\overline{L})$ are of the form $\tau(\zeta_\ell^\alpha(q^{\beta/\ell}))$ where $\alpha, \beta \in \{1, \ldots, \ell - 1\}$.

Definition 2.5 If F/K is a number field and $\mathfrak{P}_F|\mathfrak{p}$ we say that a point $(x, y) \in E(F_{\mathfrak{P}})$ is in the connected component of the unity modulo $\mathfrak{P}_F$ if it is of the form $\tau(u)$ with u a $\mathfrak{P}_F$-adic unit, and (x, y) is in the kernel of the reduction modulo $\mathfrak{P}_F$ if $u - 1 \in \mathfrak{P}_F$.

Remark 2.6 One should notice that if E is not a Tate curve over $K_\mathfrak{p}$ but over an extension of degree 2 of $K_\mathfrak{p}$, then for all points $P \in E(K_\mathfrak{p})$, $2P$ is in the connected component of unity modulo $\mathfrak{p}$.

3 Statement of results

As mentioned above, [2, Theorem] gives a double divisibility statement involving the ℓ-torsion of the Selmer group. First, we generalize his single divisibility to elliptic curves E/K defined over number fields K of finite degree with K-rational points of odd, prime order ℓ. Recall that $S(n)$ is the set of primes that can arise as the order of a rational point on an elliptic curve defined over a number field of degree n.

Theorem A *Let K be a Galois number field and choose $\ell \in S(n)\setminus\{2, 3\}$ such that $\ell \nmid \mathrm{cl}(K)$ and $\zeta_\ell \notin K$. Let E/K be an elliptic curve over K with a K-rational point P of order ℓ; let χ_H denote a primitive Hecke character of K with order ℓ; let $\mathfrak{q}$ denote a prime of $\mathcal{O}_K$ that lies above 2; and let $\mathfrak{l}$ denote a prime of $\mathcal{O}_K$ that lies above ℓ. Suppose that P is not contained in the kernel of reduction modulo $\mathfrak{l}$; in particular, this means that E is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_\mathfrak{l}(j_E) \geq 0$. Let S_E be the set of primes*

$$S_E := \left\{\mathfrak{p}|N(E)\colon \mathrm{ord}_\mathfrak{p}(\Delta_E) \not\equiv 0 \pmod{\ell},\ \chi_H(\mathfrak{p}) \neq 0,\ \text{and}\ \mathrm{ord}_\mathfrak{p}(j_E) < 0\right\}.$$

Suppose that $d \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ is negative,[1] coprime to $\mathfrak{l} \cdot N(E)$, and satisfies the following divisibility and Artin symbol conditions where $\langle\delta\rangle = \mathrm{Gal}(K(\sqrt{d})/K)$:

1. *if $\mathfrak{q}|N(E)$, then $\mathfrak{q}|\Delta_{K(\sqrt{d})/K}$;*
2. *if $\mathrm{ord}_\mathfrak{l}(j_E) < 0$, then $\left(\frac{K(\sqrt{d})/K}{\mathfrak{l}}\right) = \delta$;*
3. *if $\mathfrak{p}|N(E)$ is a prime of K with $\mathfrak{p} \notin S_E$, then*
   - *if $\mathrm{ord}_\mathfrak{p}(j_E) \geq 0$, then $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \delta$;*
   - *if $\mathrm{ord}_\mathfrak{p}(j_E) < 0$ and $E/K_\mathfrak{p}$ is a Tate curve, then $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \delta$;*
   - *otherwise, $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \mathrm{id}$.*

Then we have that the order of the ℓ-torsion of the S_E-ray class group of $K(\sqrt{d})$ divides the order of $\mathrm{Sel}_\ell(E^d, K)$. More precisely, the single divisibility statement holds:

$$\mathrm{cl}_{S_E,u}(K(\sqrt{d}))[\ell] \,\Big|\, \#\,\mathrm{Sel}_\ell(E^d, K)\,. \tag{1}$$

We also prove a stronger, more explicit version of Theorem A in the form of a double divisibility statement, which completely generalizes [2, Theorem].

Theorem B *Let K be a Galois number field of degree $n \leq 5$ such that $N_{K/\mathbf{Q}}(\mathfrak{q}) = 2$ for all $\mathfrak{q}|2$. Choose $\ell \in S(n)\setminus\{2, 3\}$ such that $\ell \nmid \mathrm{cl}(K)$ and $\zeta_\ell \notin K$. Let E/K be an elliptic curve over K with a K-rational point P of order ℓ; let χ_H denote a primitive Hecke*

[1] We say that $d \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ is negative if the image of d under each real embedding is negative.

character of K with order ℓ; let $\mathfrak{q}$ denote a prime ideal of $\mathcal{O}_K$ that lies above 2; and let $\mathfrak{l}$ denote a prime ideal of $\mathcal{O}_K$ that lies above ℓ. If $[K : \mathbf{Q}] = 5$ and $\ell = 5$, then we must make the added assumption that $(\ell)\mathcal{O}_K$ is not totally ramified. Suppose that P is not contained in the kernel of reduction modulo $\mathfrak{l}$; in particular, this means that E is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$. Let $\widetilde{S}_E$ and S_E be the sets of primes

$$\widetilde{S}_E := \left\{\mathfrak{p} | N(E) : \chi_H(\mathfrak{p}) \neq 0,\ \mathrm{ord}_{\mathfrak{p}}(\Delta_E) \not\equiv 0 \pmod{\ell}\right\},$$
$$S_E := \{\mathfrak{p} \in \widetilde{S}_E : \mathrm{ord}_{\mathfrak{p}}(j_E) < 0\}.$$

Suppose that $d \in \mathcal{O}_K^{\times}/(\mathcal{O}_K^{\times})^2$ is negative, coprime to $\mathfrak{l} \cdot N(E)$, and satisfies the following divisibility and Artin symbol conditions where $\langle \delta \rangle = \mathrm{Gal}(K(\sqrt{d})/K)$:

1. *if $\mathfrak{q} | N(E)$, then $\mathfrak{q} | \Delta_{K(\sqrt{d})/K}$;*
2. *if $\mathrm{ord}_{\mathfrak{l}}(j_E) < 0$, then $\left(\frac{K(\sqrt{d})/K}{\mathfrak{l}}\right) = \delta$;*
3. *if $\mathfrak{p} | N(E)$ is a prime of K with $\mathfrak{p} \notin S_E$, then*
   - *if $\mathrm{ord}_{\mathfrak{p}}(j_E) \geq 0$, then $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \delta$;*
   - *if $\mathrm{ord}_{\mathfrak{p}}(j_E) < 0$ and $E/K_{\mathfrak{p}}$ is a Tate curve, then $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \delta$;*
   - *otherwise, $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \mathrm{id}$.*

Then we have the following double divisibility

$$\mathrm{cl}_{S_E,u}(K(\sqrt{d}))[\ell] \,\Big|\, \#\,\mathrm{Sel}_\ell(E^d, K) \,\Big|\, \mathrm{cl}_{\widetilde{S}_E,u}(K(\sqrt{d}))[\ell] \cdot \mathrm{cl}_{S_E}(K')[\ell](\chi_\ell), \tag{2}$$

where K' is the subfield of $K(\sqrt{d}, \zeta_\ell)$ of index 2 containing neither ζ_ℓ nor $\sqrt{d}$.

Remark 3.1 In words, (2) states that the order of the ℓ-torsion of the S_E-ray class group of $K(\sqrt{d})$ divides the order of $\mathrm{Sel}_\ell(E^d, K)$, and the order of $\mathrm{Sel}_\ell(E^d, K)$ divides the order of the ℓ-torsion of the $\widetilde{S}_E$-ray class group of $K(\sqrt{d})$ times the degree of the maximal abelian extension K'' of K' of exponent ℓ unramified outside of $S_E \cup \{\mathfrak{l}\}$ such that the Galois group $\mathrm{Gal}(K'/K)$ acts on $\mathrm{Gal}(K''/K)$ by $\chi_\ell \varepsilon_d$, where ε_d is the character prescribing the Galois action on $\sqrt{d}$.

Once we have proved Theorems A, B, we can immediately extend the divisibility statements (1), (2) to elliptic curves E defined over $\mathbf{Q}$ by considering the values of $S_{\mathbf{Q}}(n)$.

Corollary C *Let $E/\mathbf{Q}$ be an elliptic curve defined over $\mathbf{Q}$. For some Galois number field K, suppose that E_K attains a K-rational point P of order ℓ where $\ell \in S_{\mathbf{Q}}(n) \setminus \{2, 3\}$ such that $\ell \nmid \mathrm{cl}(K)$ and $\zeta_\ell \notin K$. In keeping with the notation and assumptions of Theorem A, we can produce examples of quadratic twists E_K^d that satisfy the divisibility statement (1).*

Corollary D *Let $E/\mathbf{Q}$ be an elliptic curve defined over $\mathbf{Q}$; let E_K denote the base change of this curve to a Galois number field of degree $n \leq 20$ such that $N_{K/\mathbf{Q}}(\mathfrak{q}) = 2$ for all $\mathfrak{q}|2$. Choose $\ell \in S_{\mathbf{Q}}(n) \setminus \{2, 3\}$ such that $\ell \nmid \mathrm{cl}(K)$, $\zeta_\ell \notin K$, and the ramification index $e_{\mathfrak{l}}(K/\mathbf{Q})$ satisfies $1 > e_{\mathfrak{l}}(K/\mathbf{Q})/(\ell - 1) - 1$. Suppose that E_K attains a K-rational point P of order ℓ, then in keeping with the notation and assumptions of Theorem B, we can produce examples of quadratic twists E_K^d that satisfy the double divisibility statement (2).*

We can also generalize [2, Corollary], which we stated as Theorem 1.1.

Corollary E *Let* (E, ℓ, K, d) *be as in Theorem B or in Corollary D. If* $\widetilde{S}_E = \emptyset$*, then* $\mathrm{Sel}_\ell(E^d, K)$ *is non-trivial if and only if the* ℓ*-torsion of the class group of* $K(\sqrt{d})$ *is non-trivial, in particular*

$$\mathrm{cl}(K(\sqrt{d}))[\ell] \,\Big|\, \# \mathrm{Sel}_\ell(E^d, K) \,\Big|\, (\mathrm{cl}(K(\sqrt{d}))[\ell])^2.$$

Remark 3.2 In his Ph.D. thesis [16], Mailhot was able to recover and sharpen [[2], Theorem] for elliptic curves defined over $\mathbf{Q}$ using purely cohomological methods. His refinement comes from prescribing a splitting behavior of primes above K' instead of just a non-ramified condition. We remark that our methods and results are disjoint, however, we believe that [16, Corollary 2.17] can be generalized to elliptic curves defined over number fields K, using Theorem B.

4 Proof of Theorem A

In this section, we prove the divisibility statement (1). Before we proceed, we make a remark about some of the prime assumptions of Theorem A.

Remark 4.1 (Prime assumptions) If $\mathrm{ord}_{\mathfrak{p}}(j_E) < 0$, then we have that $E/K_{\mathfrak{p}}$ has a Tate parametrization. The second condition $\mathrm{ord}_{\mathfrak{p}}(\Delta_E) \not\equiv 0 \pmod{\ell}$ assists us in Lemma 4.2. In short, it allows us to understand ramification in the ℓ-division field of $E_{K_{\mathfrak{p}}}$. The final condition $\chi_H(\mathfrak{p}) \neq 0$ is used in Lemma 4.3 and is an analogue of Frey's condition that $p \equiv -1 \pmod{\ell}$. Moreover, this condition allows us to deduce, using Remark 2.2, that for a cyclic extension M_2/K of degree ℓ, $\mathfrak{p}$ is unramified in M_2.

The first step in the proof is to exhibit an element in $\mathrm{Sel}_\ell(E^d, K)$.

Lemma 4.2 *Let* $\ell > 3$ *be a rational prime; let* M/K *be a non-abelian Galois extension of degree* 2ℓ *containing* $K(\sqrt{d})$ *that is unramified over this field outside of* S_E*; let* α *be a generator of* $\mathrm{Gal}(M/K(\sqrt{d}))$*; and let* ϕ *the element in* $H^1(\mathrm{Gal}(M/K), E^d(M)[\ell])$ *determined by* $\phi(\alpha) = P$*, where* P *is a* K*-rational point of order* ℓ*. Then* ϕ *is an element of* $\mathrm{Sel}_\ell(E^d, K)$*.*

Proof First, we need to show that there exists some element

$$\phi \in H^1(\mathrm{Gal}(M/K), E^d(M)[\ell])$$

whose restriction $\overline{\phi}$ to $\mathrm{Gal}(M/K(\sqrt{d})) = \langle \alpha \rangle$ is given by $\overline{\phi}(\alpha) = P$. We identify $E^d(M)[\ell]$ with $E(M)[\ell] = \langle P \rangle$. Since $E^d(K(\sqrt{d}))[\ell] = \langle P \rangle$ and $\delta(P) = -P$ where $\langle \delta \rangle = \mathrm{Gal}(K(\sqrt{d})/K)$, we have invariance of ϕ under δ from the fact that $\delta\alpha\delta = \alpha^{-1}$. Since

$$H^1(\mathrm{Gal}(M/K), E^d(M)[\ell]) = H^1(\mathrm{Gal}(M/K(\sqrt{d})), E^d(M)[\ell])^\delta,$$

our assertions follows.

Hence it remains to show that $\overline{\phi}$ is locally trivial when regarded as an element of

$$H^1(\mathrm{Gal}(M/K(\sqrt{d})), E^d(M)).$$

We may restrict ourselves to primes $\mathfrak{P}_M | \mathfrak{l} \cdot N(E)$. By condition (1) of Theorem A, the divisors of $\mathfrak{q}$ are unramified in $M/K(\sqrt{d})$ if $\mathfrak{q}|N(E)$, and hence we may assume that $\mathfrak{P}_M \nmid \mathfrak{q}$.

Assume that $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \delta$. In this case, $\mathfrak{P}_M$ is either fully ramified or decomposed (since M/K is non-abelian). So assume that $\mathfrak{P}_M$ is fully ramified and divides $\mathfrak{p}$. Then

$\mathfrak{p} \in S_E$ and in particular $\mathfrak{p} \neq \mathfrak{l}$ and $\mathrm{ord}_{\mathfrak{p}}(\Delta_{E_K}) \not\equiv 0 \pmod{\ell}$. We claim that $E^d/K_{\mathfrak{p}}(\sqrt{d})$ is a Tate curve and that P is contained in the connected component of the unity over $K_{\mathfrak{p}}(\sqrt{d})$ corresponding to an ℓ^{th} root of unity ζ_ℓ e.g., $P = \tau(\zeta_\ell^\alpha)$ where τ is the Tate parametrization and $\alpha \in \{1, \ldots, \ell - 1\}$.

The fact that $E^d/K_{\mathfrak{p}}(\sqrt{d})$ is a Tate curve follows since $\mathfrak{p} \in S_E$ and so $\mathrm{ord}_{\mathfrak{p}}(j_E) < 0$. Since $\mathrm{ord}_{\mathfrak{p}}(\Delta_E) \not\equiv 0 \pmod{\ell}$, we know that adjoining $q^{1/\ell}$ to $K_{\mathfrak{p}}(\sqrt{d})$, where q is the $\mathfrak{p}$-adic period of E, is a non-trivial extension. Under the Tate parametrization τ, we have that torsion points of order ℓ in $E^d(K_{\mathfrak{p}}(\sqrt{d}))[\ell]$ are of the form $\tau(\zeta_\ell^\alpha q^{\beta/\ell})$ where $\alpha, \beta \in \{1, \ldots, \ell - 1\}$. Since P is a point of order ℓ defined over $K_{\mathfrak{p}}(\sqrt{d})$, we know that $\zeta_\ell^\alpha \in K_{\mathfrak{p}}(\sqrt{d})$ for some $\alpha \in \{1, \ldots, \ell - 1\}$ and that

$$\tau^{-1}(P) = \zeta_\ell^\alpha q^{\beta/\ell} \in K_{\mathfrak{p}}(\sqrt{d}).$$

In order for $\zeta_\ell^\alpha q^{\beta/\ell} \in K_{\mathfrak{p}}(\sqrt{d})$, we must have that $\beta = 0$ since q is not an $1/\ell^{\text{th}}$ power. Thus, $\tau^{-1}(P) = \zeta_\ell^\alpha$, and hence P is contained in the connected component of the unity over $K_{\mathfrak{p}}(\sqrt{d})$ corresponding to an ℓ^{th} root of unity ζ_ℓ. Since $M_{\mathfrak{P}}/K_{\mathfrak{p}}(\sqrt{d})$ is cyclic of degree ℓ, we have that $\zeta_\ell = \alpha x/x$ for some $x \in M_{\mathfrak{P}}$ by Hilbert' Theorem 90, and therefore, $\overline{\phi}$ is trivial when considered in $H^1(\mathrm{Gal}(M_{\mathfrak{P}}/K_{\mathfrak{p}}), E^d(M_{\mathfrak{P}}))$.

Next assume that $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \mathrm{id}$ and $\mathfrak{p} \neq \mathfrak{l}$. Then $\mathrm{ord}_{\mathfrak{p}}(j_E) < 0$ and E is a Tate curve over $K_{\mathfrak{p}}$, and so again P corresponds to some ℓ^{th} root of unity ζ_ℓ under the Tate parametrization of $E = E^d$ over $K_{\mathfrak{p}}(\zeta_\ell)$ and hence $\overline{\phi}$ is split by $K_{\mathfrak{p}}(\zeta_\ell)$ as seen above. But since the degree of $K_{\mathfrak{p}}(\zeta_\ell)$ over $K_{\mathfrak{p}}$ is prime to ℓ, $\overline{\phi}$ is split over $K_{\mathfrak{p}}$ already, and thus $\overline{\phi}$ is locally trivial.

There is one remaining case: $\mathfrak{p} = \mathfrak{l}$ and $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$. Let $\mathfrak{L}_M | \mathfrak{l}$. By the assumption, M/K is unramified at $\mathfrak{L}_M$, and we can find a normal extension N/K of degree prime to ℓ such that E has good reduction modulo all primes $\mathfrak{L}_N | \mathfrak{l}$. In particular, we may take $N = K(\zeta_{12}, \sqrt[12]{\mathfrak{l}})$. Now

$$H^1(\mathrm{Gal}(M_{\mathfrak{L}} \cdot N/K_{\mathfrak{l}} \cdot N), E^d(M_{\mathfrak{L}} \cdot N)) = 0$$

since the reduction of E^d modulo $\mathfrak{L}$ is good and $M_{\mathfrak{L}}N/K_{\mathfrak{l}}N$ is unramified, and hence it follows that

$$H^1(\mathrm{Gal}(M_{\mathfrak{L}}/K_{\mathfrak{l}}), E^d(M_{\mathfrak{L}})) = 0.$$

□

Next, we look at the action of δ on $H_{S_E,u}(K(\sqrt{d}))$.

Lemma 4.3 *The generator* $\langle\delta\rangle = \mathrm{Gal}(K(\sqrt{d})/K)$ *acts as* $-\mathrm{id}$ *on the Galois group* $H_{S_E,u}(K(\sqrt{d}))$.

Proof We may write

$$H_{S_E,u}(K(\sqrt{d})) = H^- \oplus H^+$$

where H^- is the part where δ acts as $-$ id, and H^+ the part with $\delta = \mathrm{id}$. Let $\widetilde{M} := M_{S_E,u}^{H^-}$, which is the fixed field of $M_{S_E,u}$ by H^-. Assume that M_1 is a subfield of $\widetilde{M}$ that is cyclic over $K(\sqrt{d})$. Hence M_1/K is cyclic of degree $2 \cdot [M_1{:}K(\sqrt{d})]$. Let M_2 be the cyclic extension of K with degree $[M_1 : K(\sqrt{d})]$ contained in M_1. Then M_2 is unramifed outside of S_E. For $\mathfrak{p} \in S_E$, we have that $\chi_H(\mathfrak{p}) \neq 0$. Since $[M_2{:}K] | \ell$ and $\ell \nmid \mathrm{cl}(K)$, it follows that M_2 is not contained in the Hilbert class field of K and is unramified at all primes K. Thus, we have that $M_2 = K$, $M_1 = K(\sqrt{d})$ and hence $\widetilde{M} = K(\sqrt{d})$. □

Proof of Theorem A The divisibility of $\#\,\mathrm{Sel}_\ell(E^d,K)$ by $\mathrm{cl}_{S_E,u}(K(\sqrt{d}))[\ell]$ follows from Lemmas 4.2, 4.3 since our element $\phi\in\mathrm{Sel}_\ell(E^d,K)$ is induced by $\alpha\in\mathrm{Gal}(M/K(\sqrt{d}))$ and the action of $\langle\delta\rangle$ on $H_{S_E,u}(K(\sqrt{d}))$ does not affect the order of α when considered as an element of $H_{S_E,u}(K(\sqrt{d}))$.

5 Proof of Theorem B

Before we proceed with a proof of Theorem B, we wish to shed some light onto our assumptions. In general, our hypotheses allow us to control the ramification in cyclic extensions of $K(\sqrt{d})$.

Remark 5.1 (Field assumptions) We assume that our field K is a number field of degree $n\leq 5$ such that $N_{K/\mathbf{Q}}(\mathfrak{q})=2$ for all $\mathfrak{q}|2$ and that for some $\ell\in S(n)\setminus\{2,3\}$, $\ell\nmid\mathrm{cl}(K)$ and $\zeta_\ell\notin K$. The degree and norm condition appear in Lemma 5.5 and allow us to deduce ramification conditions on prime divisors $\mathfrak{Q}_M|\mathfrak{q}$ where M_1/K is cyclic. The condition that $\ell\nmid\mathrm{cl}(K)$ implies that there does not exist an extension M_2/K of degree ℓ contained in the Hilbert class field of K; once again this gives us a ramification consequence. The assumption that $\zeta_\ell\notin K$ is subtle, but it allows for more ramification possibilities since Kummer theory does not restrict cyclic extensions. The final condition that $e_{\mathfrak{l}}(K/\mathbf{Q})\neq 5$ when $[K{:}\mathbf{Q}]=5$ and $\ell=5$ is due to a deep result of Katz [17] concerning the injectivity of ℓ-torsion under the reduction map; the assumption $1>e_{\mathfrak{l}}(K/\mathbf{Q})/(\ell-1)-1$ from Theorem D is the general condition. This assumption allows us to use the fact that prime to 2 torsion will inject under the reduction map.

To prove Theorem B, it suffices to prove the divisibility statement

$$\#\,\mathrm{Sel}_\ell(E^d,K)\,\Big|\,\mathrm{cl}_{\widetilde{S}_E,u}(K(\sqrt{d}))[\ell]\cdot\mathrm{cl}_{S_E}(K')[\ell](\chi_\ell)\,.$$

To begin, we discuss the Galois structure of the ℓ-division field of elliptic curves E/K from Theorem B.

5.1 Galois structure of splitting fields of ℓ-covers of E

We want to determine the Galois group structure of splitting fields of elements in $H^1(G_K,E(\overline{K})[\ell])$ for elliptic curves having a K-rational point P of order ℓ. Recall that $\zeta_\ell\notin K$. Denote the ℓ-division field by $K(E[\ell])$; this is the field obtained by adjoining the x,y coordinates of all points of order ℓ of E to K. Then $K(E[\ell])$ is a Galois extension of K containing $K(\zeta_\ell)$, and it is cyclic over $K(\zeta_\ell)$ of degree dividing ℓ. From this point on, we shall abbreviate $E(\overline{K})[\ell]$ with $E[\ell]$, and similarly for $E^d[\ell]$.

Lemma 5.2 *The Galois group $K(E[\ell])/K$ is generated by two elements $\overline{\gamma},\overline{\varepsilon}$ with $\overline{\gamma}^{\ell-1}=\mathrm{id}$, $\overline{\varepsilon}^{\ell}=\mathrm{id}$, $\overline{\gamma}|K(\zeta_\ell)$ generates $K(\zeta_\ell)/K$, and $\overline{\gamma\varepsilon\gamma}^{-1}=\overline{\varepsilon}^{\chi_\ell(\overline{\gamma})^{-1}}$.*

Proof Choose a base of the form $\{P,Q\}$ of $E[\ell]$ such that for $\sigma\in\mathrm{Gal}(K(E[\ell])/K)$ the action of σ on $E[\ell]$ induces the matrix

$$\rho_\sigma=\begin{pmatrix}1&b\\0&a\end{pmatrix}\in\mathrm{GL}_2(\mathbf{F}_\ell),$$

with $a=\det(\rho_\sigma)\equiv\chi_\ell(\sigma)\mod\ell$. Now we choose $\overline{\gamma}$ such that

$$\rho_{\overline{\gamma}}=\begin{pmatrix}1&0\\0&w\end{pmatrix}\in\mathrm{GL}_2(\mathbf{F}_\ell).$$

with w a generator of $(\mathbf{Z}/\ell\mathbf{Z})^\times$. Also, we pick $\overline{\varepsilon} = \mathrm{id}$ if $K(E[\ell]) = K(\zeta_\ell)$. If $K(E[\ell]) \neq K(\zeta_\ell)$, we choose $\overline{\varepsilon}$ such that

$$\rho_{\overline{\varepsilon}} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{F}_\ell).$$

Then $\overline{\gamma}$ and $\overline{\varepsilon}$ generate $\mathrm{Gal}(K(E[\ell])/K)$ and since

$$\begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & w^{-1} \end{pmatrix} = \begin{pmatrix} 1 & w^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{w^{-1}}$$

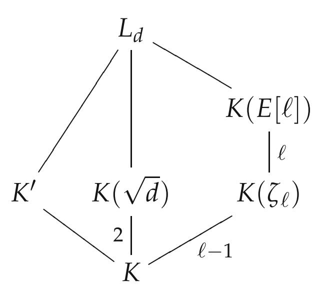
we have the relation $\overline{\gamma\varepsilon\gamma}^{-1} = \overline{\varepsilon}^{\chi_\ell(\overline{\gamma})^{-1}}$. □

Remark 5.3 The choice of $\overline{\gamma}$ and $\overline{\varepsilon}$ is closely related to the choice of base $\{P, Q\}$. In particular, we have $\overline{\varepsilon}(Q) = P + Q$ if $\overline{\varepsilon} \neq \mathrm{id}$ and $\overline{\gamma}(Q) = \chi_\ell(\overline{\gamma})Q$.

Let $d \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ be negative and relatively prime to $\ell \cdot N(E)$. We define L_d to be the quadratic extension of $K(E[\ell])$ given by the compositum $K(\sqrt{d}) \cdot K(E[\ell])$. The Galois group $\mathrm{Gal}(L_d/K)$ is generated by three elements $\delta, \gamma, \varepsilon$ with δ commuting with ε and γ and

$$\begin{aligned} \delta^2 &= \mathrm{id}, & \delta(\sqrt{d}) &= -\sqrt{d}, \\ \gamma^{\ell-1} &= \mathrm{id}, & \gamma|K(E[\ell]) &= \overline{\gamma}, \\ \varepsilon^\ell &= \mathrm{id}, & \varepsilon|K(E[\ell]) &= \overline{\varepsilon}, \\ \gamma^i\varepsilon^j|K(\sqrt{d}) &= \mathrm{id}, & \gamma\varepsilon\gamma^{-1} &= \varepsilon^{\chi_\ell(\gamma)^{-1}}. \end{aligned}$$

In particular, we have that δ operates as $-\mathrm{id}$ on $E^d[\ell]$, the points of order ℓ of E^d. The fixed field of ε is $K(\sqrt{d}, \zeta_\ell)$ and the fixed field of $\langle \varepsilon, \delta\gamma^{(\ell-1)/2} \rangle$ is K' as defined in Theorem B. Thus, we have the following field diagram:



We now describe the elements in $H^1(G_K, E^d[\ell])$. We have the exact inflation-restriction sequence

$$0 \longrightarrow H^1(\mathrm{Gal}(L_d/K), E^d[\ell]) \xrightarrow{\text{inf.}} H^1(G_K, E^d[\ell]) \xrightarrow{\text{res.}} H^1(\mathrm{Gal}(\overline{K}/L_d), E^d[\ell]),$$

where $H^1(\mathrm{Gal}(\overline{K}/L_d), E^d[\ell]) = \mathrm{Hom}_{\mathrm{Gal}(L_d/K)}(\mathrm{Gal}(\overline{K}/L_d), E^d[\ell])$.

Lemma 5.4 *The group $H^1(G_K, E^d[\ell])$ injects into $\mathrm{Hom}_{\mathrm{Gal}(L_d/K)}(\mathrm{Gal}(\overline{K}/L_d), E^d[\ell])$.*

Proof We need to show that $H^1(\mathrm{Gal}(L_d/K), E^d[\ell]) = 0$. If $\varepsilon = \mathrm{id}$, the degree of L_d/K is prime to ℓ, and the assertion follows. Now let ε be of order ℓ. Using the inflation-restriction sequence, one has that

$$H^1(\mathrm{Gal}(L_d/K), E^d[\ell]) = H^1(\langle \varepsilon \rangle, E^d[\ell])^{\langle \delta, \gamma \rangle}.$$

Let P_d, Q_d be the points of order ℓ of $E^d[\ell]$ corresponding to $P, Q \in E[\ell]$. Then $P_d = \varepsilon Q_d - Q_d$, and hence $H^1(\langle\varepsilon\rangle, E^d[\ell])$ is generated by the class of cocycle ψ which sends ε to Q_d. Since $\delta\varepsilon\delta = \varepsilon$ and $\delta Q_d = -Q_d$, we have that $\psi \notin H^1(\langle\varepsilon\rangle, E^d[\ell])^{\langle\delta\rangle}$, and thus $H^1(\mathrm{Gal}(L_d/K), E^d[\ell]) = H^1(\langle\varepsilon\rangle, E^d[\ell])^{\langle\delta,\gamma\rangle} = 0.$ □

Take an element $\widetilde{\Phi} \in H^1(G_K, E^d[\ell])$ with

$$\mathrm{res}\,\widetilde{\Phi} = \phi \in \mathrm{Hom}_{\mathrm{Gal}(L_d/K)}(\mathrm{Gal}(\overline{K}/L_d), E^d[\ell])$$

and denote by M the fixed field of the kernel of ϕ. M/K is normal and $\mathrm{Gal}(M/L_d)$ is possibly generated by two elements α_1, α_2 with $\alpha_i^\ell = \mathrm{id}$, which we may choose in such a way that

$$\phi(\alpha_1) = \mu_1 P \quad \text{and} \quad \phi(\alpha_2) = \mu_2 Q.$$

We may also assume that $\mu_i = 1$ if $\alpha_i \neq \mathrm{id}$.

We extend $\delta, \gamma, \varepsilon \in \mathrm{Gal}(L_d/K)$ to elements $\widetilde{\delta}, \widetilde{\gamma}, \widetilde{\varepsilon} \in \mathrm{Gal}(M/K)$ and compute the actions of these elements on α_i. We assume that $\widetilde{\delta}^2 = \widetilde{\gamma}^{\ell-1} = \mathrm{id}$. Since

$$\phi(\beta\alpha_i\beta^{-1}) = \beta\phi(\alpha_i) \quad \forall\, \beta \in \mathrm{Gal}(M/K)$$

via the fact that ϕ is a group homomorphism and the cocycle condition we get:

$$\begin{aligned}
\widetilde{\delta}\alpha_i\widetilde{\delta} &= \alpha_i^{-1} && (\because\ \widetilde{\delta}|E^d[\ell] = -\mathrm{id})\\
\widetilde{\gamma}\alpha_1\widetilde{\gamma}^{-1} &= \alpha_1 && (\because\ \widetilde{\gamma}P = P),\\
\widetilde{\gamma}\alpha_2\widetilde{\gamma}^{-1} &= \alpha_2^{\chi_\ell(\widetilde{\gamma})} && (\because\ \widetilde{\gamma}Q = \chi_\ell(\widetilde{\gamma})Q),\\
\widetilde{\varepsilon}\alpha_1\widetilde{\varepsilon}^{-1} &= \alpha_1 && (\because\ \widetilde{\varepsilon}P = P),\\
\widetilde{\varepsilon}\alpha_2\widetilde{\varepsilon}^{-1} &= \alpha_1\alpha_2 && \text{if } \varepsilon \neq \mathrm{id} \text{ and } \alpha_2 \neq \mathrm{id}(\because \text{ then } \varepsilon\phi(\alpha) =\\
& && \varepsilon P = P + Q = \phi(\alpha_1\alpha_2);\ \text{necessarily } \alpha_1 \neq \mathrm{id}\\
& && \text{in this case}).
\end{aligned}$$

In particular, it follows that $\langle\alpha_1\rangle$ is a normal subgroup of $\mathrm{Gal}(M/K)$ and that $\langle\alpha_2\rangle$ is normal if either $\alpha_2 = \mathrm{id}$ or $\widetilde{\varepsilon} = \mathrm{id}$.

Now we distinguish between two cases:

Case 1 $\widetilde{\varepsilon} = \mathrm{id}$. In this case $\langle\alpha_1\rangle$ and $\langle\alpha_2\rangle$ are both normal in $\mathrm{Gal}(M/K)$ and hence

$$M_i := M^{\langle\alpha_i\rangle}$$

are normal extensions of K. The Galois group of $M_2/K(\sqrt{d})$ is abelian and generated by the restriction of $\langle\widetilde{\gamma}, \alpha_1\rangle$ to M_2. Hence

$$\overline{M}_2 := M^{\langle\alpha_2,\widetilde{\gamma}\rangle}$$

is Galois over K containing $K(\sqrt{d})$ and if $\alpha_1 \neq \mathrm{id}$, then $\mathrm{Gal}(\overline{M}_2/K)$ is non-abelian of order 2ℓ. Since

$$\widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2}\alpha_2(\widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2})^{-1} = \alpha_2,$$

it follows that M_1 is abelian over K' and hence

$$\overline{M}_1 := M^{\langle\alpha_1,\widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2}\rangle}$$

is normal over K. Its Galois group is generated by

$$\overline{\alpha}_2 = \alpha_2|\overline{M}_1 \quad \text{and} \quad \overline{\gamma} = \widetilde{\gamma}|\overline{M}_1,$$

and its order is equal to $|\alpha_2| \cdot (\ell - 1)$. Also one has the relation $\overline{\gamma \alpha_2 \gamma}^{-1} = \overline{\alpha}_2^{\chi_\ell(\overline{\gamma})}$. To summarize, we have that

$$\overline{M}_1(\phi) := M^{\langle \alpha_1, \widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2} \rangle},$$
$$\overline{M}_2(\phi) := M^{\langle \alpha_2, \widetilde{\gamma} \rangle}.$$

Case 2 $|\widetilde{\varepsilon}| = \ell$. In this case, we may assume that $\alpha_1 \neq \mathrm{id}$ for $\alpha_1 = \mathrm{id}$ implies that $\alpha_2 = \mathrm{id}$, as well.

Subcase (i) $\alpha_2 = \mathrm{id}$. We assert that $\mathrm{Gal}(M/K(\zeta_\ell, \sqrt{d}))$ is not cyclic. Otherwise $\widetilde{\varepsilon}$ would be an element of order ℓ^2 with $\widetilde{\varepsilon}^{\,\ell} = \alpha_1$ (without lose of generality). So $\widetilde{\delta}\widetilde{\varepsilon}^{\,\ell}\widetilde{\delta} = \widetilde{\varepsilon}^{-\ell}$ and hence

$$\widetilde{\delta}\widetilde{\varepsilon}\widetilde{\delta} = \widetilde{\varepsilon}^{\,k} \quad \text{with } k \equiv -1 \mod \ell.$$

But since $\delta\varepsilon\delta = \varepsilon$, we would get $\delta\widetilde{\varepsilon}\delta = \widetilde{\varepsilon} \cdot (\widetilde{\varepsilon}^{\ell})^n = \widetilde{\varepsilon}^{\,1+\ell^n}$ which gives a contradiction. Hence, we can choose $\widetilde{\varepsilon}$ so that

$$\widetilde{\varepsilon}^{\,\ell} = \widetilde{\alpha}_1^{\,\ell} = \mathrm{id} \quad \text{ and } \quad \widetilde{\delta}\widetilde{\varepsilon}\widetilde{\delta} = \widetilde{\varepsilon},$$

which determines $\widetilde{\varepsilon}$ uniquely. Thus, $\overline{M}_2 := M^{\langle \widetilde{\varepsilon}, \widetilde{\gamma} \rangle}$ is normal over K and contains $K(\sqrt{d})$ and its Galois group is dihedral of order 2ℓ and generated by $\langle \alpha_1, \widetilde{\delta} \rangle$. To summarize, we say that

$$\overline{M}_1(\phi) := M^{\langle \alpha_1, \widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2} \rangle},$$
$$\overline{M}_2(\phi) := M^{\langle \widetilde{\varepsilon}, \widetilde{\gamma} \rangle}.$$

Subcase (ii) $\alpha_2 \neq \mathrm{id}$. We have that $M_1 := M^{\langle \alpha_1 \rangle}$ is normal over K and of degree ℓ over L_d. Since $\widetilde{\delta}\alpha_2\widetilde{\delta} = \alpha_2^{-1}$, we conclude as above that ε has an extension $\widetilde{\varepsilon}$ to M_1 of order ℓ with $\widetilde{\delta}\widetilde{\varepsilon}\widetilde{\delta} = \widetilde{\varepsilon}$. Since $\widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2}$ acts trivially on α_2 and $\widetilde{\varepsilon}$ acts trivially on $\alpha_2|M_1$, we have that $\langle \widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2}, \widetilde{\varepsilon} \rangle$ is a normal subgroup of $\mathrm{Gal}(M_1/K)$. Hence

$$\overline{M}_1 := M_1^{\langle \widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2}, \widetilde{\varepsilon} \rangle}$$

is normal over K containing K', and its Galois group over K' is generated by $\overline{\alpha}_2 = \alpha_2|\overline{M}_1$, which is of order ℓ and satisfies the relation

$$\overline{\gamma \alpha_2 \gamma}^{-1} = \overline{\alpha}_2^{\chi_\ell(\overline{\gamma})} \quad \text{with } \overline{\gamma} = \widetilde{\gamma}|K'.$$

In order to simplify notation, we define $\overline{M}_2(\phi) := K(\sqrt{d})$ if either $\varepsilon \neq \mathrm{id}$ or $\alpha_2 \neq \mathrm{id}$. To summarize, we say that

$$\overline{M}_1(\phi) := M_1^{\langle \widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2}, \widetilde{\varepsilon} \rangle},$$
$$\overline{M}_2(\phi) := K(\sqrt{d}).$$

Hence for a given

$$\widetilde{\Phi} \in H^1(G_K, E^d[\ell])$$

we have a field $M = M(\phi)$ which determines $\langle \phi \rangle$ completely where $\phi = \mathrm{res}(\widetilde{\Phi})$. We want to study the information we attain from the pair $(\overline{M}_1(\phi), \overline{M}_2(\phi))$. If $\varepsilon = \mathrm{id}$ or $\alpha_2 = \mathrm{id}$, then we get back $M(\phi) = M$ from $(\overline{M}_1(\phi), \overline{M}_2(\phi))$. In these cases, we shall say that ϕ is of first type. What happens if $\varepsilon \neq \mathrm{id}$ and $\alpha_2 \neq \mathrm{id}$?

Assume that

$$\phi \neq \psi \in H^1(G_K, E^d[\ell])$$

have fields $M(\phi)$ and $M(\psi)$ with Galois groups $\langle\alpha_1, \alpha_2\rangle$ and $\langle\beta_1, \beta_2\rangle$ as above such that

$$M(\phi)^{\alpha_1} = M(\psi)^{\beta_1}.$$

Let N be the composite of $M(\phi)$ and $M(\psi)$. Then the Galois group $\mathrm{Gal}(N/L_d)$ is generated by three elements $\langle\sigma_1, \sigma_2, \sigma_3\rangle$, which we can choose in such a way that

$$\sigma_1|M(\phi) = \alpha_1, \quad \sigma_1|M(\psi) = \beta_1^\lambda$$

$$\sigma_2|M(\phi) = \alpha_2, \quad \sigma_2|M(\psi) = \beta_2^\lambda$$

where $\lambda \in \{1, \ldots, \ell - 1\}$. N is a splitting field of ϕ and ψ, and

$$(\phi - \lambda^{\ell-1}\psi)(\sigma_1) = (\phi - \lambda^{\ell-1}\psi)(\sigma_2) = 0.$$

Hence the fixed field of the kernel of $\phi - \lambda\psi$ is a cyclic extension of L_d which is normal over K, and $\phi - \lambda^{-1}\psi$ is of first type.

Thus, $\overline{M}_1(\phi)$ determines $\langle\phi\rangle$ up to elements of first type, and in order to determine all elements in $H^1(G_K, E^d[\ell])$, it is enough to determine all dihedral extensions of K of degree 2ℓ containing $K(\sqrt{d})$ and all extensions M_1 of degree ℓ over K' which are normal over K such that conjugation by $\overline{\gamma}$ on $\mathrm{Gal}(\overline{M}_1, K')$ is equal to $\chi_\ell(\overline{\gamma})$.

Therefore to prove the double divisibility, one has to show that for $\phi \in \mathrm{Sel}_\ell(E^d, K)$, the field $\overline{M}_2(\phi)$ is unramified over $K(\sqrt{d})$ outside $\widetilde{S}_E$, and $\overline{M}_1(\phi)$ is unramifed over K' outside S_E and little ramified at divisors of $\mathfrak{l}$.

5.2 Splitting fields of elements in $\mathrm{Sel}_\ell(E^d, K)$

We shall continue to use the assumptions and the notations of the Theorem B and Sect. 5.1.

Lemma 5.5 *Let ϕ be an element in $\mathrm{Sel}_\ell(E^d, K)$. Then $\overline{M}_1(\phi) =: \overline{M}_1$ is unramified at $\mathfrak{q}$ over K' and $\overline{M}_2(\phi) =: \overline{M}_2$ is unramified at $\mathfrak{q}$ over $K(\sqrt{d})$.*

Proof We first prove the latter statement. Since $\mathfrak{q}|\Delta_{K(\sqrt{d})/K}$, we have that $K(\sqrt{d})$ and K' are ramified at $\mathfrak{q}$ over K. Hence the norm of $\mathfrak{Q}|\mathfrak{q}$ in $K(\sqrt{d})$ is equal to $\mathfrak{q}$, and by assumption the norm of $\mathfrak{Q}|2$ is equal to 2. Suppose that $K(\sqrt{d})$ had a cyclic extension of degree ℓ in which $\mathfrak{Q}$ is ramified. Then the completion $K(\sqrt{d})_{\mathfrak{Q}}$ admits a cyclic extension of degree ℓ ramified at $\mathfrak{Q}$. Since ℓ is odd and $\mathfrak{Q}$ has residue characteristic two, this extension is tamely ramified. By local class field theory, the tamely ramified cyclic extensions of a local field $K(\sqrt{d})_{\mathfrak{Q}}$ all have degree dividing $|\kappa^\times|$, where κ is the residue field. Since $\kappa = \mathbf{F}_2$, we have that there are no tamely ramified and ramified extensions of $K(\sqrt{d})_{\mathfrak{Q}}$. Thus, $K(\sqrt{d})$ has no cyclic extension of degree ℓ in which $\mathfrak{Q}$ ramifies, and hence $\overline{M}_2$ is unramified at $\mathfrak{q}$ over $K(\sqrt{d})$.

To prove the former statement, we shall utilize the proof of [2, Lemma 3] and look prime by prime. For $\ell = 5$, the same argument as above can be applied to $\mathfrak{Q}_{K'}|\mathfrak{q}$. For $\ell = 7$, there is only one extension $\mathfrak{Q}|\mathfrak{q}$ to K' which is ramified of order 2 and has norm 8. Assume that $\mathfrak{Q}_{K'}$ is ramified in $\overline{M}_1/K'$ and let $\mathfrak{Q}_{\overline{M}_1}$ be the unique extension of $\mathfrak{Q}_{K'}$ to $\overline{M}_1$. Let M_t be the subfield of $\overline{M}_1$ in which $\mathfrak{Q}_{\overline{M}_1}$ is tamely ramified. Then M_t is a cyclic extension of degree 7 over $K(\zeta_7+\zeta_7^{-1})$, and $\overline{M}_1$ is the compositum of M_t with K' over $K(\zeta_7+\zeta_7^{-1})$. Thus, $\mathrm{Gal}(\overline{M}_1/K(\zeta_7+\zeta_7^{-1}))$ is abelian. But this contradicts the fact that

$$\overline{\gamma}^3\overline{\alpha}\overline{\gamma}^3=\overline{\alpha}^{\chi_7(\overline{\gamma}^3)}=\overline{\alpha}^{-1},$$

where $\langle\overline{\alpha}\rangle=\mathrm{Gal}(\overline{M}_1/K')$ and $\langle\overline{\gamma}\rangle=\mathrm{Gal}(K'/K)$.

For $\ell=11, 13, 19, 37$, we can use the same proof as the first statement since

$$\begin{array}{llll} 11\nmid(2^5-1) & 13\nmid(2^2-1) & 37\nmid(2^3-1) & 37\nmid(2^{18}-1)\\ 13\nmid(2^6-1) & 19\nmid(2^9-1) & 37\nmid(2^9-1) & 37\nmid(2^2-1).\\ 13\nmid(2^3-1) & 19\nmid(2^3-1) & 37\nmid(2^6-1) & \end{array}$$

For $\ell=17$, there there is only one extension $\mathfrak{Q}|\mathfrak{q}$ to K' which is ramified of order 2 and has norm 2^8 (note that $17|(2^8-1)$). If we assume that $\mathfrak{Q}_{K'}$ is ramified in $\overline{M}_1/K'$, then we can use the above argument to construct the same contradiction. □

Remark 5.6 Since $73|(2^{36}-1)$, $73|(2^9-1)$, and $73|(2^{18}-1)$, we may not assume that there is a unique cyclic extension of K' with degree 73 in which $\mathfrak{Q}$ is ramified, and hence the above argument does work for $\ell=73$. This precludes us from extending Theorem B to number fields K of degree ≥ 6.

Therefore, we can assume that $\mathfrak{p}\nmid\mathfrak{q}\cdot\mathfrak{l}$, but $\mathfrak{p}|N(E)$.

Lemma 5.7 *Let ϕ be an element in $\mathrm{Sel}_\ell(E^d,K)$. Then $\overline{M}_1/K'$ is unramified outside of $S_E\cup\{\mathfrak{l}\}$ and $\overline{M}_2/K(\sqrt{d})$ is unramified outside $\widetilde{S}_E\cup\{\mathfrak{l}\}$.*

Proof We have to test prime numbers $\mathfrak{p}\neq\mathfrak{l}$ that divide $N(E)$.

1. If $\mathrm{ord}_\mathfrak{p}(j_E)\geq 0$, then it follows from Néron's list of minimal models of elliptic curves with potentially good reduction that ℓ must be equal to 3 [18, p.124]. Since we only consider primes $\ell>3$, we can exclude this case from consideration.
2. Now assume that $\mathrm{ord}_\mathfrak{p}(j_E)<0$. We have two subcases:

   (a) If $\mathrm{ord}_\mathfrak{p}(j_E)\equiv 0 \mod \ell$, we have that $\mathfrak{p}\notin S_E$ and so E^d is not a Tate curve over $K_\mathfrak{p}$. Moreover, $K_\mathfrak{p}(E[\ell])$ is unramified over $K_\mathfrak{p}$ and hence $\overline{M_1}/K'$ and $\overline{M_2}/K(\sqrt{d})$ are unramified at all divisors of $\mathfrak{p}$ if and only if M_1/L_d (resp. M_2/L_d) are unramified at all divisors of $\mathfrak{p}$. We now use the triviality of the $\phi\in\mathrm{Sel}_\ell(E^d,K)$ over $K_\mathfrak{p}$ from Lemma 4.2. Also recall that M is the fixed field of the kernel of ϕ. We shall show that $\mathfrak{Q}_M$ is unramified over L_d.
   There is a $\widetilde{P}\in E^d(M_\mathfrak{P})$ where $\mathfrak{P}_M|\mathfrak{p}$ such that for all $\sigma\in D(\mathfrak{P}_M)$, we have $\sigma\widetilde{P}-\widetilde{P}=\phi(\sigma)$. Hence

   $$P':=\ell\cdot\widetilde{P}\in E^d(K_\mathfrak{p})$$

   and so $2P'$ is in the connected component of unity modulo $\mathfrak{p}$ via Remark 2.6. Hence $\widetilde{P}=\widetilde{P}_1+P_2$ with $P_2\in E^d[\ell]$ and $2\widetilde{P}_1$ in the component of the unity of $E \mod \mathfrak{P}_M$, so $\widetilde{P}_1$ corresponds to a $\mathfrak{P}_M$-adic unity u under the Tate parametrization. Now take

   $$\alpha\in\langle\alpha_1,\alpha_2\rangle\cap I(\mathfrak{P}_M)$$

where $I(\mathfrak{P}_M)$ is the interia group of $\mathfrak{P}_M$. Then $2(\alpha\widetilde{P} - \widetilde{P})$ corresponds to $\alpha u/u$ and is an ℓ^{th} root of unity. By Hilbert's Theorem 90, we have that $\alpha = \text{id}$, and thus, $\mathfrak{P}_M$ is unramified over L_d.

(b) If $\text{ord}_\mathfrak{p}(j_E) \not\equiv 0 \mod \ell$, then the values at the Hecke characters χ of order ℓ tell us that either E is a Tate curve over $K_\mathfrak{p}$ or that $\mathfrak{p} \in S_E$. Consider the former situation. Our assumptions from Theorem B tell us that $\mathfrak{q}$ is not completely decomposed in $K(\sqrt{d})$ and K'. Since

$$K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^\ell \cong K_\mathfrak{p}(\sqrt{d})^\times/(K_\mathfrak{p}(\sqrt{d})^\times)^\ell \cong K_\mathfrak{P}'^\times/(K_\mathfrak{P}'^\times)^\ell$$

for all $\mathfrak{P}_{K'}|\mathfrak{p}$, we see that for all cyclic extensions $\overline{M}_1$ of K' and $\overline{M}_2/K(\sqrt{d})$ of degree ℓ and divisors $\mathfrak{P}_{M_i}|\mathfrak{p}$, one has that $\text{Gal}(\overline{M}_{i,\mathfrak{P}_{M_i}}/K_\mathfrak{q})$ is abelian of even order. But this implies that

$$\overline{M}_{1,\mathfrak{P}} = K'_\mathfrak{p} \quad \text{and} \quad \overline{M}_{2,\mathfrak{P}} = K_\mathfrak{P}(\sqrt{d}),$$

which is absurd. Thus $\mathfrak{p} \in S_E$ and our lemma follows. □

The next step is to describe the behavior of $\overline{M}_i$ at divisors of $\mathfrak{l}$.

Lemma 5.8 *Assume that* $\text{ord}_\mathfrak{l}(j_E) < 0$ *and* $\phi \in \text{Sel}_\ell(E^d, K)$. *Then* $\overline{M}_2/K(\sqrt{d})$ *is unramified at* $\mathfrak{l}$ *and* $\overline{M}_1/K'$ *is little ramified at divisors of* $\mathfrak{l}$.

Proof The assumptions tells us that $E/K_\mathfrak{l}$ is a Tate curve but that $E^d/K_\mathfrak{l}$ is not a Tate curve. Since $K_\mathfrak{l}(E[\ell]) = K_\mathfrak{l}(\zeta_\ell)$, the behavior of $\overline{M}_i$ at $\mathfrak{l}$ is determined by the behavior of M at $\mathfrak{l}$. Let $\mathfrak{L}_M|\mathfrak{l}$, let $I(\mathfrak{L}_M)$ be the inertia group of $\mathfrak{L}_M$, and let

$$\alpha \in \langle \alpha_1, \alpha_2 \rangle \cap I(\mathfrak{L}_M).$$

As in the proof of Lemma 5.7, we can use the fact that $E^d/K_\mathfrak{l}$ is not a Tate curve to show that there is a $\widetilde{Q} \in E^d(M_\mathfrak{L})$ where $\mathfrak{L}_M|\mathfrak{l}$ and $\alpha\widetilde{Q} - \widetilde{Q} = \phi(\alpha)$. Hence $2\widetilde{Q}$ is in the connected component of unity modulo $\mathfrak{L}_M$ via Remark 2.6. This implies that

$$M_{\mathfrak{L}_M} = M_{\mathfrak{L}_M}^{\langle\alpha\rangle}(\sqrt[\ell]{u})$$

where u is a $\mathfrak{L}_M$-adic unit corresponding to $2\widetilde{Q}$ under the Tate parametrization. Moreover, M_1/L_d is little ramified at $\mathfrak{l}$.

Now assume that $\alpha_2 = \text{id}$ or $\varepsilon = \text{id}$. Then $\overline{M}_2/K(\sqrt{d})$ is of degree ℓ, and we have to show that $\overline{M}_2/K(\sqrt{d})$ is unramified at $\mathfrak{L}_{\overline{M}_2}|\mathfrak{l}$. We recall the choice of point Q. Since $\gamma Q = \chi_\ell(\gamma)Q$ where $\langle\gamma\rangle = \text{Gal}(K(\zeta_\ell)/K)$, it follows that Q is in the kernel of the reduction of E modulo all divisors of $\mathfrak{l}$, and hence $P + \lambda Q$ is not in this kernel where $\lambda \in \mathbf{N}$. For $\alpha \in I(\mathfrak{L}_M)$, we saw that $\sigma\widetilde{Q} - \widetilde{Q} = \phi(\sigma)$ is in the kernel of the reduction modulo $\mathfrak{L}_M$, and hence

$$\alpha_1\alpha_2^\lambda \notin I(\mathfrak{L}_M) \quad \forall \lambda \in \mathbf{N} \text{ and } \mathfrak{L}_M|\mathfrak{l}.$$

Thus, it follows that $M^{\langle\alpha_2\rangle}/L_d$ is unramified at $\mathfrak{L}_M$ and $\overline{M}_2/K(\sqrt{d})$ is unramified at $\mathfrak{l}$. □

Finally, we look at the case where $\text{ord}_\mathfrak{l}(j_E) \geq 0$.

Lemma 5.9 *Assume that* E/K *has a* K*-rational point* P *of order* $\ell > 3$, *that* $\text{ord}_\mathfrak{l}(j_E) \geq 0$, *and that* P *is not contained in the kernel of reduction modulo* $\mathfrak{l}$, *in particular, this means that* E *is not supersingular modulo* $\mathfrak{l}$. *Let* ϕ *be an element in* $\text{Sel}_\ell(E^d, K)$ *with corresponding fields* $\overline{M}_1$ *and* $\overline{M}_2$. *Then* $\overline{M}_1/K'$ *is little ramified at* $\mathfrak{l}$, *and* $\overline{M}_2/K(\sqrt{d})$ *is unramified at* $\mathfrak{l}$.

Proof Suppose that $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$, which implies that E has potentially good reduction at $\mathfrak{l}$. Since E/K has a K-rational point P of order $\ell > 3$, we know that $\mathrm{Gal}(K(E[\ell])/K(\zeta_\ell))$ is a subgroup of the additive group $\mathbf{F}_\ell^+$. We want to show that all divisors of $\mathfrak{l}$ are not ramified in $K(E[\ell])/K(\zeta_\ell)$. If E has good reduction over $K(\zeta_\ell)$, then we are immediately done. If E does not have good reduction over $K(\zeta_\ell)$, then there must exist some extension $N/K(\zeta_\ell)$ such that $[N{:}K(\zeta_\ell)]|6$ and that E has good reduction at all divisors $\mathfrak{L}_N|\mathfrak{l}$; this divisibility condition is similar to the proof of [1, Proposition VII.5.4.c]. From our assumptions, it follows that $N_{\mathfrak{L}}$ contains $K(E[\ell])$ and that $\langle Q\rangle$ is the subgroup of order ℓ of the kernel of reduction modulo $\mathfrak{L}_N$. Hence all divisors of $\mathfrak{l}$ are not ramified in $K(E[\ell])/K(\zeta_\ell)$, and we can prove the lemma by looking at the behavior of $\mathfrak{l}$ in M/L_d.

Assume that $\mathfrak{L}_M|\mathfrak{l}$ and let $I(\mathfrak{L}_M)$ be the inertia group of $\mathfrak{L}_M$. Suppose that $\alpha_1^\mu\alpha_2^\lambda \in I(\mathfrak{L}_M)$. There there is a $\widetilde{P} \in E(M_{\mathfrak{L}})$ with

$$(\alpha_1^\mu\alpha_2^\lambda)\widetilde{P} - \widetilde{P} = \mu P + \lambda Q.$$

But we know that for $\mu \neq 0$, the point $\mu P + \lambda Q$ is not in the kernel of reduction modulo $\mathfrak{L}_M$. Let $\widetilde{E}$ be a model of E over N having good reduction modulo $\mathfrak{L}_N|\mathfrak{l}$. Since $(I(\mathfrak{L}_M) - \mathrm{id})\widetilde{E}(N \cdot M_{\mathfrak{L}})$ is contained in this kernel, we must have that $\mu = 0$, and hence

$$I(\mathfrak{L}_M) \cap \mathrm{Gal}(M/L_d) \subseteq \langle\alpha_2\rangle.$$

Thus, $M^{\langle\alpha_2\rangle}/L_d$ is unramified at $\mathfrak{L}_M$; moreover, $\overline{M}_2/K(\sqrt{d})$ is unramified above $\mathfrak{l}$.

Now assume that $I(\mathfrak{L}_M) = \langle\alpha_2\rangle$. Then $Q = \alpha_2\widetilde{Q} - \widetilde{Q}$ and since $\langle\alpha_2\rangle$ acts trivially on $\widetilde{E}(N\cdot M_{\mathfrak{L}})/\widetilde{E}_-(N\cdot M_{\mathfrak{L}})$, we may assume that $\widetilde{Q} \in \widetilde{E}_-(N\cdot M_{\mathfrak{L}})$ and hence $\ell\cdot\widetilde{Q} \in \widetilde{E}_-(N\cdot K_{\mathfrak{l}})$. Since $\widetilde{E}$ has ordinary reduction modulo $\mathfrak{L}_M$, we have that $N \cdot K_{\mathfrak{l}}(\widetilde{Q})$ is little ramified at divisors of $\mathfrak{l}$. Thus, our lemma follows. □

Lemmas 5.5, 5.7, 5.8 and 5.9 prove that for $\phi \in \mathrm{Sel}_\ell(E^d, K)$, the field $\overline{M}_2(\phi)$ is unramified over $K(\sqrt{d})$ outside $\widetilde{S}_E \cup \{\mathfrak{l}\}$, and $\overline{M}_1(\phi)$ is unramifed over K' outside S_E and little ramified at divisors of $\mathfrak{l}$. Moreover, we have proved that

$$\#\,\mathrm{Sel}_\ell(E^d, K)\,\Big|\,\mathrm{cl}_{\widetilde{S}_E,u}(K(\sqrt{d}))[\ell]\cdot \mathrm{cl}_{S_E}(K')[\ell](\chi_\ell)\,,$$

which completes the proof of Theorem B.

5.3 Proof of Corollary E

Since we have established our double divisibility statement (2), we can proceed with a proof of Corollary E. By the definitions established in Sect. 2, we have that

$$\mathrm{cl}_{\widetilde{S}_E,u}(K(\sqrt{d}))[\ell]\cdot \mathrm{cl}_{S_E}(K')[\ell](\chi_\ell)\,\Big|\,\mathrm{cl}_{\emptyset,u}(K(\sqrt{d}))[\ell]\cdot \mathrm{cl}_{\emptyset}(K')[\ell](\chi_\ell)\cdot\varepsilon_S$$

where ε_S is a number depending only on $\widetilde{S}_E$. Note that when $\widetilde{S}_E = \emptyset$, we have that $\varepsilon_S = 1$ and that $\mathrm{cl}_{\emptyset,u}(K(\sqrt{d}))[\ell] = \mathrm{cl}(K(\sqrt{d}))[\ell]$ by Remark 2.4. Corollary E follows immediately from the following lemma.

Lemma 5.10 $\mathrm{cl}_{\emptyset}(K')[\ell](\chi_\ell) \mid \mathrm{cl}(K(\sqrt{d}))[\ell]$.

Proof Let M/K be a Galois extension containing K' with $\langle\alpha\rangle = \mathrm{Gal}(M/K)$, with the relations

$$\alpha^\ell = \mathrm{id} \quad \text{and} \quad \overline{\gamma\alpha\gamma}^{-1} = \alpha^{\chi_\ell(\overline{\gamma})} \text{ where } \langle\overline{\gamma}\rangle = \mathrm{Gal}(K'/K).$$

We assume that M is unramified outside $\mathfrak{l}$ and little ramified at $\mathfrak{l}$; hence

$$M(\zeta_\ell) = K'(\sqrt{d})(\sqrt[\ell]{c}),$$

with $c \in M(\sqrt{d})$ and the principal divisor of c is a ℓ^{th} power. We want to extend c to an element of order ℓ in the divisor class group of $K(\sqrt{d})$.

Let $\widetilde{\gamma}$ be an extension of $\overline{\gamma}$ to $\mathrm{Gal}(M(\sqrt{d})/K)$ such that $\widetilde{\gamma}^{\ell-1} = \mathrm{id}$, $\widetilde{\gamma}|K(\zeta_\ell)$ generates $\mathrm{Gal}(K(\zeta_\ell)/K)$, and $\widetilde{\gamma}|K(\sqrt{d}) = \mathrm{id}$. Since $M(\sqrt{d})/K$ is normal, we have $\widetilde{\gamma}(c) = c^i \cdot e^\ell$ with $1 \le i \le \ell - 1$ and $e \in K'(\sqrt{d})$. Hence,

$$\widetilde{\gamma}(\sqrt[\ell]{c}) = (\sqrt[\ell]{c})^i \cdot e \cdot \xi_{\widetilde{\gamma}}$$

with $\xi_{\widetilde{\gamma}}^\ell = 1$. Let $\widetilde{\alpha}$ be an extension of α to $M(\sqrt{d})$ of order ℓ. We can see that $i = 1$ since

$$\widetilde{\gamma}\widetilde{\alpha}(\sqrt[\ell]{c}) = \xi_{\widetilde{\alpha}}^{\chi_\ell(\overline{\gamma})}\widetilde{\gamma}(\sqrt[\ell]{c})$$

and

$$\widetilde{\alpha}^{\chi_\ell(\gamma)}\widetilde{\gamma}(\sqrt[\ell]{c}) = \widetilde{\alpha}^{\chi_\ell(\gamma)}(\xi_{\widetilde{\gamma}}(\sqrt[\ell]{c})^i \cdot e) = \xi_{\widetilde{\alpha}}^{i \cdot \chi_\ell(\overline{\gamma})} \cdot \widetilde{\gamma}(\sqrt[\ell]{c}),$$

and hence

$$M(\sqrt{d}) = K(\sqrt{d}, \sqrt[\ell]{c}, \zeta_\ell).$$

There exists an element $\widetilde{c} = c^{\ell-1} \cdot e'^\ell \in M(\sqrt{d})$ with $e' \in K'(\sqrt{d})$ such that the divisor of $\widetilde{c}$ is a ℓth power. However, since $\pm\widetilde{c}$ is not an ℓ^{th} power in $K(\sqrt{d})$, it is an element of order ℓ in the divisor class group of $K(\sqrt{d})$. □

6 Elliptic curves satisfying Corollary D

Let E be an elliptic curve over a number field K. In a recent work [13], Zywina has described all known, and conjecturally all, pairs $(E/\mathbf{Q}, \ell)$ such that mod ℓ image of Galois, $\rho_{E,\ell}(G_\mathbf{Q})$, is non-surjective. Using Zywina's classification, we can find elliptic curves $E/\mathbf{Q}$ that will satisfy the conditions of Corollary D. First, we present an example of this technique for the case when $\ell = 3$. We remark that this case does not apply to Corollary D; however, it best illustrates the technique.

Let $E/\mathbf{Q}$ be a non-CM elliptic curve over $\mathbf{Q}$ such that $\rho_{E,3}(G_\mathbf{Q})$ is conjugate to

$$B(3) := \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset \mathrm{GL}_2(\mathbf{F}_3).$$

We can use Galois theory to prove the following result:

Proposition 6.1 *Let $E/\mathbf{Q}$ have mod 3 image of Galois conjugate to $B(3)$. Then $\mathbf{Q}(E[3]) = \mathbf{Q}(x(E[3])) \cdot K$ where K is an explicitly computable quadratic extension.*

Before we prove Proposition 6.1, we prove the following lemma which tells us over which extension E obtains a 3-torsion point.

Lemma 6.2 *For $E/\mathbf{Q}$ from Proposition 6.1, there exists some quadratic extension K such that E has a K-rational 3-torsion point. In particular, $E(K)[3] = \langle P \rangle$.*

Proof Let $E\colon y^2 = x^3 - Ax - B$ for $A, B \in \mathbf{Q}$. Via the Weil-pairing, we know that $\mathbf{Q}(\zeta_3) \subseteq \mathbf{Q}(E[3])$. It is also a well known fact that $B(3) \cong S_3 \times \mathbf{Z}/2\mathbf{Z}$. Combining these results with our assumptions, we have the following diagram of Galois sub-fields of $\mathbf{Q}(E[3])$:

$$\begin{array}{c} \mathbf{Q}(E[3]) \\ \Big|\,{\scriptstyle 2} \\ \mathbf{Q}(x(E[3])) \\ \Big|\,{\scriptstyle 3} \\ \mathbf{Q}(\zeta_3) \\ \Big|\,{\scriptstyle 2} \\ \mathbf{Q} \end{array}$$

where the extension $\mathbf{Q}(x(E[3]))$ is the index 2 sub-field of $\mathbf{Q}(E[3])$ generated by the x-coordinates of points in $E(\overline{\mathbf{Q}})[3]$. Recall that the roots of the 3-division polynomial

$$\psi_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$$

correspond to x-coordinates of $E(\overline{\mathbf{Q}})[3]$. In particular, $\psi_3(x)$ is the minimal polynomial of the degree 6, Galois extension $\mathbf{Q}(x(E[3]))$.

Since S_4 does not contain any transitive subgroups of order 6, we know that $\psi_3(x)$ must have a linear factor, so we write $\psi_3(x) = (x-\alpha)g(x)$ where $\alpha \in \mathbf{Q}$ and $g(x)$ is an irreducible cubic. This implies that there exists some $P \in E(\overline{\mathbf{Q}})[3]$ with $\mathbf{Q}$-rational x-coordinate given by α. Moreover, we see that there is a 3-torsion point

$$P = (\alpha, \sqrt{f(\alpha)}).$$

that is defined over the quadratic extension $\mathbf{Q}(\sqrt{f(\alpha)})$. □

Remark 6.3 From the above proof, one can easily see that $\mathrm{Gal}(\mathbf{Q}(x(E[3]))/\mathbf{Q}) \cong S_3$. Indeed, since $\mathbf{Q}(x(E[3]))$ is Galois, we showed that the Galois group of $\psi_3(x)$ is actually the Galois group of the cubic $g(x)$. Since $[\mathbf{Q}(x(E[3])) : \mathbf{Q}] = 6$, we know $g(x)$ must be an irreducible cubic with non-square discriminant, which immediately implies our claim.

Proof of Proposition 6.1 (Proof of Proposition 6.1) Let K denote the quadratic extension from Lemma 6.2. It is clear that $K \subset \mathbf{Q}(E[3])$ and that $K \not\subseteq \mathbf{Q}(x(E[3]))$, so we have $\mathbf{Q}(E(3))$ is the compositum of $\mathbf{Q}(x(E[3]))$ and K. □

The idea behind finding elliptic curves over $\mathbf{Q}$ such that $E(\mathbf{Q})[\ell] = \{\mathcal{O}\}$ and $E(K)[\ell] = \langle P \rangle$ is to consider $E/\mathbf{Q}$ with $\rho_{E,\ell}(G_{\mathbf{Q}})$ conjugate to a subgroup H such that

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \subsetneq H \subseteq \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} =: B(\ell).$$

We can see that E will attain an ℓ torsion point over an extension K where the degree of $K/\mathbf{Q}$ is determined the cardinality of the upper left entry. For $\ell = 3$, we saw that $H = B(3)$ and thus the upper left entry has order 2, which gives a less explicit proof of Proposition 6.1.

Let $\ell \in \{5, 13\}$. Below, we provide examples of elliptic curves $E/\mathbf{Q}$ that do not have a $\mathbf{Q}$-rational point of order ℓ but attain a K-rational point P of order ℓ over some extension of small degree K that satisfies the conditions of Corollary D. The final step in our verification is showing P is not contained in the kernel of reduction modulo $\mathfrak{l}$; in particular, this means that E/K is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$. This condition is computable via the `Magma` command `IsSupersingular`.

In order to conduct a thorough search, we consider all subgroups H which can occur as an image of Galois for a non-CM $E/\mathbf{Q}$ and satisfy the above containment. In particular, we run through a large list elliptic curves $E/\mathbf{Q}$ with prescribed non-surjective mod ℓ image of Galois coming from the modular curves X_H of Zywina [13]. Since this list is comprehensive, we also give examples of elliptic curves over $\mathbf{Q}$ that do not satisfy and potentially satisfy Corollary D, modulo some computations.

For $\ell = 5$, we only have one example.

Example 6.3.1 ($\ell = 5$) Let $E/\mathbf{Q}$ be the elliptic curve

$$E\colon y^2 = f(x) = x^3 - \frac{185193}{185193}x + \frac{185193}{149}.$$

E has mod 5 image of Galois conjugate to $B(5) \subset \mathrm{GL}_2(\mathbf{F}_5)$, and hence E attains a K-rational point of order 5 over a bi-quadratic extension K of $\mathbf{Q}$. The first quadratic extension $L/\mathbf{Q}$ is given by adjoining the quadratic root α of the 5-division polynomial ψ_5, and then the second quadratic is given by adjoining the square root of the $f(\alpha)$. For E defined above, we compute that $\mathrm{cl}(K) = 8$, $\zeta_5 \notin K$, 2 is ramified in $\mathcal{O}_K$, and that E/K is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$ where $\mathfrak{l}|5$. Therefore, the elliptic curve E and the number field K satisfy the conditions of Corollary D.

For $\ell = 7$, we have two possibilities.

Potential example 6.3.2 ($\ell = 7$) Let $E/\mathbf{Q}$ be the elliptic curve

$$E\colon y^2 = f(x) = x^3 - \frac{81469949623875}{3017401762489}x + \frac{162939899247750}{3017401762489},$$

which has mod 7 image conjugate to $B(7)$. E attains a K-rational point of order 7 over an extension K of degree 6. The extension K is given by first adjoining the root α of the cubic factor of ψ_7 and then adjoining the square root of $f(\alpha)$. We verify almost all of the conditions from Corollary D for E and K; however, we are not able to verify that $7 \nmid \mathrm{cl}(K)$.

Non-example 6.3.3 ($\ell = 7$) Suppose that $E/\mathbf{Q}$ has $\rho_{E,7}(G_{\mathbf{Q}})$ conjugate to

$$H := \begin{pmatrix} a^2 & * \\ 0 & * \end{pmatrix} \quad \text{where } a \in \mathbf{F}_7.$$

Since $\#(\mathbf{F}_7^{\times})^2 = 3$, we have that E attains a K-rational point of order 7 over a cubic extension K. Moreover, this extension is given adjoining the root of the cubic factor of the 7-division polynomial ψ_7. In our search, we find that all E/K are supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$ where $\mathfrak{l}|7$.

For $\ell = 11$, there do not exist any subgroups coming from [13] that have our desired condition. For $\ell = 13$, we find a few examples of curves satisfying Corollary D.

Example 6.3.4 ($\ell = 13$) Suppose that $E/\mathbf{Q}$ has $\rho_{E,13}(G_{\mathbf{Q}})$ conjugate to

$$H = \begin{pmatrix} a^3 & * \\ 0 & * \end{pmatrix} \quad \text{where } a \in \mathbf{F}_{13},$$

then E attains a K-rational point of order 13 over a bi-quadratic extension $K/\mathbf{Q}$ since $\#(\mathbf{F}_{13}^{\times})^3 = 4$. As an example, consider the elliptic curve

$$E\colon y^2 = x^3 - \frac{2248091}{180353}x + \frac{4496182}{180353},$$

which has mod 13 image conjugate to H. E attains a K-rational point of order 13 over a bi-quadratic extension K of $\mathbf{Q}$. The first quadratic extension $L/\mathbf{Q}$ is given by adjoining a quadratic root α of the 13-division polynomial ψ_{13}, and then the second quadratic is given by adjoining the square root of the $f(\alpha)$. We compute that $\mathrm{cl}(K) = 2$, $\zeta_{13} \notin K$, (2) splits in $\mathcal{O}_K$, and E/K is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$ where $\mathfrak{l}|13$. Therefore, the elliptic curve E and the number field K satisfy the conditions of Corollary D.

Example 6.3.5 ($\ell = 13$) Suppose that $E/\mathbf{Q}$ has $\rho_{E,13}(G_{\mathbf{Q}})$ conjugate to

$$H := \begin{pmatrix} a^4 & * \\ 0 & * \end{pmatrix} \quad \text{where } a \in \mathbf{F}_{13}.$$

Since $\#(\mathbf{F}_{13}^{\times})^4 = 3$, E attains a K-rational point of order 13 over cubic extension $K/\mathbf{Q}$. For example, consider the elliptic curve

$$E\colon y^2 = x^3 + 13674069x + 324405221670.$$

Using [13], E has mod 13 image conjugate to H. Now let $K/\mathbf{Q}$ denote the number field defined by the cubic factor of ψ_{13}. For notational purposes, we shall write $K = \mathbf{Q}(\alpha)$ where α is the primitive element of K. By base changing to K, we find that $E_K = E \times_{\mathbf{Q}} K$ has K-rational 13-torsion point. We also compute that $\mathrm{cl}(F) = 1$, 2 splits in $\mathcal{O}_K$, $\zeta_{13} \notin K$, and that E/K is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$ where $\mathfrak{l}|13$. Therefore, the elliptic curve E and the number field K satisfy the conditions of Corollary D.

Example 6.3.6 ($\ell = 13$) Suppose that an elliptic curve has $\rho_{E,13}(G_{\mathbf{Q}})$ conjugate to

$$\begin{pmatrix} a^2 & * \\ 0 & * \end{pmatrix} \quad \text{where } a \in \mathbf{F}_{13}.$$

Since $\#(\mathbf{F}_{13}^{\times})^2 = 6$, E will attain a K-rational point of order 13 over an extension of degree 6. As an example, consider the elliptic curve

$$E\colon y^2 = x^3 - \frac{12096}{529}x + \frac{24192}{529},$$

which satisfies the above property. E attains a K-rational point of order 13 over a sextic extension K of $\mathbf{Q}$. The first cubic extension $L/\mathbf{Q}$ is given by adjoining a cubic root α of the 13-division polynomial ψ_{13}, and then the second quadratic is given by adjoining the square root of the $f(\alpha)$. We also compute that $\mathrm{cl}(F) = 4$, 2 splits in $\mathcal{O}_K$, $\zeta_{13} \notin K$, and that E/K is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$ where $\mathfrak{l}|13$. Therefore, the elliptic curve E and number field K satisfy the conditions of Corollary D.

Potential example 6.3.7 ($\ell = 13$) Suppose that an elliptic curve $E/\mathbf{Q}$ has mod 13 image conjugate to $B(13)$. The curve E will attain a K-rational point of order 13 over an extension of degree 12. The difficultly in verifying the conditions of Corollary D is computing the class number and ramification indicies for the duodecic extension K.

Finally for $\ell = 37$, there is only one $E/\overline{\mathbf{Q}}$ that we need to consider.

Potential example 6.3.8 ($\ell = 37$) Suppose that $E/\mathbf{Q}$ is the elliptic curve with j-invariant $-7 \cdot 11^3$, which has affine equation

$$E\colon y^2 = x^3 - \frac{251559}{11045}x + \frac{503118}{11045}.$$

From [13, Theorem 1.10.(ii)], we know that the mod 37 image of E is conjugate to

$$H := \begin{pmatrix} a^3 & * \\ 0 & * \end{pmatrix} \quad \text{where } a \in \mathbf{F}_{37}.$$

Since $\#(\mathbf{F}_{37}^{\times})^3 = 12$, E attains a K-rational point of order 37 over a duodecic extension $K/\mathbf{Q}$.

As before, the difficultly in verifying the conditions of Corollary D is computing the class number and ramification indicies for the duodecic extension K.

Acknowledgements

The author wishes to thank Ken Ono for initially suggesting this project, David Zureick-Brown for his guidance and patience in explaining the finer details and for his help generalizing the conditions of [2] in a series of conversations, [19] for help in Lemma 5.5, and [20] for help in Remark 2.2. The computations in this paper were performed using the `Magma` computer algebra system [21]. For `Magma` code verifying the claims in Sect. 6, we refer the reader to [22].

Received: 26 February 2016 Accepted: 20 September 2016
Published online: 05 October 2016

References

1. Silverman, J.H.: The arithmetic of elliptic curves, vol. 106. Springer, Berlin (2009)
2. Frey, G.: On the Selmer group of twists of elliptic curves with **Q**-rational torsion points. Can. J. Math. **XL**, 649–665 (1988)
3. Mazur, B.: Modular functions of one variable V, pp. 107–148. Springer, Berlin (1977)
4. Ono, K.: Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves. Journal fur die reine und angewandte Mathematik **533**, 81–98 (2001)
5. Balog, A., Ono, K.: Elements of class groups and Shafarevich-Tate groups of elliptic curves. Duke Math. J. **120**(1), 35–63 (2003)
6. Sutherland, A.V.: Torsion subgroups of elliptic curves over number fields. Preprint (2012)
7. Derickx, M.: Torsion points on elliptic curves and gonalities of modular curves. Master's thesis, Universiteit Leiden (2012)
8. Kamienny, S.: Torsion points on elliptic curves and q-coefficients of modular forms. Invent. Math. **109**(1), 221–229 (1992)
9. Parent, P.: No 17-torsion on elliptic curves over cubic number fields. Journal de théorie des nombres de Bordeaux **15**(3), 831–838 (2003)
10. Kamienny, S., Stein, W., Stoll, M.: Torsion points on elliptic curves over quartic number fields. Preprint
11. Derickx, M., Kamienny, S., Stein, W., Stoll, M.: Torsion points on elliptic curves over number fields of small degree. In preparation (private communication)
12. Lozano-Robledo, Á.: On the field of definition of p-torsion points on elliptic curves over the rationals. Math. Ann. **357**(1), 279–305 (2013)
13. Zywina, D.: On the possible images of the mod ℓ representations associated to elliptic curves over **Q**. http://www.math.cornell.edu/~zywina/papers/PossibleImages/index.html (2015)
14. Neukirch, J.: Algebraic number theory. Springer, Berlin (1999)
15. Washington, L.C.: Introduction to cyclotomic fields, vol. 83. Springer, Berlin (2012)
16. Mailhot, J.: Selmer groups for elliptic curves with isogenies of prime degree. PhD thesis, University of Washington (2003)
17. Katz, N.M.: Galois properties of torsion points on abelian varieties. Invent. Math. **62**(3), 481–502 (1980)
18. Néron, A.: Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. Inst. Hautes Études Sci. Publ. Math. No. **21**, 128 (1964)
19. Epargyreus: Lack of ramification in cyclic extensions. Mathematics stack exchange. http://math.stackexchange.com/q/1585179
20. Mo, G.: Hecke characters and Conductors. MathOverflow. http://mathoverflow.net/q/223873
21. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**(3–4), 235–265 (1997). doi:10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993)
22. Morrow, J.S.: Electronic transcript of computations for the manuscript "The Selmer group of twists of elliptic curves over K with K-rational torsion points". https://drive.google.com/open?id=0Bx7T-L2ZBv-NNjllZFVtNXBsMUk