International Journal of Number Theory
© World Scientific Publishing Company

BOUNDS FOR THE TORSION OF ELLIPTIC CURVES OVER EXTENSIONS WITH BOUNDED RAMIFICATION.

ÁLVARO LOZANO-ROBLEDO
Dept. of Mathematics, University of Connecticut U-3009, 196 Auditorium Rd. MSB312
Storrs, CT 06269, USA
alozano@math.uconn.edu

BENJAMIN LUNDELL
Dept. of Mathematics, Cornell University, 120 Malott Hall
Ithaca, NY 14853, USA
blundell@math.cornell.edu

Received (Day Month Year)
Accepted (Day Month Year)

Communicated by xxx

Let E be a semi-stable elliptic curve defined over $\mathbb{Q}$, and fix $N \geq 2$. Let $K_N/\mathbb{Q}$ be a maximal algebraic Galois extension of $\mathbb{Q}$ whose ramification indices are all at most N. We show that there exists a computable bound $B(N)$, which depends only on N and not on the choice of $E/\mathbb{Q}$, such that the size of $E(K_N)_{\text{Tors}}$ is always at most $B(N)$.

Keywords: Torsion; elliptic curves; bounds; semi-stable.

Mathematics Subject Classification 2000: 14H52, 14G05

1. Introduction

Let K be a number field and let E/K be an elliptic curve. The Mordell-Weil Theorem states that $E(K)$, the set of K-rational points on E, can be given the structure of a finitely generated abelian group. In this note we consider elliptic curves defined over the rationals $\mathbb{Q}$ and provide bounds for the size of $E(K)_{\text{Tors}}$, where K is an algebraic Galois extension of $\mathbb{Q}$.

Theorem 1. *Let $E/\mathbb{Q}$ be an elliptic curve, let $S_{E,add}$ be the set of primes of additive reduction of $E/\mathbb{Q}$, and let $N \geq 2$ be fixed. Let K be an algebraic Galois extension of $\mathbb{Q}$ (not necessarily finite) unramified at primes in $S_{E,add}$ such that the ramification index of any other prime p in $K/\mathbb{Q}$ is finite and bounded by N. Then $E(K)_{\text{Tors}}$ is finite and there is a computable bound $B = B(E, N)$ for its size. Moreover, if E is semi-stable, then the bound B is independent of E.*

The bound will follow from a more general result, Theorem 16, and will be made explicit in Theorem 17. The proofs of Theorems 16 and 17 are elementary in that they require little more than the theory of Tate curves and standard results from a first course on elliptic curves. However, they rely on deep results of Mazur (Theorems 4 and 14 below) and Serre (Propositions 11 and 12 of [12]).

Applying Theorem 1 when K is an unramified extension of a finite extension F of $\mathbb{Q}$, we are able to obtain the following.

Theorem 2. *Let $E/\mathbb{Q}$ be a semi-stable elliptic curve. Let $F/\mathbb{Q}$ be a finite Galois extension of degree $d > 7$. Let K be the maximal unramified extension of F. Suppose that P is a point of exact order ℓ^n for some prime number ℓ defined over K, then $\ell \leq d+1$ and $\ell^n < \left(\frac{3}{2}\right)^4 (d+1)^2 d^4$ if ℓ is odd, or $2^n \leq 2^9 d^4$ if $\ell = 2$.*

Notice, in particular, that these bounds are *polynomial* in the degree d of the extension $F/\mathbb{Q}$. Compare this to the celebrated results on the Uniform Boundedness Conjecture, proved by Merel in 1996 and improved by Parent in 1999, where the assumptions are much more general, but the bounds are *exponential* in d.

Theorem 3 (Merel, [8], Theorem, and Parent, [9], Theorem 1.3). *Let K be a number field of degree $[K : \mathbb{Q}] = d > 1$. Then:*

(1) (Merel, 1996) Let E/K be an elliptic curve. If $E(K)$ contains a point of exact prime order ℓ, then $\ell \leq d^{3d^2}$.[a]

(2) (Parent, 1999) If P is a point of exact prime power order ℓ^n, then

(a) $\ell^n \leq 65(3^d - 1)(2d)^6$, if $\ell \geq 5$

(b) $\ell^n \leq 65(5^d - 1)(2d)^6$, if $\ell = 3$

(c) $\ell^n \leq 129(3^d - 1)(3d)^6$, if $\ell = 2$.

Merel and Parent proved these results by extending methods of Kamienny and Mazur using the theory of Jacobian varieties and Hecke Algebras (see [1] for a survey of the work of Kamienny and Mazur).

The improvement in Theorem 2 is not too surprising given that it applies only to *semi-stable* elliptic curves *defined over* $\mathbb{Q}$, as opposed to a general elliptic curve as in Theorem 3. Still, this difference is important because it quantifies how difficult it is for a semi-stable elliptic curve defined over $\mathbb{Q}$ to acquire torsion in an arbitrary degree d number field.

One would like to write down the complete (finite) collection of possible isomorphism types of $E(K)_{\mathrm{Tors}}$, for E an arbitrary elliptic curve defined over a degree d number field K. Moreover, one would like to know the sub-collection of groups for semi-stable curves defined over $\mathbb{Q}$. However, the general case is only known for $d = 1$ and 2, i.e., for $K = \mathbb{Q}$ and for quadratic fields (as stated in [11], Theorem 6.9).

[a] In [8], Merel claims that Oesterlé can lower this to $\ell \leq (1 + 3^{d/2})^2$.

Theorem 4 (Mazur, [6], Theorem 8). *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathbb{Q})_{\text{Tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \textit{with } 1 \le M \le 10 \textit{ or } M = 12, \textit{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \textit{with } 1 \le M \le 4. \end{cases}$$

Theorem 5 (Kenku and Momose, [4], Kamienny, [3]). *Let $K/\mathbb{Q}$ be a quadratic field and let E/K be an elliptic curve. Then*

$$E(K)_{\text{Tors}} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \textit{with } 1 \le M \le 16 \textit{ or } M = 18, \textit{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \textit{with } 1 \le M \le 6, \textit{ or} \\ \mathbb{Z}/3M\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \textit{with } M = 1 \textit{ or } 2, \textit{ only if } K = \mathbb{Q}(\sqrt{-3}), \textit{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \textit{only if } K = \mathbb{Q}(\sqrt{-1}). \end{cases}$$

In our restricted case, we present results (see Proposition 21) which are analogous to, but less specific than, Theorems 4 and 5; we provide bounds for the possible group structures for $E(K)$ when K satisfies the assumptions of Theorem 1 but do not determine the precise list of possible torsion subgroups over these large fields. It is important to notice, however, that our bounds only depend on the ramification indices of the field, and not on the degree of the extension.

The layout of the paper is as follows: Section 2 gives a brief discussion of linear algebra over the ring $\mathbb{Z}/\ell^n\mathbb{Z}$ for a prime number ℓ; Section 3 covers some preliminary results; the proofs of Theorems 1 and 2 are presented in Section 4; and Section 5 discusses an application of the main theorem to fields with very small ramification.

2. Linear algebra over $\mathbb{Z}/\ell^n\mathbb{Z}$

Let E be an elliptic curve defined over any field F. For all prime numbers ℓ not equal to the characteristic of F, the kernel of the multiplication-by-ℓ^m map (defined over $\bar{F}$), $E[\ell^m]$, is isomorphic to $\mathbb{Z}/\ell^m\mathbb{Z} \oplus \mathbb{Z}/\ell^m\mathbb{Z}$ as an abelian group.

If $\rho_\ell\colon \operatorname{Gal}(\bar{F}/F) \to \operatorname{Aut}(T_\ell)$ is the ℓ-adic representation associated to E, then reducing modulo ℓ^m gives a representation

$$\bar{\rho}_{\ell^m}\colon \operatorname{Gal}(\bar{F}/F) \to \operatorname{Aut}(T_\ell/\ell^m T_\ell) \simeq \operatorname{Aut}(E[\ell^m]) \simeq \operatorname{Aut}(\mathbb{Z}/\ell^m\mathbb{Z} \oplus \mathbb{Z}/\ell^m\mathbb{Z}),$$

and after choosing a basis $\langle P_m, Q_m\rangle$ for $E[\ell^m]$, we obtain a map

$$\bar{\rho}_{\ell^m}\colon \operatorname{Gal}(\bar{F}/F) \to \operatorname{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z}).$$

Moreover, if $n < m$, then we can reduce again modulo ℓ^n to get a map

$$\bar{\rho}_{\ell^n}\colon \operatorname{Gal}(\bar{F}/F) \to \operatorname{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}),$$

where our basis for $E[\ell^n]$ is given by $\langle P_n, Q_n\rangle$, with $P_n = [\ell^{m-n}]P_m$ and $Q_n = [\ell^{m-n}]Q_m$.

Now let $R_m = a_m P_m + b_m Q_m \in E[\ell^m]$ be any point of exact order ℓ^m. Let ν_ℓ be the standard ℓ-adic valuation of $\mathbb{Q}$, i.e. $\nu_\ell(\ell) = 1$. By abuse of notation, we will also use ν_ℓ on elements of $\mathbb{Z}/\ell^m\mathbb{Z}$ so that if a_m and b_m are elements of $\mathbb{Z}/\ell^m\mathbb{Z}$, then their ℓ-adic valuations satisfy $0 \leq \nu_\ell(a_m), \nu_\ell(b_m) \leq m$. In particular, since R_m is of exact order ℓ^m, we must have that one of $\nu_\ell(a_m)$ or $\nu_\ell(b_m)$ is zero (i.e. one of a_m or b_m is a unit modulo ℓ^m). Note also that the ℓ-adic valuation being equal to m is equivalent to that coefficient being zero.

Now suppose that we take some multiple $R_n = [\ell^{m-n}]R_m$ (with $n < m$) of R_m. Then R_n is a point of exact order ℓ^n and we have that $R_n = a_nP_n + b_nQ_n$ with P_n and Q_n as above, $a_m \equiv a_n \bmod \ell^n$, and $b_m \equiv b_n \bmod \ell^n$. The next lemma is elementary and we omit the proof.

Lemma 6. *If $a_n \neq 0$, then $\nu_\ell(a_m) = \nu_\ell(a_n)$, and if $b_n \neq 0$ then $\nu_\ell(b_m) = \nu_\ell(b_n)$.*

3. Remarks on ramification indices

Let $E/\mathbb{Q}$ be an elliptic curve and fix, once and for all, a global minimal model for E. Let $\ell \geq 2$ be a prime number and let $R_n \in E[\ell^n]$ be a point of exact order ℓ^n. Let M_n be the Galois closure of $\mathbb{Q}(R_n)$ over $\mathbb{Q}$. In this section we collect information about the ramification in the extensions $M_n/\mathbb{Q}$ and $\mathbb{Q}(E[\ell^n])/\mathbb{Q}$ for any prime ℓ and natural number n. These extensions can only be ramified at the prime ℓ and primes of bad reduction for E by the criterion of Néron-Ogg-Shafarevich.

Our main method will be to study the ramification in certain local Galois extensions $L_n/\mathbb{Q}_p$ where p is a prime of bad (multiplicative) reduction for E, or $p = \ell$. To do so, we choose an embedding of $\bar{\mathbb{Q}}$ into $\bar{\mathbb{Q}}_p$ for each p and fix it for the remainder of this paper.

Additionally, we adopt the convention that when we choose a basis $\{P_n, Q_n\}$ for $E[\ell^n]$, we are actually choosing a basis for all $E[\ell^\infty]$. That is, we are choosing bases $\{P_n, Q_n\}$ for all n simultaneously such that $P_n = [\ell]P_{n+1}$ and $Q_n = [\ell]Q_{n+1}$ for all $n \geq 0$.

3.1. *Good reduction*

Suppose that E has good reduction at ℓ. For this section, set L_n to be the compositum $M_n\mathbb{Q}_p$. Let $\bar{\mathbb{Z}}_\ell$ be the ring of integers of $\bar{\mathbb{Q}}_\ell$ and let $\mathcal{M}_\ell$ be the maximal ideal of $\bar{\mathbb{Z}}_\ell$. We will denote by ν the valuation on $\bar{\mathbb{Q}}_\ell$ which extends the usual ℓ-adic valuation ν_ℓ of $\mathbb{Q}$, i.e. we require $\nu(\ell) = 1$. Finally, let I_ℓ be the inertia subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$.

Since E has good reduction at ℓ, we have an exact sequence of $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-modules:

$$0 \to E_1(\bar{\mathbb{Q}}_\ell)[\ell^n] \to E(\bar{\mathbb{Q}}_\ell)[\ell^n] \to \tilde{E}(\bar{\mathbb{F}}_\ell)[\ell^n] \to 0, \tag{3.1}$$

where $\tilde{E}$ is a non-singular elliptic curve, $E \to \tilde{E}$ is given by reduction modulo $\mathcal{M}_\ell$, and E_1 is its kernel. Notice that $E_1(\bar{\mathbb{Q}}_\ell)$ is a $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-submodule of E. If E has ordinary reduction, then $E_1(\bar{\mathbb{Q}}_\ell)[\ell^n]$ has order ℓ^n and it has order ℓ^{2n} if the reduction is supersingular. We will divide our study into three parts:

(1) Understand the ramification in $L_n/\mathbb{Q}_p$ when the reduction of R_n is trivial;

(2) Understand the ramification in $L_n/\mathbb{Q}_p$ when the reduction of R_n generates $\tilde{E}(\bar{\mathbb{F}}_\ell)[\ell^n]$; and

(3) Understand the ramification in $L_n/\mathbb{Q}_p$ when the reduction of R_n is neither trivial nor generates $\tilde{E}(\bar{\mathbb{F}}_\ell)[\ell^n]$.

We begin with a result of Serre which explains the case $n = 1$.

Proposition 7. *[Serre, [12], Section 1.11] Suppose first that E has ordinary reduction at ℓ. Then $\mathrm{Gal}(\mathbb{Q}_\ell(E[\ell])/\mathbb{Q}_\ell)$ is isomorphic to a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Moreover, the image of I_ℓ under $\bar{\rho}_\ell$ has order $\ell - 1$ or $\ell(\ell - 1)$ and is of the form*

$$\left\{\begin{pmatrix} \star & 0 \\ 0 & 1 \end{pmatrix}\right\} \quad \text{or} \quad \left\{\begin{pmatrix} \star & \star \\ 0 & 1 \end{pmatrix}\right\},$$

with respect to any basis $\{P_1, Q_1\}$ with $P_1 \in E_1(\bar{\mathbb{Q}}_\ell)$.

If, instead, E has supersingular reduction at ℓ, then the images of I_ℓ and $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ under $\bar{\rho}_\ell$ are a non-split Cartan subgroup (cyclic of order $\ell^2 - 1$) and its normalizer (of order $2(\ell^2 - 1)$), respectively.

We remind the reader that the normalizer of a non-split Cartan subgroup is a group of the form

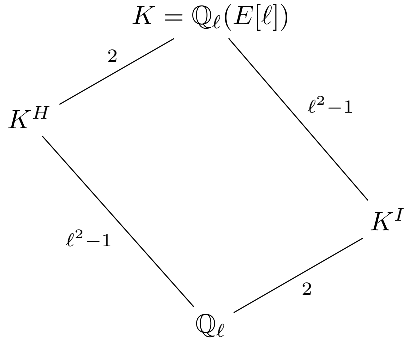
$$N = \left\{\begin{pmatrix} a & b\epsilon \\ b & a \end{pmatrix}, \begin{pmatrix} a & b\epsilon \\ -b & -a \end{pmatrix} : a, b \in \mathbb{Z}/\ell\mathbb{Z},\ (a, b) \neq (0, 0)\right\},$$

where ϵ is an arbitrary quadratic non-residue in $\mathbb{Z}/\ell\mathbb{Z}$.

Lemma 8. *Let R_1 be a point of exact order ℓ in $E_1(\bar{\mathbb{Q}}_\ell)$, the kernel of the reduction map. Then the extension $\mathbb{Q}_\ell(R_1)/\mathbb{Q}_\ell$ is always non-trivial and ramified, and its ramification index is either $\ell - 1$ if the reduction is ordinary or $\ell^2 - 1$ if the reduction is supersingular.*

Proof. Choose any other point $Q_1 \in E[\ell]$ such that $\langle R_1, Q_1 \rangle = E[\ell]$. If E has ordinary reduction at ℓ, then the lemma is immediate from Proposition 7: as R_1 is in the kernel of the reduction map, the fields $\mathbb{Q}_\ell(R_1)$ and $\mathbb{Q}_\ell(\zeta_l)$ are equal, and the ramification index in the extension $\mathbb{Q}_\ell(R_1)/\mathbb{Q}_\ell$ is therefore $\ell - 1$.

If E has supersingular reduction at ℓ, then we need to consult the field diagram



where $H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\}$ is the subgroup of $\mathrm{Gal}(K/\mathbb{Q}_\ell)$ (the normalizer of a non-split Cartan subgroup) which fixes R_1 (here we are using the fact that we took R_1 to be the first element in the basis for $E[\ell]$). Because I is a non-split Cartan subgroup, $\langle I, H\rangle = \mathrm{Gal}(K/\mathbb{Q}_\ell)$, so that $K^H \cap K^I = \mathbb{Q}_\ell$. Thus, $K^H = \mathbb{Q}_l(R_1)$ is totally ramified extension of $\mathbb{Q}_\ell$ of degree $\ell^2 - 1$. □

We now move on to values of $n > 1$. For such n and any $0 < i < n$, set $R_i = [\ell^{n-i}]R_n$. Note that R_i is a point of exact order ℓ^i.

Lemma 9. *Let $n > 1$ and suppose that $R_n \in E_1(\bar{\mathbb{Q}}_\ell)$, that is, suppose that R_n reduces to the origin modulo $\mathcal{M}_\ell$. Then the ramification index in the extension $\mathbb{Q}_\ell(R_n)/\mathbb{Q}_\ell$ is at least $\varphi(\ell^n) = \ell^{n-1}(\ell - 1)$ if the reduction is ordinary and $(\ell^2 - 1)\ell^{n-1}$ if the reduction is supersingular.*

Proof. Note first that each of the multiples of R_n is in the kernel of the reduction modulo $\mathcal{M}_\ell$ map. Next, the theory of formal groups (see [13], IV, Proposition 2.2) shows that $E_1(\bar{\mathbb{Q}}_\ell) \cong \widehat{E}(\mathcal{M}_\ell)$, where $\widehat{E}$ is the formal group associated to E. The isomorphism is given by $(x, y) \mapsto t((x, y)) = -x/y$.

Put $t_i = t(R_i) \in \widehat{E}$. Since $t_i \in \mathcal{M}_\ell$, we have that $\nu(t_i) > 0$. On the other hand, by Theorem IV.6.1 of [13],

$$\nu(t_i) \leq \frac{\nu(\ell)}{\ell^i - \ell^{i-1}} \leq 1$$

for all $1 \leq i \leq n$. Further, by Corollary IV.4.4 of [13], there exist power series $f(T), g(T) \in \bar{\mathbb{Z}}_\ell[[T]]$ with $f(0) = g(0) = 0$ such that

$$[\ell](T) = \ell f(T) + g(T^\ell).$$

In particular, $t_i = [\ell](t_{i+1}) = \ell f(t_{i+1}) + g(t_{i+1}^\ell)$. If $\nu(t_{i+1}) \geq \nu(t_i)$, then the right hand side of the previous equation would have strictly larger valuation than t_i. Thus, we must have $0 < \nu(t_{i+1}) < \nu(t_i) \leq 1$, for all $1 \leq i \leq n$. Hence, the extension $\mathbb{Q}_\ell(t_{i+1})/\mathbb{Q}_\ell(t_i)$ is ramified, and therefore the extension $\mathbb{Q}_\ell(R_{i+1})/\mathbb{Q}_\ell(R_i)$ is ramified at ℓ.

By Lemma 8, the ramification in the extension $\mathbb{Q}_\ell(R_1)/\mathbb{Q}_\ell$ is either $\ell - 1$ or $\ell^2 - 1$ according to the type of good reduction, and the extension $\mathbb{Q}_\ell(E[\ell])/\mathbb{Q}_\ell(R_1)$ is either unramified or the ramification degree is ℓ. Moreover, the extension $\mathbb{Q}_\ell(E[\ell^{i+1}])/\mathbb{Q}_\ell(E[\ell^i])$ is Galois, and its degree is a divisor of ℓ^4. Since $\mathbb{Q}_\ell(R_n) \subseteq \mathbb{Q}_\ell(E[\ell^n])$, we conclude that the ramification of the extension $\mathbb{Q}_\ell(R_n)/\mathbb{Q}_\ell(R_1)$ is a power of ℓ, and we showed above that $\mathbb{Q}_\ell(R_{i+1})/\mathbb{Q}_\ell(R_i)$ is ramified for all $i \geq 1$ (thus, the ramification at every step is at least ℓ). Hence, the ramification of $\mathbb{Q}_\ell(R_n)/\mathbb{Q}_\ell(R_1)$ must be at least $(\ell - 1)\ell^{n-1} = \varphi(\ell^n)$ or $(\ell^2 - 1)\ell^{n-1}$ according to the reduction type, as claimed. □

We now understand the ramification coming from points in the kernel of reduction. In particular if E has supersingular reduction at ℓ, then $E_1(\bar{\mathbb{Q}}_\ell)[\ell^n] =$

$E(\bar{\mathbb{Q}}_\ell)[\ell^n]$ and the previous Lemma applies for every point of order ℓ^n. Next we consider the case of ordinary reduction, and in particular we study the case where the reduction of R_n generates $\tilde{E}(\bar{\mathbb{F}}_\ell)[\ell^n]$.

Lemma 10. *Let $n > 1$ ($n > 3$ if $\ell = 2$) and suppose that the reduction of R_n modulo $\mathcal{M}_\ell$ generates $\tilde{E}(\bar{\mathbb{F}}_\ell)[\ell^n]$. Then the residual degree of $\mathbb{Q}_\ell(R_n)/\mathbb{Q}_\ell$ satisfies $f_{\mathbb{Q}_\ell(R_n)} \geq n$. In particular, there is a sub-extension $F \subset \mathbb{Q}_\ell(R_n)$ such that $F/\mathbb{Q}_\ell$ is unramified and of degree at least n.*

Proof. Let $t < n$, $q = \ell^t$ and let $\mathbb{F}_q$ be a finite field with q elements. The Hasse bound implies that

$$0 < q + 1 - 2\sqrt{q} \leq \#\tilde{E}(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q} < \ell^n,$$

due to our assumption that $n > 1$ (and $n > 3$ if $\ell = 2$).

Thus, there cannot be any points of exact order ℓ^n defined over $\mathbb{F}_q$. Since extensions of the residue field are in one-to-one correspondence with unramified sub-extensions of $\mathbb{Q}_\ell(R_n)$, we are done. □

We now suppose that E has ordinary reduction at ℓ and consider the case where R_n is neither in the kernel of reduction, nor reduces to a generator of $E(\bar{\mathbb{F}}_\ell)[\ell^n]$. This is the step where we will need the fact that $L_n = M_n\mathbb{Q}_\ell$ is a Galois extension of $\mathbb{Q}_\ell$. We distinguish between the cases $\ell > 2$ and $\ell = 2$.

Lemma 11. *Suppose that $E/\mathbb{Q}$ has good ordinary reduction at ℓ. Let $n > 1$ ($n > 4$ if $\ell = 2$) and suppose that $R_n \in E(\bar{\mathbb{Q}}_\ell)[\ell^n]$ is a point of exact order ℓ^n which is neither in the kernel of reduction, nor reduces to a generator of $\tilde{E}(\bar{\mathbb{F}}_\ell)[\ell^n]$. Then:*

(1) If $\ell > 2$ then the ramification index of $L_n/\mathbb{Q}_\ell$ is at least $\varphi(\ell^n)$;

(2) If $\ell = 2$ then either the ramification index of $L_n/\mathbb{Q}_\ell$ is at least $\varphi(2^{n-1}) \geq 2$, or the residual degree of $L_n/\mathbb{Q}_\ell$ satisfies $f_{L_n} \geq n - 1$. In particular, there is a sub-extension $F \subset L_n$ such that $F/\mathbb{Q}_\ell$ is unramified and of degree at least $n - 1$.

Proof. Let $\{P_n, Q_n\}$ be a $\mathbb{Z}/\ell^n\mathbb{Z}$-basis of $E[\ell^n]$ such that P_n is in the kernel of reduction and Q_n generates all the image of the reduction map, i.e. the reduction of Q_n is a point of exact order ℓ^n in $\tilde{E}(\bar{\mathbb{F}}_\ell)$. Recall that $E_1(\bar{\mathbb{Q}}_\ell)$ is a $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-stable submodule (see Equation 3.1) so that $G_n = \mathrm{Gal}(\mathbb{Q}_\ell(E[\ell^n])/\mathbb{Q}_\ell)$ is a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

Because the action of Galois on $\tilde{E}(\bar{\mathbb{F}}_\ell)$ factors through the map $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathrm{Gal}(\bar{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ (composed with the natural action of $\mathrm{Gal}(\bar{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ on $\tilde{E}(\bar{\mathbb{F}}_\ell)$) and I_ℓ is the kernel of this map, $\tilde{E}(\bar{\mathbb{F}}_\ell)$ is fixed by I_ℓ. Thus, $G_n \cap I_\ell$ is a subgroup of the form:

$$\left\{ \begin{pmatrix} \chi & \delta \\ 0 & 1 \end{pmatrix} \right\}.$$

Notice that the upper left corner, the character χ, must be the full ℓ^nth cyclotomic character because $\mathbb{Q}_\ell(\zeta_{\ell^n}) \subseteq \mathbb{Q}_\ell(E[\ell^n])$ and $\mathbb{Q}_\ell(\zeta_{\ell^n})/\mathbb{Q}_\ell$ is certainly ramified.

Let $R_n = a_nP_n + b_nQ_n \in E(\bar{\mathbb{Q}}_\ell)$. Since R_n is not in the kernel of reduction, we know that $b_n \neq 0$; since $\tilde{R}_n$ does not generate $\tilde{E}(\bar{\mathbb{F}}_\ell)$, we know that b_n is not a unit. Thus $b_n \equiv 0 \bmod \ell$, and $\nu_\ell(b_n) < n$. Since R_n is of exact order n, the coefficient a_n must be a unit modulo ℓ^n.

(1) Suppose $\ell > 2$. Let $\sigma \in I_\ell$ be a matrix congruent to $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \bmod \ell$ (such an element exists because $\ell > 2$ and Prop. 7). Then,

$$\sigma(R_n) = (a_n\chi(\sigma) + b_n\delta(\sigma))P_n + b_nQ_n$$

is defined over L_n because $L_n/\mathbb{Q}_\ell$ is Galois, and

$$\sigma(R_n) - R_n = (a_n(\chi(\sigma) - 1) + b_n\delta(\sigma))P_n \equiv a_nP_n \bmod \ell.$$

Since a_n is a unit mod ℓ^n, the point $\sigma(R_n) - R_n$ has exact order ℓ^n, it is in the kernel of reduction (it is a multiple of P_n) and defined over L_n (recall that E is defined over $\mathbb{Q}$, so the addition in E is defined over $\mathbb{Q}$). Hence, by Lemma 9, the ramification degree of $L_n/\mathbb{Q}_\ell$ is at least $\varphi(\ell^n)$.

(2) Suppose $\ell = 2$, $n > 4$, and $b_n \equiv 0 \bmod 2$. Let us write $b_n = 2d_n$, for some non-zero $d_n \in \mathbb{Z}$. Let $\tau \in I_\ell$ be such that $\chi(\tau) \equiv 3 \bmod 8$ (recall that χ is the cyclotomic character, thus, for every $\alpha \in (\mathbb{Z}/8\mathbb{Z})^\times$ there must be an element τ of I_ℓ such that $\chi(\tau) \equiv \alpha \bmod 8$).

(a) If $b_n\delta(\tau) \equiv 0 \bmod 4$, then:

$$\tau(R_n) - R_n = (a_n(\chi(\tau) - 1) + b_n\delta(\tau))P_n \equiv 2P_n \bmod 4$$

because $a_n \in (\mathbb{Z}/8\mathbb{Z})^\times$. Thus, $\tau(R_n) - R_n$ is a point of exact order 2^{n-1} in the kernel of reduction and defined over L_n. Therefore, the ramification index of $L_n/\mathbb{Q}_2$ is at least $\varphi(2^{n-1})$, by Lemma 9.

(b) If $b_n\delta(\tau) \equiv 2 \bmod 4$, then $b_n = 2d_n$ for some odd integer d_n. Thus, $R_n = a_nP_n + d_n(2Q_n) = a_nP_n + d_nQ_{n-1}$, and d_n is a unit in $\mathbb{Z}/2^n\mathbb{Z}$. Therefore, the reduction of R_n modulo $\mathcal{M}_2$ generates $\tilde{E}(\bar{\mathbb{F}}_2)[2^{n-1}]$. As we are assuming that $n > 4$, we may apply Lemma 10 to conclude that the residual degree of $L_n/\mathbb{Q}_\ell$ satisfies $f_{L_n} \geq n - 1$. □

The following proposition is an immediate corollary of Lemmas 10 and 11 and the criterion of Néron-Ogg-Shafarevich.

Proposition 12. *Let $E/\mathbb{Q}$ be an elliptic curve given by a minimal model with good reduction at a prime ℓ. Let $n > 1$ (or $n > 4$ if $\ell = 2$). Let R_n be a point of exact order ℓ^n, and let $M_n/\mathbb{Q}$ be the Galois closure of $\mathbb{Q}(R_n)$.*

(1) Let $\ell \geq 3$ and $n > 1$. Either the ramification index of ℓ in $M_n/\mathbb{Q}$ is at least $\varphi(\ell^n)$ or there is some prime p of bad reduction which ramifies in $M_n/\mathbb{Q}$.

(2) Let $\ell = 2$ and $n > 4$. Either the ramification index of $\ell = 2$ in $M_n/\mathbb{Q}$ is at least $\varphi(2^{n-1})$ or there is some prime p of bad reduction which ramifies in $M_n/\mathbb{Q}$.

3.2. *Bad multiplicative reduction*

We now drop the assumption that E has good reduction at ℓ. Instead, we let p be a prime of multiplicative reduction ($p = \ell$ is possible). The theory of Tate curves (see Chapter V of [14], for instance), gives an extension $F/\mathbb{Q}_p$ such that $E(\bar{F}) \cong \bar{F}^\times/q^{\mathbb{Z}}$, for some $q \in F$ such that $j(E) = j(q)$. In fact, if E has split multiplicative reduction at p, we can take $F = \mathbb{Q}_p$; otherwise, $F/\mathbb{Q}_p$ is a quadratic unramified extension. For this section, set L_n to be the compositum M_nF. Notice that L_n/F is Galois and it is the minimal field of definition of R_n over F (because $E(\bar{\mathbb{Q}}) \subseteq E(\bar{\mathbb{Q}}_p)$).

Under this isomorphism, $E(\bar{F})[\ell^n] \simeq \langle \zeta_{\ell^n}, q^{1/\ell^n}\rangle/q^{\mathbb{Z}}$. Let P_n be the inverse image of ζ_{ℓ^n} and let Q_n be the inverse image of q^{1/ℓ^n}. Then $\langle P_n, Q_n\rangle = E(\bar{F})[\ell^n]$, and we will write $R_n = a_nP_n + b_nQ_n$ with $a_n, b_n \in \mathbb{Z}/\ell^n\mathbb{Z}$. Finally, note that $F(E[\ell^n]) = F(\zeta_{\ell^n}, q^{1/\ell^n})$ and $F(R_n) = F(\zeta_{\ell^n}^{a_n} \cdot q^{b_n/\ell^n})$.

Let ν_ℓ and ν_p be the usual prime valuations on $\mathbb{Q}$. Set

$$\alpha_p = \nu_\ell(\nu_p(q)) = \nu_\ell(-\nu_p(j(E)))$$

and let γ_n be the smallest integer such that there is an $\ell^{n-\gamma_n}$ root of q defined over F, i.e., $q' = q^{1/\ell^{n-\gamma_n}} \in F$ and $q^{1/\ell^n} = (q')^{1/\ell^{\gamma_n}}$. Note that α_p is independent of n and $\alpha_p \geq n - \gamma_n$, for all n.

Recalling that L_n/F is Galois and the minimal field of definition of R_n over F and that $R_n \mapsto \zeta_{\ell^n}^{a_n} \cdot q^{b_n/\ell^n}$, we have

$$L_n = \begin{cases} F(\zeta_{\ell^n}, q^{b_n/\ell^n}) & \text{if } b_n \notin (\mathbb{Z}/\ell^n\mathbb{Z})^\times; & (3.2)\\ F(\zeta_{\ell^{\delta_n}}, q^{1/\ell^n}) & \text{if } b_n \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times, & (3.3)\end{cases}$$

where $\delta_n = \max\{\gamma_n, n - \nu_\ell(a_n)\}$. Because $F/\mathbb{Q}_p$ is unramified, the ramification index $e_p = e(L_n/\mathbb{Q}_p)$ of the extension $L_n/\mathbb{Q}_p$ equals the ramification index of the extension L_n/F. Moreover, we know that the ramification index of the extension $F(q^{b_n/\ell^n})/\mathbb{Q}_p$ is $\max(\ell^{n-v_\ell(b_n)-\alpha_p}, 1)$. Thus, we may conclude:

(1) If $L_n = F(\zeta_{\ell^n}, q^{b_n/\ell^n})$, then

$$e_p = \begin{cases} \varphi(\ell^n) \cdot \max(\ell^{n-v_\ell(b_n)-\alpha_p}, 1) & \text{if } p = \ell; & (3.4)\\ \max(\ell^{n-v_\ell(b_n)-\alpha_p}, 1) & \text{if } p \neq \ell. & (3.5)\end{cases}$$

(2) If $L_n = F(\zeta_{\ell^{\delta_n}}, q^{1/\ell^n})$, then

$$e_p = \begin{cases} \varphi(\ell^{\delta_n}) \cdot \max(\ell^{n-\alpha_p}, 1) & \text{if } p = \ell; & (3.6)\\ \max(\ell^{n-\alpha_p}, 1) & \text{if } p \neq \ell;. & (3.7)\end{cases}$$

3.3. *The Full Division Field*

In this section we review the necessary results about the full division field $\mathbb{Q}(E[\ell^n])$.

Lemma 13. *Let E be an elliptic curve defined over $\mathbb{Q}$, let ℓ be a prime, and let K be an algebraic Galois extension of $\mathbb{Q}$. Then $\mathbb{Q}(\mu_{\ell^n}) \subset \mathbb{Q}(E[\ell^n])$. Thus the ramification index of ℓ in the extension $\mathbb{Q}(E[\ell^n])/\mathbb{Q}$ is at least $\varphi(\ell^n)$. In particular, if ℓ*

is finitely ramified in K and $\varphi(\ell^n)$ is larger than the ramification index of ℓ in K, then $\mathbb{Q}(E[\ell^n])$ cannot be contained in K.

Proof. The non-degeneracy of the Weil pairing guarantees that any field containing all of the points of order ℓ^n contains the ℓ^n-th roots of unity, i.e.

$$\mathbb{Q}(\mu_{\ell^n}) \subseteq \mathbb{Q}(E[\ell^n]).$$

If we assume that $\mathbb{Q}(E[\ell^n]) \subseteq K$ then, in particular, $\mathbb{Q}(\mu_{\ell^n}) \subseteq K$, and the ramification index of ℓ in the extension $K/\mathbb{Q}$ is at least $\varphi(\ell^n)$. □

We quote a deep theorem of Mazur regarding the image of the ℓ-adic representation of E:

Theorem 14 (Mazur, [7] Theorems 3 and 4). *Let $E/\mathbb{Q}$ be an elliptic curve and ℓ a prime number. Let L be the set of prime numbers $L := \{p \leq 19\} \cup \{37, 43, 67, 163\}$. Then either $\ell \in L$ or the image of the representation $\bar{\rho}_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ attached to E is irreducible. Moreover, if E is semistable, then $\bar{\rho}_\ell$ is surjective for $\ell > 7$.*

Corollary 15. *Let $E/\mathbb{Q}$ be an elliptic curve and ℓ a prime number. Let L be the set of prime numbers $L := \{p \leq 19\} \cup \{37, 43, 67, 163\}$. Let K be an algebraic, Galois extension of $\mathbb{Q}$, and suppose R_1 is a point of exact order ℓ defined over K. Then $\ell \in L$ or the ramification at ℓ in $K/\mathbb{Q}$ is at least $\varphi(\ell) = \ell - 1$. If $E/\mathbb{Q}$ is semistable and $\ell > 7$, then the ramification index of $K/\mathbb{Q}$ is at least $\ell - 1$.*

Proof. If the image of $\bar{\rho}_\ell$ is surjective or irreducible then $E[\ell]$ has no non-trivial $\mathbb{Z}/\ell\mathbb{Z}[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$-submodules. Therefore, if R_1 is a non-trivial point of order ℓ defined over K, and $K/\mathbb{Q}$ is Galois, then $E[\ell]$ must be defined over K. Thus, by Lemma 13, $\mu_\ell \subset K$ and the ramification of $K/\mathbb{Q}$ at ℓ must be at least $\varphi(\ell)$. Thus, the result follows directly from Mazur's theorem. □

4. The proofs of Theorems 1 and 2

In this section, $K/\mathbb{Q}$ is an algebraic Galois extension. The ramification index of a rational prime ℓ in $K/\mathbb{Q}$ will be denoted by $e_K(\ell)$ when it is finite. For an elliptic curve E defined over $\mathbb{Q}$, we set the following notation for the remainder of the section:

- Let $S_{E,\mathrm{mult}}$ and $S_{E,\mathrm{add}}$ denote, respectively, the sets of rational primes where E has multiplicative and additive bad reduction;
- Let $S = S_{E,\mathrm{add}} \cup S_{E,\mathrm{mult}} \cup \{\ell\}$ for a fixed prime ℓ;
- Let $e_K = \max\limits_{p \in S}(e_K(p))$;
- Let $a(\ell, C)$ be the least integer such that $\varphi(\ell^a) > C$ if ℓ is odd (or $\varphi(2^{a-1}) > C$ if $\ell = 2$), for a given $C > 0$;
- Let $a = a(\ell, e_K)$;

- Let $b = b(\ell, E) \geq 0$ be the largest integer such that there exists a point of E of exact order ℓ^b defined over $\mathbb{Q}$;
- Let $n = \max(a, b+1, 2)$ if ℓ is odd and $n = \max(a, b+1, 5)$ if $\ell = 2$; and
- Set $m = a + 2n$.

Theorem 16. *Let $\ell \geq 2$ be a prime and let $E/\mathbb{Q}$ be an elliptic curve. Suppose that K is an algebraic Galois extension of $\mathbb{Q}$ such that any prime in S is finitely ramified in K, and any prime in $S_{E,add}$ is unramified in K. Then, there are no points of E of exact order ℓ^m defined over K.*

Proof. We may assume that $E/\mathbb{Q}$ is given by a minimal model, because the isomorphism class of $E(K)_{\mathrm{Tors}}$ only depends on the $\mathbb{Q}$-isomorphism class of E. Let R_m be a point in E of exact order ℓ^m. Then $R_n = [\ell^{m-n}]R_m$ is a point of exact order ℓ^n. Denote by M_m and M_n the Galois closures of $\mathbb{Q}(R_m)$ and $\mathbb{Q}(R_n)$ respectively. As $n > b$, $M_n/\mathbb{Q}$ is a non-trivial extension. We will show that if $R_m \in E(K)$, then $M_n/\mathbb{Q}$ is a non-trivial extension which is unramified at all rational primes. Since such extensions do not exist, the theorem will follow.

The proof has two steps. We will prove that the extension $M_n/\mathbb{Q}$ is unramified at primes of bad reduction using (mainly) the results of Section 3.2. Then, we will be able to deduce the theorem using (mainly) Proposition 12.

To begin, let p be a prime of bad additive reduction. By assumption p does not ramify in K. Since $M_n/\mathbb{Q}$, $M_m/\mathbb{Q}$, and $K/\mathbb{Q}$ are all Galois extensions, and we are assuming that $R_m \in E(K)$, we must have that $M_n \subset K$. Thus, M_n is unramified at all primes at which E has bad additive reduction.

Next, let p be a prime of bad multiplicative reduction, and define $F/\mathbb{Q}_p$, q, α_p, γ_m, δ_m, $M_mF = L_m$, and L_n as in Section 3.2. In particular, these choices assume that we have chosen compatible bases $\{P_m, Q_m\}$ and $\{P_n, Q_n\}$ for $E[\ell^m]$ and $E[\ell^n]$, respectively. Write $R_m = a_mP_m + b_mQ_m$ and $R_n = a_nP_n + b_nQ_n$.

Our next step is to analyze the extension $L_n/\mathbb{Q}_p$. We divide our study into three cases, based on the ℓ-adic valuation of b_n. In each case we will either reach a contradiction or show that $L_n/\mathbb{Q}_p$ is unramified.

$\boxed{\textit{Case 1: } \nu_\ell(b_n) = n}$

In this case, Equation (3.2) shows $L_n = F(\zeta_{\ell^n})$. If $p = \ell$, this extension is totally ramified of degree $\varphi(\ell^n) \geq \varphi(\ell^a) > e_K$, which is a contradiction. If $p \neq \ell$, this extension is unramified, as desired.

$\boxed{\textit{Case 2: } 0 < \nu_\ell(b_n) < n}$

In this case, Equation (3.2) shows $L_m = F(\zeta_{\ell^m}, q^{b_m/\ell^m})$. If $p = \ell$, Equation (3.4) shows that the ramification index is at least $\varphi(\ell^m) > \varphi(\ell^a) > e_K$, again a contradiction. If $p \neq \ell$, Equation (3.5) shows that the ramification index in $L_m/\mathbb{Q}_p$ is at least

$$\begin{aligned}\ell^{m-v_\ell(b_m)-\alpha_p} &= \ell^{m-v_\ell(b_n)-\alpha_p} \text{ by Lemma 6,}\\ &> \ell^{m-n-\alpha_p}\\ &= \ell^{a+n-\alpha_p}\end{aligned}$$

We will return to this case in a moment.

$\boxed{\textit{Case 3: } \nu_\ell(b_n) = 0}$

In this case, Lemma 6 shows that b_m is also a unit. Equation (3.3) then shows that $L_m = F(\zeta_{\ell^{\delta_m}}, q^{1/\ell^m})$. If $p = \ell$, then Equation (3.6) shows that the ramification index in $L_m/\mathbb{Q}_p$ is at least $\varphi(\ell^{\delta_m})$. This forces $\delta_m < a$. Consequently, $m - \delta_m > m - a = 2n > n$. Thus $L_n \subseteq L_{m-\delta_m}$.

If R_m corresponds locally to the point $\zeta_{\ell^m}^{a_m} \cdot q^{b_m/\ell^m}$, then $R_{m-\delta_m} = [\ell^{\delta_m}](R_m)$ corresponds locally to the point $(\zeta_{\ell^m}^{a_m})^{\ell^{\delta_m}} \cdot (q^{b_m/\ell^m})^{\ell^{\delta_m}}$. Since $\delta_m \geq m - \nu_\ell(a_m)$ then $(\zeta_{\ell^m}^{a_m})^{\ell^{\delta_m}} = 1$. Similarly, since $\delta_m \geq \gamma_m$, then $(q^{b_m/\ell^m})^{\ell^{\delta_m}} \in F$ by the definition of γ_m. Hence, $L_{m-\delta_m} = F$ and we have shown that $L_n \subseteq L_{m-\delta_m} = F$. Since $F/\mathbb{Q}_p$ is unramified, this is the desired result. Now, if $p \neq \ell$, then Equation (3.7) shows that the ramification of $L_m/\mathbb{Q}_p$ is at least $\ell^{m-\alpha_p} > \ell^{a+n-\alpha_p}$.

	$p = \ell$	$p \neq \ell$
$\nu_\ell(b_n) = n$	Contradiction	Unramified
$0 < \nu_\ell(b_n) < n$	Contradiction	$e_{L_m}(p) > \ell^{a+n-\alpha_p}$
$\nu_\ell(b_n) = 0$	Unramified	$e_{L_m}(p) > \ell^{a+n-\alpha_p}$

Table 1. A summary of our findings so far.

It remains to deal with the two cases in the bottom right of Table 1. Suppose that $\alpha_p < n$. Then $a + n - \alpha_p > a + n - n = a$. In particular, the ramification index of $L_m/\mathbb{Q}_p$ would be at least $\ell^a \geq \varphi(\ell^a) > e_K$, a contradiction. Thus, we conclude that $\alpha_p \geq n$. However, Equations (3.5) and (3.7) show that if $\alpha_p \geq n$, then $L_n/\mathbb{Q}_p$ is unramified. Thus, $M_n/\mathbb{Q}$ is unramified at all primes p at which E has bad multiplicative reduction. This completes our first step, namely, we have shown that $M_n/\mathbb{Q}$ is unramified at all primes p at which E has bad reduction.

By the criterion of Néron-Ogg-Shafarevich, the primes p which ramify in $M_n/\mathbb{Q}$ are a subset of those contained in $S = S_{E,\mathrm{add}} \cup S_{E,\mathrm{mult}} \cup \{\ell\}$. However, since $M_n/\mathbb{Q}$ is unramified at all primes at which E has bad reduction, we are left to conclude that either $M_n/\mathbb{Q}$ is unramified at all rational primes (a contradiction because $M_n/\mathbb{Q}$ is non-trivial), or E has good reduction at ℓ and $M_n/\mathbb{Q}$ is ramified at ℓ. Let us assume the latter possibility.

Notice that our choice of n satisfies the hypothesis of Proposition 12. In particular, since $M_n/\mathbb{Q}$ is unramified at all primes of bad reduction, the ramification index at ℓ must satisfy

$$e_{M_n}(\ell) \geq \varphi(\ell^n) \text{ (or } e_{M_n}(2) \geq \varphi(2^{n-1})).$$

As $n \geq a$, this is a contradiction. Thus, we have reached a contradiction in all cases, and our original assumption that $R_m \in E(K)$ is impossible. □

Theorem 17 (Explicit Version of Theorem 1). *Let $E/\mathbb{Q}$ be an elliptic curve, and let $N \geq 2$ be fixed. Let K be an algebraic Galois extension of $\mathbb{Q}$ (not necessarily finite) unramified at primes in $S_{E,add}$ such that the ramification index of any other prime p in $K/\mathbb{Q}$ is finite and bounded by N. Then $E(K)_{\mathrm{Tors}}$ is a subgroup of*

$$\mathbb{Z}/(2^{m(2,N)-1})\mathbb{Z} \times \mathbb{Z}/(2^{a(2,N)-2})\mathbb{Z} \times \prod_{\substack{\ell \in L \cup R \\ \ell \geq 3}} \mathbb{Z}/(\ell^{m(\ell,N)-1})\mathbb{Z} \times \mathbb{Z}/(\ell^{a(\ell,N)-1})\mathbb{Z},$$

where L is defined in Theorem 14 and $R := \{\text{primes } \ell \colon \ell \leq N+1\}$. In particular, $E(K)_{\mathrm{Tors}}$ is finite and $\#E(K)_{\mathrm{Tors}}$ divides

$$B(E,N) = 2^{m(2,N)+a(2,N)-3} \prod_{\substack{\ell \in L \cup R \\ \ell \geq 3}} \ell^{m(\ell,N)+a(\ell,N)-2}.$$

This bound depends on E because the field K depends on the primes of additive reduction of E. Thus, if E is semi-stable, then $E(K)_{\mathrm{Tors}}$ is a subgroup of

$$\mathbb{Z}/(2^{m(2,N)-1})\mathbb{Z} \times \mathbb{Z}/(2^{a(2,N)-2})\mathbb{Z} \times \prod_{3 \leq \ell \leq A} \mathbb{Z}/(\ell^{m(\ell,N)-1})\mathbb{Z} \times \mathbb{Z}/(\ell^{a(\ell,N)-1})\mathbb{Z},$$

where $A = \max(7, N+1)$, and $\#E(K)_{\mathrm{Tors}}$ divides

$$B(N) = 2^{m(2,N)+a(2,N)-3} \prod_{3 \leq \ell \leq A} \ell^{m(\ell,N)+a(\ell,N)-2}$$

depending only upon N, independent of E.

Proof. Note that K satisfies the hypotheses of Theorem 16 simultaneously for all primes ℓ. Consequently, there are no points of order ℓ^m defined over K, for any ℓ. Moreover, by Lemma 13, $\mathbb{Q}(E[\ell^a])$ cannot be contained in K for any odd prime ℓ. If $\ell = 2$, then $\mathbb{Q}(E[2^{a-1}])$ cannot be contained in K. Thus, $E(K)[\ell^\infty]$ is isomorphic to a subgroup of $\mathbb{Z}/\ell^{m-1}\mathbb{Z} \times \mathbb{Z}/\ell^{a-1}\mathbb{Z}$ for odd primes ℓ and of $\mathbb{Z}/2^{m-1}\mathbb{Z} \times \mathbb{Z}/2^{a-2}\mathbb{Z}$ for $\ell = 2$.

If $\ell \notin L \cup R$, then $\varphi(\ell) = \ell - 1 > N$ and, by Corollary 15, the ramification at ℓ in the extension $K/\mathbb{Q}$ is at least $\varphi(\ell) > N$, which contradicts our hypothesis. If we assume further that E is semi-stable, then the same argument shows that no prime $\ell > \max(7, N+1)$ can divide the order of $E(K)_{\mathrm{Tors}}$.

Finally, note that if E is semi-stable, then $S_{E,\mathrm{add}} = \emptyset$, so that our field K no longer depends on E, hence our bound does not depend on E either. □

Corollary 18 (Theorem 2). *Let $E/\mathbb{Q}$ be a semi-stable elliptic curve. Let $F/\mathbb{Q}$ be a finite Galois extension of degree $d > 7$. Let K be the maximal unramified extension* *of F. Suppose that P is a point of exact order ℓ^n for some prime number ℓ defined over K, then $\ell \leq d+1$ and $\ell^n < \left(\frac{3}{2}\right)^4 (d+1)^2 d^4$ if ℓ is odd, or $2^n \leq 2^9 d^4$ if $\ell = 2$.*

Proof. We apply Theorem 17 with $N = d$ since $e_K \leq d$. In particular, no prime larger than $\max(7, d+1) = d+1$ can divide $\#E(K)_{\mathrm{Tors}}$. If ℓ is odd, our choice of a gives $\ell^{a-2}(\ell-1) \leq d$. Thus,

$$\ell^a \leq \frac{\ell^2}{\ell-1} d. \tag{4.1}$$

If $\ell = 2$, our choice of a gives $2^{a-3} \leq d$, so that

$$2^a \leq 8d. \tag{4.2}$$

In the notation of Theorem 16, we need to estimate

$$m(\ell, d) + a(\ell, d) - 2 = 2a + 2\max(a, b+1, 2) - 2$$

if ℓ is odd, and

$$m(2, d) + a(2, d) - 3 = 2a + 2\max(a, b+1, 5) - 3$$

if $\ell = 2$. Since $d > 7$, we have that $a(2, d) \geq 6$, $a(3, d) \geq 3$, $a(5, d) \geq 2$, and $a(7, d) \geq 2$. In particular, Mazur's classification theorem (Theorem 4) shows that $\max(a, b+1, 2 \text{ or } 5) = a$ for all primes ℓ. Combining this with Equations (4.1) and (4.2) yields

$$\begin{aligned} n &\leq 2a + 2\max(a, b+1, 2) - 2 \\ &= 4a - 2 \end{aligned}$$

so that

$$\begin{aligned} \ell^n &\leq (\ell^a)^4 \ell^{-2} \\ &\leq \left(\frac{\ell^2}{\ell-1} d\right)^4 \ell^{-2}, \text{ by Equation (4.1)} \\ &= \left(\frac{\ell}{\ell-1}\right)^4 \ell^2 d^4 \\ &< \left(\frac{3}{2}\right)^4 (d+1)^2 d^4, \text{ since } 3 \leq \ell \leq d+1 \end{aligned}$$

if ℓ is odd, and

$$\begin{aligned} n &\leq 2a + 2\max(a, b+1, 5) - 3 \\ &= 4a - 3 \end{aligned}$$

so that

$$\begin{aligned} 2^n &\leq (2^a)^4 2^{-3} \\ &\leq \left(2^3 d\right)^4 2^{-3}, \text{ by Equation (4.2)} \\ &= 2^9 d^4 \end{aligned}$$

if $\ell = 2$. □

Corollary 19. *Let E, F, $d > 7$ and K be as in the previous corollary. Then $|E(K)_{\text{Tors}}| < 2^9(d+1)^{5d+4}$.*

Proof. As above, our choice of a for odd ℓ gives $\ell^{a-2} \le \varphi(\ell^{a-1}) \le d$ so that $a \le \log_\ell d + 2$.

By the previous corollary, we have

$$\#E(K)_{\text{Tors}} \le 2^9 d^4 \prod_{3 \le \ell \le A} \ell^{4a(\ell,d)-2}.$$

Noting that $A = d+1$ and combining the previous equation with the logarithmic bounds for $a(\ell, d)$ above gives

$$\begin{aligned}
\#E(K)_{\text{Tors}} &\le 2^9 d^4 \prod_{3 \le \ell \le d+1} \ell^{4(\log_\ell d+2)-2} \\
&= 2^9 d^4 \prod_{3 \le \ell \le d+1} d^4 \ell^6 \\
&\le 2^9 d^{4+4\cdot\frac{d}{2}} \prod_{3 \le \ell \le d+1} \ell^6 \\
&\le 2^9 (d+1)^{2d+4} \prod_{3 \le \ell \le d+1} (d+1)^6 \\
&\le 2^9 (d+1)^{5d+4},
\end{aligned}$$

as desired, where we have used the fact that there are at most $\frac{d}{2}$ odd numbers ℓ with $3 \le \ell \le d+1$. □

Remark: In the above corollaries, the assumption that $d > 7$ is made solely to simplify the algebra. It is entirely possible to produce similar results for all $d > 1$ using the same methods.

5. An application of Theorem 17

In this section, as an example, we apply our results to provide bounds on the torsion of elliptic curves over $\mathbb{Q}$, upon base change by a field with everywhere low ramification. Our results are, thus, in the same vein as Fujita's result below which, in turn, builds on previous work by Laska and Lorenz (see [5]):

Theorem 20 (Fujita, [2], Theorem 2). *Let E be an elliptic curve over $\mathbb{Q}$. Let $F := \mathbb{Q}(\{\sqrt{m} : m \in \mathbb{Z}\})$. Then, the torsion subgroup $E(F)_{\text{Tors}}$ is finite, and it is isomorphic to one of the following* 20 *groups:*

$$\begin{aligned}
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} && \textit{for } M = 1,2,3,4,5,6,8, \\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4M\mathbb{Z} && \textit{for } M = 1,2,3,4, \\
&\mathbb{Z}/2M\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} && \textit{for } M = 3,4
\end{aligned}$$

or $\{0\}$*,* $\mathbb{Z}/3\mathbb{Z}$*,* $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$*,* $\mathbb{Z}/5\mathbb{Z}$*,* $\mathbb{Z}/7\mathbb{Z}$*,* $\mathbb{Z}/9\mathbb{Z}$*,* $\mathbb{Z}/15\mathbb{Z}$*. Moreover, each group listed above appears as* $E(F)_{\text{Tors}}$ *for some elliptic curve* E *defined over* $\mathbb{Q}$*.*

In this context, we can apply Theorem 1 to get the following generalization (at least in the case that E is semi-stable) of Theorem 20:

Proposition 21. *Let* $E/\mathbb{Q}$ *be a semi-stable elliptic curve and let* $K/\mathbb{Q}$ *be an algebraic Galois extension (not necessarily finite or abelian) such that* $e_K(\ell) \leq 5$ *for all primes* $\ell \geq 2$*. Then,* $E(K)_{\text{Tors}}$ *is a subgroup of*

$$(\mathbb{Z}/2^{14}\mathbb{Z} \times \mathbb{Z}/2^4\mathbb{Z}) \times (\mathbb{Z}/3^7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5^5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/7^4\mathbb{Z}.$$

Moreover, if $E(\mathbb{Q})[9]$ *is trivial, then* $E(K)_{\text{Tors}}$ *is a subgroup of*

$$(\mathbb{Z}/2^{14}\mathbb{Z} \times \mathbb{Z}/2^4\mathbb{Z}) \times (\mathbb{Z}/3^5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5^5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}/7^4\mathbb{Z}.$$

Thus, $|E(K)_{\text{Tors}}|$ *is a divisor of* $2^{19} \cdot 3^8 \cdot 5^6 \cdot 7^4$*.*

Proof. One can quickly compute that

$$a(2,5) = 5,\ a(3,5) = a(5,5) = 2,\ \text{and } a(\ell,5) = 1 \text{ for all } \ell > 5.$$

Recall that $m(\ell, N) = a(\ell, N) + 2\max(a(\ell, N), b(\ell) + 1, 2 \text{ or } 5)$. Thus,

$$\begin{aligned} m(2,5) = 5 + 2\max(5, b(2)+1, 5) &= 15 \text{ since } b(2)+1 \leq 4; \\ m(3,5) = 2 + 2\max(2, b(3)+1, 2) &= \begin{cases} 6 & \text{if } b(3) = 0 \text{ or } 1 \\ 8 & \text{if } b(3) = 2; \end{cases} \\ m(5,5) = 2 + 2\max(2, b(5)+1, 2) &= 6 \text{ since } b(5) = 0 \text{ or } 1; \\ m(7,5) = 1 + 2\max(1, b(7)+1, 2) &= 5 \text{ since } b(7) = 0 \text{ or } 1. \end{aligned}$$

The proposition now follows from Theorem 17. □

In the previous proposition, one may take K to be the maximal unramified extension of the field $F = \mathbb{Q}(\{\sqrt{m} : m \in \mathbb{Z}\})$ that appears in Fujita's theorem, because $e_K(2) = 4$ and $e_K(\ell) \leq 2$ for all $\ell > 2$. Notice, though, that K/F is an infinite extension (see, for example, [10], Corollary 7). Moreover, there are many other possibilities for K which do not fit in Fujita's setup. For an obvious example, K may be the maximal unramified extension of a cyclic Galois extension $F/\mathbb{Q}$ of degree 3, 4 or 5.

Acknowledgments

The authors would like to extend many thanks to Ravi Ramakrishna for all his input and advice along the way. We also thank Robert Pollack and Karl Rubin for their contributions. We are also grateful to the anonymous referee for a careful reading and for pointing out gaps in a previous version of the manuscript. The first author (Álvaro) would like to thank the Department of Mathematics at Cornell University (where much of this work was done) for their hospitality during his stay as a postdoctoral assistant professor.

References

[1] B. Edixhoven. Rational torsion points on elliptic curves over number fields. Séminaire N. Bourbaki **782** (1993-1994), 209–227.

[2] Y. Fujita. Torsion subgroups of elliptic curves in elementary abelian 2-extensions of $\mathbb{Q}$. J. Number Theory **114** (2005), 124–134.

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

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

[5] M. Laska and M. Lorenz. Rational points on elliptic curves over $\mathbf{Q}$ in elementary abelian 2-extensions of $\mathbf{Q}$. J. Reine Angew. Math. **355** (1985), 163–172.

[6] B. Mazur. Modular curves and the Eisenstein ideal. Publications Mathématiques de l'IHES **47** (1977), 33–186.

[7] B. Mazur. Rational isogenies of prime degree. Inventiones Math. **44** (1978), 129–162.

[8] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math. **124** (1996), 437–449.

[9] P. Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. J. Reine Angew. Math. **506** (1999).

[10] P. Roquette. On class field towers. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*. Thompson, Washington, D.C. (1967) 231–249.

[11] S. Schmitt and H. Zimmer. *Elliptic Curves*, volume 31 of *de Gruyter Studies in Mathematics*. Walter de Gruyter & Co., Berlin (2003). A computational approach, With an appendix by Attila Pethö.

[12] J. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Inventiones Math. **15** (1972), 259–331.

[13] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York (1986).

[14] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York (1994).