UNIFORM BOUNDEDNESS IN TERMS OF RAMIFICATION

ÁLVARO LOZANO-ROBLEDO

ABSTRACT. Let $d \geq 1$ be fixed. Let F be a number field of degree d, and let E/F be an elliptic curve. Let $E(F)_{\text{tors}}$ be the torsion subgroup of $E(F)$. In 1996, Merel proved the uniform boundedness conjecture, i.e., there is a constant $B(d)$, which depends on d but not on the chosen field F or on the curve E/F, such that the size of $E(F)_{\text{tors}}$ is bounded by $B(d)$. Moreover, Merel gave a bound (exponential in d) for the largest prime that may be a divisor of the order of $E(F)_{\text{tors}}$. In 1996, Parent proved a bound (also exponential in d) for the largest p-power order of a torsion point that may appear in $E(F)_{\text{tors}}$. It has been conjectured, however, that there is a bound for the size of $E(F)_{\text{tors}}$ that is polynomial in d. In this article we show that under certain hypotheses there is a linear bound for the largest p-power order of a torsion point defined over F, which in fact is linear in the maximum ramification index of a prime ideal of the ring of integers F over (p).

1. INTRODUCTION

Let F be a number field, and let E/F be an elliptic curve defined over F. The Mordell–Weil theorem states that $E(F)$, the set of F-rational points on E, can be given the structure of a finitely generated abelian group. In particular, the torsion subgroup of $E(F)$, henceforth denoted by $E(F)_{\text{tors}}$, is a finite group. In 1996, Merel proved that there is a uniform bound for the size of $E(F)_{\text{tors}}$, which is independent of the chosen curve E/F and, in fact, the bound only depends on the degree of $F/\mathbb{Q}$. The bounds were improved by Oesterlé, and later by Parent in 1999.

Definition 1.1. *For each $n \geq 1$, we define $S^n(d)$ as the set of primes p for which there exists a number field F of degree $\leq d$ and an elliptic curve E/F such that $E(F)$ contains a point of exact order p^n. We also define $T(d)$ as the supremum of $|E(F)_{tors}|$, over all F and E as above. Finally, we define $S^n_{non\text{-}CM}(d)$ (resp. $S^n_{CM}(d)$) as before, except that we only consider elliptic curves E/F without CM (resp. with CM).*

We remark that $S^{n+1}(d) \subseteq S^n(d)$ for all $n \geq 1$, and if $p \in S^n(d)$, then $p^n \leq T(d)$. Mazur ([31]) has shown that $S^1(d) = \{2, 3, 5, 7\}$ and $T(1) = 16$. Results of Kenku, Kamienny, and Momose imply that $S^1(2) = \{2, 3, 5, 7, 11, 13\}$ and $T(2) = 24$. Parent determined $S^1(3) = S^1(2)$. In addition, Derickx, Kamienny, Stein, and Stoll ([6]) have shown that $S^1(4) = S^1(3) \cup \{17\}$, $S^1(5) = S^1(4) \cup \{19\}$, $S^1(6) = S^1(5) \cup \{37\}$, and $S^1(7) \subseteq \{p \leq 23\} \cup \{37, 43, 59, 61, 67, 71, 73, 113, 127\}$. Let us cite Merel, Oesterlé, and Parent's work more precisely (Oesterlé's bound is unpublished, but appears in [6]).

Theorem 1.2 (Merel, [33], and Parent, [37])**.** *Let $d > 1$ be a fixed integer.*

1. *(Merel, 1996) $T(d)$ is finite. Moreover, if $p \in S^1(d)$, then $p \leq d^{3d^2}$.*
2. *(Oesterlé, 1996) If $p \in S^1(d)$, then $p \leq (1 + 3^{d/2})^2$.*
3. *(Parent, 1999) If $p \in S^n(d)$, then $p^n \leq 129(5^d - 1)(3d)^6$.*

1991 *Mathematics Subject Classification.* Primary: 11G05, Secondary: 14H52.

It is a "folklore" conjecture that $T(d)$ should be sub-exponentially bounded (see for instance [12], [15]). We reproduce an explicit version of the conjecture, as in Conjecture 1 of [3].

Conjecture 1.3. *There is a constant C_1 such that $T(d) \leq C_1 \cdot d \log\log d$, for all $d \geq 1$.*

Flexor and Oesterlé ([12]) have shown that if E/F has at least one place of additive reduction, then $|E(F)_{\text{tors}}| \leq 48d$, and if it has at least two places of additive reduction, then $|E(F)_{\text{tors}}| \leq 12$. Hindry and Silverman ([15, Théorème 1]) show that if E/F has everywhere good reduction then $|E(F)_{\text{tors}}| \leq 1977408 \cdot d \log d$. Turning our attention once again to $S^n(d)$, we propose the following conjecture. Here $\varphi(\cdot)$ is the Euler phi function.

Conjecture 1.4. *There is a constant C_2 such that if $p \in S^n(d)$, then $\varphi(p^n) \leq C_2 \cdot d$, for all $d \geq 1$.*

If we restrict our attention to CM curves, then Conjecture 1.4 follows from work of Silverberg ([42]), and Prasad and Yogananda ([38]; see also [3]), and the constant is ≤ 6, i.e., if $p \in S^n_{\text{CM}}(d)$, then $\varphi(p^n) \leq 6d$. See Theorem 6.9 below for a precise statement. In addition, in [28], the author has shown that Conjecture 1.4 holds (with $C_2 = 24$) when E/F has potential supersingular reduction at a prime above p.

Theorem 1.5 ([28, Theorem 1.3])**.** *Let p be a prime, let $d > 1$ be a fixed integer, let F be a number field of degree $\leq d$, and let E/F be an elliptic curve. Suppose that F has a prime $\mathfrak{P}$ over p such that E/F has potential good supersingular reduction at $\mathfrak{P}$. Then,*

$$\varphi(p^n) \leq 24e(\mathfrak{P}|p) \leq 24d,$$

where $\varphi(\cdot)$ is the Euler phi function, and $e(\mathfrak{P}|p)$ is the ramification index of $\mathfrak{P}$ in $F/\mathbb{Q}$.

In this article, we restrict our study of $E(F)_{\text{tors}}$ to the simpler case of elliptic curves E/F that arise from elliptic curves defined over a fixed number field L (contained in F), whose base field has been extended to F.

Definition 1.6. *Let L be a fixed number field, let d be an integer with $d \geq [L : \mathbb{Q}]$, and let $S^n_L(d)$ be the set of pairs (p, F), where p is a prime for which there exists a finite extension F/L of number fields with $[F : \mathbb{Q}] \leq d$, and an elliptic curve E/L (either without CM, or with CM by a maximal order), such that $E(F)_{tors}$ contains a point of exact order p^n. If $\Sigma \subseteq L$ is specified, then $S^n_L(d, \Sigma)$ is as before, except that we only consider elliptic curves E with $j(E) \notin \Sigma$. Finally, we define $S^n_{L,max\text{-}CM}(d)$ when we restrict to curves E/L with CM by a maximal order.*

In [27], we showed that if $p \in S^1_{\mathbb{Q}}(d)$ with $p \geq 11$ and $p \neq 13$, then $\varphi(p) \leq 3d$, and if $p \neq 37$, then $\varphi(p) \leq 2d$. Moreover, we gave a conjectural formula for $S^1_{\mathbb{Q}}(d)$, and showed that the formula holds for all $1 \leq d \leq 42$. Our theorems here provide bounds in terms of certain ramification indices that we define next. In the rest of the paper, if $\mathbb{F}$ is a number field or a local field, then $\mathcal{O}_{\mathbb{F}}$ denotes its ring of integers.

Definition 1.7. *Let p be a prime, and let F/L be an extension of number fields. We define $e_{min}(p, F/L)$ (resp. $e_{max}(p, F/L)$) as the smallest (resp. largest) ramification index $e(\mathfrak{P}|\wp)$ for a prime $\mathfrak{P}$ of $\mathcal{O}_F$ over a prime $\wp$ of $\mathcal{O}_L$ lying above the rational prime p.*

Now we can state our main theorems.

Theorem 1.8. *Let F be a number field with degree $[F : \mathbb{Q}] = d \geq 1$, and let p be a prime such that $(p, F) \in S^n_{max\text{-}CM}(d)$. Then,*

$$\varphi(p^n) \leq 12 \cdot e_{max}(p, F/\mathbb{Q}) \leq 12d.$$

Theorem 1.9. *Let L be a number field, and let $p > 2$ be a prime with $(p, F) \in S_L^n(d)$. Then, there is a constant C_L such that*

$$\varphi(p^n) \leq C_L \cdot e_{max}(p, F/\mathbb{Q}) \leq C_L \cdot d.$$

Moreover, there is a computable finite set Σ_L such that if $(p, F) \in S_L^n(d, \Sigma_L)$, then

$$\varphi(p^n) \leq 588 \cdot e_{max}(p, F/\mathbb{Q}) \leq 588 \cdot d.$$

The finite set Σ_L is computable (or decidable) in the sense that given $j_0 \in L$, there is an algorithm to check whether j_0 belongs to Σ_L. We emphasize here that the notation $S_L^n(d)$, as in Definition 1.6, excludes elliptic curves with CM by non-maximal orders for technical reasons (that we hope to address in future work). However, there are only finitely many elliptic curves with CM by non-maximal orders defined over L, so such j-invariants could be included in Σ_L, and the second bound in Theorem 1.9 would apply to all elliptic curves E defined over L with $j(E)$ not in the finite set Σ_L.

When $L = \mathbb{Q}$, the set Σ_L can be made explicit (it is formed by the six j-invariants without CM of Table 1 of Section 3), and our methods yield an improved bound.

Theorem 1.10. *If $p > 2$ and $(p, F) \in S_{\mathbb{Q}}^n(d)$, then $\varphi(p^n) \leq 222 \cdot e_{max}(p, F/\mathbb{Q}) \leq 222 \cdot d$.*

In light of Theorems 1.5, 1.8, 1.9, and 1.10, we revisit Conjecture 1.4 and propose the following stronger version.

Conjecture 1.11. *There is a constant C_3 such that if $(p, F) \in S^n(d)$ for a prime p and an extension $F/\mathbb{Q}$ of degree $\leq d$, then*

$$\varphi(p^n) \leq C_3 \cdot e_{max}(p, F/\mathbb{Q}) \leq C_3 \cdot d.$$

Theorem 1.5 shows Conjecture 1.11 when E/F has a prime of potential supersingular reduction above p, with $C_3 = 24$. When E/F has at least one prime $\mathfrak{P}$ of additive reduction, then Conjecture 1.11 follows from the aforementioned work of Flexor and Oesterlé ([12, Théorèm 2 and Remarque 2]), for they in fact show that $|E(F)_{\text{tors}}| \leq 48 e(\mathfrak{P}|p)$, where $e(\mathfrak{P}|p)$ denotes the ramification index of $\mathfrak{P}$ over (p) in $F/\mathbb{Q}$.

Our theorems follow from explicit lower bounds (divisibility properties, in fact) on the ramification of primes above p, in the extensions generated by points of p-power order, and recent work of Larson and Vaintrob on isogenies ([23]). In Section 2 we state our refined bound (Theorem 2.1), we specialize the bounds to elliptic curves over $\mathbb{Q}$ in Theorem 2.2 (which proves Theorem 1.10). The proof of Theorem 1.8 will be delayed to Section 6.3 (see Theorem 6.10), and we put everything together to prove Theorem 1.9 in Section 8.

Acknowledgements. The author would like to thank Kevin Buzzard, Pete Clark, Brian Conrad, Harris Daniels, Benjamin Lundell, Robert Pollack, James Stankewicz, Jeremy Teitelbaum, Ravi Ramakrishna, John Voight, Felipe Voloch and David Zywina for their helpful suggestions and comments. In addition, the author would like to express his gratitude to the anonymous referees for very detailed reports, and pointing out a crucial oversight in an earlier version of the paper.

2. Refined bounds

Let L be a number field, let p be a prime, let $n \geq 1$, and let $\zeta = \zeta_{p^n}$ be a primitive p^n-th root of unity. Let $\wp$ be a prime ideal of the ring of integers $\mathcal{O}_L$ of L lying above p. The ramification index of the primes above $\wp$ in the extension $L(\zeta)/L$ is a divisor of $\varphi(p^n)$, and it is divisible by $\varphi(p^n)/\gcd(\varphi(p^n), e(\wp|p))$. In this article we study the ramification above p in the extension $L(R)/L$,

where R is a torsion point of exact order p^n in an elliptic curve E defined over L. We show the following:

Theorem 2.1. *Let $p > 2$ be a prime. Let L be a number field, and let $\wp$ be a prime ideal of $\mathcal{O}_L$ with ramification index $e(\wp|p) \geq 1$ in $L/\mathbb{Q}$. Let E/L be an elliptic curve, and let $a \geq 1$ be an integer such that one of the following conditions is satisfied:*

1. *E/L does not admit an L-rational isogeny of degree p^a, or*
2. *Let $L_\wp^{nr}$ be the maximal unramified extension of $L_\wp$, the completion of L at $\wp$, and let $K/L_\wp^{nr}$ is the smallest extension such that E/K has good or multiplicative reduction. If E/L admits an L-rational isogeny ϕ of degree p, such that $\ker(\phi) = \langle S \rangle \subset E[p]$, then the ramification index of $K(S)/K$ is > 1, or the ramification index of $\wp$ in the Galois extension $L(S)/L$ satisfies that the quotient $e(\wp, L(S)/L)/\gcd(e(\wp, L(S)/L), e(K/L_\wp^{nr})) > 1$. If so, let $a = 1$.*

Let $R \in E[p^n]$ be an arbitrary point of exact order p^n, for some $n \geq a$. Then, there is a number $c = c(E/L, R, \wp)$, with $1 \leq c \leq 12e(\wp|p)$, and a prime Ω_R of $L(R)$ above $\wp$ such that the ramification index $e(\Omega_R|\wp)$ is divisible either by

$$\varphi(p^n)/\gcd(\varphi(p^n), c \cdot p^{a-1}), \text{ or } p^{n-a+1}.$$

If $e(\wp|p) = 1$, then there is a prime Ω_R of $L(R)$ above $\wp$ such that $e(\Omega_R|\wp)$ is divisible either by

$$\varphi(p^n)/\gcd(\varphi(p^n), t \cdot p^{a-1}), \quad \text{or } p^{n-a+1},$$

where $t \in \{6, 9\}$ if $p = 3$, and $t \in \{4, 6\}$ if $p > 3$.

Proof. Let E/L be an elliptic curve, and let $\wp$ be a prime ideal of $\mathcal{O}_L$. Then, E/L either has potential multiplicative reduction, or potential good reduction at $\wp$, which may be ordinary or supersingular.

- The case of potential multiplicative reduction is treated in Section 5. In particular, if E/L satisfies hypothesis (1) or (2), then Theorem 5.1, parts (e) and (f), imply that there is a prime Ω_R of $L(R)$ above $\wp$ such that the ramification index $e(\Omega_R|\wp)$ is divisible either by

  $$\varphi(p^n)/\gcd(\varphi(p^n), 2e(\wp|p)p^{a-1}), \text{ or } p^{n-a+1},$$

  and the theorem follows in this case.
- The case of potential good ordinary reduction is treated in Section 6.1. In particular, if E/L satisfies hypotheses (1) or (2), then Theorem 6.3 implies that there is a prime Ω_R of $L(R)$ above $\wp$ such that the ramification index $e(\Omega_R|\wp)$ is divisible either by

  $$\varphi(p^n)/\gcd(\varphi(p^n), e \cdot p^{a-1}) \text{ or } p^{n-a+1},$$

  where $e = e(K/\mathbb{Q}_p)$ is the ramification index of $K/\mathbb{Q}_p$. If $p = 3$, then $\varphi(p^n) = 2 \cdot 3^{n-1}$ and e is a divisor of $12e(\wp|p)$, so if $e(\wp|p) = 1$ then $\varphi(p^n)/\gcd(\varphi(p^n), e \cdot p^{a-1})$ is divisible by $\varphi(p^n)/\gcd(\varphi(p^n), t \cdot p^{a-1})$ with $t = 9$ or 6. If $p > 3$, then e is a divisor of either $4e(\wp|p)$ or $6e(\wp|p)$, and the theorem follows in this case.
- The case of potential good supersingular reduction is treated in Section 6.2, where we quote our results from previous works ([26] and [28]). Theorem 6.7 implies that there is a number $c = c(E/L, R, \wp)$ with $1 \leq c \leq 12e(\wp|p)$ (with $c \leq 6e(\wp|p)$ if $p > 3$), such that the ramification index $e(\Omega_R|\wp)$ of any prime Ω_R above $\wp$ in the extension $L(R)/L$ is divisible by $\varphi(p^n)/\gcd(c, \varphi(p^n))$. Moreover, if $e(\wp|p) = 1$ and $p > 3$, then $e(\Omega_R|\wp)$ is divisible by $(p^2 - 1)p^{2(n-1)}/6$, or $(p - 1)p^{2(n-1)}/\gcd(p - 1, 4)$, therefore it is also divisible by

$\varphi(p^n)/\gcd(\varphi(p^n),t)$ with $t = 4$ or 6. If $d = 1$ and $p = 3$, then $e(\Omega_R|\wp)$ is divisible by $\varphi(3^n)/\gcd(\varphi(3^n),t)$ with $t = 6$ or 9.

□

When $L = \mathbb{Q}$, the previous theorem can be improved because we have a complete classification of non-cuspidal $\mathbb{Q}$-points on the modular curves $X_0(N)$, which correspond to all possible $\mathbb{Q}$-rational isogenies of elliptic curves over $\mathbb{Q}$, as discussed in Section 3.

Theorem 2.2. *Let $E/\mathbb{Q}$ be an elliptic curve. For each prime p, we define $b = b(p)$ to be*

p	3	5	7	13	37	*else*
$b(p)$	3	3	2	2	$\begin{cases} 2, & \text{if } j(E) = -7\cdot 11^3 \\ 1, & \text{otherwise} \end{cases}$	1

Suppose that $R \in E(\overline{\mathbb{Q}})$ is a torsion point of exact order p^n with $n \geq b(p)$ and $p > 2$. Then, there is a prime Ω_R of $\mathbb{Q}(R)$ above p such that $e(\Omega_R|p)$ is divisible either by

$$\varphi(p^n)/\gcd(\varphi(p^n), t\cdot p^{b-1}), \quad \text{or} \quad p^{n-b+1},$$

where $t \in \{6,9\}$ if $p = 3$, and $t \in \{4,6\}$ if $p > 3$. In particular,

$$\varphi(p^n) \leq t\cdot p^{b-1}\cdot e(\Omega_R|p) \leq 222\cdot e(\Omega_R|p).$$

Proof. Let $E/\mathbb{Q}$ be an elliptic curve, and let $p > 2$ be a prime. By Theorem 3.3, the curve E cannot admit isogenies of degree $p^{a(\mathbb{Q},p)}$, where $a(\mathbb{Q},p)$ is given by the following table:

p	3	5	7	11	13	17	19	37	43	67	163	else
$a(\mathbb{Q},p)$	4	3	2	2	2	2	2	2	2	2	2	1.

Suppose first that $E/\mathbb{Q}$ does not admit isogenies of degree $p^{b(p)}$. Then Theorem 2.1 implies part (a). Thus, it remains to deal with those elliptic curves $E/\mathbb{Q}$ that admit isogenies of degree $p^{b(p)}$ with $b(p) < a(\mathbb{Q},p)$, i.e., $E/\mathbb{Q}$ admits an isogeny of degree 11, 17, 19, 27, 37, 43, 67, or 163. By Theorem 3.3, there are only finitely many such j-invariants, and they are given in Table 1 of Section 3.

Let (j_0,p) be any of the j-invariants that are listed in Table 1, with $p \neq 37$, and let $E/\mathbb{Q}$ be an elliptic curve with $j(E) = j_0$. Then $E/\mathbb{Q}$ has potential supersingular reduction at p (see Section 6.2, Table 2). Let $R \in E[p^n]$ be a point of exact order p^n. Theorem 6.8 shows that the ramification index of any prime Ω_R that lies above p in the extension $\mathbb{Q}(R)/\mathbb{Q}$ is divisible by $(p-1)p^{2n-2}/2$ if $p > 3$ and $n \geq 1$, and by 3^{2n-4} if $p = 3$ and $n \geq 3$. In particular, $e(\Omega_R|p)$ is divisible by $\varphi(p^n)/2$ for $p > 3$ (which in turn is divisible by $\varphi(p^n)/\gcd(\varphi(p^n),t)$ for $t = 4$ or $t = 6$ as claimed), and when $p = 3$, it is divisible by 3^{n-2}, which is divisible by $\varphi(3^n)/\gcd(\varphi(3^n), t\cdot 3^{b(3)-1})$, for $t = 6$ or 9, because $b(3) = 3$.

It remains to consider the two j-invariants with a $\mathbb{Q}$-rational isogeny of degree 37, namely $j_0 = -7\cdot 11^3$ and $j_0' = -7\cdot 137^3\cdot 2083^3$. Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be elliptic curves with j-invariants $j(E) = j_0$ and $j(E') = j_0'$. Let $f = 1$ if $E/\mathbb{Q}$ has good reduction at $p = 37$, and let $f = 2$ otherwise (and define f' similarly). Then Proposition 6.4 shows the following:

- Let $R \in E$ be a point of exact order 37^n, for $n \geq 2$. Then, there is a prime Ω_R of $\mathbb{Q}(R)$ over (37) such that $e(\Omega_R|37)$ is divisible by $\varphi(37^n)/37 = \varphi(37^{n-1})$, or $f\cdot 37^{n-1}$.

- Let $R \in E'$ be a point of exact order 37^n, for $n \geq 1$. Then, there is a prime Ω_R of $\mathbb{Q}(R)$ over (37) such that $e(\Omega_R|37)$ is divisible by $\varphi(37^n)$, or $f' \cdot 37^n$.

This concludes the proof of the first claim of part (a). The second claim follows directly from the first, by noting that the maximum value of $t \cdot p^{b-1}$ is 222, as $t \leq 6$ when $p > 3$. □

Remark 2.3. Our methods here can also show that, with the notation of Theorem 2.2, if $R \in E[p^n]$ is a point of exact order p^n, with $n \geq b(p)$, and $K/\mathbb{Q}$ is a Galois extension such that $\mathbb{Q}(R) \subseteq K$, then the ramification index of p in $K/\mathbb{Q}$, denoted by $e(K,p)$, and the degree of $K/\mathbb{Q}$, are divisible by

$$(p-1)p^{n-b}/2 = \frac{\varphi(p^{n-b+1})}{2}$$

when p is odd, and by $\varphi(2^{n-4})$ when $p = 2$. In [25], Lundell and the author had shown a similar result but under the additional assumption that $E/\mathbb{Q}$ is semistable.

3. Rational points on the modular curve $X_0(N)$

Let $\mathbb{H}$ be the complex upper half-plane, let $N \geq 1$ and let $\Gamma_0(N)$ be the usual congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$ given by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : c \equiv 0 \bmod N \right\}.$$

The group $\mathrm{SL}(2,\mathbb{Z})$ acts on $\mathbb{H}$ by linear fractional transformations, i.e., if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ then we define an action $Mz = \frac{az+b}{cz+d}$, for any $z \in \mathbb{H}$. Let $Y_0(N) = \mathbb{H}/\Gamma_0(N)$ and let $X_0(N)$ be the compactification of $Y_0(N)$. The finite set of points in $X_0(N) \setminus Y_0(N)$ are called the cusps of $X_0(N)$, and can be identified with $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N)$. Thus constructed, $X_0(N)$ is a projective and non-singular algebraic curve, and a model defined over $\mathbb{Q}$ can be constructed (see [30], §2, or [7], Ch. 7). Moreover, $X_0(N)$ is a moduli space of isomorphism classes of ordered pairs (E, C), where E is a complex elliptic curve and C is a cyclic subgroup of E of order N (see [7], Section 1.5). In the following theorem, we provide a formula for the genus of $X_0(p^n)$. This is a specialization of the formulae that appear in [45], Prop. 1.40.

Theorem 3.1. *Let p be a prime and let $a \geq 1$. Then, the genus of $X_0(p^a)$ is given by*

$$g = 1 - \frac{\nu_2}{4} - \frac{\nu_3}{3} + \frac{1}{12}\left(\mu - 6\nu_\infty\right),$$

where

$$\nu_2 = \begin{cases} 1 & \text{if } p = 2 \text{ and } a = 1, \\ 0 & \text{if } p = 2 \text{ and } a > 1, \\ 2 & \text{if } p \equiv 1 \bmod 4, \\ 0 & \text{if } p \equiv 3 \bmod 4, \end{cases}, \quad \nu_3 = \begin{cases} 1 & \text{if } p = 3 \text{ and } a = 1, \\ 0 & \text{if } p = 3 \text{ and } a > 1, \\ 2 & \text{if } p \equiv 1 \bmod 3, \\ 0 & \text{if } p \equiv 2 \bmod 3, \end{cases}$$

and

$$\mu - 6\nu_\infty = \begin{cases} (p+1)p^{\frac{a}{2}-1}(p^{\frac{a}{2}} - 6) & \text{if } a \text{ is even, or} \\ p^{\frac{a-1}{2}}(p^{\frac{a-1}{2}}(p+1) - 12) & \text{if } a \text{ is odd.} \end{cases}$$

Using the formula for the genus of $X_0(p^a)$, we can find all those with genus 1 and 2.

Corollary 3.2. *For a fixed prime number p, the genus of $X_0(p^a)$ is an increasing function as a increases. For each $i \geq 1$, we define a function $a_i(p)$ such that $a_i = a_i(p)$ is the smallest positive integer a such that $X_0(p^a)$ has genus $g \geq i$. Then:*

(1) *$a_1(p) = 1$ for all $p \geq 17$, and $a_2(p) = 1$ for all $p \geq 23$.*
(2) *Moreover, the values of $a_1(p)$ and $a_2(p)$ are given by the following table.*

p	2	3	5	7	11	13	17	19	*else*
$a_1(p)$	5	3	3	2	1	2	1	1	1
$a_2(p)$	6	4	3	3	2	2	2	2	1

The $\mathbb{Q}$-rational points on $X_0(N)$ have been described completely in the literature, for all $N \geq 1$. Certainly, one decisive step in their classification was [31], where Mazur dealt with the case when N is prime. The complete classification of $\mathbb{Q}$-rational points on $X_0(N)$, for any N, was completed due to work of Fricke, Kenku, Klein, Kubert, Ligozat, Mazur and Ogg, among others (see the references at the bottom of Table 1).

Theorem 3.3. *Let $N \geq 2$ be a number such that $X_0(N)$ has a non-cuspidal $\mathbb{Q}$-rational point associated to a non-CM j-invariant. Then, N is one of the numbers in lists (1) or (2) below, and for each N in one of the two lists $X_0(N)$ contains non-CM non-cuspidal $\mathbb{Q}$-rational points:*

(1) *$N \leq 10$, or $N = 12, 13, 16, 18$ or 25. In this case $X_0(N)$ is a curve of genus 0 and its $\mathbb{Q}$-rational points form an infinite 1-parameter family; or*
(2) *$N = 11, 14, 15, 17, 21$, or 37. In this case $X_0(N)$ is a curve of genus ≥ 1 and there exist a finite number of non-CM non-cuspidal $\mathbb{Q}$-rational points on the curve.*

In addition, the curve $X_0(N)$, for $N = 19, 27, 43, 67$, or 163, has non-cuspidal $\mathbb{Q}$-rational points, but all are associated to j-invariants with complex multiplication.

About Table 1. For the convenience of the reader, we have collected in Table 1 a complete list of all non-cuspidal $\mathbb{Q}$-rational points on the modular curves $X_0(N)$, where $N = p^n$ is a power of a prime, and the genus of $X_0(p^n)$ is positive. For each j-invariant, we indicate whether it has complex multiplication. If it does, we list the associated quadratic discriminant. These points are well-known, but seem to be spread out accross the literature. Our main references are [2], [31] and [21], but we have consulted many other references, which we list at the bottom of the table. The description of the non-cuspidal $\mathbb{Q}$-rational points for $X_0(N)$ when the genus is 0 is not needed in this paper, but can be found accross the literature. For instance, see [8] eq. (80); [9]; [13], [14] pp. 370-458; [16] p. 1889; [29]; or the tables in [27].

Table 1: All non-cuspidal rational points on $X_0(p^n)$, genus > 0 case

N, genus$(X_0(N))$	j-invariants	Examples	Conductor	CM?
11, $g = 1$	$j = -11 \cdot 131^3$	121A1, 121C2	11^2	No
	$j = -2^{15}$	121B1, 121B2	11^2	-11
	$j = -11^2$	121A2, 121C1	11^2	No
17, $g = 1$	$j = -17^2 \cdot 101^3/2$	14450P1	$2 \cdot 5^2 \cdot 17^2$	No
	$j = -17 \cdot 373^3/2^{17}$	14450P2	$2 \cdot 5^2 \cdot 17^2$	No
19, $g = 1$	$j = -2^{15} \cdot 3^3$	361A1, 361A2	19^2	-19
27, $g = 1$	$j = -2^{15} \cdot 3 \cdot 5^3$	27A2, 27A4	3^3	-27
37, $g = 2$	$j = -7 \cdot 11^3$	1225H1	$5^2 \cdot 7^2$	No
	$j = -7 \cdot 137^3 \cdot 2083^3$	1225H2	$5^2 \cdot 7^2$	No
43, $g = 3$	$j = -2^{18} \cdot 3^3 \cdot 5^3$	1849A1, 1849A2	43^2	-43
67, $g = 5$	$j = -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	4489A1, 4489A2	67^2	-67
163, $g = 13$	$j = -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	26569A1, 26569A2	163^2	-163
Remark: the Cremona labels are the representatives in this class of least conductor.				
References: [2, pp. 78-80], [31], [21], [24], [36], [22], [32], [17], [18], [19], [20].				

4. Borel subgroups

In order to prove Theorem 2.1 in the cases of potential multiplicative reduction, or potential good ordinary reduction, we shall need results about ramification indices when the image of $\rho_{E,p}\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[p^n])$ is a Borel subgroup of $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$, for some finite extension K of $L_\wp^{\mathrm{nr}}$. In this section we study Borel subgroups in general.

Definition 4.1. *Let $p > 2$ be a prime, and $n \geq 1$. We say that a subgroup B of $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is Borel if every matrix in B is upper triangular, i.e.,*

$$B \leq \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}/p^n\mathbb{Z},\ a, c \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}.$$

We say that B is a non-diagonal Borel subgroup if none of the conjugates of B in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is formed solely by diagonal matrices. If B is a Borel subgroup, we denote by B_1 the subgroup of B formed by those matrices in B whose diagonal coordinates are $1 \bmod p^n$, and we denote by B_d the subgroup of B formed by diagonal matrices, i.e.,

$$B_1 = B \cap \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}/p^n\mathbb{Z} \right\},\ \text{and } B_d = B \cap \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} : a, c \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}.$$

Lemma 4.2. *Let $p > 2$ be a prime, $n \geq 1$ and let $B \leq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ be a Borel subgroup, such that B contains a matrix $g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ with $a \not\equiv c \bmod p$. Then, there is a Borel subgroup $B' \leq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ such that:*

1. *B and B' are conjugates, more precisely $B' = h^{-1}Bh$ with $h = \begin{pmatrix} 1 & b/(c-a) \\ 0 & 1 \end{pmatrix}$.*
2. *$B' = B'_d B'_1$, i.e., for every $M \in B'$ there is $U \in B'_d$ and $V \in B'_1$ such that $M = UV$.*
3. *$[B, B] = B_1$ and $[B', B'] = B'_1$. In particular, $[B, B]$ and $[B', B']$ are cyclic groups whose order is p^s, for some $0 \leq s \leq n$.*
4. *$B/[B, B] \cong B'/[B', B']$ is isomorphic to a subgroup of $(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$.*
5. *If $n = 1$, then $B \cong B' = B'_d B'_1$ for any Borel subgroup $B \leq \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$.*

Hence, if $B \leq \mathrm{GL}(2, \mathbb{Z}_p)$ is a closed Borel subgroup, and there is a $g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in B$ with $a \not\equiv c \bmod p$, then there is a conjugate subgroup $B' \leq \mathrm{GL}(2, \mathbb{Z}_p)$, such that $B' = B'_d B'_1$, with commutator subgroup $B'_1 = [B', B']$ and the quotient $B'/[B', B']$ is a subgroup of $(\mathbb{Z}_p)^\times \times (\mathbb{Z}_p)^\times$.

Proof. Let $g \in B$ and $h \in \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ be matrices as in the statement of the lemma, and define $B' = h^{-1}Bh$. Notice that $h^{-1}gh = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in B'$. If B' only contains diagonal matrices, then $B' = B'_1$ and the statement is trivial. Otherwise, let $v(B') \geq 0$ be the smallest valuation among all the top-right coordinates of matrices in B', and let $\begin{pmatrix} e & f \\ 0 & l \end{pmatrix} \in B'$ such that $f \not\equiv 0 \bmod p^n$ and the valuation of f is precisely $v(B')$. Then, the following commutator belongs to B':

$$k = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} e & f \\ 0 & l \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}^{-1} \begin{pmatrix} e & f \\ 0 & l \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \frac{f}{l}\left(\frac{a}{c} - 1\right) \\ 0 & 1 \end{pmatrix}.$$

Since e, l are units and $a \not\equiv c \bmod p$, we conclude that $f(a/c-1)/l$ also has valuation $v(B')$. Let $m \in \mathbb{Z}$ be an integer such that to $(f(a/c-1)/l) \cdot m \equiv p^{v(B')} \bmod p^n$. Then, $k^m = \begin{pmatrix} 1 & p^{v(B')} \\ 0 & 1 \end{pmatrix} \in B'$. Now, if $\beta \equiv 0 \bmod p^{v(B')}$, then there is some β' such that $\beta \equiv \beta' p^{v(B)} \bmod p^n$. Thus, if $M = \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}$ is an arbitrary non-diagonal element of B', we have

$$\begin{aligned} M = \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} &= \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} (k^m)^{-\beta'/\alpha} (k^m)^{\beta'/\alpha} \\ &= \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \begin{pmatrix} 1 & -\frac{\beta' p^{\nu(B')}}{\alpha} \\ 0 & 1 \end{pmatrix} (k^m)^{\beta'/\alpha} \\ &= \begin{pmatrix} \alpha & 0 \\ 0 & \gamma \end{pmatrix} (k^m)^{\beta'/\alpha}. \end{aligned}$$

Thus, we have shown that with $U = M(k^m)^{-\beta'/\alpha} \in B'_d$, $V = (k^m)^{\beta'/\alpha} \in B'_1$ we have $M = UV \in B'_d B'_1$. This shows (1) and (2). Moreover, it is clear that any commutator in $[B', B']$ has diagonal coordinates congruent to 1 modulo p^n and, therefore, $[B', B'] \leq B'_1$. Notice that if $M \in B'_1$, i.e., $\alpha \equiv \gamma \equiv 1 \bmod p^n$, and $m \in \mathbb{Z}$ as above, then U is the identity and $M = V = (k^m)^{\beta'} \in B'_1$. Since

k is a commutator, this shows that $B_1' \leq [B', B']$. Thus, $[B', B'] = B_1'$. Notice that $B_1 = hB_1'h^{-1}$. Hence, $[B, B] = h[B', B']h^{-1} = hB_1'h^{-1} = B_1$, as claimed in (3). Finally, $B \cong B'$, so

$$B/[B, B] \cong B'/[B', B'] \cong (B_d'B_1')/B_1' \cong B_d' \leq (\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

This shows (4). Now suppose that B is a closed Borel subgroup of $\mathrm{GL}(2, \mathbb{Z}_p)$. Since $(c - a) \in \mathbb{Z}_p^\times$, we may define $h \in \mathrm{GL}(2, \mathbb{Z}_p)$ as in (1) and put $B' = h^{-1}Bh$. Now let $M \in B'$. Put

$$M = \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \in B',\ U = \begin{pmatrix} \alpha & 0 \\ 0 & \gamma \end{pmatrix},\ \text{ and } \ V = \begin{pmatrix} 1 & \beta/\alpha \\ 0 & 1 \end{pmatrix}.$$

Define $g' \in B'$ by $g' = h^{-1}gh$, construct a commutator $k \in B'$ as before and, for a fixed $n \geq 1$, let $m = m(n) \in \mathbb{Z}$ such that $k^m \equiv \begin{pmatrix} 1 & p^{v(B')} \\ 0 & 1 \end{pmatrix} \bmod p^n$. The previous arguments show that $U \equiv M(k^{m(n)})^{-\beta'/\alpha}$ and $V \equiv (k^{m(n)})^{\beta'/\alpha} \bmod p^n$. Since B is closed, so is B', and since M and k belong to B', we conclude that U and V belong to B' as well. It follows that $M = UV \in B_d'B_1'$, and $B' = B_d'B_1'$. The proofs of $B_1' = [B', B']$ and the structure of the quotient $B'/[B', B']$ follow as above. This shows (1)–(4).

For (5), suppose that $n = 1$. If B contains an element g as in the statement of the lemma, then we are done by (1)-(5) above. If there is no such g, then each matrix in B has congruent (mod p) diagonal entries. If $B = B_d$, then we are done. Otherwise, let $g' = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ be an arbitrary element of B with $b \not\equiv 0 \bmod p$. Then,

$$(g')^m = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^m = \begin{pmatrix} a^m & ma^{m-1}b \\ 0 & a^m \end{pmatrix},$$

for each $m \geq 1$. In particular, $(g')^{p-1} = \begin{pmatrix} 1 & -a^{p-2}b \\ 0 & 1 \end{pmatrix}$ and since $a^{p-2}b \not\equiv 0 \bmod p$, there is a $q \geq 1$ such that $-qa^{p-2}b \equiv 1 \bmod p$. Thus, $T = ((g')^{(p-1)})^q = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in B$ and we conclude that

$$g' = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} 1 & b/a \\ 0 & 1 \end{pmatrix} = (g' \cdot T^t) \cdot T^{-t},$$

where $t \geq 1$ is an integer such that $t \equiv -b/a \bmod p$. Since $g' \cdot T^t \in B_d$ and $T^{-t} \in B_1$, and $g' \in B \setminus B_d$ was arbitrary, we conclude that $B = B_dB_1$.

Finally, if $B \leq \mathrm{GL}(2, \mathbb{Z}_p)$ is a closed Borel subgroup, and there is a $g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in B$ with $a \not\equiv c \bmod p$, we can set h as in (1), and $B' = h^{-1}Bh$. Then, $B_n = B \bmod p^n$ and $B_n' = B' \bmod p^n$ satisfy properties (1)–(4) as subgroups of $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. Thus, B' requires all the required properties because B and therefore B' are closed subgroups of $\mathrm{GL}(2, \mathbb{Z}_p)$. □

Remark 4.3. The result of the previous lemma is simply false for $p = 2$, i.e., the assumption $p > 2$ is not just technical. For instance, the Borel group

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in (\mathbb{Z}/4\mathbb{Z})^\times,\ b \equiv 2 \bmod 4 \right\} \leq \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$$

is *abelian*, so the commutator of B is trivial. The results of the lemma are also not necessarily true if the diagonal entries of each element in the Borel subgroup B are congruent modulo p^n (i.e., if there

is no such element g as in the statement of the lemma). For instance, let B be the subgroup

$$B = \left\{ \begin{pmatrix} 1+p^{n-1} & p^{n-1} \\ 0 & 1+p^{n-1} \end{pmatrix}^t = \begin{pmatrix} (1+p^{n-1})^t & t(1+p^{n-1})^{t-1}p^{n-1} \\ 0 & (1+p^{n-1})^t \end{pmatrix} : t = 1, \dots, p \right\}$$

of $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. Suppose there is a subgroup B' conjugate to B, such that $B' = B'_d B'_1$. Since B has order p, it follows that either $B \cong B'_d$ or $B \cong B'_1$. However, the matrices in B are not diagonalizable, and 1 is not a common eigenvalue so neither isomorphism can hold.

Lemma 4.4. *Let p be a prime, $n \geq 1$, $V \cong (\mathbb{Z}/p^n\mathbb{Z}) \times (\mathbb{Z}/p^n\mathbb{Z})$ and let B be a Borel subgroup of $\mathrm{GL}(V) \cong \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ with respect to a $\mathbb{Z}/p^n\mathbb{Z}$-basis $\{P, Q\}$ of V. For a point $R = \lambda P + \mu Q \in V$ of exact order p^n, let B_R be the subgroup of B that fixes each vector in $\langle R \rangle$. Then:*

(1) *If $\lambda \not\equiv 0 \bmod p$, and $\nu_p(\mu) = t$ for some $1 \leq t \leq n$, then*

$$B_R = \left\{ \begin{pmatrix} 1 - bp^t/\lambda & b \\ 0 & c \end{pmatrix} : b \in \mathbb{Z}/p^n\mathbb{Z},\ c \equiv 1 \bmod p^{n-t} \right\} \cap B,$$

(2) *If $\mu \not\equiv 0 \bmod p$, and $\nu_p(\lambda) = t$ for some $0 \leq t \leq n$, then*

$$B_R = \left\{ \begin{pmatrix} a & (1-a)p^t/\mu \\ 0 & 1 \end{pmatrix} : a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\} \cap B.$$

Proof. Notice that $A \in \mathrm{GL}(V)$ fixes R if and only if A fixes δR, for all $\delta \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Hence, $B_R = B_{\delta R}$, for all $\delta \in (\mathbb{Z}/p^n\mathbb{Z})^\times$.

If $R = (\lambda, \mu)$ with $\lambda \not\equiv 0 \bmod p$ and $\nu_p(\mu) = t$, then $\mu = \mu' p^t$, with μ' a unit. Thus, if we put $R' = 1/\mu' R = (\lambda/\mu', p^t)$, then $B_R = B_{R'}$. Hence, without loss of generality, we may assume λ is a unit and $\mu = p^t$. Similarly, if $\nu_p(\lambda) = t$, we may assume μ is a unit and $\lambda = p^t$. Now the lemma follows easily from the fact that a matrix $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in B$ belongs to B_R if and only if

$$\lambda(a-1) + b\mu \equiv (c-1)\mu \equiv 0 \bmod p^n.$$

This concludes the proof ot the lemma. □

Lemma 4.5. *Let $n \geq 1$, let $p > 2$ be a prime, and let $J \leq (\mathbb{Z}/p^n\mathbb{Z})^\times$ be a subgroup. Let $1 \leq b \leq n$ be a positive integer, and let $J_{1,b}$ be the subgroup of J formed by those $a \in J$ such that $a \equiv 1 \bmod p^b$. Then:*

$$|J_{1,b}| = \begin{cases} \max\{1, p^{n-b}\} & ,\ \text{if } n - \nu_p(|J|) \leq b \leq n, \\ p^{\nu_p(|J|)} & ,\ \text{if } 1 \leq b < n - \nu_p(|J|). \end{cases}$$

Moreover, if we define $J_{-1,b}$ similarly, and $|J|$ is even, then $|J_{-1,b}| = |J_{1,b}|$.

Proof. Since $p > 2$, there exists a generator g of $(\mathbb{Z}/p^n\mathbb{Z})^\times$, and J is cyclic, generated by some power of g, say g^k, where $k = dp^j$ for some $0 \leq j \leq n-1$, and some positive divisor d of $(p-1)$. In this case,

$$J = \left\{ (g^k)^n : n = 1, \dots, \frac{(p-1)}{d} p^{n-j-1} \right\},$$

so $|J| = (p-1)p^{n-j-1}/d$ and $j = n - \nu_p(|J|) - 1$. The subgroup $J_{1,b}$ is formed by those powers $(g^k)^n$ such that $\varphi(p^b)$ divides kn. If $b - 1 \geq j$, then

$$J_{1,b} = \left\{ (g^k)^n : n = \frac{(p-1)}{d} p^{b-1-j}, 2\frac{(p-1)}{d} p^{b-1-j}, \dots, p^{n-b}\frac{(p-1)}{d} p^{b-1-j} \right\}.$$

Hence, $|J_{1,b}| = p^{n-b}$. Otherwise, if $b-1 < j$, i.e., when $1 \leq b < n - \nu_p(|J|)$, then

$$J_{1,b} = \left\{ (g^k)^n : n = \frac{(p-1)}{d}, 2\frac{(p-1)}{d}, \ldots, p^{n-j-1}\frac{(p-1)}{d} \right\},$$

so that $|J_{1,b}| = p^{n-j-1} = p^{\nu_p(|J|)}$.

Finally, if $|J|$ is even, then there exists $m \in J$ such that $m \equiv -1 \bmod p^n$, and there is a bijection $J_{-1,b} \to J_{1,b}$ given by $a \mapsto m \cdot a$. □

Remark 4.6. Let $p > 2$ be a prime, let $J \subseteq (\mathbb{Z}/p^n\mathbb{Z})^\times$ be a subgroup, and let $\psi\colon J \to \{\pm 1\}$ be a quadratic character (note that we assume here that the word *quadratic* implies non-trivial). Then, $\mathrm{Ker}(\psi) = J^2$ and $\psi(a) = -1$ if and only if $a \in J$ is a quadratic non-residue mod p^n, if and only if a is a quadratic non-residue mod p. In particular, if $a\psi(a) \equiv 1 \bmod p$, then $a \equiv \psi(a) \bmod p$ and so either $a \equiv \psi(a) \equiv 1 \bmod p$ or $a \equiv \psi(a) \equiv -1 \bmod p$, and therefore -1 is a quadratic non-residue and $p \equiv 3 \bmod 4$. Thus, if $p \equiv 1 \bmod 4$ and $a\psi(a) \equiv 1 \bmod p$, then we must necessarily have $a \equiv \psi(a) \equiv 1 \bmod p$.

Lemma 4.7. *Let $p > 2$ be a prime, $n \geq 1$, $m \geq 0$, let $V \cong (\mathbb{Z}/p^n\mathbb{Z}) \times (\mathbb{Z}/p^n\mathbb{Z})$ and let B be a Borel subgroup $B \leq \mathrm{GL}(V) \cong \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. Let $J \leq (\mathbb{Z}/p^n\mathbb{Z})^\times$ be a subgroup, and suppose $I \leq B$ is a subgroup of the form*

$$I = \left\{ \begin{pmatrix} a\psi(a) & b \\ 0 & \psi^{-1}(a) \end{pmatrix} : a \in J, b \equiv 0 \bmod p^m \right\},$$

where $\psi\colon J \to \{\pm 1\}$ is a trivial or quadratic character. Let $\delta = \delta(\psi) = 1$ if ψ is trivial or $p \equiv 1 \bmod 4$, and $\delta = 2$ otherwise (i.e., ψ is quadratic and $p \equiv 3 \bmod 4$). Let $f = f(\psi) = 1$ or 2 if ψ is trivial or quadratic, respectively. For $R \in V$, we write I_R for the subgroup of I that fixes every element of $\langle R \rangle$.

1. *Suppose $R = \lambda P + \mu Q$, with $\lambda \not\equiv 0 \bmod p$ and $\nu_p(\mu) = t$, for some $1 \leq t \leq n$.*
   (a) *If ψ is trivial, or $1 \leq t \leq n-1$, or $p \equiv 1 \bmod 4$, then*

$$|I|/|I_R| = \begin{cases} |J| & , \text{ if } n - \nu_p(|J|) \leq t + m \leq n, \\ |J| p^{n-m-\nu_p(|J|)-t} & , \text{ if } 1 \leq t + m < n - \nu_p(|J|). \end{cases}$$

   (Note: in the second case, $n - m - \nu_p(|J|) - t > 0$.)
   (b) *Otherwise, if ψ is non-trivial, $t = n$ and $p \equiv 3 \bmod 4$, then $|I|/|I_R| = |J|/2$.*

   Thus, in all cases, $|I|/|I_R|$ is divisible by $|J|/\delta(\psi)$.
2. *Suppose that $R = \lambda P + \mu Q$, with $\mu \not\equiv 0 \bmod p$, and $\nu_p(\lambda) = t$:*
   (a) *If $t = n \leq m$ or $0 \leq m \leq t \leq n$, then $|I|/|I_R| = f \cdot \max\{1, p^{n-m}\}$. In particular, if $n \leq m$ and $R \in \langle Q \rangle$, then $|I|/|I_R| = f$.*
   (b) *If $0 \leq t < \min\{m, n\}$, then*

$$|I|/|I_R| = \begin{cases} \frac{|J|}{p^t} & , \text{ if } n - \nu_p(|J|) \leq \min\{m,n\} - t \leq n, \\ \frac{|J| \cdot p^n}{p^{\min\{m,n\} + \nu_p(|J|)}} & , \text{ if } 1 \leq \min\{m,n\} - t < n - \nu_p(|J|). \end{cases}$$

   In particular, $|I|/|I_R|$ is divisible by $(|J|/p^{\nu_p(|J|)})p^{n-m}$ if $m < n$, and it is divisible by $|J|/p^{\nu_p(|J|)}$ if $n \leq m$.

Proof. Let $R = \lambda P + \mu Q$ be a vector of exact order p^n. Then, one of λ and μ is $\not\equiv 0 \bmod p$. We distinguish two cases:

(1) Suppose first that $\lambda \not\equiv 0 \bmod p$ and $\mu \equiv 0 \bmod p^t$, for some $1 \leq t \leq n$. By Lemma 4.4, the subgroup of B that fixes R is

$$I_R = I \cap B_R = I \cap \left\{ \begin{pmatrix} 1 - bp^t/\lambda & b \\ 0 & c \end{pmatrix} : b \in \mathbb{Z}/p^n\mathbb{Z},\ c \equiv 1 \bmod p^{n-t} \right\}.$$

If a matrix $\begin{pmatrix} 1 - bp^t/\lambda & b \\ 0 & c \end{pmatrix}$ is in I_R, then $b \equiv 0 \bmod p^m$, and then $a = (1 - bp^t/\lambda) \in J$ is congruent to 1 mod p^{t+m}. Let $J_{1,b}$ be those elements of J that are congruent to 1 mod p^b, so that $a \in J_{1,t+m}$. If ψ is trivial, or $1 \leq t \leq n-1$, or $p \equiv 1 \bmod 4$ (see Remark 4.6), then $I \cap B_R$ is given by:

$$\begin{aligned} I_R &= \left\{ \begin{pmatrix} 1 - bp^t/\lambda & b \\ 0 & 1 \end{pmatrix} : b \equiv 0 \bmod p^m, 1 - bp^t/\lambda \in J_{1,t+m} \right\} \\ &= \left\{ \begin{pmatrix} 1 - \delta p^{t+m} & (\delta + \tau)p^m\lambda \\ 0 & 1 \end{pmatrix} : \tau \in (p^{n-t}\mathbb{Z}/p^n\mathbb{Z}), 1 - \delta p^{t+m} \in J_{1,t+m} \right\}. \end{aligned}$$

Thus, Lemma 4.5 implies that

$$|I_R| = |J_{1,t+m}| \cdot p^t = \begin{cases} p^{n-(t+m)}p^t = p^{n-m} & ,\ \text{if } n - \nu_p(|J|) \leq t + m \leq n, \\ p^{\nu_p(|J|)}p^t = p^{\nu_p(|J|)+t} & ,\ \text{if } 1 \leq t + m < n - \nu_p(|J|). \end{cases}$$

If we put $N = N(m,n) = \max\{1, p^{n-m}\}$, then

$$|I|/|I_R| = \frac{|J| \cdot N}{|I_R|} = \begin{cases} |J| \cdot N/N = |J| & ,\ \text{if } n - \nu_p(|J|) \leq t + m \leq n, \\ |J| \cdot N/p^{\nu_p(|J|)+t} = |J|p^{n-m-\nu_p(|J|)-t} & ,\ \text{if } 1 \leq t + m < n - \nu_p(|J|). \end{cases}$$

Notice that in the second case the quantity $n - m - \nu_p(|J|) - t$ is greater than 0, and $n - m > t + \nu_p(|J|) \geq 1$, so $N = p^{n-m}$. Thus, in both cases, $|I|/|I_R|$ is divisible by $|J|$

Otherwise, if ψ is non-trivial, $t = n$ and $p \equiv 3 \bmod 4$ (again, Remark 4.6 plays a role here), then it is given by:

$$I \cap B_R = \left\{ \begin{pmatrix} 1 & b \\ 0 & \pm 1 \end{pmatrix} : b \in p^m\mathbb{Z}/p^n\mathbb{Z} \right\}.$$

Hence, $|I_R| = |I \cap B_R| = 2N$. It follows that $|I|/|I_R| = |J| \cdot N/2N = |J|/2$. This shows part (1).

(2) Now, suppose that $\mu \not\equiv 0 \bmod p$ and $\lambda \equiv 0 \bmod p^t$, for some $0 \leq t \leq n$. By Lemma 4.4, the subgroup of I that fixes R is

$$I_R = I \cap \left\{ \begin{pmatrix} a & -(a-1)p^t/\mu \\ 0 & 1 \end{pmatrix} : a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}.$$

Thus, I_R is given by

$$I_R = \left\{ \begin{pmatrix} a & -(a-1)p^t/\mu \\ 0 & 1 \end{pmatrix} : a \in J,\ \psi(a) = 1,\ (a-1)p^t \equiv 0 \bmod p^{\min\{n,m\}} \right\}.$$

Notice that if ψ is trivial, then $\mathrm{Ker}(\psi) = \{a \in J : \psi(a) = 1\}$ has size $|J|$. Otherwise, if ψ is quadratic, then $\mathrm{Ker}(\psi)$ has size $|J|/2$. Next, we distinguish two cases according to whether $m \leq t$.

- If $0 \leq m \leq t \leq n$ or $t = n \leq m$, then $|I_R| = |\operatorname{Ker}(\psi)|$ and $|I|/|I_R| = N = \max\{1, p^{n-m}\}$ or $2N$ depending on whether ψ is trivial or quadratic, respectively. In particular, if $n \leq m$ and $R = \mu Q$ with ψ trivial, then $|I|/|I_R| = 1$.
- If $0 \leq t < \min\{m, n\}$, then

$$I_R = \left\{ \begin{pmatrix} a & -(a-1)p^t/\mu \\ 0 & 1 \end{pmatrix} : a \in J,\ \psi(a) = 1,\ a \equiv 1 \bmod p^{\min\{m,n\}-t} \right\}.$$

Since $\min\{m, n\} > t$, any $a \equiv 1 \bmod p^{\min\{m,n\}-t}$ satisfies $a \equiv 1 \bmod p$ and $\psi(a) = 1$ is automatic. Thus, we have $|I_R| = |J_{1,\min\{m,n\}-t}|$. It follows from Lemma 4.5 that

$$|I|/|I_R| = \begin{cases} \frac{|J| \cdot p^{n-\min\{m,n\}}}{p^{n-(\min\{m,n\}-t)}} = \frac{|J|}{p^t} & , \text{ if } n - \nu_p(|J|) \leq \min\{m, n\} - t \leq n, \\ \frac{|J| \cdot p^{n-\min\{m,n\}}}{p^{\nu_p(|J|)}} = \frac{|J| \cdot p^n}{p^{\min\{m,n\}+\nu_p(|J|)}} & , \text{ if } 1 \leq \min\{m, n\} - t < n - \nu_p(|J|). \end{cases}$$

If $n - \nu_p(|J|) \leq m - t$ and $m \leq n$, then $t \leq \nu_p(|J|) + m - n$ and $|I|/|I_R| = |J|/p^t$ is divisible by $(|J|/p^{\nu_p(|J|)})p^{n-m}$. If $m \geq n$, then $n - \nu_p(|J|) \leq n - t$ implies $t \leq \nu_p(|J|)$ and $|I|/|I_R|$ is divisible by $|J|/\nu_p(|J|)$.

This shows part (2), and concludes the proof of the lemma.

□

Remark 4.8. Let L be a number field with ring of integers $\mathcal{O}_L$, and let $\wp$ be a prime ideal of $\mathcal{O}_L$ lying above a rational prime p. Let E/L be an elliptic curve, and let $R \in E(\overline{L})[p^n]$ be a point of exact order p^n. Let $\iota\colon \overline{L} \hookrightarrow \overline{L}_\wp$ be a fixed embedding. Let $F = L(R)$ and let Ω_R be the prime of F above $\wp$ associated to the embedding ι. Let K be a finite Galois extension of $L_\wp^{\mathrm{nr}}$, such that the ramification index of K over $\mathbb{Q}_p$ is e. Let $\tilde{E}/K$ be a curve isomorphic to E over K, and let $T \in \tilde{E}(K)[p^n]$ be the point that corresponds to $\iota(R)$ on $E(\overline{L}_\wp)$. Suppose that the degree of the extension $K(T)/K$ is g. Since $K/L_\wp^{\mathrm{nr}}$ is of degree $e/e(\wp|p)$, it follows that the degree of $K(T)/L_\wp^{\mathrm{nr}}$ is $eg/e(\wp|p)$.

Let $\mathcal{F} = \iota(F) \subseteq \overline{L}_\wp$. Since E and $\tilde{E}$ are isomorphic over K, it follows that $K(T) = K\mathcal{F}$ and, therefore, the degree of the extension $K\mathcal{F}/L_\wp^{\mathrm{nr}}$ is $eg/e(\wp|p)$. Since $K/L_\wp^{\mathrm{nr}}$ is Galois by assumption, it follows that $g = [K(T) : K] = [\mathcal{F}L_\wp^{\mathrm{nr}} : K \cap \mathcal{F}L_\wp^{\mathrm{nr}}]$, so the degree of $[\mathcal{F}L_\wp^{\mathrm{nr}} : L_\wp^{\mathrm{nr}}]$ equals $g \cdot k$ where $k = [K \cap \mathcal{F}L_\wp^{\mathrm{nr}} : L_\wp^{\mathrm{nr}}]$. Hence, the degree of $\mathcal{F}/L_\wp$ is divisible by gk and, in particular, the ramification index of the prime ideal Ω_R over $\wp$ in the extension $L(R)/L$ is divisible by gk, where $g = [K(T) : K]$.

Moreover, let Ω be the prime of $L(E[p^n])$, lying above $\wp$, associated to the embedding ι, and let $G = \mathrm{Gal}(L(E[p^n])/L)$. Let $I_\Omega \subset D_\Omega \subset G$ be the inertia and decomposition groups associated to Ω. It follows that $I_\Omega \cong \mathrm{Gal}(L_\wp^{\mathrm{nr}}(\iota(E[p^n]))/L_\wp^{\mathrm{nr}})$. Let K and $\tilde{E}$ be as before. Then, by the same argument as above, we have that I_Ω has a subgroup $I_{K,\Omega}$ isomorphic to $\mathrm{Gal}(K(\tilde{E}[p^n])/K)$ such that $\sigma \in I_{K,\Omega}$ acts on $R \in E[p^n]$ just like $\sigma \in \mathrm{Gal}(K(\tilde{E}[p^n])/K)$ acts on $\iota(R) \in \tilde{E}[p^n]$.

Now let Ω' be another prime of $L(E[p^n])$ lying above $\wp$, and let ι' be the corresponding embedding of $\overline{L}$ into $\overline{L}_\wp$. Then ι and ι' differ by an automorphism ρ of $\overline{L}_\wp$, i.e., $\rho \circ \iota' = \iota$, which sends $\iota(\Omega')$ to $\iota(\Omega)$, i.e., $\rho(\iota(\Omega')) = \iota(\Omega)$. By abuse of notation we will also call ρ the restriction of ρ to $\iota'(L(E[p^n])) \cong L(E[p^n])$, so that ρ may be regarded as an element of $\mathrm{Gal}(L(E[p^n])/L)$. As such, $\rho(\Omega') = \Omega$. Moreover,

$$D_\Omega = \rho D_{\Omega'} \rho^{-1}, \quad \text{and} \quad I_\Omega = \rho I_{\Omega'} \rho^{-1}.$$

Let $R' \in E[p^n]$ and let $I_{R'}$ be the elements of $I_{\Omega'}$ that fix R'. If $\rho(R') = R$, then

$$I_R = \rho I_{R'} \rho^{-1}.$$

Let Ω_R be the prime of $L(R)$ lying above $\wp$ and below Ω, and let $\Omega_{R'}$ be the prime of $L(R')$ lying above $\wp$ and below Ω'. It follows from our comments above that

$$e(\Omega_R|\wp) = \frac{|I_\Omega|}{|I_R|} = \frac{|I_{\Omega'}|}{|I_{R'}|} = e(\Omega_{R'}|\wp),$$

where $\rho(\Omega_{R'}) = \Omega_R$.

Theorem 4.9. *Let L be a number field with ring of integers $\mathcal{O}_L$, and let $\wp$ be a prime ideal of $\mathcal{O}_L$, lying above a rational prime p. Let $n \geq 1$ be fixed, let E/L be an elliptic curve, let Ω be a prime of $L(E[p^n])$ lying above $\wp$ and let I_Ω be the associated inertia subgroup in $\mathrm{Gal}(L(E[p^n])/L)$. Suppose that there is a $\mathbb{Z}/p^n\mathbb{Z}$-basis $\{P, Q\}$ of $E[p^n]$ such that the inertia subgroup I_Ω contains a subgroup I of the form*

$$I = \left\{ \begin{pmatrix} \chi_n\psi & * \\ 0 & \psi^{-1} \end{pmatrix} : * \equiv 0 \bmod p^m \right\} \subseteq I_\Omega,$$

for some $m \geq 0$, where $\chi_n \colon I \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ is the p^n-th cyclotomic character, and $\psi \colon I \to \{\pm 1\}$ is a trivial or quadratic character. Let $\delta = \delta(\psi)$ and $f = f(\psi)$ be as in the statement of Lemma 4.7, and write $|\chi_n|$ for the size of the image of χ_n. If $R \in E[p^n]$, we write Ω_R for the prime of $L(R)$ below Ω and above $\wp$.

(i) *There exists a point $R \in E[p^n]$ of exact order p^n with $e(\Omega_R|\wp)$ divisible by $f(\psi)\max\{1, p^{n-m}\}$ (and equality if $I = I_\Omega$). If $m \geq n$, $I = I_\Omega$, $L(R)/L$ is Galois and ψ is unramified (over $\wp$), then the extension is unramified at $\wp$. Otherwise, there is another prime Ω' of $L(E[p^n])$ over $\wp$ such that $e(\Omega'_R|\wp)$ is either $|\chi_n|/\delta(\psi)$ or divisible by $|\chi_n|/p^{\nu_p(|\chi_n|)}$.*

(ii) *If $0 \leq m < n$, then the ramification index of any prime ideal Ω_R over $\wp$ in the extension $L(R)/L$ is divisible by $|\chi_n|/\delta(\psi)$ or $f(\psi)\cdot p^{n-m}$, or $(|\chi_n|/p^{\nu_p(|\chi_n|)})p^{n-m}$, for any point $R \in E$ of exact order p^n.*

(iii) *If R is a point of exact order p^n, the subgroup $\langle [p^{n-a}]R\rangle \subset E[p^a]$ is not $\mathrm{Gal}(\overline{L}/L)$-stable for some $a \geq 1$, then there is a prime Ω''_R of $L(R)$ over $\wp$ such that $e(\Omega''_R|\wp)$ is divisible by $|\chi_n|/\delta(\psi)$, or $f(\psi)p^{n-a+1}$, or $|\chi_n|/p^{\min\{a-1,\nu_p(|\chi_n|)\}}$.*

(iv) *If R is a point of exact order p^n, and the subgroup $\langle [p^{n-a}]Q\rangle \subset E[p^a]$ is not $\mathrm{Gal}(\overline{L}/L)$-stable for some $a \geq 1$, then the same conclusion as in part (iii) holds for $L(R)$.*

(v) *If $\langle [p^{n-a}]Q\rangle \subset E[p^a]$ is $\mathrm{Gal}(\overline{L}/L)$-stable for some $1 \leq a \leq n$, then $m \geq a$. Equivalently, if $m \leq a-1$ for some $1 \leq a \leq n$, then $\langle [p^{n-a}]Q\rangle$ is not $\mathrm{Gal}(\overline{L}/L)$-stable.*

Proof. Let E/L, $R \in E[p^n]$, $\wp$, and Ω be as in the statement of the theorem, let $L_\wp$ be the completion of L at $\wp$, let $I_\Omega = I(\Omega|\wp)$ be the inertia subgroup of associated to Ω, and suppose that $I \subseteq I_\Omega \subseteq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is of the form given in the statement of the theorem, with respect to a basis $\{P, Q\}$ of $E[p^n]$. By putting $V = E[p^n]$, $I = I$, and letting J be the image of χ_n, we may use the results of Lemma 4.7. Moreover, notice that if $R \in E[p^n]$ and $I_{\Omega,R}$ is the subgroup of I_Ω that fixes R, then

$$e(\Omega_R|\wp) = |I_\Omega|/|I_{\Omega,R}|,$$

where Ω_R is the prime of $L(R)$ below Ω. In particular, if we write $I_R = I \cap I_{\Omega,R}$, then $|I|/|I_R|$ is a divisor of $e(\Omega_R|\wp)$, with equality if $I = I_\Omega$.

First, by Lemma 4.7 part (2a), if $R \in \langle Q\rangle$, then the ramification index $e(\Omega_R|\wp)$ of $L(R)/L$ is divisible by $f(\psi)\max\{1, p^{n-m}\}$. If $L(R)/L$ is Galois, $m \geq n$, $I = I_\Omega$, and ψ is unramified over $\wp$, then all the primes above $\wp$ in $L(R)/L$ would be unramified. On the other hand, suppose that $m \geq n$, $I = I_\Omega$, and the prime Ω_R of $L(R)/L$ is unramified (or ramification index of 2 for some $R \in \langle Q\rangle$ of exact order p^n, if ψ is ramified) but the extension is not Galois. This implies that $R \in \langle Q\rangle$, and there is a $\sigma \in \mathrm{Gal}(L(E[p^n])/L)$ such that $L(\sigma(R)) \not\subset L(R)$. Thus, $\sigma(R) \notin \langle R\rangle = \langle Q\rangle$. When $m \geq n$, our Lemma 4.7 implies that $e(\Omega_{\sigma(R)}|\wp)$ is either $|\chi_n|/\delta(\psi)$, or divisible by $|\chi_n|/p^{\nu_p(|\chi_n|)}$, in all cases. Hence, the ramification index of $\Omega'_R = \sigma^{-1}(\Omega_{\sigma(R)})$ in $L(R)/L$ is either $|\chi_n|/\delta(\psi)$, or divisible by $|\chi_n|/p^{\nu_p(|\chi_n|)}$, by Remark 4.8. This completes the proof of (i).

Part (ii) follows directly from Lemma 4.7.

For (iii), suppose that $\langle [p^{n-a}]R\rangle$ is not Galois-stable, for some $1 \leq a \leq n$. Let $P_a = [p^{n-a}]P$ and $Q_a = [p^{n-a}]Q$, so that $\{P_a, Q_a\}$ is a basis of $E[p^a]$. Since $\langle [p^{n-a}]R\rangle$ is not Galois-stable, it follows that there is $\tau \in \mathrm{Gal}(L(E[p^a])/L)$ such that $\tau([p^{n-a}]R) \notin \langle [p^{n-a}]Q\rangle = \langle Q_a\rangle$, i.e., $[p^{n-a}](\tau(R)) \notin \langle Q_a\rangle$. Hence, if $\tau(R) = \lambda P + \mu Q$, we must have $\lambda \not\equiv 0 \bmod p^a$, i.e., $0 \leq \nu_p(\lambda) < a$. By Lemma 4.7, if $\Omega_{\tau(R)}$ is the prime of $L(\tau(R))$ below Ω, then the ramification index $e(\Omega_{\tau(R)}|\wp)$ is divisible by

- (Case (1)): $|\chi_n|/\delta(\psi)$, if $\nu_p(\lambda) = 0$ and $1 \leq \nu_p(\mu) \leq n$.
- (Case (2a)): $f(\psi)p^{n-m} \geq f(\psi)p^{n-a+1}$, if $\nu_p(\mu) = 0$ and $0 \leq m \leq \nu_p(\lambda) < a \leq n$ (notice that in the case (2.a) we cannot have $\nu_p(\lambda) = n \leq m$ because $\nu_p(\lambda) < a \leq n$).
- (Case (2b.i)): $|\chi_n|/p^{\nu_p(\lambda)}$, if $\nu_p(\mu) = 0$, and $0 \leq \nu_p(\lambda) < \min\{m, n\}$, and $n - \nu_p(|\chi_n|) \leq \min\{m, n\} - \nu_p(\lambda) \leq n$. In this case, $\nu_p(|\chi_n|) - \nu_p(\lambda) \geq n - \min\{m, n\} \geq 0$, so $|\chi_n|/p^{\nu_p(\lambda)} \in \mathbb{Z}$. Since $\nu_p(\lambda) < a$, then $e(\Omega_{\tau(R)}|\wp)$ is divisible by $|\chi_n|/p^{\min\{a-1,\nu_p(|\chi_n|)\}}$.
- (Case (2b.ii)): $(|\chi_n|/p^{\nu_p(|\chi_n|)})p^{n-\min\{m,n\}}$, if $\nu_p(\mu) = 0$, and $0 \leq \nu_p(\lambda) < \min\{m, n\}$, and $n - \nu_p(|\chi_n|) > \min\{m, n\} - \nu_p(\lambda) \geq 1$. Notice that in this case, $n - \min\{m, n\} > \nu_p(|\chi_n|) - \nu_p(\lambda)$, and also $n - \min\{m, n\} \geq 0$. Thus,

$$\begin{aligned} n - \min\{m, n\} &\geq \max\{0, \nu_p(|\chi_n|) - \nu_p(\lambda)\} \\ &\geq \max\{0, \nu_p(|\chi_n|) - (a-1)\} \\ &= \nu_p(|\chi_n|) - \min\{a-1, \nu_p(|\chi_n|)\}. \end{aligned}$$

  Thus, $(|\chi_n|/p^{\nu_p(|\chi_n|)})p^{n-\min\{m,n\}}$ is divisible by $|\chi_n|/p^{\min\{a-1,\nu_p(|\chi_n|)\}}$.

Hence, the ramification index of $\Omega''_R = \tau^{-1}(\Omega_{\tau(R)})$ in $L(R)/L$ is divisible by $|\chi_n|/\delta(\psi)$, or $f(\psi)p^{n-a+1}$, or $|\chi_n|/p^{\min\{a-1,\nu_p(|\chi_n|)\}}$. This shows (iii).

Finally, for (iv), suppose that $\langle [p^{n-a}]Q\rangle$ is not Galois-stable, for some $1 \leq a \leq n$. Let $P_a = [p^{n-a}]P$ and $Q_a = [p^{n-a}]Q$, so that $\{P_a, Q_a\}$ is a basis of $E[p^a]$. Since $\langle [p^{n-a}]Q\rangle$ is not Galois-stable, it follows that there is $\tau \in \mathrm{Gal}(L(E[p^a])/L)$ such that $\tau([p^{n-a}]R) \notin \langle [p^{n-a}]Q\rangle = \langle Q_a\rangle$, i.e., $[p^{n-a}](\tau(R)) \notin \langle Q_a\rangle$. The rest of the argument can now proceed as in (iii).

Part (v) is clear, as $\langle [p^{n-s}]Q\rangle$ is not stable under $I \subseteq I_\Omega$ as long as $s > m$. This concludes the proof of the theorem. □

Remark 4.10. Let $\Xi_n \colon \mathrm{Gal}(L(E[p^n])/L) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ be the p^n-th cyclotomic character, so that χ_n is the restriction of Ξ_n to the inertia subgroup I_Ω for a fixed prime Ω of $L(E[p^n])$ above $\wp$. Since $L(E[p^n])/L$ is Galois and Ξ_n is a character, the image of χ_n is independent of the chosen prime Ω above $\wp$. Let $|\Xi_n|$ be the size of the image of Ξ_n. The character Ξ_n factors through

$$\mathrm{Gal}(L(E[p^n])/L)/\mathrm{Gal}(L(E[p^n])/L(\mu_{p^n})) \cong \mathrm{Gal}(L(\mu_{p^n})/L) \to (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Let $\chi\colon \mathrm{Gal}(L(\mu_{p^n})/L) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$, let $\mathfrak{P}$ be the prime of $L(\zeta_{p^n})$ below Ω, and let $I_{\mathfrak{P}}$ be the inertia subgroup in $\mathrm{Gal}(L(\mu_{p^n})/L)$. Then $I_{\mathfrak{P}} \cong \chi(I_{\mathfrak{P}}) \cong \chi_n(I_\Omega)$, and $|I_{\mathfrak{P}}| = |\chi_n(I_\Omega)| = |\chi_n|$ is divisible by the quantity $\varphi(p^n)/\gcd(\varphi(p^n), e(\wp|p))$, by Lemma 7.5.

In what follows, the subgroup $I \subseteq I_\Omega$ is isomorphic to the Galois group $\mathrm{Gal}(K(E'[p^n])/K)$, where K is a finite extension of $L_\wp^{\mathrm{nr}}$, and E'/K is an elliptic curve isomorphic to E/K, but given by a model with good reduction. In particular, χ_n restricted to I is the p^n-th cyclotomic character

$$\chi_K\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K(E'[p^n])/K) \to (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

A similar argument to the one above (but this time working locally) shows that $|\chi_K|$ is divisible by $\varphi(p^n)/\gcd(\varphi(p^n), e)$, where e is the ramification index in the extension $K/\mathbb{Q}_p$. Finally, notice that $e = e(K/L_\wp^{\mathrm{nr}}) \cdot e(\wp|p)$.

Corollary 4.11. *Let L, $\wp$ a prime of L above $p \geq 2$, E/L, and $I \subseteq I_\Omega$ and $m \geq 0$ as in the statement of Theorem 4.9. Suppose that I corresponds to a Galois group $\mathrm{Gal}(K(E'[p^n])/K)$, where $K/L_\wp^{nr}$ is a finite Galois extension, and E' is a curve isomorphic to E over K. Let e be the ramification index in the extension $K/\mathbb{Q}_p$. Let $\chi_n\colon \mathrm{Gal}(\overline{K}/K) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ be the p^n-th cyclotomic character. Let $R \in E[p^n]$ be a point of exact order p^n.*

1. *Suppose that either E/L does not admit a L-rational isogeny of degree p^a, or $m \leq a-1$. If $n \geq a$, then there is a prime Ω_R of $L(R)$ over $\wp$ such that $e(\Omega_R|\wp)$ is divisible by $|\chi_n|/\delta(\psi)$, or $f(\psi)p^{n-a+1}$, or $|\chi_n|/p^{\min\{a-1,\nu_p(|\chi_n|)\}}$. In particular, $e(\Omega_R|\wp)$ is divisible by $\varphi(p^n)/\gcd(\varphi(p^n), \delta(\psi)ep^{a-1})$ or $f(\psi)p^{n-a+1}$.*
2. *Suppose that $m \geq 1$, and if E/L admits a L-rational isogeny ϕ of degree p, such that $\ker(\phi) = \langle S\rangle \subset E[p]$, then the ramification index of $K(S)/K$ is $> f(\psi)$, or the ramification index of $\wp$ in the Galois extension $L(S)/L$ satisfies*

$$e(\wp, L(S)/L)/\gcd(e(\wp, L(S)/L), e(K/L_\wp^{nr})) > f(\psi).$$

   Then, there is a prime Ω_R of $L(R)$ over $\wp$ such that $e(\Omega_R|\wp)$ is divisible by $|\chi_n|/\delta(\psi)$, or $f(\psi)p^n$, or $|\chi_n|$. In particular, $e(\Omega_R|\wp)$ is divisible by $\varphi(p^n)/\gcd(\varphi(p^n), \delta(\psi)e)$ or $f(\psi)p^n$.
3. *The size of $I \subseteq I_\Omega \subseteq \mathrm{Gal}(L(E[p^n])/L)$ is exactly $|\chi_n|$, for $n \leq m$, and $|\chi_n|p^{n-m}$, for all $n > m$. In particular, $e(\Omega|\wp)$ is divisible by $\varphi(p^n)/\gcd(\varphi(p^n), e)$ for $n \leq m$, and by $\varphi(p^n)p^{n-m}/\gcd(\varphi(p^n), e)$ if $n > m$.*
4. *Let $n \geq 2$, let $\{P, Q\}$ be the basis defined in Theorem 4.9, let $P_1 = [p^{n-1}]P$, and let $H_n = \langle R, E[p^{n-1}]\rangle \subset E[p^n]$, where $[p^{n-1}]R = P_1$. Then, the ramification index in the extension $K(H_n)/K$ is $|\chi_n|$ if $n \leq m$, and $|\chi_n|p^{n-m-1}$ if $n > m$. In particular, the ramification index of a prime above $\wp$ in $L(H_n)/L$ is divisible by $\varphi(p^n)/\gcd(\varphi(p^n), e)$ for $n \leq m$, and by $\varphi(p^n)p^{n-m-1}/\gcd(\varphi(p^n), e)$ if $n > m$.*
5. *Let $n \geq 2$ and $p > 2$, assume that $\nu_p(|\chi_n|) \geq 1$, let $\{P, Q\}$ be as in (3), let $Q_1 = [p^{n-1}]Q$, and let $H_n = \langle R, E[p^{n-1}]\rangle \subset E[p^n]$, where $[p^{n-1}]R = Q_1$. Then, the ramification index in the extension $K(H_n)/K$ is $|\chi_n|/p$ if $n \leq m$ and $|\chi_n|p^{n-m-1}$ if $n > m$. In particular, the ramification index of a prime above $\wp$ in $L(H_n)/L$ is divisible by $\varphi(p^{n-1})/\gcd(\varphi(p^n), e)$ for $n \leq m$, and by $\varphi(p^n)p^{n-m-1}/\gcd(\varphi(p^n), e)$ if $n > m$.*

Proof. We show (1) first. If E/L does not admit a L-rational isogeny of degree p^a, then $\langle S\rangle \subset E[p^a]$ is not $\mathrm{Gal}(\overline{L}/L)$-stable for any $S \in E[p^a]$. In particular, $\langle [p^{n-a}]R\rangle$ is not $\mathrm{Gal}(\overline{L}/L)$-stable. Now we can apply Theorem 4.9, part (iii). If $m \leq a-1$, then $\langle [p^{n-a}]Q\rangle$ is not $\mathrm{Gal}(\overline{L}/L)$-stable (by Thm.

4.9, part (v)). Now we can apply Theorem 4.9, part (iv). The last piece of (1) follows from Remark 4.10, because $|\chi_n|$ is divisible by $\varphi(p^n)/\gcd(\varphi(p^n), e)$.

For (2), suppose that $m \geq 1$, and if E/L admits a L-rational isogeny ϕ of degree p, such that $\ker(\phi) = \langle S \rangle \subset E[p]$, then the ramification index of $K(S)/K$ is $> f(\psi)$, or the ramification index of $\wp$ in the Galois extension $L(S)/L$ satisfies $g = e(\wp, L(S)/L)/\gcd(e(\wp, L(S)/L), e(K/L_\wp^{\mathrm{nr}})) > f(\psi)$. Then, we claim that $\langle Q_1 \rangle \subset E[p]$, with $Q_1 = [p^{n-1}]Q$, cannot be $\mathrm{Gal}(\overline{L}/L)$-stable, and Theorem 4.9, part (iv) can be used with $a = 1$ to conclude (2). Suppose for a contradiction that $\langle Q_1 \rangle \subset E[p]$ is $\mathrm{Gal}(\overline{L}/L)$-stable. Then, there is an isogeny ϕ of degree p with kernel $\langle Q_1 \rangle$. By the structure of $I = \mathrm{Gal}(K(E'[p^n])/K)$, and Lemma 4.7, the ramification index in $K(Q_1)/K$ is $f(\psi)$. However, the ramification in $K(Q_1)/K$ is divisible by

$$\frac{e(L_\wp^{\mathrm{nr}}(Q_1)/L_\wp^{\mathrm{nr}})}{\gcd(e(L_\wp^{\mathrm{nr}}(Q_1)/L_\wp^{\mathrm{nr}}), e(K/L_\wp^{\mathrm{nr}}))} = \frac{e(\wp, L(Q_1)/L)}{\gcd(e(\wp, L(Q_1)/L), e(K/L_\wp^{\mathrm{nr}}))} > f(\psi),$$

a contradiction. This proves (2).

It is clear from our assumptions on the shape of I that $I = \left\{ \begin{pmatrix} \chi_n\psi & 0 \\ 0 & \psi^{-1} \end{pmatrix} \right\}$ for $n \leq m$, and $I = \left\{ \begin{pmatrix} \chi_n\psi & b \\ 0 & \psi^{-1} \end{pmatrix} : b \equiv 0 \bmod p^m \right\}$ for $n \geq m$. Thus, $|I| = |\chi_n| \cdot \max\{1, p^{n-m}\}$ for all $n \geq 1$, which shows (3).

For part (4), let $\{P', Q'\}$ the $\mathbb{Z}/p^n\mathbb{Z}$-basis of $E'[p^n]$ that corresponds to $\{P, Q\}$ via the isomorphism of E and E', and let $R' \in E'$ the point that correspond to $R \in E$. Let $H_n' = \langle R', E'[p^{n-1}] \rangle$, where $[p^{n-1}]R' = P_1'$. Thus, $H_n' = \langle P', E'[p^{n-1}] \rangle$. Let us identify $I = \mathrm{Gal}(K(E'[p^n])/K)$. Then, the group $G_n = \mathrm{Gal}(K(E'[p^n])/K(H_n'))$ is given by

$$G_n = \left\{ A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : A \in I,\ a \equiv 1 \bmod p^n,\ b \equiv 0 \bmod p^{n-1},\ c \equiv 1 \bmod p^{n-1} \right\} \leq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z}).$$

Then, the ramification index of $K(E'[p^n])/K(H_n')$ is given by the size of $I \cap G_n$. Moreover $|I \cap G_n| = 1$ if $2 \leq n \leq m$, and $|I \cap G_n| = p$ if $n > m \geq 2$. Hence, using part (2) we conclude that the ramification in $K(H_n')/K$ is $|\chi_n|$ if $2 \leq n \leq m$, and $|\chi_n|p^{n-m-1}$ if $n > m$ (and $n \geq 2$). Since E and E' are isomorphic over K, the ramification in $K(H_n')/K$ and $K(H_n)/K$ is the same, and this shows (4).

Let $p > 2$ and $n \geq 2$, and let P', Q', and R' be as above. If $H_n' = \langle R', E'[p^{n-1}] \rangle$, where $[p^{n-1}]R' = Q_1'$, then $H_n' = \langle Q', E'[p^{n-1}] \rangle$. Then, the group $G_n = \mathrm{Gal}(K(E'[p^n])/K(H_n'))$ is given by

$$G_n = \left\{ A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : A \in I,\ a \equiv 1 \bmod p^{n-1} \right\} \leq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z}).$$

Moreover $|I \cap G_n|$ is the number of elements in the image of χ_n that are $\equiv 1 \bmod p^{n-1}$. Thus, $|I \cap G_n| = 1$ if $\nu_p(|\chi_n|) = 0$ and $|I \cap G_n| = p$ if $\nu_p(|\chi_n|) \geq 1$. Since we are assuming the latter, using part (2) we conclude that the ramification in $K(H_n')/K$ is $|\chi_n|/p$ if $2 \leq n \leq m$, and $|\chi_n|p^{n-m-1}$ if $n > m$ (and $n \geq 2$), as claimed in (5). □

Lemma 4.12. *Let F be a field of characteristic 0, and let E/F and E'/F be isomorphic elliptic curves (over a fixed algebraic closure $\overline{F}$) with $j(E) = j(E') \neq 0$ or 1728. Let $\phi\colon E \to E'$ be an isomorphism. Then:*

1. *E and E' are isomorphic over F or E' is a quadratic twist of E.*
2. *For all $R \in E(\overline{F})$, we have $F(x(R)) = F(x(\phi(R)))$.*

(3) *Moreover, if* $F(R)/F$ *is Galois, cyclic, and* $[F(x(R)) : F]$ *is even, then the quotient* $[F(\phi(R)) : F]/[F(R) : F] = 1$ *or* 2.

Proof. Let E and E', respectively, be given by Weierstrass equations $y^2 = x^3 + Ax + B$ and $y^2 = x^3 + A'x + B'$, with coefficients in F. Since $j(E) = j(E') \neq 0, 1728$, none of the coefficients is zero. By [43, Ch. III, Prop. 3.1(b)], the isomorphism $\phi\colon E \to E'$ is given by $(x, y) \mapsto (u^2x, u^3y)$ for some $u \in \overline{F} \setminus \{0\}$. Hence $A' = u^4A$ and $B' = u^6B$, and so $u^2 \in F$. Thus, either $E \cong_F E'$, or E' is the quadratic twist of E by u. This shows (1).

Let $R \in E(\overline{F})$. If $E \cong_{\mathbb{Q}} E'$ then $F(R) = F(\phi(R))$ and the same holds for the subfields of the x-coordinates, so (2) and (3) are immediate. Let us assume for the rest of the proof that E' is the quadratic twist of E by $\sqrt{d}$, for some $d \in F \setminus F^2$. It follows that $\phi((x, y)) = (dx, d\sqrt{d} \cdot y)$ and, therefore, $F(x(\phi(R))) = F(d \cdot x(R)) = F(x(R))$. This proves (2).

Let $x = x(R)$ and $y = y(R)$. Then $F(R) = F(x, y)$ and $F(\phi(R)) = F(x, \sqrt{d} \cdot y)$. The degree of $F(x, y)/F(x)$ is 1 or 2 because y is given by the Weierstrass equation $y^2 = x^3 + Ax + B$.

- If $F(x) = F(x, y) = F(R)$, then $y \in F(x)$ and $F(x, \sqrt{d} \cdot y) = F(x, \sqrt{d})$. Thus, we have $[F(\phi(R)) : F] = [F(x, \sqrt{d}) : F(x)] \cdot [F(x) : F]$ and hence $[F(\phi(R)) : F]/[F(R) : F] = 1$ or 2.
- Suppose $F(x, y)/F(x)$ is quadratic. If $F(x, \sqrt{d} \cdot y)/F(x)$ is also quadratic, then we have $[F(\phi(R)) : F]/[F(R) : F] = 1$. Otherwise, assume that $F(x, \sqrt{d} \cdot y) = F(x)$ and we will reach a contradiction. Indeed, in this case $\sqrt{d} \cdot y \in F(x)$. Hence, there is $z \in F(x)$ such that $y = \sqrt{d} \cdot z$ and we may conclude that $F(x, y) = F(x, \sqrt{d})$. It follows that $\sqrt{d} \in F(R)$. Let $K = F(\sqrt{d}) \subseteq F(R)$. Since $F(R)/F$ is Galois and cyclic, K is the unique quadratic extension of F contained in $F(R)$. Moreover, $F(x)/F$ is of even degree by assumption, and Galois, cyclic because $F(x) \subseteq F(R)$. Thus, $K = F(\sqrt{d}) \subseteq F(x)$. It would follow that $F(x, y) = F(x, \sqrt{d}) = F(x)$ which is a contradiction, since we have assumed that $F(R)/F(x)$ is quadratic.

This proves (3) and concludes the proof of the lemma. □

5. Potential multiplicative reduction

Let L be a number field, and let E/L be an elliptic curve. We say that E/L has *potential multiplicative reduction* at a prime ideal $\wp$ of $\mathcal{O}_L$ if there is an extension of number fields F/L and a prime $\mathfrak{P}$ of $\mathcal{O}_F$ lying above $\wp$ such that E/F has multiplicative reduction at $\mathfrak{P}$. The curve E/F has bad multiplicative reduction at $\mathfrak{P}$ if and only if $\nu_{\mathfrak{P}}(c_4) = 0$ and $\nu_{\mathfrak{P}}(\Delta) > 0$ (for a minimal model at $\mathfrak{P}$), if and only if $\nu_{\mathfrak{P}}(j) < 0$ (because $j = c_4^3/\Delta$; see [43, Proposition 5.1, Ch. VII.5]). If E is defined over $L \subseteq F$, then $\nu_{\mathfrak{P}}(j) < 0$ if and only if $\nu_{\wp}(j) < 0$. Thus, E/L has potential multiplicative reduction at $\wp$ if and only if $\nu_{\wp}(j) < 0$.

Elliptic curves with non-integral j-invariant can be treated using the theory of Tate curves (see [44], Chapter V). Let $L_{\wp}$ be the completion of L at $\wp$, and let $q \in L_{\wp}^*$ such that $\nu_{\wp}(q) > 0$. Let E_q be the elliptic curve given by

$$y^2 + xy = x^3 + a_4x + a_6,$$

with

$$a_4 = -5\sum_{n\geq 1} \frac{n^3q^n}{1-q^n}, \quad \text{and} \quad a_6 = -\frac{1}{12}\sum_{n\geq 1} \frac{(7n^5 + 5n^3)q^n}{1-q^n}.$$

Then, $E_q(\overline{L}_\wp) \cong \overline{L}_\wp^*/q^{\mathbb{Z}}$ as $\mathrm{Gal}(\overline{L}_\wp/L_\wp)$-modules ([44, Ch. V, Thm. 3.1]). Moreover, for each $j_0 \in L_\wp^*$ with $\nu_\wp(j) < 0$ there is a $q \in L_\wp^*$ such that $\nu_\wp(q) > 0$ and $j(E_q) = j_0$ ([44, Ch. V, Lemma 5.1]).

Theorem 5.1. *Let L be a number field, let $\wp$ be a prime ideal of $\mathcal{O}_L$, and let E/L be an elliptic curve with potential multiplicative reduction at $\wp$ (i.e., $\nu_\wp(j) < 0$). Fix an embedding $\iota : \overline{L} \hookrightarrow \overline{L}_\wp$, so that E may be regarded as defined over $L_\wp$ via ι. Then:*

(a) *There is a $q \in L_\wp^*$ such that $\nu_\wp(q) > 0$, and $E/L_\wp$ is a twist of $E_q/L_\wp$ by a trivial or quadratic character $\psi_\wp \colon \mathrm{Gal}(\overline{L}_\wp/L_\wp) \to \{\pm 1\}$.*

(b) *Let $n \geq 1$ be fixed, let Ω be a prime of $L(E[p^n])$ lying above $\wp$, associated to the embedding ι, and let I_Ω be the associated inertia subgroup in $\mathrm{Gal}(L(E[p^n])/L)$. Then, there is a $\mathbb{Z}/p^n\mathbb{Z}$-basis $\{P, Q\}$ of $E[p^n]$ such that the inertia subgroup I_Ω is of the form*

$$I_\Omega = \left\{ \begin{pmatrix} \chi_n\psi & * \\ 0 & \psi^{-1} \end{pmatrix} : * \equiv 0 \bmod p^m \right\},$$

for some $m \geq 0$, where $\chi_n \colon I_\Omega \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ is the p^n-th cyclotomic character, and $\psi \colon I_\Omega \to \{\pm 1\}$ is induced by the character $\psi_\wp$ of part (1).

(c) *The reduction of E/L at $\wp$ is bad multiplicative if and only if the character $\psi_\wp$ is unramified at $\wp$ (i.e., ψ is trivial on I_Ω), if and only if $f(\psi) = 1$ (in the notation of Theorem 4.9).*

(d) *The number m that appears in part (b) satisfies $m \leq \nu_p(-\nu_\wp(j))$.*

(e) *Let χ_n, $\delta(\psi)$, and $f(\psi)$ be as in Theorem 4.9. Suppose that there is a number $a \geq 1$ such that*

- *E/L does not admit a L-rational isogeny of degree p^a, or*
- *$m \leq \nu_p(-\nu_\wp(j)) \leq a - 1$, or*
- *Suppose that $m \geq 1$ (where m is as in (b)), and if E/L admits a L-rational isogeny ϕ of degree p, such that $\ker(\phi) = \langle S \rangle \subset E[p]$, then the ramification index of $\wp$ in the Galois extension $L(S)/L$ satisfies $e(\wp, L(S)/L) > f(\psi)$. If so, here set $a = 1$.*

Then, the conclusions of Cor. 4.11 hold, for every $R \in E[p^n]$ of exact order p^n, with $n \geq a$. Then there is a prime Ω_R of $L(R)$ over $\wp$ such that $e(\Omega_R|\wp)$ is divisible by $|\chi_n|/\delta(\psi)$, or $f(\psi)p^{n-a+1}$, or $|\chi_n|/p^{\min\{a-1, \nu_p(|\chi_n|)\}}$. In particular, $e(\Omega_R|\wp)$ is divisible by

$$\varphi(p^n)/\gcd(\varphi(p^n), \delta(\psi)e(\wp|p)p^{a-1}) \text{ or } f(\psi)p^{n-a+1}.$$

(f) *Suppose that $m \geq 1$ (where m is as in (b)), and if E/L admits a L-rational isogeny ϕ of degree p, such that $\ker(\phi) = \langle S \rangle \subset E[p]$, then the ramification index of $K(S)/K$ is > 1, or the ramification index of $\wp$ in the Galois extension $L(S)/L$ satisfies*

$$e(\wp, L(S)/L)/\gcd(e(\wp, L(S)/L), e(K/L_\wp^{nr})) > 1,$$

where $K/L_\wp^{nr}$ is the smallest extension such that E/K has multiplicative reduction. Then, there is a prime Ω_R of $L(R)$ over $\wp$ such that $e(\Omega_R|\wp)$ is divisible by

$$\varphi(p^n)/\gcd(\varphi(p^n), [K : L_\wp^{nr}]e(\wp|p)) \text{ or } p^n,$$

where $[K : L_\wp^{nr}] = 1$ or 2.

Proof. Let L, $\wp$, E/L, and ι be as in the statement of the theorem and let $j_0 = j(E)$. By assumption, $\nu_\wp(j_0) < 0$. By the theory of Tate curves (see our remarks at the beginning of this section), there is a $q \in L_\wp^*$ such that $\nu_\wp(q) > 0$ and $j(E_q) = j_0$. By Lemma 4.12, part (1), the curves $E/L_\wp$ and $E_q/L_\wp$ are either isomorphic over $L_\wp$, or they are a quadratic twist of each other. This proves (a).

Since $E_q(L_\wp) \cong L_\wp/q^{\mathbb{Z}}$ (see [44, Ch. V, Theorem 3.1.(d)]), it follows that

$$L_\wp(E_q[p^n]) \cong L_\wp(\zeta_{p^n}, q^{1/p^n}).$$

In particular, there is a basis $\{P, Q\}$ of $E_q[p^n]$ such that the inertia subgroup I of $\mathrm{Gal}(L_\wp(E_q[p^n])/L_\wp)$ is of the form

$$I = \left\{ \begin{pmatrix} \chi_n & b \\ 0 & 1 \end{pmatrix} : b \equiv 0 \bmod p^m \right\},$$

where $\chi_n \colon I \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ is the p^n-th cyclotomic character, and m is the largest non-negative integer such that $q \in (L_\wp^*)^{p^m}$. By part (a), the curve $E/L_\wp$ is a twist of E_q by some trivial or quadratic character $\psi_\pi \colon \mathrm{Gal}(\overline{L_\wp}/L_\wp) \to \{\pm 1\}$. Since $I_\Omega = I(\Omega|\pi) \cong I$, and if we define $\psi \colon I_\Omega \cong I \to \{\pm 1\}$ character induced by ψ_π, then it is clear that I_Ω has the shape claimed by the statement of the theorem. This shows (b).

Part (c) follows from the fact that E and E_q are isomorphic over $L_\wp$ if and only if E/L has split multiplicative reduction at $\wp$ ([44, Ch. V, Theorem 5.3(b)]). If E/L has non-split multiplicative reduction, then E and E_q are isomorphic over a quadratic unramified extension of $L_\wp$, and so in this case $\psi_\wp$ is non-trivial, but its restriction to inertia is trivial (i.e., ψ is unramified). Finally, if E/L has additive reduction (potential multiplicative), then E and E_q are isomorphic over a quadratic ramified extension of $L_\wp$, and in this case ψ is quadratic, non-trivial, and ramified.

We have seen that m is the largest non-negative integer such that $q \in (L_\wp^*)^{p^m}$. Since $q \in L_\wp^*$ and $\nu_\wp(q) > 0$, it follows that $\nu_\wp(q)$ is a positive multiple of p^m. Hence, $-\nu_\wp(j) = \nu_\wp(q)$ is a multiple of p^m or, in other words, $\nu_p(-\nu_\wp(j)) \geq m$. This shows (d).

Suppose that one of the three conditions listed in (e) is satisfied for $a \geq 1$. In order to apply Corollary 4.11, we let $K = L_\wp^{\mathrm{nr}}$ and the needed hypothesis is that $e(L_\wp^{\mathrm{nr}}(S)/L_\wp^{\mathrm{nr}}) = e(\wp, L(S)/L) > f(\psi)$. Thus, the results cited in (e) follow from Cor. 4.11.

Otherwise, for (f), let $K/L_\wp^{\mathrm{nr}}$ be the smallest extension such that E/K has multiplicative reduction. In this case, K is the fixed field by the kernel of $\psi_\wp$ which is a trivial or quadratic character, so $[K : L_\wp^{\mathrm{nr}}] = 1$ or 2, and over K, $\psi_\wp$ is trivial (so $f(\psi) = 1$ in this case). Now the needed hypothesis to apply Cor. 4.11 is that $K(S)/K > 1$ or $e(\wp, L(S)/L)/\gcd(e(\wp, L(S)/L), e(K/L_\wp^{\mathrm{nr}})) > 1$. Moreover, $e = e(K/\mathbb{Q}_p) = [K : L_\wp^{\mathrm{nr}}]e(\wp|p)$. Hence, there is a prime Ω_R of $L(R)$ over $\wp$ such that $e(\Omega_R|\wp)$ is divisible by

$$\varphi(p^n)/\gcd(\varphi(p^n), [K : L_\wp^{\mathrm{nr}}]e(\wp|p)) \text{ or } p^n,$$

as desired. □

6. Potential good reduction

Let L be a number field with ring of integers $\mathcal{O}_L$, let $p \geq 2$ be a prime, let $\wp$ be a prime ideal of $\mathcal{O}_L$ lying above p, and let $L_\wp$ be the completion of L at $\wp$. Let E be an elliptic curve defined over L with potential good (ordinary or supersingular) reduction at $\wp$. Let us fix an embedding $\iota : \overline{L} \hookrightarrow \overline{L}_\wp$. Via ι, we may regard E as defined over $L_\wp$. Let $L_\wp^{\mathrm{nr}}$ be the maximal unramified extension of $L_\wp$.

We follow Serre and Tate (see in particular [41] p. 498, Cor. 3) to define an extension K_E of $L_\wp^{\mathrm{nr}}$ of minimal degree such that E has good reduction over K_E. Let ℓ be any prime such that $\ell \neq p$, and let $T_\ell(E)$ be the ℓ-adic Tate module. Let $\rho_{E,\ell} \colon \mathrm{Gal}(\overline{L_\wp^{\mathrm{nr}}}/L_\wp^{\mathrm{nr}}) \to \mathrm{Aut}(T_\ell(E))$ be the usual representation induced by the action of Galois on $T_\ell(E)$. We define the field K_E as the extension of $L_\wp^{\mathrm{nr}}$ such that

$$\mathrm{Ker}(\rho_{E,\ell}) = \mathrm{Gal}(\overline{L_\wp^{\mathrm{nr}}}/K_E).$$

In particular, the field K_E enjoys the following properties:

(1) E/K_E has good (ordinary or supersingular) reduction.
(2) K_E is the smallest extension of $L_\wp^{\mathrm{nr}}$ such that E/K_E has good reduction, i.e., if $K'/L_\wp^{\mathrm{nr}}$ is another extension such that E/K' has good reduction, then $K_E \subseteq K'$.
(3) $K_E/L_\wp^{\mathrm{nr}}$ is finite and Galois. Moreover (see [39], §5.6, p. 312 when $L = \mathbb{Q}$, but the same reasoning holds over number fields, as the work of Néron is valid for any local field, [35] pp. 124-125):
   - If $p > 3$, then $K_E/L_\wp^{\mathrm{nr}}$ is cyclic of degree $1, 2, 3, 4$, or 6.
   - If $p = 3$, the degree of $K_E/L_\wp^{\mathrm{nr}}$ is a divisor of 12.
   - If $p = 2$, the degree of $K_E/L_\wp^{\mathrm{nr}}$ is $2, 3, 4, 6, 8$, or 24.

Let e be the ramification index in $K_E/\mathbb{Q}_p$. Since $e/e(\wp|p) = [K_E : L_\wp^{\mathrm{nr}}]$, the value of e can be obtained directly from $e(\wp|p)$ and a model of E/L, thanks to the classification of Néron models. As a reference for the following theorem, the reader can consult [35], pp. 124-125, or [39], §5.6, p. 312, where $\mathrm{Gal}(K_E/L_\wp^{\mathrm{nr}})$ is denoted by Φ_p, and therefore $e/e(\wp|p) = \mathrm{Card}(\Phi_p)$. Notice, however, that the section we cite of [39] restricts its attention to the case $L = \mathbb{Q}$.

Theorem 6.1. *Let $p > 3$, let E/L be an elliptic curve with potential good reduction, and let Δ_L be the discriminant of any model of E defined over L. Let K_E be the smallest extension of $L_\wp^{nr}$ such that E/K_E has good reduction. Then $e/e(\wp|p) = [K_E : L_\wp^{nr}] = 1, 2, 3, 4,$ or 6. Moreover:*

- *$e/e(\wp|p) = 2$ if and only if $\nu_\wp(\Delta_L) \equiv 6 \bmod 12$,*
- *$e/e(\wp|p) = 3$ if and only if $\nu_\wp(\Delta_L) \equiv 4$ or $8 \bmod 12$,*
- *$e/e(\wp|p) = 4$ if and only if $\nu_\wp(\Delta_L) \equiv 3$ or $9 \bmod 12$,*
- *$e/e(\wp|p) = 6$ if and only if $\nu_\wp(\Delta_L) \equiv 2$ or $10 \bmod 12$.*

Let $K = K_E$, and let ν_K be a valuation on K such that $\nu_K(p) = e$ and $\nu_K(\pi) = 1$, where π is a uniformizer for K. Let A be the ring of elements of K with valuation ≥ 0, let $\mathcal{M}$ be the maximal ideal of A, and let $\mathbb{F} = A/\mathcal{M}$ be the residue field of K. We fix a minimal model of E over A with good reduction, given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in A$. In particular, the discriminant Δ is a unit in A. Moreover, since E/A has good reduction, we have an exact sequence

$$0 \to X_{p^n} \to E(\overline{K})[p^n] \to \widetilde{E}(\overline{\mathbb{F}})[p^n] \to 0,$$

where $\pi_n \colon E(\overline{K})[p^n] \to \widetilde{E}(\overline{\mathbb{F}})[p^n]$ is the homomorphism given by reduction modulo $\mathcal{M}$, and X_{p^n} is the kernel of π_n (see [43, Ch. VII, Thm. 2.1]). By taking inverse limits and tensoring with $\mathbb{Q}_p$, we obtain another exact sequence

$$0 \to X \to V_p(E) \to V_p(\widetilde{E}) \to 0,$$

where $X = (\varprojlim X_{p^n}) \otimes \mathbb{Q}_p$, and $V_p(E) = T_p(E) \otimes \mathbb{Q}_p$. We distinguish two cases, according to whether the Hasse invariant of $E/\mathbb{F}$ is non-zero (ordinary reduction) or zero (supersingular reduction).

6.1. **Good ordinary reduction.** Let E/K be an elliptic curve with good ordinary reduction, i.e., the reduction of E mod $\mathcal{M}$, denoted by $\widetilde{E}/\mathbb{F}$, is an elliptic curve and its Hasse invariant is non-zero. It follows that X_{p^n} and $\widetilde{E}(\overline{\mathbb{F}})[p^n]$ are groups with p^n elements ([43, Ch. V, Thm. 3.1]). The Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ fixes X_{p^n}. If we choose a $\mathbb{Z}/p^n\mathbb{Z}$-basis $\{P_n, Q_n\}$ of $E(\overline{K})[p^n]$, such that

$X_{p^n} = \langle P_n \rangle$, then $D_{K,n}$, the image of G_K in $\mathrm{Aut}(E[p^n]) = \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$, is contained in a Borel subgroup, i.e.,

$$D_{K,n} \leq \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}.$$

Let $I_K \leq G_K$ be the inertia subgroup and let $I_{K,n}$ be the image of I_K in $\mathrm{Aut}(E[p^n]) = \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. Then I_K acts on X_{p^n} via $\chi\colon G_K \to (\mathbb{Z}/p^n\mathbb{Z})^\times$, the cyclotomic character modulo p^n, and I_K acts on $\widetilde{E}(\overline{\mathbb{F}})[p^n]$, trivially (see [39, Prop. 11]). Thus,

$$I_{K,n} \leq \left\{ \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix} \right\}.$$

In what follows, we fix a prime $\overline{\Omega}$ of $\overline{L}$ over $\wp$, and let $\iota : \overline{L} \hookrightarrow \overline{L}_\wp$ be the embedding associated to $\overline{\Omega}$. Via ι, we may consider an elliptic curve E/L as an elliptic curve defined over $L_\wp$. Let Ω be a prime of $L(E[p^n])$ lying under $\overline{\Omega}$, and let $D_{\Omega,n}$ and $I_{\Omega,n}$ be respectively the decomposition and inertia subgroups of $\mathrm{Gal}(L(E[p^n])/L)$ associated to Ω. In this setting $D_{K,n}$, the image of G_p in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$, can be identified with a subgroup of $D_{\Omega,n}$, and $I_{K,n}$ is a subgroup of the inertia subgroup of $I_{\Omega,n}$, with equality if $K = L_\wp^{\mathrm{nr}}$ (i.e., if E/L has good reduction and not just *potential* good reduction).

Lemma 6.2. *Let $p > 2$. Let E/L be an elliptic curve with potential good ordinary reduction at a prime $\wp$ of L, and let $K/L_\wp^{nr}$ be as before. With notation as above, suppose that $I_{K,m}$ is diagonalizable but $I_{K,m+1}$ is not, for some $m \geq 1$ (or $m = \infty$ if $I_{K,m}$ is diagonalizable for all $m \geq 1$). Then there is a $\mathbb{Z}_p$-basis $\mathcal{B}$ of $T_p(E)$ such that the image of inertia, I_K, has the following structure:*

$$I_K = \left\{ \begin{pmatrix} \chi & b \\ 0 & 1 \end{pmatrix} : b \equiv 0 \bmod p^m \right\} \leq \mathrm{GL}(2, \mathbb{Z}_p),$$

where $\chi\colon \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}_p^\times$ is the cyclotomic character.

Proof. By the remarks at the beginning of this section, we know that each $I_{K,n}$ and $I_K = \varprojlim I_{K,n}$ are Borel subgroups of the form $\left\{ \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix} \right\}$, with respect to some basis $\{P, Q\}$ of $E[p^n]$ or $T_p(E)$, respectively, where χ is the cyclotomic character. By Lemma 4.2, there is a basis $\{P, Q'\}$ such that $I_K = I_d I_1$, where

$$I_d = \left\{ \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix} \right\}, \quad \text{and} \quad I_1 = I_K \cap \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}.$$

Since I_1 is an abelian subgroup of I_K, the top right coordinates of the matrices in I_1 form an additive subgroup H of $\mathbb{Z}_p$, say $H = p^t\mathbb{Z}_p$ for some $t \geq 0$. Thus,

$$I_1 = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in p^t\mathbb{Z}_p \right\}.$$

First, suppose that m is finite. Since $I_{K,m} \equiv I_K \bmod p^m$ is diagonalizable, we must have $t \geq m$, and since $I_{K,m+1}$ is not diagonalizable, it follows $t = m$. This shows that

$$I_K = \left\{ \begin{pmatrix} \chi & b \\ 0 & 1 \end{pmatrix} : b \equiv 0 \bmod p^m \right\} \leq \mathrm{GL}(2, \mathbb{Z}_p),$$

as desired. If $m = \infty$, then t must be arbitrarily large, and so $b \in (0)$. □

By Lemma 6.2, the inertia subgroup I_K is a Borel (with trivial character ψ as in the notation of Lemma 4.7, so $\delta(\psi) = f(\psi) = 1$), and we can use the machinery of Section 4. In particular, Theorem 4.9 and Corollary 4.11, together with our previous remarks in this section, imply the following result.

Theorem 6.3. *Let L be a number field, $\wp$ a prime of L above $p > 2$, and let E/L be an elliptic curve with potential good ordinary reduction at $\wp$. Let $K/L_\wp^{nr}$ be smallest extension such that there is a curve E'/K, isomorphic to E over K, with good reduction. Let $I_{K,n}$ be inertia subgroup of $\mathrm{Gal}(K(E'[p^n])/K)$. Suppose there is $m \geq 1$ such that $I_{K,m}$ is diagonalizable, but $I_{K,m+1}$ is not (or put $m = \infty$). Further, suppose that there is a number $a \geq 1$ such that*

1. *E/L does not admit a L-rational isogeny of degree p^a, or*
2. *$m \leq a - 1$, or*
3. *If E/L admits a L-rational isogeny ϕ of degree p, with $\ker(\phi) = \langle S \rangle \subset E[p]$, then the ramification index of $K(S)/K$ is > 1, or the ramification index of $\wp$ in the Galois extension $L(S)/L$ satisfies*

$$e(\wp, L(S)/L)/\gcd(e(\wp, L(S)/L), e(K/L_\wp^{nr})) > 1.$$

In this case, the conclusions below work with $a = 1$.

Then, Cor. 4.11 holds for E/L and the value of a given by (1), (2), or (3). *In particular, if $R \in E[p^n]$ is a point of exact order p^n, with $n \geq a$, then there is a prime Ω_R of $L(R)$ over $\wp$ such that $e(\Omega_R|\wp)$ is divisible by $|\chi_n|$, or p^{n-a+1}, or $|\chi_n|/p^{\min\{a-1,\nu_p(|\chi_n|)\}}$. In particular, $e(\Omega_R|\wp)$ is divisible by*

$$\varphi(p^n)/\gcd(\varphi(p^n), e \cdot p^{a-1}) \text{ or } p^{n-a+1}.$$

Moreover, the number e is a divisor of $12e(\wp|p)$. If $p > 3$, the number e is a divisor of 4 if $\nu_\wp(\Delta_L) \equiv 3, 6$, or $9 \bmod 12$, and e is a divisor of 6 if $\nu_\wp(\Delta_L) \equiv 2, 4, 8$, or $10 \bmod 12$.

We apply Theorem 6.3 to study elliptic curves over $\mathbb{Q}$ with potential good ordinary reduction.

Proposition 6.4. *Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be elliptic curves with j-invariants $j(E) = -7 \cdot 11^3$ and $j(E') = -7 \cdot 137^3 \cdot 2083^3$. Let $f = 1$ if $E/\mathbb{Q}$ has good reduction at $p = 37$, and let $f = 2$ otherwise (and define f' similarly). Then:*

1. *E (resp. E') is a quadratic twist of $E_1/\mathbb{Q}$ (resp. $E_1'/\mathbb{Q}$), the curve with Cremona label "1225h1" (resp. "1225h2") and good ordinary reduction at $p = 37$.*
2. *E and E' admit a $\mathbb{Q}$-rational isogeny of degree 37, but do not admit one of degree 37^2.*
3. *There is a point $R \in E$ of exact order 37 such that the ramification index of the primes above 37 in $\mathbb{Q}(R)/\mathbb{Q}$ is $f(\psi)$, where E (resp. E') is a quadratic twist of $E_1/\mathbb{Q}$ (resp. $E_1'/\mathbb{Q}$) by the character ψ.*
4. *Let $R \in E$ be a point of exact order 37^n, for $n \geq 2$. Then, there is a prime Ω_R of $\mathbb{Q}(R)$ over (37) such that $e(\Omega_R|37)$ is divisible by $\varphi(37^n)/37 = \varphi(37^{n-1})$, or $f \cdot 37^{n-1}$.*
5. *Let $R \in E'$ be a point of exact order 37^n, for $n \geq 1$. Then, there is a prime Ω_R of $\mathbb{Q}(R)$ over (37) such that $e(\Omega_R|37)$ is divisible by $\varphi(37^n)$, or $f' \cdot 37^n$.*

Proof. Let $E_1/\mathbb{Q}$ and $E_1'/\mathbb{Q}$ be the elliptic curves with Cremona labels "1225h1" and "1225h2", respectively. Then, $j(E_1) = -7 \cdot 11^3$ and $j(E_1') = -7 \cdot 137^3 \cdot 2083^3$. By Lemma 4.12, the curves E and E' are, respectively, quadratic twists of E_1 and E_1' associated to some characters ψ_1 and ψ_2. Notice that $f = f(\psi)$ and $f' = f(\psi')$, where $f(\psi)$ is defined in Theorem 4.9, i.e., $f(\psi) = 1$ if ψ is unramified above 37, and $= 2$ otherwise. Note that $\delta(\psi) = \delta(\psi') = 1$ because $p = 37 \equiv 1 \bmod 4$. The fact that the elliptic curves with $j = -7 \cdot 11^3$ and $j = -7 \cdot 137^3 \cdot 2083^3$ have a $\mathbb{Q}$-rational isogeny of degree 37

was discussed in Section 3. The classification of rational isogenies also implies that no elliptic curve over $\mathbb{Q}$ admits an isogeny of degree 37^2.

We can calculate the 37th division polynomial of $E_1/\mathbb{Q}$, using Sage or Magma, and find that there is one non-trivial point $Q_1 \in E_1[37]$ such that $\mathbb{Q}(Q_1)$ is the number field defined by the polynomial

$$\begin{aligned} q(x) = x^{12} + 91x^{11} - 510286x^{10} - 5285035x^9 - 13216280x^8 + 29005256x^7 + 166375776x^6 \\ + 155428049x^5 - 180670105x^4 - 273432740x^3 - 9522366x^2 + 10706059x + 1010821. \end{aligned}$$

Moreover, $\mathbb{Q}(Q_1)/\mathbb{Q}$ is Galois, abelian, and its discriminant is

$$551709470703125 = 5^9 \cdot 7^{10}.$$

Therefore, $\mathbb{Q}(Q_1)$ is unramified at 37. If E is a quadratic twist of E_1 by a quadratic character ψ, then there is some Q_1 such that $\mathbb{Q}(Q_1)$ is Galois, and the ramification at 37 is $f(\psi)$, equal 1 or 2, depending on whether ψ is respectively unramified (E will have good reduction at 37) or ramified at 37 (and E will have bad additive reduction at 37). This shows (3) by choosing $R = Q_1$.

Since $E/\mathbb{Q}$ does not admit isogenies of degree 37^2, we can take $a = 2$. Then, there is a prime Ω_R of $\mathbb{Q}(R)$ over (37) such that $e(\Omega_R|37)$ is divisible by

$$\varphi(37^n)/\gcd(\varphi(37^n), f \cdot 37) = \varphi(37^n)/37 = \varphi(37^{n-1}) \text{ or } f \cdot 37^{n-1},$$

for all $n \geq 2$, as claimed. This shows (4).

The curve E_1' admits a $\mathbb{Q}$-isogeny ϕ of degree 37. The kernel of ϕ, the subgroup $\langle S \rangle$, can be calculated explicitly. The x-coordinates of the points in $\langle S \rangle$ form a Galois extension $\mathbb{Q}(x(S))/Q$, where $x(S)$ is a root of the polynomial

$$\begin{aligned} p(x) = x^{18} + 4540x^{17} + 9432590x^{16} + 11849891575x^{15} + 9976762132800x^{14} \\ + 5848587595725875x^{13} + 2353459307197093375x^{12} + 568092837455595073750x^{11} \\ + 1049716690155251701875 0x^{10} - 581677197638272565035156 25x^9 \\ - 291239579816727642594045625 00x^8 - 864253487447873395174759031 2500x^7 \\ - 181306788248880207598976382743 7500x^6 \\ - 280530629803275669434587526141796875x^5 \\ - 320923174592951987009017556294203906 25x^4 \\ - 265364776129956997628028623910045664062 5x^3 \\ - 150512357183694499353889242415640015234375x^2 \\ - 525141102271763847437919446615343235742187 5x \\ - 3148881707222283483037230006935969560314453125/37. \end{aligned}$$

The extension $\mathbb{Q}(S)/\mathbb{Q}$ is Galois, with discriminant $5^9 \cdot 7^{12} \cdot 37^{17}$, totally ramified at 37 (calculations performed with Magma, and Sage). In particular,

$$e(37, \mathbb{Q}(S)/\mathbb{Q})/\gcd(e(37, \mathbb{Q}(S)/\mathbb{Q}), f) \geq 18/2 = 9 > 1.$$

Hence, E satisfies conditions (b) or (c) of Theorem 6.3 with $a = 1$: either $m(E) = 0$ and (b) applies with $a = 1$, or if $m(E) \geq 1$, then we can pick $a = 1$ by (c). In particular, there is a prime Ω_R of

$\mathbb{Q}(R)$ over (37) such that $e(\Omega_R|37)$ is divisible by

$$\varphi(37^n) \text{ or } f \cdot 37^n,$$

for all $n \geq 1$, as claimed. □

Remark 6.5. Suppose E/L has potential good ordinary reduction, but E is not a CM curve. There is a criterion of Gross to find m such that $I_{K,m}$ is diagonalizable, but $I_{K,m+1}$ is not. We give a version here for curves over $\mathbb{Q}$.

Theorem 6.6 (Gross; see [11], p. 514; see also §14-15)**.** *Let p be a prime, and let $E/\mathbb{Q}$ be an elliptic curve with ordinary good reduction at p, with $j \neq 0, 1728$, and assume that $E[p]$ is an irreducible $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. Let $D_n \leq \mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}) \leq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ be a decomposition group at p. Let $j_E = j(E)$ be the j-invariant of E and let j_0 be the j-invariant of the "canonical lifting" of the reduction of $j(E)$ modulo p, i.e., j_0 is the j-invariant of the unique elliptic curve $E_0/\mathbb{Q}_p$ which satisfies $E_0 \equiv E \bmod p$ and $\mathrm{End}_{\mathbb{Q}_p}(E_0) \equiv \mathrm{End}_{\mathbb{F}_p}(E)$. Then, D_n is diagonalizable if and only if $j_E \equiv j_0 \bmod p^{n+1}$ if p is odd, and $j_E \equiv j_0 \bmod 2^{n+2}$ if $p = 2$.*

6.2. **Good supersingular reduction.** The bounds on the ramification indices of extensions generated by torsion points, in the case of potential supersingular reduction were studied separately by the author in the articles [26] and [28] (see §1 of [26], or §2 of [28] for the definition of e_1). Here we simply quote the two theorems that are needed to show Theorem 2.1 and Theorem 2.2.

Theorem 6.7 ([28, Theorem 5.9])**.** *Let $\eta \geq 1$ and $n \geq 1$ be fixed. Let p be a prime, let L be a number field, and let $\wp$ be a prime ideal of $\mathcal{O}_L$ lying above p, such that $e(\wp|p) \leq \eta$. Let E/L be an elliptic curve with potential supersingular reduction at $\wp$, let $R \in E[p^n]$ be a point of exact order p^n. Then, there is a number $c = c(E/L, R, \wp)$ with $1 \leq c \leq 24\eta$ (with $c \leq 12\eta$ if $p > 2$, and $c \leq 12\eta$ if $p > 3$), such that the ramification index $e(\mathfrak{P}|\wp)$ of any prime $\mathfrak{P}$ above $\wp$ in the extension $L(R)/L$ is divisible by $\varphi(p^n)/\gcd(c, \varphi(p^n))$. Moreover, the following are true.*

1. *There is a constant $f(\eta)$, which depends only on η, such that $c|f(\eta)$. Moreover $f(\eta)$ is a divisor of $F(\eta) = \mathrm{lcm}(\{n : 1 \leq n < 24\eta,\ \gcd(n, 6) \neq 1\})$. If $p > 3$, then $f(\eta)$ is a divisor of $F_0(\eta) = \mathrm{lcm}(\{n : 1 \leq n < 6\eta,\ \gcd(n, 6) \neq 1\})$.*
2. *Let σ be the smallest non-negative integer such that $8\eta \leq 2^\sigma$ (or such that $\eta \leq 5^\sigma$, if $p > 3$). If $n > \sigma + 1$, then $e(\mathfrak{P}|\wp)$ is divisible by $(p-1)p^{2(n-1)-\sigma}/\gcd((p-1)p^{2(n-1)-\sigma}, c)$.*
3. *If $p > 3\eta$, then $e(\mathfrak{P}|\wp)$ is divisible by $(p-1)p^{n-1}/\gcd(p-1, c)$.*
4. *If $\eta = 1$ and $p > 3$, then $e(\mathfrak{P}|\wp)$ is divisible by $(p^2-1)p^{2(n-1)}/6$, or $(p-1)p^{2(n-1)}/\gcd(p-1, 4)$. If $\eta = 1$ and $p = 3$, then $e(\mathfrak{P}|\wp)$ is divisible by $\varphi(3^n)/\gcd(\varphi(3^n), t)$ with $t = 6$ or 9.*

In Table 2, we give a list of every non-cuspidal $\mathbb{Q}$-rational point on the modular curves $X_0(p^n)$ of genus ≥ 1, which correspond to elliptic curves with potential supersingular reduction at the prime p, together with Cremona labels for curves with the given j-invariant and least conductor. See Section 6 of [28]. We also give the values of e and e_1 for each j, which we define next.

We assume from now on that E is an elliptic curve defined over L with potential good supersingular reduction at $\wp$. Let ι, $K = K_E$, and A be as before. We fix a minimal model of E over A with good reduction, given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

Table 2: Elliptic curves with potential supersingular reduction on $X_0(p^n)$

j-invariant	p	Examples	Good reduction over	e	e_1
$j = -2^{15} \cdot 3 \cdot 5^3$	3	27A2, 27A4	$\mathbb{Q}(\sqrt[4]{3}, \beta^3 - 120\beta + 506 = 0)$	12	2
$j = -11 \cdot 131^3$	11	121C2	$\mathbb{Q}(\sqrt[3]{11})$	3	1
$j = -2^{15}$		121B1, 121B2	$\mathbb{Q}(\sqrt[4]{11})$	4	2
$j = -11^2$		121C1	$\mathbb{Q}(\sqrt[3]{11})$	3	2
$j = -17^2 \cdot 101^3/2$	17	14450P1	$\mathbb{Q}(\sqrt[3]{17})$	3	2
$j = -17 \cdot 373^3/2^{17}$		14450P2	$\mathbb{Q}(\sqrt[3]{17})$	3	1
$j = -2^{15} \cdot 3^3$	19	361A1, 361A2	$\mathbb{Q}(\sqrt[4]{19})$	4	2
$j = -2^{18} \cdot 3^3 \cdot 5^3$	43	1849A1, 1849A2	$\mathbb{Q}(\sqrt[4]{43})$	4	2
$j = -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	67	4489A1, 4489A2	$\mathbb{Q}(\sqrt[4]{67})$	4	2
$j = -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	163	26569A1, 26569A2	$\mathbb{Q}(\sqrt[4]{163})$	4	2

Remark: the Cremona labels are the representatives in this class of least conductor.

with $a_i \in A$. Let $\widehat{E}/A$ be the formal group associated to E/A, with formal group law given by a power series $F(X, Y) \in A[[X, Y]]$, as defined in Ch. IV of [43]. Let

$$[p](Z) = \sum_{i=1}^{\infty} s_i Z^i$$

be the multiplication-by-p homomorphism in $\widehat{E}$, for some $s_i \in A$ for all $i \geq 1$. Since E/K has good supersingular reduction, the formal group $\widehat{E}/A$ associated to E has height 2 (see [43, Ch. V, Thm. 3.1]). Thus, $s_1 = p$ and the coefficients s_i satisfy $\nu_K(s_i) \geq 1$ if $i < p^2$ and $\nu_K(s_{p^2}) = 0$. Let $q_0 = 1$, $q_1 = p$ and $q_2 = p^2$, and put $e_i = \nu_K(s_{q_i})$. In particular $e_0 = \nu_K(s_1) = \nu_K(p) = e$, and $e_1 = \nu_K(s_p)$, and $e_2 = \nu_K(s_{p^2}) = 0$. Then, the multiplication-by-p map can be expressed as

$$[p](Z) = pf(Z) + \pi^{e_1} g(Z^p) + h(Z^{p^2}),$$

where $f(Z)$, $g(Z)$ and $h(Z)$ are power series in $Z \cdot A[[Z]]$, with $f'(0) = g'(0) = h'(0) \in A^\times$. The value of e_1 is independent of the chosen minimal model for E/A (see [26, Cor. 3.2]).

Theorem 6.8 ([28, Theorem 6.1])**.** *Let (j_0, p) be any of the j-invariants that are listed in* Table 2*, together with the corresponding prime p of potential supersingular reduction. Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) = j_0$, and let $T_n \in E[p^n]$ be a point of exact order p^n. Then, the ramification index of any prime $\wp$ that lies above p in the extension $\mathbb{Q}(T_n)/\mathbb{Q}$ is divisible by $(p-1)p^{2n-2}/2$ if $p > 3$ and $n \geq 1$, and by 3^{2n-4} if $p = 3$ and $n \geq 3$.*

6.3. **CM curves.** The goal of this section is to show Theorem 1.8. We begin by citing some work of Silverberg, Prasad, and Yogananda (see also [3] for related work).

Theorem 6.9 (Silverberg [42], Prasad-Yogananda [38])**.** *Let L be a number field of degree d, and let E/L be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in the imaginary quadratic field k. Let $w = w(\mathcal{O}) = |\mathcal{O}^\times|$ (so $w = 2, 4$ or 6) and let $\theta \in \mathbb{Z}^+$ be the maximal order of an element of $E(L)_{tors}$. Then:*

1. *$\varphi(\theta) \leq w \cdot d$.*
2. *If $k \subseteq L$, then $\varphi(\theta) \leq \frac{w}{2} d$.*
3. *If L does not contain k, then $\varphi(\#E(L)_{tors}) \leq w \cdot d$.*

An elliptic curve with CM has integral j-invariant and therefore potential good reduction everywhere. Thus, we can apply our results from Section 6 to prove the following theorem, which is analogous to (1) of Theorem 6.9, except that the bound here is in terms of ramification.

Theorem 6.10. *Let L be a number field and let E/L be an elliptic curve with CM by a maximal order $\mathcal{O}_F$ of a quadratic imaginary field F. Let $p \geq 2$ be a prime, $n \geq 1$, and let $R \in E(\overline{L})[p^n]$ be a torsion point of exact order p^n. Then, there if a prime $\mathfrak{P}$ of $\mathcal{O}_{L(R)}$ above a prime $\wp$ of $\mathcal{O}_L$, and an integer $c = c(E/L, \mathfrak{P})$ such that $e(\mathfrak{P}|\wp)$ is divisible by*

$$\varphi(p^n)/\gcd(\varphi(p^n), c).$$

Moreover, if $K_E/L_\wp^{nr}$ is the smallest extension such that E/K_E has good reduction, and $e = e(K_E/\mathbb{Q}_p)$, then $1 \leq c \leq e$. In particular,

$$\varphi(p^n) \leq e \cdot e(\mathfrak{P}|\wp) \leq 24 e(\wp|p) e(\mathfrak{P}|\wp) \leq 24 e(\mathfrak{P}|p).$$

Proof. Let E/L be an elliptic curve with CM by the maximal order $\mathcal{O}_F$ of an imaginary quadratic field F, let p be a prime, and let $R \in E(\overline{L})$ be a point of exact order p^n, for some $n \geq 1$. We distinguish two cases, according to whether p splits in $F/\mathbb{Q}$, or p is inert or ramified in $F/\mathbb{Q}$.

Suppose first that p is inert or ramified in $F/\mathbb{Q}$. Then E has potential supersingular reduction at any prime $\wp$ of $\mathcal{O}_L$ above p. Hence, by Theorem 6.7, for each prime of $\wp$ of $\mathcal{O}_L$ there is a constant $1 \leq c = c(E/L, \wp) \leq 24 e(\wp|p)$, and a prime $\mathfrak{P}$ above $\wp$ in the extension $L(R)/L$ such that $e(\mathfrak{P}|\wp)$ is divisible by

$$\varphi(p^n)/\gcd(\varphi(p^n), c).$$

Hence,

$$\varphi(p^n) \leq c \cdot e(\mathfrak{P}|\wp) \leq 24 e(\wp|p) e(\mathfrak{P}|\wp) = 24 e(\mathfrak{P}, L(R)/\mathbb{Q}).$$

Now suppose that p is split in $F/\mathbb{Q}$. Then E has potential ordinary reduction at primes of $\mathcal{O}_L$ above p. Suppose that $p\mathcal{O}_F = \mathfrak{p}\overline{\mathfrak{p}}$. Then, $E[p^n] \cong E[\mathfrak{p}^n] \oplus E[\overline{\mathfrak{p}}^n]$. Let $\{P, Q\}$ be a $\mathbb{Z}/p^n\mathbb{Z}$-basis of $E[p^n]$ such that P and Q are generators of $E[\mathfrak{p}^n]$ and $E[\overline{\mathfrak{p}}^n]$, respectively. Let us write $R = \lambda P + \mu Q$. Since R has exact order p^n, it follows that one of λ or μ is non-zero modulo p. Let us assume that $\lambda \not\equiv 0 \bmod p$.

By Lemma 15 of [3], the quadratic imaginary field F is contained in $L(E[p]) \subseteq L(E[p^n])$. Let $\mathcal{P}$ be a prime of $L(E[p^n])$ lying above $\mathfrak{p}$, let $\mathfrak{P}$ be a prime of $L(R)$ below $\mathcal{P}$, and let $\wp$ a prime of L below $\mathfrak{P}$. Since $E[\mathfrak{p}^n]$ coincides with the kernel of reduction of $E(\overline{K})[p^n]$ modulo $\mathcal{M}$ (the maximal ideal of K, which is a prime above $\wp$ of $L_\wp^{\mathrm{nr}}$; see Lemma 6.11 below), the action of inertia on $P \in E[\mathfrak{p}^n]$ is given by the cyclotomic character modulo p^n. In particular our results from Section 6.1 (specifically Lemma 4.7, Theorem 4.9 and Remark 4.10) imply that there is a prime $\mathfrak{P}$ above $\wp$ in the extension $L(R)/L$ such that $e(\mathfrak{P}|\wp)$ is divisible by

$$\varphi(p^n)/\gcd(\varphi(p^n), e),$$

where $e = e(K_E/\mathbb{Q}_p) = e(K_E/L_\wp^{\mathrm{nr}})e(\wp|p) \leq 24e(\wp|p)$ as usual. Hence,

$$\varphi(p^n) \leq e \cdot e(\mathfrak{P}, L(R)/L) \leq 24e(\wp|p)e(\mathfrak{P}, L(R)/L) \leq 24e(\mathfrak{P}, L(R)/\mathbb{Q}).$$

Thus, it only remains to show the following lemma.

Lemma 6.11. *Let E/L, $K = K_E/L_\wp^{nr}$, $\mathcal{P}$, $\mathfrak{P}$, $\wp$, and $\mathfrak{p}$ be as above (p splits in $F/\mathbb{Q}$ and $p\mathcal{O}_F = \mathfrak{p}\overline{\mathfrak{p}}$), such that E/K has good ordinary reduction, and let X_{p^n} be the kernel of reduction of $E(\overline{K})[p^n]$ modulo $\wp$, so that*

$$0 \to X_{p^n} \to E(\overline{K})[p^n] \to E(\overline{\mathbb{F}})[p^n] \to 0$$

is an exact sequence. Then, $X_{p^n} = E[\mathfrak{p}^n]$.

Proof. First, let us show that we may increase the base field K by a finite extension if we need to. Suppose K'/K is a finite extension of local fields, base-extend E to be defined over K', let $\mathcal{M}'$ be the maximal ideal of K' above $\mathcal{M}$ of K (which in turn is a finite extension of $L_\wp^{\mathrm{nr}}$). Since E/K has good (ordinary) reduction at $\mathcal{M}$, the curve E/K' has good (ordinary) reduction at $\mathcal{M}'$. Now suppose that the kernel of reduction mod$\mathcal{M}'$ of $E(\overline{K}')[p^n]$ is $X'_{p^n} = E[\mathfrak{p}^n]$. Since E is originally defined over K, we have that $E(\overline{K})[p^n] \cong E(\overline{K}')[p^n]$, and if a point R reduces to the origin modulo $\mathcal{M}$, then it also reduces to the origin modulo $\mathcal{M}'$, because $\mathcal{M}'$ divides $\mathcal{M}$. Hence, $X'_{p^n} \subseteq X_{p^n}$. Since $|X'_{p^n}| = |X_{p^n}| = p^n$, we conclude $X'_{p^n} = X_{p^n} = E[\mathfrak{p}]$ as desired.

Let $E \cong \mathbb{C}/\Lambda$ and let $E' \cong E/E[\mathfrak{p}^n] \cong \mathbb{C}/\mathfrak{p}^{-n}\Lambda$, so that the isogeny $\phi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{p}^{-n}\Lambda$ has kernel $E[\mathfrak{p}^n] \cong \mathfrak{p}^{-n}\Lambda/\Lambda$. Notice that $E[\mathfrak{p}^n]$ is $\mathrm{Gal}(\overline{L}/FL)$-stable in this case, so $E' = E/E[\mathfrak{p}^n]$ is defined over FL. Let us replace K by FK if necessary (which is finite, and ok by our previous remarks), so we will regard both E and E' as defined over K. The curve E' may not have good reduction at $\mathcal{M}$. However, we can find a finite extension of K such that E' has good reduction at a prime above $\mathcal{M}$. By our preliminary remarks this is ok, so without loss of generality let us assume that both E and E' have good (ordinary) reduction modulo $\mathcal{M}$. Now one can show that the reduction of ϕ mod $\mathcal{M}$ is inseparable (this is done in [44], Ch II, §4, p. 126-127), and therefore the reduction of ϕ is *essentially* a qth power Frobenius map (where q is a power of p), i.e.,

$$\tilde{\phi} = \tilde{\psi} \circ \mathrm{Frob}_q : \tilde{E} \longrightarrow \tilde{E}^{(q)} \longrightarrow \tilde{E}'$$

where $\mathrm{Frob}_q\colon \tilde{E} \to \tilde{E}^{(q)}$ is qth power Frobenius, and $\tilde{\psi}\colon \tilde{E}^{(q)} \to \tilde{E}'$ is an isomorphism. Moreover, the diagram

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\tilde{\phi}} & \tilde{E}' \end{array}$$

is commutative, where both vertical arrows are reduction modulo $\mathcal{M}$. Since $E[\mathfrak{p}^n]$ is the kernel of ϕ, we must have that $\tilde{\phi}(E[\mathfrak{p}^n] \bmod \mathcal{M}) = 0$. However, the only point mapped to 0 by the qth power Frobenius is 0 itself, and the isomorphism $\tilde{\psi}\colon \tilde{E}^{(q)} \to \tilde{E}'$ maps 0 to 0, so we conclude that $E[\mathfrak{p}^n] \bmod \mathcal{M} = 0$, i.e., $X_{p^n} = E[\mathfrak{p}^n]$ as desired. □

This concludes the proof of 6.10. □

Remark 6.12. The proof of Theorem 6.10 carries over to elliptic curves with CM by a non-maximal order $\mathcal{O}$, except, perhaps, for the case when p splits in $F/\mathbb{Q}$ but p divides the conductor of the order $\mathcal{O}$. This remaining case will be dealt with in future work.

We refer the reader to Section 6.2 for the definition of e_1, a quantity that appears in the next two results (see also §1 of [26], or §2 of [28]). Moreover, we remark that by Corollary 4.8 of [28], if $p > 3e(\wp|p)$, then e_1 is not divisible by p.

Theorem 6.13. *Let $p > 2$ be a prime, let E/L be an elliptic curve with CM by a maximal order $\mathcal{O}_F$ in an imaginary quadratic field F, and let $\phi\colon E \to E'$ be an isogeny of degree p defined over L. Let $\langle S\rangle \subset E$ be the kernel of ϕ and let $\rho_\phi\colon \mathrm{Gal}(\overline{L}/L) \to (\mathbb{Z}/p\mathbb{Z})^\times$ be the representation associated to the action of Galois on S, i.e., $\sigma(S) = \rho_\phi(\sigma)\cdot S$, for each $\sigma \in \mathrm{Gal}(\overline{L}/L)$. Then:*

1. *If p is inert or ramified in $\mathcal{O}_F$, and $\wp$ is a prime of L above p, let $K = K_E$ be an extension of $L_\wp^{nr}$ such that E/K_E has good reduction, and let $I_K \subseteq \mathrm{Gal}(\overline{K}/K)$ be the inertia subgroup. Assume that e_1 is not divisible by p. Then, ρ_ϕ restricted to I is either $\theta_{p-1}^{e-e_1}$, or $\theta_{p^2-1}^{e}$, where $\theta_{q-1}\colon I \to \mathbb{F}_q^\times$ with $q = p^h$ is a fundamental character of level h, and e and e_1 are the usual quantities as defined in Section 6.2. If $\rho_\phi|_I = \theta_{p^2-1}^e$, then $p+1|e$ and the values are in $\mathbb{F}_p^\times$.*
2. *If p is split, i.e., $p\mathcal{O}_F = \mathfrak{p}\overline{\mathfrak{p}}$, then either*
   (a) *$\langle S\rangle = E[\mathfrak{p}]$ or $E[\overline{\mathfrak{p}}]$, and if $\wp$ is a prime of L above $\mathfrak{p}$ (resp. $\wp'$ above $\mathfrak{p}$) and $K_E/L_\wp^{nr}$ and $I_K = I_{K,\wp}$ are as before (resp. $K_E/L_{\wp'}^{nr}$ and $I_{K,\wp'}$), then ρ_ϕ restricted to $I_{K,\wp}$ (resp. $I_{K,\wp'}$) is given by θ_{p-1}^e, or*
   (b) *The character $\theta_{p-1}^e\colon I_{K,\wp} \to \mathbb{F}_p^\times$ is trivial, for any prime $\wp$ of $\mathcal{O}_L$ above p.*

Proof. If p is inert or ramified in $\mathcal{O}_F$, then E/L has potential supersingular reduction at any prime $\wp$ of $\mathcal{O}_L$. By the results of [39], §1.10 and §1.11,

- If $pe/(p+1) > e_1$, then there is an $\mathbb{F}_p$-basis $\{P, Q\}$ of $E[p]$ such that the action of I_K in on $E[p]$ is given by a Borel subgroup B of $\mathrm{GL}(2,\mathbb{F}_p)$ such that the diagonal characters are $\theta_{p-1}^{e-e_1}$ and $\theta_{p-1}^{e_1}$. Moreover, since e_1 is not divisible by p, the ramification in the extension $K_E(E[p])/K_E$ is divisible by p (by Proposition 5.6 of [28]) and therefore the upper right hand corner of the Borel B is non-trivial. It follows that the only inertia-stable subspace of $E[p]$ is $\langle P\rangle$, and the action is given by $\theta_{p-1}^{e-e_1}$. We conclude that $\rho_\phi|_{I_K} = \theta_{p-1}^{e-e_1}$ as claimed.
- If $pe/(p+1) \leq e_1$, then the action of inertia I_K on $E[p]$ is given by $\theta_{p^2-1}^e$, and therefore the action in terms of a basis of $E[p]$ is given by the e-th power of a (full) non-split Cartan subgroup C_{ns} of $\mathrm{GL}(2,\mathbb{F}_p)$. Since the eigenvalues of a non-diagonal matrix in C_{ns} are not in $\mathbb{F}_p$, then $E[p]$ has a 1-dimensional $\mathbb{F}_p$-submodule that is fixed by inertia if and only if C_{ns}^e only contains diagonal entries. In particular, $(p+1)|e$ and $\rho_\phi|_{I_K} = \theta_{p^2-1}^e$.

If p splits in $\mathcal{O}_F$ with $p\mathcal{O}_F = \mathfrak{p}\overline{\mathfrak{p}}$, then we may write $E[p] = E[\mathfrak{p}] \oplus E[\overline{\mathfrak{p}}] = \langle P, Q\rangle$, where P generates $E[\mathfrak{p}]$ and $Q = \overline{P}$ generates $E[\overline{\mathfrak{p}}]$. Then the action of $\mathrm{Gal}(\overline{L}/L)$ on $E[p]$ in terms of the $\mathbb{F}_p$-basis $\{P, Q\}$ is given by a subgroup of the normalizer of a split Cartan subgroup of $\mathrm{GL}(2,\mathbb{F}_p)$. Suppose E/L admits a L-rational isogeny of degree p, with kernel $\langle S\rangle$ with $S = \lambda P + \mu Q$.

Suppose that there is a prime $\wp$ of $\mathcal{O}_L$ above p such that the character $\theta_{p-1}^e\colon I_{K,\wp} \to \mathbb{F}_p^\times$ is non-trivial. Now let $\mathfrak{P}$ be a prime of $L(E[p])$ above $\wp$. Since $F \subset L(E[p])$, we have that $\mathfrak{P}$ is above $\mathfrak{p}$ or $\overline{\mathfrak{p}}$ of $\mathcal{O}_F$. Without loss of generality let us assume $\mathfrak{P}$ is above $\mathfrak{p}$. Let $K = K_E$ be the smallest extension

of $L_\wp^{\mathrm{nr}}$ such that E/K has good reduction. By our previous lemma, $I_{K,\wp}$ acts on $E[p] = \langle P, Q\rangle$ as

$$\begin{pmatrix} \theta_{p-1}^e & * \\ 0 & 1 \end{pmatrix}.$$

Since θ_{p-1}^e is non-trivial, there is $\sigma \in I_{K,\wp}$ such that $\theta = \theta_{p-1}^e(\sigma) \not\equiv 1 \bmod p$. Let σ' be an element of $I_{K,\wp}$ whose action on $E[p]$ is given by a diagonal matrix with diagonal entries θ and 1 (such a σ' exists because $\theta_{p-1}^e(I_{K,\wp})$ is a Borel subgroup, and when $p > 2$ we can use Lemma 4.2). Thus,

$$\sigma'(S) = \sigma'(\lambda P + \mu Q) = \lambda\theta P + \mu Q,$$

and $\sigma'(S) = nS$ for some $n \geq 1$ if and only if $\mu \equiv n\mu \bmod p$, so $\mu \equiv 0$ (so $\langle S\rangle = E[\mathfrak{p}]$), or $n \equiv 1 \bmod p$. But if $n \equiv 1 \bmod p$, then $\lambda\theta \equiv \lambda$ which implies $\lambda \equiv 0$, so $\langle S\rangle = E[\overline{\mathfrak{p}}]$.

Hence $\langle S\rangle = E[\mathfrak{p}]$ or $E[\overline{\mathfrak{p}}]$, unless all characters $\theta_{p-1}^e \colon I_{K,\wp} \to \mathbb{F}_p^\times$ are trivial for all $\wp$ above p. □

Corollary 6.14. *Let $p > 2$, E/L with CM by the maximal order $\mathcal{O}_F \subseteq F$, $K = K_E$, ϕ, $\langle S\rangle$, and ρ_ϕ be as before. If p is ramified or inert in $\mathcal{O}_F$, assume that e_1 is not divisible by p. Let K_1 be the subfield of $K(S)$ fixed by the kernel of ρ_ϕ^{12}. Then, either $p-1$ is a divisor of e (which in turn is a divisor of $24e(\wp|p)$) for any $\wp$ of $\mathcal{O}_L$ above p, or there is a prime $\wp$ of $\mathcal{O}_L$ and a prime $\mathfrak{P}$ of L_1, such that the ramification index $e(\mathfrak{P}|\wp)$ is divisible by $(p-1)/\gcd(p-1, 12t)$ for $t = e$, or $e - e_1$, and the ramification in K_1/K is also divisible by $(p-1)/\gcd(p-1, 12t)$.*

Proof. By Theorem 6.13, either θ_{p-1}^e is trivial for all $\wp$ over p, or $\rho_\phi|_{I_K} = \theta_{p-1}^{e-e_1}$ or $\theta_{p^2-1}^e$ and $p+1|e$.

If θ_{p-1}^e is trivial for all $\wp$ over p, and since the fundamental character θ_{p-1} is surjective ([39], §1.7), it follows that e is divisible by $p-1$.

If $\rho_\phi^{12}|_{I_K} = \theta_{p-1}^{12(e-e_1)}$ or $\theta_{p^2-1}^{12e}$, and K_1 is the subfield of $K(S)$ fixed by the image of $\rho_\phi^{12}|_{I_K}$, then the ramification in the extension K_1/K is divisible by $(p-1)/\gcd(p-1, 12(e-e_1))$ or by $(p^2-1)/\gcd(p^2-1, 12e)$. In particular, the ramification in K_1/K is divisible by $(p-1)/\gcd(p-1, 12t)$ with $t = e - e_1$ or e. Hence, by Remark 4.8 there is a prime $\mathfrak{P}$ of $\mathcal{O}_{L(S)}$ above $\wp$ such that $e(\mathfrak{P}|\wp)$ is divisible by $(p-1)/\gcd(p-1, 12t)$, as claimed. □

7. Auxiliary results for the proof of Theorem 1.9

In this section we collect a number of auxiliary results that will be used in the proof of Theorem 1.9 in Section 8. In order to apply Theorem 2.1 to all elliptic curves defined over a number field L, we need some control on those curves that admit L-rational isogenies of p-power order. For an elliptic curve E/L we denote by $\rho_{E,p}$ the Galois representation $\mathrm{Gal}(\overline{L}/L) \to \mathrm{Aut}(T_p(E))$ associated to the natural action of Galois on the p-adic Tate module $T_p(E)$ of the curve E.

Theorem 7.1. *Let p be a prime, and let L be a number field. Fix an element $j_0 \in L$. Then, there is a number $n = n(p, j_0)$ such that for any elliptic curve E/L without CM and with $j(E) = j_0$ we have $1 + p^n M_2(\mathbb{Z}_p) \subseteq \rho_{E,p}(\mathrm{Gal}(\overline{L}/L))$. In particular, E/L does not admit L-rational isogenies of degree $p^{a(p,j_0)}$ with $a(p, j_0) = n(p, j_0) + 1$.*

Proof. The existence of $n = n(p, j_0)$ is shown in [1, Lemma 2.8]. Let E/L be an elliptic curve without CM, and suppose

$$1 + p^n \mathrm{M}_2(\mathbb{Z}_p) \subseteq \rho_{E,p}(\mathrm{Gal}(\overline{L}/L)).$$

Then, E/L cannot admit a L-rational isogeny of degree p^{n+1}. Indeed, if E/L admits an isogeny ϕ of degree p^{n+1}, then there is a point $R \in E$ of order p^{n+1} such that $\langle R\rangle$ is $\mathrm{Gal}(\overline{L}/L)$-invariant.

Hence, there is some $S \in E[p^{n+1}]$, such that $\{R, S\}$ is a $\mathbb{Z}/p^{n+1}\mathbb{Z}$-basis of $E[p^{n+1}]$, and such that $\rho_{E,p}(\mathrm{Gal}(\overline{L}/L)) \bmod p^{n+1}$ is a Borel subgroup of $\mathrm{GL}(2, \mathbb{Z}/p^{n+1}\mathbb{Z})$. But, by assumption, $1 + p^n \mathrm{M}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}) \subseteq \rho_{E,p}(\mathrm{Gal}(\overline{L}/L)) \bmod p^{n+1}$, which contradicts the fact that $\rho_{E,p}(\mathrm{Gal}(\overline{L}/L)) \bmod p^{n+1}$ is a Borel subgroup of $\mathrm{GL}(2, \mathbb{Z}/p^{n+1}\mathbb{Z})$. □

Momose has given a classification of isogenies of prime degree over number fields (see [34, Theorem A]), but here we use another classification recently shown by Larson and Vaintrob, which we cite next.

Theorem 7.2 (Larson, Vaintrob, [23])**.** *Let L be a number field. Then, there exists a finite set S_L of prime numbers, depending only on L, such that for a prime $p \notin S_L$, and an elliptic curve E/L for which $E[p] \otimes \overline{\mathbb{F}}_p$ is reducible with degree 1 associated character ψ, one of the following holds.*

(1) *There exists a CM elliptic curve E', which is defined over L and whose CM-field is contained in L, with a p-adic degree 1 associated character whose mod p reduction $\overline{\psi}'$ satisfies*
$$\overline{\psi}^{12} = \left(\overline{\psi}'\right)^{12}.$$
(2) *The Generalized Riemann Hypothesis fails for $L(\sqrt{-p})$, and*
$$\overline{\psi}^{12} = \overline{\chi_p}^{6},$$
where χ_p is the cyclotomic character. (Moreover, in this case we must have $p \equiv 3 \bmod 4$ and the representation $\rho_{E,p} \bmod p$ is already reducible.)

For technical reasons, we need to strengthen Larson and Vaintrob's result, so that the curve E' in (1) hash CM by a maximal order. Before we do that, we recall that if E'/L is an elliptic curve with CM by an order $\mathcal{O}_f$ of conductor $f \geq 1$ of an imaginary quadratic field F, such that $F(j(E')) \subseteq L$, then there is an elliptic curve E''/L with CM by the full ring of integers $\mathcal{O}_F$, and an L-rational isogeny $E' \to E''$ that is cyclic of degree f. Indeed, the isogeny arises from the inclusion $\mathcal{O}_f \subseteq \mathcal{O}_F$ which induces a map $E' \cong \mathbb{C}/\mathcal{O}_f \to \mathbb{C}/\mathcal{O}_F \cong E''$, with kernel $\mathcal{O}_F/\mathcal{O}_f \cong \mathbb{Z}/f\mathbb{Z}$. Note that the kernel is isomorphic to $\mathcal{O}_F/\mathcal{O}_f \cong f\mathcal{O}_F/f\mathcal{O}_f \subseteq \mathcal{O}_f/f\mathcal{O}_f$, which is a cyclic group of order f that is invariant under the action of Galois (recall that $\mathrm{Gal}(L(E'[f])/L) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_f/f\mathcal{O}_f}(E'[f]) \cong (\mathcal{O}_f/f\mathcal{O}_f)^\times$ as long as $F(j(E')) \subseteq L$; see [44, Ch 2., Theorem 2.3]). Hence, $T = f\mathcal{O}_F/f\mathcal{O}_f$ is a cyclic L-rational subgroup of order f, the quotient $E'' = E'/T$ is an elliptic curve defined over L, and the map $E' \to E''$ is an L-rational isogeny.

Lemma 7.3. *Let L be a number field, let E'/L be an elliptic curve with CM by an order $\mathcal{O}_f$ of conductor $f \geq 1$, contained in an imaginary quadratic field F, and suppose that the CM-field of E' is contained in L. Further, assume that E' has a p-isogeny with associated mod-p character ψ' of degree 1, where p is a prime with $\gcd(p, f) = 1$. Then, there is an elliptic curve E''/L with CM by the maximal order $\mathcal{O}_F$, such that $F(j(E'')) \subseteq L$ and E'' has another p-isogeny with the same associated mod-p character ψ' of degree 1.*

Proof. Suppose E/L is an elliptic curve with CM by the order $\mathcal{O}_f$ of conductor $f \geq 1$ inside the quadratic imaginary field F, and such that $F(j(E)) \subseteq L$. Then, there exists an elliptic curve E''/L with CM by $\mathcal{O}_F$ and a canonical L-rational isogeny $\phi\colon E' \to E''$ that is cyclic of degree f (see the paragraph before the statement of the lemma). Since $\gcd(p, f) = 1$, the isogeny ϕ induces an isomorphism $\phi\colon E'[p] \cong E''[p]$ defined over L. Now suppose that E' has a p-isogeny with kernel $\langle P \rangle$ and its associated isogeny character is $\psi'\colon \mathrm{Gal}(\overline{L}/L) \to (\mathbb{Z}/p\mathbb{Z})^\times$, such that $\sigma(P) = \psi'(\sigma)P$ for

any $\sigma \in \mathrm{Gal}(\overline{L}/L)$. Then, the isomorphism $E'[p] \cong E''[p]$ implies that E'' also has a p-isogeny with kernel $\langle \phi(P) \rangle$ and $\sigma(\phi(P)) = \phi(\sigma(P)) = \phi(\psi'(\sigma)P) = \psi'(\sigma)\phi(P)$, where the action of σ commutes with both ϕ and $[\psi'(\sigma)]$ because both maps are defined over L. Hence, the isogeny character for E'' is also ψ' as claimed. □

Now we are ready to prove the following variant of Theorem 7.2.

Theorem 7.4. *Let L be a number field. Then, there exists a finite set S_L of prime numbers, depending only on L, such that for a prime $p \notin S_L$, and an elliptic curve E/L for which $E[p] \otimes \overline{\mathbb{F}}_p$ is reducible with degree 1 associated character ψ, one of the following holds.*

(1) *There exists an elliptic curve E'' with CM by the full ring of integers $\mathcal{O}_F$ of an imaginary quadratic field F, such that E'' is defined over L, its CM-field is contained in L, and has a p-adic degree 1 associated character whose mod p reduction $\overline{\psi}'$ satisfies*

$$\overline{\psi}^{12} = \left(\overline{\psi}'\right)^{12}.$$

(2) *The Generalized Riemann Hypothesis fails for $L(\sqrt{-p})$, and*

$$\overline{\psi}^{12} = \overline{\chi_p}^{6},$$

where χ_p is the cyclotomic character. (Moreover, in this case we must have $p \equiv 3 \bmod 4$ and the representation $\rho_{E,p} \bmod p$ is already reducible.)

Proof. Let L be a number field of degree d. It is well known that there are only finitely many imaginary quadratic fields with class number less or equal than a given bound d (see [10]). Moreover, the class number of an order contained in a maximal order grows with the conductor ([4, Theorem 7.24]). Hence, there are only finitely many j-invariants with CM defined over L (see also [5] for some bounds on the number of j-invariants defined over a number field), say $\{j_1, \ldots, j_n\}$, associated to orders $\mathcal{O}_{f_1}, \ldots, \mathcal{O}_{f_n}$ with conductors $f_1, \ldots, f_n \geq 1$. Let S_L be the set of primes given by Theorem 7.2, and enlarge it by adding to S_L all the prime divisors of $f_1, \ldots, f_n$ (in particular, S_L is still a finite set of prime numbers).

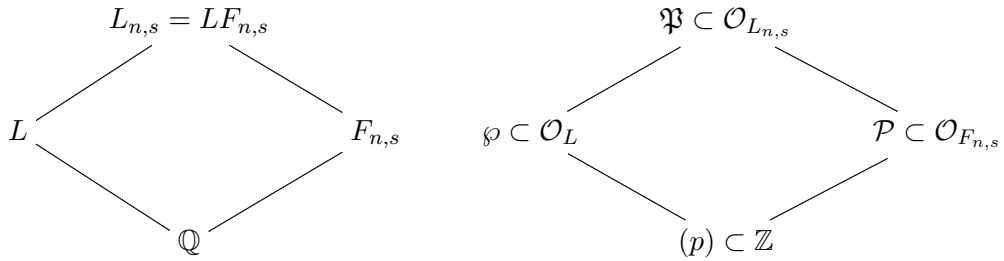
Now, for a prime $p \notin S_L$, and an elliptic curve E/L for which $E[p] \otimes \overline{\mathbb{F}}_p$ is reducible with degree 1 associated character ψ, either (1) or (2) of Theorem 7.2 holds. If (2) holds, we are done. If (1) holds, then there exists a CM elliptic curve E', which is defined over L and whose CM-field is contained in L, with a p-adic degree 1 associated character whose mod p reduction $\overline{\psi}'$ satisfies $\overline{\psi}^{12} = \left(\overline{\psi}'\right)^{12}$. If E' has CM by an order $\mathcal{O}_f$ of conductor $f \geq 1$, and since $F(j(E')) \subseteq L$ by assumption, we must have $f = f_i$ for some $1 \leq i \leq n$. Since $p \notin S_L$, and S_L contains all prime divisors of f, we have $\gcd(p, f) = 1$. Hence, Lemma 7.3 applies, and there is an elliptic curve E''/L with CM by the maximal order $\mathcal{O}_F$, such that $F(j(E'')) \subseteq L$ and E'' has a p-isogeny with the same associated mod-p character ψ' of degree 1, as claimed. □

In order to apply Theorem 7.4 in the proof of Theorem 1.9, we need uniform bounds on the ramification in the fixed fields by kernels of powers of the cyclotomic character.

Lemma 7.5. *Let $p > 2$, and let $e(\wp|p)$ be the ramification index in $L/\mathbb{Q}$ of a prime $\wp$ of $\mathcal{O}_L$ lying above p. Then, the ramification index of any prime ideal of $L(\zeta_{p^n})$ above $\wp$ is divisible by the quantity $\varphi(p^n)/\gcd(\varphi(p^n), e(\wp|p))$.*

More generally: let $G_L = \mathrm{Gal}(\overline{L}/L)$, and let $\chi_{p,n}\colon G_L \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ be the p^n-th cyclotomic character. Let $s \geq 1$, and let $L_{n,s} \subseteq L(\zeta_{p^n})$ be the fixed field by the kernel of $\chi^s_{p,n}$. Then, the ramification index of any prime ideal of $L_{n,s}$ above $\wp$ is divisible by $\varphi(p^n)/\gcd(\varphi(p^n), s \cdot e(\wp|p))$.

Proof. Let $p > 2$, and let $\zeta = \zeta_{p^n}$ be a primitive p^n-th root of unity. Let $J_n = \chi_p(G_L) \cong \mathrm{Gal}(L(\zeta_{p^n})/L)$. In particular, J_n and $J_n^s = \chi^s_{p,n}(G_L)$ are cyclic subgroups of $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Moreover, $J_n^s \cong \mathrm{Gal}(L_{n,s}/L)$, where $L_{n,s}$ is the fixed field by the kernel of $\chi^s_{p,n}$. Note that $|J_n^s| = |J_n|/\gcd(|J_n|, s)$ because J_n is cyclic. Let $F_{n,s}$ be a Galois extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{p^n})$ such that $\mathrm{Gal}(F_{n,s}/\mathbb{Q}) \cong ((\mathbb{Z}/p^n\mathbb{Z})^\times)^s$. It follows that the compositum of $F_{n,s}$ and L is $L_{n,s}$. Consider the following diagram of fields, and primes above p.



Thus, by the multiplicativity of ramification indices in towers, we have

$$\begin{aligned} e(\mathfrak{P}|\wp) \cdot e(\wp|p) &= e(\mathfrak{P}|\mathcal{P}) \cdot e(\mathcal{P}|p) = e(\mathfrak{P}|\mathcal{P}) \cdot [F_{n,s} : \mathbb{Q}] \\ &= e(\mathfrak{P}|\mathcal{P}) \cdot \frac{\varphi(p^n)}{\gcd(\varphi(p^n), s)} \\ &= e(\mathfrak{P}|\mathcal{P}) \cdot \frac{\frac{\varphi(p^n)}{\gcd(\varphi(p^n),s)}}{\gcd(\frac{\varphi(p^n)}{\gcd(\varphi(p^n),s)}, e(\wp|p))} \cdot \gcd\left(\frac{\varphi(p^n)}{\gcd(\varphi(p^n), s)}, e(\wp|p)\right) \\ &= e(\mathfrak{P}|\mathcal{P}) \cdot \frac{\varphi(p^n)}{\gcd(\varphi(p^n), s \cdot e(\wp|p))} \cdot \gcd(\varphi(p^n), s \cdot e(\wp|p)). \end{aligned}$$

Therefore, $\varphi(p^n)/\gcd(\varphi(p^n), s \cdot e(\wp|p))$ is a divisor of $e(\mathfrak{P}|\wp)$, for any prime $\mathfrak{P}$ above $\wp$, as claimed. □

8. Proof of Theorem 1.9

Let L be a number field and let E/L be an elliptic curve either without CM, or with CM by a maximal order. Let $p > 2$ be a prime, and let $R \in E(\overline{L})[p^n]$ be a point of exact order p^n, for some $n \geq 1$. If E/L has CM by a maximal order, then Theorem 6.10 shows that there if a prime Ω_R of $\mathcal{O}_{L(R)}$ above a prime $\wp$ of $\mathcal{O}_L$, such that

$$\varphi(p^n) \leq 12 e(\wp|p) e(\Omega_R|\wp) \leq 12 e(\Omega_R|p).$$

Hence, we may restrict ourselves to study curves E/L without CM. For the rest of this proof, let $\wp$ be a prime of $\mathcal{O}_L$ such that $e(\wp|p) = e_{\min}(p, L/\mathbb{Q})$ as in Definition 1.7. Let S_L be the finite set of primes whose existence is shown in Theorem 7.4. Define a new set S'_L by

$$S'_L = S_L \cup \{p : p - 1 \leq 12^2 \cdot e(\wp|p)\},$$

and define

$$\Sigma_L = \bigcup_{p \in S'_L} \Sigma(L,p),$$

where each $\Sigma(L,p)$ is defined as follows. Let $a(L,p) \geq 1$ be the smallest integer such that $X_0(p^a)$ is of genus ≥ 2, or $X_0(p^a)$ is of genus 1 but $X_0(p^a)(L)$ is finite. By Corollary 3.2, we have $a(L,p) \leq a_2(p) \leq 4$ for all $p \geq 3$. By our assumption in the genus 1 case, or Faltings' theorem in the genus ≥ 2 case, the set $X_0(p^a)(L)$ has only finitely many non-cuspidal L-rational points. We define $\Sigma(L,p) \subset L$ as the set formed by any j-invariant of an elliptic curve over L without CM that corresponds to non-cuspidal L-rational point on $X_0(p^a)$. So, for a given number field L, the set S'_L is a finite set of primes. Hence, Σ_L is a finite subset of L.

For each $j_0 \in \Sigma(L,p)$, we let $a = a(p,j_0)$ be the least positive integer a such that any curve E/L with $j(E) = j_0$ does not admit L-rational isogenies of degree p^a. The existence of $a(p,j_0)$ is guaranteed by Theorem 7.1 since Σ_L only contains non-CM j-invariants. Let $A(L,p) = \max\{a(L,p), a(p,j_0) : j_0 \in \Sigma(L,p)\}$. The number $A(L,p)$ is well-defined because $\Sigma(L,p)$ is a finite set.

In order to prove Theorem 1.9, we distinguish the following cases:

$$\begin{cases} E/L \text{ does not admit } L\text{-rational isogenies of degree } p, \text{ or} \\ \\ E/L \text{ admits } L\text{-rational isogenies of degree } p, \text{ and } \begin{cases} p \notin S'_L, \text{ or} \\ \\ p \in S'_L, \text{ and } \begin{cases} j(E) \notin \Sigma_L, \text{ or} \\ j(E) \in \Sigma_L. \end{cases} \end{cases} \end{cases}$$

First, suppose that E/L does not admit L-rational isogenies of degree p. Then, Theorem 2.1 shows that there is a constant $c = c(E/L, \wp)$ with $1 \leq c \leq 12e(\wp|p)$, and a prime Ω_R of $L(R)$ above $\wp$ such that the ramification index $e(\Omega_R|\wp)$ is divisible either by

$$\varphi(p^n)/\gcd(\varphi(p^n), c), \text{ or } p^n.$$

In particular, either $\varphi(p^n) \leq p^n \leq e(\Omega_R|\wp)$, or

$$[L(R):L] \geq e(\Omega_R|\wp) \geq \frac{\varphi(p^n)}{\gcd(\varphi(p^n),c)} \geq \frac{\varphi(p^n)}{c}.$$

Thus, in all cases $\varphi(p^n) \leq c \cdot e(\Omega_R|\wp) \leq 12e(\wp|p)e(\Omega_R|\wp) \leq 12e(\Omega_R|p)$.

Next, suppose that E/L admits a L-rational isogeny ϕ of degree p^a, for some $a \geq 1$. Let $\psi\colon \mathrm{Gal}(\overline{L}/L) \to (\mathbb{Z}/p^a\mathbb{Z})^\times$ be the character associated to the isogeny ϕ. Note that the existence of ϕ implies the existence of a L-rational isogeny ϕ_1 of degree p, with associated character $\psi_1 = \overline{\psi}$, the mod p reduction of ψ. Let $\langle S \rangle \subseteq E[p]$ be the kernel of ϕ_1.

Suppose first that $p \notin S'_L$. In particular, $p \notin S_L$, and Theorem 7.4 shows that two options, (1) or (2), may occur:

- If we are in option (1), then there exists an elliptic curve E'', with CM by a full ring of integers $\mathcal{O}_k$, which is defined over L and whose CM-field is contained in L, with a p-adic degree 1 associated character whose mod p reduction $\overline{\psi}'$ satisfies

  $$\overline{\psi}^{12} = \left(\overline{\psi}'\right)^{12}.$$

  Let K be the smallest extension of $L_\wp^{\mathrm{nr}}$ such that E'/K has good reduction. Let K_1 be the subfield of $K(S)$ fixed by the kernel of $\rho_{\phi_1}^{12}$, and similarly define L_1. Since $p \notin S'_L$, $p > 3e(\wp|p)$, and by [28, Corollary 4.8], if $p > 3e(\wp|p)$, then e_1 is not divisible by p (see §1 of [26], or §2 of

[28] for the definition of e_1). Then, by Corollary 6.14, either $p-1$ is a divisor of $e = e(K/\mathbb{Q}_p)$ (which in turn is a divisor of $12e(\wp|p)$) for any $\wp$ of $\mathcal{O}_L$ above p, or the ramification index in K_1/K is divisible by $(p-1)/\gcd(p-1, 12t)$ for $t = e$, or $e - e_1$. Since $p \notin S'_L$, we have $p - 1 > 12^2 \cdot e(\wp|p) \geq 12e \geq 12t$, and therefore the ramification in $K(S)/K$ is > 1. It follows from Theorem 2.1 that there is a constant $c = c(E/L, \wp)$ with $1 \leq c \leq 12e(\wp|p)$, and a prime Ω_R of $L(R)$ above $\wp$ such that the ramification index $e(\Omega_R|\wp)$ is divisible either by $\varphi(p^n)/\gcd(\varphi(p^n), c)$, or p^n. In particular, $\varphi(p^n) \leq c \cdot e(\Omega_R|\wp) \leq 12e(\wp|p)e(\Omega_R|\wp) \leq 12e(\Omega_R|p)$, as before.

- Now consider option (2) of Theorem 7.4. In this case GRH fails for $L(\sqrt{-p})$ and $\overline{\psi}^{12} = \overline{\chi}_p^6$, where $\overline{\psi}$ and $\overline{\chi}_p$ are, respectively, the mod p reductions of ψ and χ_p, the p-adic cyclotomic character. Let $L_{1,6}$ be the fixed field of $\overline{L}$ by the kernel of $\overline{\chi}_p^6$. Then, $L_{1,6} \subseteq L(S)$ and, by Lemma 7.5, the ramification index of any prime ideal of $L_{1,6}$ above $\wp$ is divisible by $(p-1)/\gcd(p-1, 6 \cdot e(\wp|p))$. Then

$$A = A(\wp, L, S) := e(\wp, L(S)/L)/\gcd(e(\wp, L(S)/L), e(K/L_\wp^{\mathrm{nr}}))$$

is divisible by

$$\left(\frac{p-1}{\gcd(p-1, 6 \cdot e(\wp|p))}\right) / \gcd\left(\frac{p-1}{\gcd(p-1, 6 \cdot e(\wp|p))}, e(K/L_\wp^{\mathrm{nr}})\right) = \frac{p-1}{\gcd(p-1, 6 \cdot e(\wp|p) \cdot e(K/L_\wp^{\mathrm{nr}}))}.$$

Since $p \geq 3$, then $e(K/L_\wp^{\mathrm{nr}})$ is a divisor of 12. Hence, A is divisible by

$$\frac{p-1}{\gcd(p-1, 72 \cdot e(\wp|p))},$$

and this quantity is > 1 because $p \notin S'_L$. Indeed, notice that if $p - 1 \geq 144e(\wp|p)$, then $(p-1)/\gcd(p-1, 72 \cdot e(\wp|p)) \geq 2$ (because $\gcd(p-1, 72 \cdot e(\wp|p)) \leq 72e(\wp|p)$).

Hence, $A(\wp, L, S) > 1$ and by our Theorem 2.1, there is a constant $c = c(E/L, \wp)$ with $1 \leq c \leq 12e(\wp|p)$, and a prime Ω_R of $L(R)$ above $\wp$ such that the ramification index $e(\Omega_R|\wp)$ is divisible either by

$$\varphi(p^n)/\gcd(\varphi(p^n), c), \text{ or } p^n.$$

So, as before, $\varphi(p^n) \leq c \cdot e(\Omega_R|\wp) \leq 12e(\wp|p)e(\Omega_R|\wp) \leq 12e(\Omega_R|p)$.

It remains to consider the case when E/L admits a L-rational isogeny ϕ of degree p^a, for some $a \geq 1$ and $p \in S'_L$. If $j(E) \notin \Sigma_L = \cup_{p \in S'_L} \Sigma(L, p)$, then our definition of Σ_L implies that $X_0(p^a)$ has genus ≤ 1, and therefore $a \leq a_1(p) \leq 3$ for all $p \geq 3$, by Cor. 3.2, and $a < a(L, p) \leq a_2(p)$ (because $j(E) \notin \Sigma(L, p)$). Hence E does not admit L-isogenies of degree $p^{a(L,p)}$. In particular, Theorem 2.1 implies that

$$[L(R) : L] \geq e(\Omega_R|\wp) \geq \frac{\varphi(p^n)}{\gcd(\varphi(p^n), c(E/L, \wp) \cdot p^{a(L,p)-1})}.$$

Hence,

$$\varphi(p^n) \leq c \cdot p^{a(L,p)-1} \cdot e(\Omega_R|\wp) \leq 12 \cdot p^{a_2(p)-1} \cdot e(\wp|p) \cdot e(\Omega_R|\wp) \leq 588 \cdot e(\Omega_R|p),$$

where we have used the fact that the maximum value of $p^{a_2(p)-1}$ for $p > 2$ is 49 (see Cor. 3.2).

If $j(E) \in \Sigma_L$, then $a < a(L,p) \leq A(L,p)$ by definition of $A(L,p)$, and therefore

$$[L(R) : L] \geq e(\Omega_R|\wp) \geq \frac{\varphi(p^n)}{\gcd(\varphi(p^n), c(E/L,\wp) \cdot p^{A(L,p)-1})}.$$

Let us define

$$C_L = 12 \cdot \max\{p^{A(L,p)-1} : p \in S'_L\},$$

which is well-defined because S'_L is a finite set. Moreover, C_L only depends on L. It follows from our previous work in this proof that, in all cases, we have

$$\varphi(p^n) \leq c(E/L,\wp) \cdot p^{A(L,p)-1} \cdot e(\Omega_R|\wp) \leq C_L \cdot e(\Omega_R|p) \leq C_L \cdot [L(R) : \mathbb{Q}],$$

where, as usual, $c \leq 12e(\wp|p)$. This concludes the proof of Theorem 1.9.

References

[1] K. Arai, *On uniform lower bound of the Galois images associated to elliptic curves*, Tome 20, n. 1 (2008), pp. 23-43. 7

[2] B. J. Birch, W. Kuyk (Editors), *Modular functions of one variable IV*, Lecture Notes in Mathematics 476, Berlin-Heidelberg-New York, Springer 1975. 3

[3] P. L. Clark, B. Cook, J. Stankewicz, *Torsion points on elliptic curves with complex multiplication*, International Journal of Number Theory 9 (02), pp. 447-479. 1, 1, 6.3, 6.3

[4] D. A. Cox., *Primes of the form x^2+ny^2. Fermat, class field theory and complex multiplication*, A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. . 7

[5] H. Daniels, Á. Lozano-Robledo, *On the number of isomorphism classes of CM elliptic curves defined over a number field*, J. Number Th., 157 (2015), pp. 367-396. 7

[6] M. Derickx, S. Kamienny, W. Stein, M. Stoll, *Torsion points on elliptic curves over number fields of small degree*, Arxiv preprint, `https://arxiv.org/abs/1707.00364`. 1

[7] F. Diamond, J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics 228, Springer-Verlag, 2nd Edition, New York, 2005. 3

[8] N. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, in Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin (D.A. Buell and J.T. Teitelbaum, eds.; AMS/International Press, 1998), pp. 21-76. 3

[9] N. Elkies, *Explicit modular towers*, in Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing (1997, T. Basar, A. Vardy, eds.), Univ. of Illinois at Urbana-Champaign 1998, pp. 23-32 (math.NT/0103107 on the arXiv). 3

[10] D. Goldfeld, *Gauss's class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. (N.S.), 13(1):23-37, 1985. 7

[11] B. H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Mathematical Journal, Vol. 61, No. 2, pp. 445-517. 6.6

[12] M. Flexor, J. Oesterlé, *Sur les points de torsion des courbes elliptiques*, Astérisque 183 (1990), pp. 25-36. 1, 1, 1

[13] R. Fricke, F. Klein, *Vorlesungen über die Theorie der elliptischen Modulfunctionen* (Volumes 1 and 2), B. G. Teubner, Leipzig 1890, 1892. 3

[14] R. Fricke, *Die elliptischen Funktionen und ihre Anwendungen.* Leipzig-Berlin: Teubner 1922. 3

[15] M. Hindry, J. H. Silverman, *Sur le nombre de points de torsion rationnels sur une courbe elliptique.* C. R. Acad. Sci. Paris Ser. I Math., 329(2), (1999), pp. 97-100. 1, 1

[16] N. Ishii, *Rational expression for j-invariant function in terms of generators of modular function fields*, International Mathematical Forum, 2, 2007, no. 38, pp. 1877-1894. 3

[17] M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. 85 (1979), pp. 21-23. 3

[18] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. 87 (1980), pp. 15-20. 3

[19] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) 22 (1980), pp. 239-244. 3

[20] M. A. Kenku, *The modular curve $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) 23 (1981), pp. 415-427. 3

[21] M. A. Kenku, *On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class*, J. Number Th. 15 (1982), pp. 199-202. 3

[22] S. D. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3), 33 (1976), pp. 193 - 237. 3

[23] E. Larson, D. Vaintrob, *Determinants of subquotients of Galois representations associated to abelian varieties*, Journal of the Institute of Mathematics of Jussieu, Volume 13, Issue 03, July 2014, pp. 517-559. 1, 7.2

[24] G. Ligozat, *Courbes modulaires de genre 1*, Bull. Soc. Math. France (1975), pp. 1-80. 3

[25] Á. Lozano-Robledo, B. Lundell, *Bounds for the torsion of elliptic curves over extensions with bounded ramification*, International Journal of Number Theory, Volume: 6, Issue: 6 (2010), pp. 1293-1309. 2.3

[26] Á. Lozano-Robledo, *Formal groups of elliptic curves with potential good supersingular reduction*, Pacific Journal of Mathematics, 261 (2013), no. (1), pp. 145-164. 2, 6.2, 6.2, 6.3, 8

[27] Á. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Annalen, Vol 357, Issue 1 (2013), 279-305. 1, 3

[28] Á. Lozano-Robledo, *Ramification in the division fields of elliptic curves with potential supersingular reduction*, Research in Number Theory (2016), 2:8, pp. 1-25. 1, 1.5, 2, 6.2, 6.7, 6.2, 6.8, 6.3, 6.3, 8

[29] R. Maier, *On rationally parametrized modular equations*, J. Ramanujan Math. Soc. 24 (2009), pp. 1-73. 3

[30] B. Mazur, *Rational points on modular curves* (in [40]), Proceedings of Conference on Modular Functions held in Bonn, Lecture Notes in Math. 601, Springer-Verlag, Berlin-Heiderberg-New York (1977), pp. 107-148. 3

[31] B. Mazur, *Rational isogenies of prime degree*, Inventiones Math. 44 (1978), pp. 129-162. 1, 3, 3

[32] B. Mazur, J. Vélu, *Courbes de Weil de conducteur 26*, C. R. Acad. Sc. Paris, t. 275 (1972), série A, pp. 743-745. 3

[33] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), no. 1-3, 437-449. 1.2

[34] F. Momose, *Isogenies of prime degree over number fields*, Compositio Math., 97, no. 3 (1995), pp. 329-348. 7

[35] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Inst. Hautes Etudes Sci. Publ. Math. (1964), No. 21, p. 128. 3, 6

[36] A. Ogg, *Rational points on certain elliptic modular curves*, Proc. Symp. Pure Math. XXIX, AMS, (1973) pp. 221-231. 3

[37] P. Parent. *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. 506 (1999). 1.2

[38] D. Prasad, C. S. Yogananda, *Bounding the torsion in CM elliptic curves*. C. R. Math. Acad. Sci. Soc. R. Can. 23 (2001), pp. 1-5. 1, 6.9

[39] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), pp. 259-331. 3, 6, 6.1, 6.3, 6.3

[40] J.-P. Serre, D. B. Zagier (Editors), *Modular Functions of One Variable V: Proceedings International Conference*, University of Bonn, Sonderforschungsbereich Theoretische Mathematik, July 2-14, 1976: No. V (Lecture Notes in Mathematics 601). 30

[41] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, Ann. of Math. 88 (1968), pp. 492-517. 6

[42] A. Silverberg, *Torsion points on abelian varieties of CM-type*. Compositio Math. 68 (1988), no. 3, pp. 241-249. 1, 6.9

[43] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 2nd Edition, New York, 2009. 4, 5, 6, 6.1, 6.2

[44] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York. 5, 5, 6.3, 7

[45] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press; 1st edition (August 1, 1971). 3

Department of Mathematics, University of Connecticut, Storrs, CT 06269, USA
E-mail address: alvaro.lozano-robledo@uconn.edu