RAMIFICATION IN THE DIVISION FIELDS OF ELLIPTIC CURVES WITH POTENTIAL SUPERSINGULAR REDUCTION

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 if E/F has potential supersingular reduction at a prime ideal above p, then 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 ramification index of the prime of supersingular reduction.

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.

Theorem 1.1 (Merel, [7], and Parent, [9])**.** *Let p be a prime, let $d > 1$ be a fixed integer, let F be a number field F of degree $\leq d$ and let E/F be an elliptic curve. Then:*

- *(Oesterlé, 1996) If $E(F)$ contains a point of exact order p, then $p \leq (1 + 3^{d/2})^2$.*
- *(Parent, 1999) If $E(F)$ contains a point of exact order p^n, then $p^n \leq 129(5^d - 1)(3d)^6$.*

In this article, we study the ramification index in the field of definition of p^n-th torsion points. 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 $\varphi(p^n)$, where $\varphi(\cdot)$ is the Euler phi function, and, in fact, it is easy to see that the index 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. In particular, we concentrate on the case when E/L has potential good supersingular reduction at $\wp$. We show the following:

Theorem 1.2. *Let $n \geq 1$ 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. Let E/L be an elliptic curve with potential supersingular reduction at $\wp$, let*

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

$R \in E[p^n]$ be a point of exact order p^n. Then, there is a computable constant $c = c(E/L, R, \wp)$ with $1 \leq c \leq 24e(\wp|p)$ (with $c \leq 12e(\wp|p)$ if $p > 2$, and $c \leq 6e(\wp|p)$ 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

$$\varphi(p^n)/\gcd(\varphi(p^n), c(E/L, R, \wp)).$$

Moreover:

1. *For each $\eta \geq 1$, there is a constant $f(\eta)$ such that if L is a any number field with $e(\wp|p) \leq \eta$, and E/L and R are as above, then $e(\mathfrak{P}|\wp)$ is divisible by $\varphi(p^n)/\gcd(\varphi(p^n), f(\eta))$.*
2. *If $e(\wp|p) = 1$ and $p > 3$, then $e(\mathfrak{P}|\wp)$ is divisible by either $(p^2-1)p^{2(n-1)}/6$, or the quantity $(p-1)p^{2(n-1)}/\gcd(p-1, 4)$.*

Theorem 1.2 is shown by providing a complete description and exact formulas of the slopes of the formal group of E/L (see Corollary 4.2). These formulas lead to exact formulas for the valuation of the roots of the formal group (see Lemma 5.3), which in turn lead to exact formulas for the ramification indices above p of the extension $L(R)/L$ when $R \in E[p^n]$ is a point of exact order p^n (see Proposition 5.6). For instance, if $E/\mathbb{Q} : y^2 + y = x^3 - 30x + 63$, and if $R_n \in E(\overline{\mathbb{Q}})$ is a point of exact order 3^n with $n \geq 3$, then the ramification index of any prime lying above 3 in the extension $\mathbb{Q}(R_n)/\mathbb{Q}$ is divisible by 3^{2n-4}, and that is precisely the ramification index for certain choices of R_n (see Example 5.10). Similarly, if $E/\mathbb{Q}$ is the curve with Cremona label $121c2$, and $R_n \in E(\overline{\mathbb{Q}})$ is a point of exact order 11^n with $n \geq 1$, then the ramification index of any prime lying above 11 in the extension $\mathbb{Q}(R_n)/\mathbb{Q}$ is divisible by $5 \cdot 11^{2(n-1)}$, and this is again best possible (see Example 5.11).

Moreover, under the assumptions of Theorem 1.2 we have

$$[L(R) : L] \geq e(\mathfrak{P}|\wp) \geq \frac{\varphi(p^n)}{\gcd(\varphi(p^n), c(E/L, R, \wp))} \geq \frac{\varphi(p^n)}{24e(\wp|p)},$$

and therefore

$$\varphi(p^n) \leq 24e(\wp|p)e(\mathfrak{P}|\wp) = 24e(\mathfrak{P}|p) \leq 24 \cdot [L(R) : L].$$

Hence, as a consequence of our main Theorem 1.2, we show a similar bound to Theorem 1.1 in the supersingular reduction case, which is linear in d (instead of exponential as in Theorem 1.1) and, in fact, it only depends on the ramification index of a prime of F above p.

Theorem 1.3. *Let p be a prime, let $d \geq 1$ be a fixed integer, let F be a number field of degree $\leq d$, and let E/F be an elliptic curve, such that $E(F)$ contains a point of exact order p^n. Suppose that F has a prime $\mathfrak{P}$ over p such that E/F has potential good supersingular reduction at $\mathfrak{P}$. Then,*

$$\varphi(p^n) \leq \begin{cases} 24e(\mathfrak{P}|p) \leq 24d & \text{if } p = 2, \\ 12e(\mathfrak{P}|p) \leq 12d & \text{if } p = 3, \\ 6e(\mathfrak{P}|p) \leq 6d & \text{if } p > 3, \end{cases}$$

and $e(\mathfrak{P}|p)$ is the ramification index of $\mathfrak{P}$ in $F/\mathbb{Q}$.

Thus, Theorem 1.2 when applied uniformly recovers bounds previously found by Flexor and Oesterlé, who show $|E(F)_{\text{tors}}| \leq 48d$ under similar hypotheses (see [2], Théorème 2). Our results, however, emphasize that there is a bound which is linear with respect to a ramification index of $F/\mathbb{Q}$, and can be regarded as evidence towards the following conjecture of the author, which will be discussed more in depth in an upcoming article.

Conjecture 1.4 ([6]). *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, such that $E(F)$ contains a point of exact order p^n. There is a constant C_3 that does not depend on p, d, F or E, such that*

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

where $e_{max}(p, F/\mathbb{Q})$ is the largest ramification index $e(\mathfrak{P}|p)$ for a prime $\mathfrak{P}$ of $\mathcal{O}_F$ over the rational prime p.

The paper is organized as follows. In Section 2 we discuss generalities about elliptic curves with potential good reduction, concentrating on the potential supersingular reduction case. In Section 3 we summarize results on the formal group of elliptic curves with potential supersingular reduction from [4], which we generalize in Section 4. In Section 5, we use these results to study the p-adic valuation of p^n-th torsion points, and the ramification index of the extensions generated by torsion points. It is here that we show Theorem 5.9, which subsumes Theorem 1.2. Throughout the paper, we exemplify our results with the elliptic curves $E_{27a4}/\mathbb{Q}$ and $E_{121c2}/\mathbb{Q}$ with Cremona labels "27a4" and "121c2", and the primes $p = 3$ and 11, respectively. In the last section of the article, Section 6, we discuss several other examples that correspond to non-cuspidal rational points on the modular curves $X_0(p^n)$, which appear in applications such as [5], and also we work out an example with an elliptic curve defined over a (quadratic) number field (see Example 6.2).

Acknowledgements. I would like to thank Kevin Buzzard, Brian Conrad, Harris Daniels, and Felipe Voloch for several useful references and suggestions.

2. 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 [11] 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 $\rho_{E,\ell} : \mathrm{Gal}(\overline{L_\wp^{\mathrm{nr}}}/L_\wp^{\mathrm{nr}}) \to \mathrm{Aut}(T_\ell(E))$ 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 [10], §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, [8] p. 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.

Example 2.1. Let $E = E_{27a4}$ be the elliptic curve with Cremona label "27a4", with j-invariant $j(E) = -2^{15} \cdot 3 \cdot 5^3$, given by a Weierstrass equation

$$y^2 + y = x^3 - 30x + 63.$$

The elliptic curve E has bad additive reduction at $p = 3$. The extension $K = K_E$ of $\mathbb{Q}_3^{\mathrm{nr}}$ is given by adjoining $\alpha = \sqrt[4]{3}$ and a root β of $x^3 - 120x + 506 = 0$. The result is an extension $K = \mathbb{Q}_3^{\mathrm{nr}}(\alpha, \beta)$ of degree $e = 12$.

Let (π) be the unique prime ideal of K above (3). Let E'/K be an elliptic curve isomorphic to E over K given by an integral model, minimal at (π), with good reduction at $\wp$. The reduction of E'/A modulo π is given by $y^2 \equiv x^3 + x + 2$ over $\mathbb{F}_3$, which is a supersingular elliptic curve. Thus, E/K is an elliptic curve with supersingular good reduction at the prime above $p = 3$.

Example 2.2. Let $E = E_{121c2}$ be the elliptic curve with Cremona label "121c2", with j-invariant $j(E) = -11 \cdot 131^3$, and discriminant $\Delta = -11^8$, given by a Weierstrass equation

$$y^2 + xy = x^3 + x^2 - 3632x + 82757.$$

The elliptic curve E has bad additive reduction at $p = 11$, but potential good supersingular reduction at the same prime. The extension $K = K_E$ of $\mathbb{Q}_{11}^{\mathrm{nr}}$ is given by adjoining $\pi = \sqrt[3]{11}$, thus $e = 3$. The curve E has a minimal model with good supersingular reduction of the form

$$y^2 + \sqrt[3]{11}xy = x^3 + \sqrt[3]{11^2}x^2 + 3\sqrt[3]{11}x + 2$$

over $\mathbb{Q}_{11}^{\mathrm{nr}}(\pi)$, where $\pi = \sqrt[3]{11}$, and the discriminant of this model is $\Delta = -1$.

Let e be the ramification index of $K/\mathbb{Q}_p$. 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 [8], p. 124-125, or [10], §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 [10] restricts its attention to the case $L = \mathbb{Q}$.

Theorem 2.3. *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 $10 \bmod 12$.*

Example 2.4. Let $E = E_{121c2}$, defined over $L = \mathbb{Q}$, so $e(\wp|p) = 1$. Since $\nu_\wp(\Delta) = 8$, we conclude that $e = 3$ by Theorem 2.3, which agrees with $K_E = \mathbb{Q}_{11}^{\mathrm{nr}}(\sqrt[3]{11})$ as we saw in Example 2.2.

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 $\pi_n : E(\overline{K})[p^n] \to \widetilde{E}(\overline{\mathbb{F}})[p^n]$ is the homomorphism given by reduction modulo $\mathcal{M}$, and X_{p^n} is the kernel of π_n (see [12], 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).

In this paper, we only discuss the supersingular reduction case (the multiplicative and the ordinary case will be treated in [6]). 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

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

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 [12]. 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 [12], 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 [4], Cor. 3.2).

Example 2.5. Let $E/\mathbb{Q}$ be the elliptic curve with Cremona label "27a4" as in Example 2.1. The multiplication-by-3 map on the associated formal group $\widehat{E}$ is given by a power series:

$$[3](Z) = 3Z + s_3Z^3 + O(Z^4),$$

where $\nu_K(s_3) = 2$. Hence, $e_1 = 2$ in this case. (The number s_3 was given in Example 2.2 of [4]. We will calculate e_1 in a different way below, in Example 3.4.)

Example 2.6. Let $E = E_{121c2}$ be the elliptic curve with Cremona label "121c2". The multiplication-by-11 map on the associated formal group $\widehat{E}$ is given by a power series:

$$\begin{aligned}[11](Z) = 11Z - 55\pi Z^2 - 275\pi^2 Z^3 + 42350Z^4 - 181148\pi Z^5 - 659417\pi^2 Z^6 + 96265708Z^7 \\ - 341161040\pi Z^8 - 1521191342\pi^2 Z^9 + 183261837077Z^{10} - 497606935519\pi Z^{11} + O(Z^{12}).\end{aligned}$$

Since $497606935519 = 17 \cdot 23 \cdot 151 \cdot 8428159$ is relatively prime to 11, we conclude that

$$e_1 = \nu_K(s_{11}) = \nu_K(-497606935519\pi) = 1.$$

3. Previous results

In [4], the author has shown several results on the values of e and e_1, that we quote here for the convenience of the reader. Before we state the results, we define quantities $r(p)$ and $s(p)$ for each prime $p > 3$, by

$$r(p) = \begin{cases} 1, & \text{if } p \equiv 5 \text{ or } 11 \bmod 12, \\ 0, & \text{if } p \equiv 1 \text{ or } 7 \bmod 12, \end{cases} \quad \text{and} \quad s(p) = \begin{cases} 1, & \text{if } p \equiv 3 \bmod 4, \\ 0, & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

Equivalently, $r(p) = \frac{1}{2}\left(1 - \left(\frac{-3}{p}\right)\right)$ and $s(p) = \frac{1}{2}\left(1 - \left(\frac{-4}{p}\right)\right)$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. We also need to define a polynomial $Q_p(T)$, whose existence and properties were shown in Lemma 3.6 of [4].

Definition 3.1. *Let $p > 3$ be a prime and let $P_p(X, Y)$ be the polynomial in $\mathbb{Z}[X, Y]$ defined by*

$$P_p(X,Y) = \sum_{\substack{m,n \geq 0 \\ 4m+6n=p-1}} (-1)^{m+n} \binom{\frac{p-1}{2}}{m+n} \binom{m+n}{m} (27X)^m (54Y)^n.$$

We define $Q_p(T) \in \mathbb{Z}[T]$ as the unique polynomial with integer coefficients such that

$$P_p(X,Y) = X^{r(p)} Y^{s(p)} \Delta^{\lfloor \frac{p}{12} \rfloor} Q_p(j),$$

where Δ and j are defined by $1728\Delta = X^3 - Y^2$ and $\Delta \cdot j = X^3$, where $\lfloor \cdot \rfloor$ is the greatest integer function.

Example 3.2. For instance,

$$P_5 = -54X, \ P_7 = -162Y, \ P_{11} = 29160XY,$$

and

$$P_{13} = -393660X^3 + 43740Y^2 = \Delta(E)(-349920j(E) - 75582720).$$

The corresponding polynomials $Q_p(T)$ are:

$$Q_5(T) = -54, \ Q_7(T) = -162, \ Q_{11}(T) = 29160, \ Q_{13}(T) = -349920T - 75582720.$$

Theorem 3.3 ([4], Thm. 3.9)**.** *Let E/L be an elliptic curve with potential good supersingular reduction at a prime $\wp$ above a prime p. Let $K = K_E$ be the extension of $L_\wp^{nr}$ defined above, let A, $e = \nu_K(p)$, and e_1 be as before, and let $e(\wp|p)$ be the ramification index of $\wp$ in $L/\mathbb{Q}$. Let $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be a minimal model for E/A with good reduction, and let $c_4, c_6 \in A$ be the usual quantities associated to this model (as defined in* [12]*, Chapter III, §1). Then:*

(1) *If $p = 2$, and $\frac{\nu_K(c_4)}{4} < e$, then*

$$e_1 = \frac{\nu_K(c_4)}{4} = \frac{\nu_K(j(E))}{12} = \frac{e \cdot \nu_\wp(j(E))}{12e(\wp|p)}.$$

(2) *If $p = 3$, and $\frac{\nu_K(c_4)}{2} < e$, then*

$$e_1 = \frac{\nu_K(c_4)}{2} = \frac{\nu_K(j(E))}{6} = \frac{e \cdot \nu_\wp(j(E))}{6e(\wp|p)}.$$

(3) *If $p > 3$, and $\lambda = r(p)\nu_K(c_4) + s(p)\nu_K(c_6) + \nu_K(Q_p(j(E))) < e$, then*

$$\begin{aligned} e_1 &= \lambda \\ &= r(p)\frac{\nu_K(j(E))}{3} + s(p)\frac{\nu_K(j(E)-1728)}{2} + \nu_K(Q_p(j(E))) \\ &= \frac{e}{e(\wp|p)} \cdot \left(r(p)\frac{\nu_\wp(j(E))}{3} + s(p)\frac{\nu_\wp(j(E)-1728)}{2} + \nu_\wp(Q_p(j(E))) \right). \end{aligned}$$

Otherwise, $e_1 \geq e$.

Example 3.4. In Example 2.5 we looked at the elliptic curve $E/\mathbb{Q}$ with label "27a4", for $p = 3$, and concluded that $e_1 = 2$. Alternatively, and much easier to compute, we use Theorem 3.3:

$$\lambda = \frac{e \cdot \nu_3(j(E))}{6} = \frac{12 \cdot \nu_3(-2^{15} \cdot 3 \cdot 5^3))}{6} = 2.$$

Since $2 = \lambda < e = 12$, we conclude that $e_1 = \lambda = 2$.

If we combine Theorems 3.3 and 2.3, then we reach the following corollary.

Corollary 3.5. *Let $p > 3$ be a prime and let E/L be an elliptic curve with potential supersingular good reduction at a prime $\wp$ above p. Let $e(\wp|p)$ be the ramification index of $\wp$ in $L/\mathbb{Q}$. Let $j(E) \in L$ be its j-invariant, let Δ_L be the discriminant of a model for E over L, and define an integer λ as follows:*

- *If $\nu_\wp(\Delta_L) \equiv 6 \bmod 12$, then $e/e(\wp|p) = 2$. Let*
$$\lambda = \frac{2}{3}r(p)\nu_\wp(j(E)) + s(p)\nu_\wp(j(E)-1728) + 2\nu_\wp(Q_p(j(E))),$$
- *If $\nu_\wp(\Delta_L) \equiv 4$ or $8 \bmod 12$, then $e/e(\wp|p) = 3$. Let*
$$\lambda = r(p)\nu_\wp(j(E)) + \frac{3}{2}s(p)\nu_\wp(j(E)-1728) + 3\nu_\wp(Q_p(j(E))),$$
- *If $\nu_\wp(\Delta_L) \equiv 3$ or $9 \bmod 12$, then $e/e(\wp|p) = 4$. Let*
$$\lambda = \frac{4}{3}r(p)\nu_\wp(j(E)) + 2s(p)\nu_\wp(j(E)-1728) + 4\nu_\wp(Q_p(j(E))),$$
- *If $\nu_\wp(\Delta_L) \equiv 2$ or $10 \bmod 12$, then $e/e(\wp|p) = 6$. Let*
$$\lambda = 2r(p)\nu_\wp(j(E)) + 3s(p)\nu_\wp(j(E)-1728) + 6\nu_\wp(Q_p(j(E))).$$

If $\lambda < e$, then $e_1 = \lambda$. Otherwise, if $\lambda \geq e$, then $e_1 \geq e$.

Example 3.6. Let us return to the curve $E/\mathbb{Q}$ with label "121c2". In Examples 2.2 and 2.4 we showed a minimal model over $\mathbb{Q}_{11}^{\mathrm{nr}}(\sqrt[3]{11})$ and we proved that $e_1 = 1$. We may also verify this value using the formula in Corollary 3.5. Here $p = 11$, so $r(11) = s(11) = 1$, and $L = \mathbb{Q}$, so $e(\wp|p) = 1$. The discriminant of the model for $E/\mathbb{Q}$ given in Example 2.2 is $\Delta_\mathbb{Q} = -11^8$, we have $j(E) = -11 \cdot 131^3$ and $j(E) - 1728 = -4973^2$. Hence:

$$\lambda = r(p)\nu_p(j(E)) + \frac{3}{2}s(p)\nu_p(j(E)-1728) + 3\nu_p(Q_p(j(E))) = 1 \cdot 1 + \frac{3}{2} \cdot 1 \cdot 0 + 3 \cdot 0 = 1.$$

and so, $e_1 = \lambda = 1$.

4. Additional results on the formal group

As we will show below in Corollary 4.2, the values of e and e_1 are restricted to certain values in certain cases. First, we need a lemma.

Lemma 4.1. *Let $p > 3$ be a prime.*

(1) *If $\nu_\wp(j) > 0$, then $\nu_\wp(Q_p(j)) = 0$.*
(2) *If $\nu_\wp(j - 1728) > 0$ and $\nu_\wp(j) = 0$, then $\nu_\wp(Q_p(j)) = 0$.*

Proof. It follows from the formulae in [4], Lemma 3.6 and Remark 3.8, that

$$Q_p(T) = q_d T^d + \ldots + q_1 T + q_0 = \sum d_f T^f (T - 1728)^{\lfloor \frac{p}{12} \rfloor - f},$$

where $f, g \geq 0$, and $0 \leq f \leq \lfloor \frac{p}{12} \rfloor$, and

$$d_f = (-1)^{m+n} \cdot \binom{\frac{p-1}{2}}{m+n} \cdot \binom{m+n}{m} \cdot 27^m \cdot 54^n,$$

where $m = 3f + r(p)$, and $n = 2g + s(p)$. It follows that the constant term in $Q_p(T)$ is given by $q_0 = d_0 \cdot (-1728)^{\lfloor \frac{p}{12} \rfloor}$. When $f = 0$ we have $m = r(p)$ and $n = 2 \cdot \lfloor \frac{p}{12} \rfloor + s(p)$. Then the constant term of $Q_p(T)$ is given by:

$$q_0 = d_0 \cdot (-1728)^{\lfloor \frac{p}{12} \rfloor} = (-1)^{m+n} \cdot \binom{\frac{p-1}{2}}{m+n} \cdot \binom{m+n}{m} \cdot 27^m \cdot 54^n \cdot (-1728)^{\lfloor \frac{p}{12} \rfloor}.$$

Since $p > 3$, the constant term q_0 is not divisible by p. If $\nu_\wp(j) > 0$, then $\nu_\wp(Q_p(j)) = \nu_\wp(q_0) = 0$. This shows part (1).

For part (2), note that we may write

$$Q_p(j) = d_{\lfloor \frac{p}{12} \rfloor} j^{\lfloor \frac{p}{12} \rfloor} + \sum_{0 \leq f < \lfloor \frac{p}{12} \rfloor} d_f j^f (j - 1728)^{\lfloor \frac{p}{12} \rfloor - f}.$$

If we set $m = 3 \cdot \lfloor \frac{p}{12} \rfloor + r(p)$ and $n = s(p)$, then the coefficient $d_{\lfloor \frac{p}{12} \rfloor}$ is given by

$$d_{\lfloor \frac{p}{12} \rfloor} = (-1)^{m+n} \cdot \binom{\frac{p-1}{2}}{m+n} \cdot \binom{m+n}{m} \cdot 27^m \cdot 54^n.$$

Since $d_{\lfloor \frac{p}{12} \rfloor}$ is not divisible by $p > 3$, and $\nu_\wp(j) = 0$ and $\nu_\wp(j - 1728) > 0$ by assumption, it follows that $\nu_\wp(Q_p(j)) = 0$, as desired. □

The following result extends Corollary 4.6 of [4], which only covered the case when $e(\wp|p) = 1$.

Corollary 4.2. *Let E/L be an elliptic curve with potential supersingular reduction at a prime $\wp$ lying above a prime $p > 3$, and let e and e_1 be defined as in Section 2. Assume that $e_1 < e$. Then,*

(1) *If $j(E) \not\equiv 0$ or $1728 \bmod \wp$, then $e_1 = e/e(\wp|p) \cdot \nu_\wp(Q_p(j))$;*
(2) *If $j(E) \equiv 0 \bmod \wp$, then $e_1 = e \cdot \nu_\wp(j)/3e(\wp|p)$, with $1 \leq \nu_\wp(j) < 3e(\wp|p)$. If $\nu_\wp(j)$ is not divisible by 3, then $e/e(\wp|p) = 3$ or 6, and $e_1 = \nu_\wp(j)$ or $2\nu_\wp(j)$.*
(3) *If $j(E) \equiv 1728 \bmod \wp$, then $e_1 = e \cdot \nu_\wp(j - 1728)/2e(\wp|p)$, with $1 \leq \nu_\wp(j - 1728) < 2e(\wp|p)$. If $\nu_\wp(j - 1728)$ is even, then $e/e(\wp|p) = 2$ or 4, and $e_1 = \nu_\wp(j - 1728)$ or $2\nu_\wp(j - 1728)$.*

Proof. Let $p > 3$ be a prime, assume that $e_1 < e$, let K_E be the extension of degree e of $L_{\wp}^{\mathrm{nr}}$ defined above, and fix a minimal model of E over K_E with good supersingular reduction. Let Δ be its discriminant, and let c_4 and c_6 be the usual quantities. Let $\lambda = r(p)\nu_K(c_4) + s(p)\nu_K(c_6) + \nu_K(Q_p(j(E)))$ as in Theorem 3.3. If $\lambda \geq e$ then $e_1 \geq e$, but we have assumed that $e_1 < e$, and hence $e_1 = \lambda$. Let us write $e' = e/e(\wp|p)$. In this case, $\nu_K(Q_p(j(E))) = e' \cdot \nu_{\wp}(Q_p(j(E)))$ is a multiple of e'. Under our assumptions

$$\begin{aligned} e_1 &= r(p)\nu_K(c_4) + s(p)\nu_K(c_6) + \nu_K(Q_p(j)) \\ &= e' \cdot (r(p)\nu_{\wp}(c_4) + s(p)\nu_{\wp}(c_6) + \nu_{\wp}(Q_p(j))). \end{aligned} \tag{1}$$

Since $\nu_K(\Delta) = 0$ and $p \neq 2, 3$, the equality $1728\Delta = c_4^3 - c_6^2$ implies that $\nu_K(c_4)$ and $\nu_K(c_6)$ cannot be simultaneously positive. We note that $c_4^3/\Delta = j$ and $c_6^2 = \Delta \cdot (j - 1728)$. Since $\nu_K(\Delta) = 0$, it follows that $\nu_K(c_4) = \nu_K(j)/3$ and $\nu_K(c_6) = \nu_K(j - 1728)/2$. Since $c_4, c_6 \in L$, it follows that $\nu_K(c_4) = 0$ (resp. $\nu_K(c_6) = 0$) if and only if $\nu_{\wp}(j) = 0$ (resp. $\nu_{\wp}(c_6) = 0$), if and only if $j \not\equiv 0 \bmod \wp$ (resp. $j - 1728 \not\equiv 0 \bmod \wp$).

- If $\nu_K(c_4) = \nu_K(c_6) = 0$, then $e_1 = e' \cdot \nu_{\wp}(Q_p(j))$.
- If $\nu_K(c_4) > 0$ and $\nu_K(c_6) = 0$, then $\nu_K(j(E)) = \nu_K(c_4^3/\Delta) = 3\nu_K(c_4) > 0$. Since $j(E) \in L$, it follows that $j(E) \equiv 0 \bmod \wp$. In particular, $\nu_K(j) = e' \cdot \nu_{\wp}(j)$ is a multiple of $e/e(\wp|p) = e'$, say $\nu_K(j) = e' \cdot \nu_{\wp}(j)$. Theorem 3.3 and Corollary 4.1 say that

  $$e_1 = r(p)\nu_K(c_4) + s(p)\nu_K(c_6) + \nu_K(Q_p(j)) = e' \cdot \left(r(p)\frac{\nu_{\wp}(j)}{3} \right).$$

  Thus, we must have $r(p) = 1$ (in particular, $p \equiv 5 \bmod 6$ in this case) and $e_1 = \nu_K(c_4)$, otherwise $0 = e_1 \geq 1$, a contradiction. Hence,

  $$e_1 = \nu_K(c_4) = \frac{\nu_K(j)}{3} = \frac{e' \cdot \nu_{\wp}(j)}{3}.$$

  Since $e_1 < e$ by assumption, it follows that $1 \leq \nu_{\wp}(j) < 3e(\wp|p)$. In addition, e_1 is a positive integer, so $e'\nu_{\wp}(j) \equiv 0 \bmod 3$. If $\nu_{\wp}(j)$ is not a multiple of 3, then $e' \equiv 0 \bmod 3$. Finally, $e' = 1, 2, 3, 4$, or 6, so $e' = 3$ or 6 in this case, and $e_1 = \nu_{\wp}(j)$ or $2\nu_{\wp}(j)$, as claimed.
- If instead we have $\nu_K(c_4) = 0$ and $\nu_K(c_6) > 0$, Theorem 3.3 and Corollary 4.1 now say that $e_1 = \nu_K(c_6)$ (we must have $p \equiv 3 \bmod 4$ in this case). It follows that $j \equiv 1728 \bmod \wp$ and $\nu_K(j - 1728) = e'h$ where $h = \nu_{\wp}(j - 1728) \geq 1$. Since $e_1 < e$, we have $h < 2e(\wp|p)$. Since e_1 is an integer, and if h is odd, then $e' \equiv 0 \bmod 2$. Thus, $e' = 2$, 4, or 6, and therefore, $e_1 = h$, $2h$, or $3h$. However, we shall show next that $j \equiv 1728 \bmod \wp$ and $e' = 6$ is not possible. Thus, $e_1 = h$, or $2h$, and the proof of the corollary would be finished.

  Indeed, suppose $j \equiv 1728 \bmod \wp$ and $e' = 6$. Let Δ_L, $c_{4,L}$ and $c_{6,L}$ be the discriminant and the usual constants associated to the original model of E over L. By the work of Néron on minimal models (Theorem 2.3), the degree $e' = 6$ occurs if and only if $\nu_{\wp}(\Delta_L) \equiv 2$ or $10 \bmod 12$. Since $\Delta_L \cdot j(E) = (c_{4,L})^3$, and $j \equiv 1728 \bmod \wp$, with $p > 3$, it follows that

  $$\nu_{\wp}(\Delta_L) = 3\nu_{\wp}(c_{4,L})$$

  and therefore $\nu_{\wp}(\Delta_L) \equiv 0 \bmod 3$, and we cannot have $\nu_{\wp}(\Delta_L) \equiv 2$ or $10 \bmod 12$. This is a contradiction, and therefore $e' = 6$ and $j \equiv 1728 \bmod \wp$ are incompatible. This ends the proof of the corollary.

□

Corollary 4.3. *With notation as in Corollary 4.2, if $e_1 < e$, and $p > \max\{3e(\wp|p) - 1, 3\}$, then $pe/(p+1) > e_1$.*

Proof. Suppose $e_1 < e$. According to Cor. 4.2, the biggest possible value of e_1 is $(3e(\wp|p) - 1)e/3e(\wp|p)$. Since the function $k(x-1)/x$ is increasing for any $k > 0$ and any $x > 1$, it follows that if $p + 1 > 3e(\wp|p)$, then

$$e_1 \leq \frac{(3e(\wp|p) - 1)e}{3e(\wp|p)} < \frac{pe}{p+1}.$$

□

Example 4.4. Here we illustrate the last three results with the curve $E/\mathbb{Q}$ with label "121c2". The discriminant of the chosen model for $E/\mathbb{Q}$ is $\Delta_{\mathbb{Q}} = -11^8$, we have $j(E) = -11 \cdot 131^3$ and $j(E) - 1728 = -4973^2$.

Since $\nu_{11}(j) = 1$, Lemma 4.1 implies that $\nu_{11}(Q_{11}(j)) = 0$. Indeed, we know that $Q_{11}(j)$ is constant, equal to $29160 = 2^3 \cdot 3^6 \cdot 5$, so its 11-adic valuation is zero.

Moreover, $\nu_{11}(j) = 1 > 0$ so Corollary 4.2 says that $e_1 = e \cdot \nu_{\wp}(j)/3e(\wp|p) = (3 \cdot 1)/3 = 1$, as we had already computed in Example 2.6.

Finally, we have $pe/(p+1) = 33/12 > 1 = e_1$, in agreement with Corollary 4.3.

The next three results concern not only e and e_1, but also the values of $e - p^u e_1$, for every $u \geq 0$ such that $e - p^u e_1 \geq 1$. As we shall see later (Lemma 5.3 and Prop. 5.6), these values are closely related to the constants $c(E/L, R, \wp)$ of Theorem 1.2 in the introduction.

Corollary 4.5. *Let $\eta \geq 1$ be a fixed positive integer. Let L be a number field, and let $\wp$ be a prime ideal of $\mathcal{O}_L$ lying above a prime p, such that $e(\wp|p) = \eta$. Let E/L be an elliptic curve with potential good supersingular reduction at $\wp$. Then, there is a constant $f(\eta, p)$, which depends only on η when $p > 3$ (and does not on $\wp$, L, or E), such that e is a divisor of $f(\eta, p)$, and if $e_1 < e$, then the quantities e_1, and $e - p^u e_1$, for every $u \geq 0$ such that $e - p^u e_1 \geq 1$, are also divisors of $f(\eta, p)$. Moreover,*

1. *For any p, the constant $f(\eta, p)$ is a divisor of $F(\eta) = \operatorname{lcm}(\{n : 1 \leq n < 24\eta,\ \gcd(n, 6) \neq 1\})$.*
2. *The constant $f(\eta, 2)$ is a divisor of $F(\eta, 2) = \operatorname{lcm}(\{2n : 1 \leq n < 12\eta\})$.*
3. *The constant $f(\eta, 3)$ is a divisor of $F(\eta, 3) = \operatorname{lcm}(\{2n : 1 \leq n < 6\eta\})$.*
4. *If $p > 3$, the constant $f(\eta, p)$ is a divisor of $F_0(\eta) = \operatorname{lcm}(\{n : 1 \leq n < 6\eta,\ \gcd(n, 6) \neq 1\})$.*
5. *If $\eta = 1$ and $p > 3$, then e divides 4 or 6, and e_1 and $e - e_1$ are divisors of 4.*

Proof. Let $\eta \geq 1$, L, $\wp$, $e(\wp|p) = \eta$, and E/L be as in the statement. We shall write $e' = e/e(\wp|p)$. Notice that, as defined, the quantities $F_0(\eta)$, $F(\eta, 2)$, and $F(\eta, 3)$, are divisors of $F(\eta)$, so to show (1) through (4) it suffices to show that $f(\eta, p)$ divides $F(\eta, p)$ for $p = 2, 3$, and $f(\eta, p)$ divides $F_0(\eta)$ for $p > 3$.

By our discussion at the beginning of Section 2, we have $e = e'\eta$, where e' is a divisor of 24, 12, or 6 according to whether $p = 2$, 3, or > 3, respectively. Thus, e is clearly a divisor of $F(\eta, p)$, for all $p = 2$ or 3, and a divisor of $F_0(\eta)$ for $p > 3$.

Let us assume from now on that $e_1 < e$. If $p = 2$, then Theorem 3.3 says that $e_1 = e' \cdot t/12$, and we must have $1 \leq t < 12\eta$ to satisfy $e_1 < e$. Since $p = 2$, the number e' is a divisor of 24. Hence, e_1 is a divisor of $2t$, with $1 \leq t < 12\eta$, and $e - p^u e_1 = e'(\eta - p^u t/12) \geq 1$ is a divisor of $2(12\eta - p^u t)$. It follows that both e_1 and $e - p^u e_1$ are divisors of $F(\eta, 2) = \operatorname{lcm}(\{2n : 1 \leq n < 12\eta\})$. The number e is a divisor of 24η. Since $24\eta = \operatorname{lcm}(8\eta, 3\eta)$, then e divides $F(\eta, 2)$.

If $p = 3$, then Theorem 3.3 says that $e_1 = e' \cdot t/6$, and we must have $1 \leq t < 12\eta$. Since $p = 3$, the number e' is a divisor of 12. Hence, e_1 is a divisor of $2t$, with $1 \leq t < 12\eta$, and $e - p^u e_1 = e'(\eta - p^u t/6)$ is a divisor of $2(12\eta - p^u t)$. It follows that both e_1 and $e - p^u e_1$ are divisors of $F(\eta, 3) = \mathrm{lcm}(\{2n : 1 \leq n < 12\eta\})$. The number e is a divisor of 12η. Since $12\eta = \mathrm{lcm}(4\eta, 3\eta)$, then e divides $F(\eta, 3)$.

Now assume that $p > 3$. It follows that e' is 1, 2, 3, 4, or 6. In particular, e' is a divisor of 4 or 6. By Corollary 4.2, we have $e_1 = e' \cdot r$ with $1 \leq r < \eta$, or $e_1 = e' \cdot s/3$ with $e_1 \in \mathbb{Z}$ and $1 \leq s < 3\eta$, or $e_1 = e' \cdot t/2$ with $e_1 \in \mathbb{Z}$ and $1 \leq t < 2\eta$. In particular, e_1 is a divisor of a number in the set

$$\{4\alpha : 1 \leq \alpha < \eta\} \cup \{2\beta : 1 \leq \beta < 3\eta\} \cup \{2\gamma : 1 \leq \gamma < 2\eta\} \cup \{3\delta : 1 \leq \delta < 2\eta\}.$$

Note that $\{4\alpha : 1 \leq \alpha < \eta\} \subseteq \{2\beta : 1 \leq \beta < 3\eta\}$, and so the number e_1 is a divisor of a number in the set

$$\{2\beta : 1 \leq \beta < 3\eta\} \cup \{3\delta : 1 \leq \delta < 2\eta\} = \{n : 1 \leq n < 6\eta,\ \gcd(n, 6) \neq 1\}.$$

Similarly, $e - p^u e_1 = e'(\eta - p^u r)$ with $1 \leq p^u r < \eta$, or $e - p^u e_1 = e'(\eta - p^u s/3)$ with $e_1 \in \mathbb{Z}$ and $1 \leq p^u s < 3\eta$, or $e_1 = e'(\eta - p^u t/2)$ with $e_1 \in \mathbb{Z}$ and $1 \leq p^u t < 2\eta$. Hence, $e - p^u e_1$ is a divisor of a number in the set

$$\begin{aligned}&\{4(\eta - \lambda) : 1 \leq \lambda < \eta\} \cup \{2(3\eta - \mu) : 1 \leq \mu < 3\eta\} \cup \{2(2\eta - \psi) : 1 \leq \psi < 2\eta\} \cup \{3(2\eta - \rho) : 1 \leq \rho < 2\eta\} \\ &= \{4\alpha : \alpha < \eta\} \cup \{2\beta : \beta < 3\eta\} \cup \{2\gamma : \gamma < 2\eta\} \cup \{3\delta : \delta < 2\eta\}.\end{aligned}$$

Therefore, $e - p^u e_1$ also is a divisor of a number in $\{n : 1 \leq n < 6\eta,\ \gcd(n, 6) \neq 1\}$. Hence, both e_1 and $e - p^u e_1$ are divisors of $\mathrm{lcm}(\{n : 1 \leq n < 6\eta,\ \gcd(n, 6) \neq 1\})$. The number e is a divisor of 4η or 6η. Since 4η divides $F_0(\eta)$ and $6\eta = \mathrm{lcm}(2\eta, 3\eta)$, then e divides $F_0(\eta)$.

If $\eta = 1$ and $1 \leq e_1 < e$, then $e_1 = e' \cdot \nu_\wp(Q_p(j))$ is impossible. Thus, by Corollary 4.2, either

- $e_1 = e \cdot \nu_\wp(j)/3$ with $1 \leq \nu_\wp(j) < 3$. In this case $\nu_\wp(j) = 1$ or 2, so $e = 3$ or 6, and therefore $e_1 = 1$, 2, or 4. Note that $e_1 = 4$ can only happen if $e = 6$, and if $e = 6$, then $e_1 = 2$ or 4. Since $p \geq 5$, $pe_1 > e$, and we only need to consider e, e_1, and $e - e_1$. In particular, $e - e_1 = 1$, 2, or 4; or
- $e_1 = e \cdot \nu_\wp(j - 1728)/2$ with $1 \leq \nu_\wp(j - 1728) < 2$. In this case $\nu_\wp(j - 1728) = 1$, so $e = 2$ or 4, and therefore $e_1 = 1$, or 2, respectively. Since $p \geq 5$, $pe_1 > e$, and we only need to consider e, e_1, and $e - e_1$. Thus, $e - e_1 = 1$, or 2, respectively.

Hence, in all cases e divides 4 or 6, and e_1 and $e - e_1$ are divisors of 4. □

Example 4.6. In previous examples we calculated $e = 12$ and $e_1 = 2$ for the elliptic curve $E/\mathbb{Q}$ with label "27a4". Let us calculate $F(1, 3)$. By definition

$$F(1, 3) = \mathrm{lcm}(\{2n : 1 \leq n < 6\}) = \mathrm{lcm}(2, 4, 6, 8, 10) = 8 \cdot 3 \cdot 5 = 120.$$

Thus, $e = 12$, $e_1 = 2$, and $e - e_1 = 10$, and $e - 3e_1 = 6$ are divisors of $F(1, 3) = 120$, as predicted by Corollary 4.5.

Example 4.7. Let $\eta \geq 1$, and put $F_0(\eta) = \mathrm{lcm}(\{n : 1 \leq n < 6\eta,\ \gcd(n, 6) \neq 1\})$. In this example we list a few values of $F_0(\eta)$:

$F_0(1)$	$F_0(2)$	$F_0(3)$	$F_0(4)$	$F_0(5)$	$F_0(6)$
$2^2 \cdot 3$	$2^3 \cdot 3^2 \cdot 5$	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	$2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$

Corollary 4.8. *With notation as in Cor. 4.2, if $p > 3e(\wp|p)$, then e, e_1, and $e - p^u e_1 \geq 1$ are not divisible by p.*

Proof. Since $p > 3$, Theorem 2.3 says that $e' = e/e(\wp|p)$ is a divisor of 12. Hence, if $p > 3e(\wp|p)$, then $e = e' \cdot e(\wp|p)$ is relatively prime to p. By Cor. 4.5, there is a constant $f(\eta)$ with $\eta = e(\wp|p)$ such that e, e_1 and $e - p^u e_1$ are divisors of $f(\eta)$, for all $u \geq 0$ such that $1 \leq e - p^u e_1$. Moreover, $f(\eta)$ can be chosen to be

$$F(\eta) = \operatorname{lcm}(\{n : 1 \leq n < 6\eta,\ \gcd(n, 6) \neq 1\}) = \operatorname{lcm}(\{2\beta : 1 \leq \beta < 3\eta\} \cup \{3\delta : 1 \leq \delta < 2\eta\}).$$

Since $p > 3\eta$, there is no $\beta < 3\eta$ or $\delta < 2\eta$ such that p is a divisor of 2β or 3δ. Thus, $f(\eta)$ is not divisible by p, and it follows that neither e, e_1 nor $e - p^u e_1$ is divisible by p. □

Example 4.9. Let E be the curve with label "121c2". We have previously calculated $e = 3$ and $e_1 = 1$. The values $e = 3$, $e_1 = 1$ and $e - e_1 = 2$ are divisors of $F_0(1) = 12$, as stated in Cor. 4.5, and none of them are divisible by 11, as it follows from Cor. 4.8.

We finish this section with two lemmas about quadratic twists of elliptic curves that we will need later on.

Lemma 4.10. *Let E/L be an elliptic curve with potential good reduction at a prime $\wp$ lying above a prime $p \geq 3$, and let E'/L be a quadratic twist of E. Let F/L be the quadratic extension such that $E \cong_F E'$. Let $K = K_E$ (resp. $K' = K_{E'}$) be the smallest extension of $L_\wp^{nr}$ such that E/K (resp. E'/K') has good reduction. Let π and π' be uniformizers for K and K' respectively, and let $\nu = \nu_K$ and $\nu' = \nu_{K'}$ be normalized valuations such that $\nu(\pi) = \nu'(\pi') = 1$. Let $e = \nu(p)$, $e' = \nu'(p)$ and suppose that $e \leq e'$. Then:*

1. *Either $K = K'$ or $K' = FK$.*
2. *Suppose E has potential supersingular reduction. Let e_1 and e_1' be the valuation of the coefficient of X^p in the power series $[p](X)$ for the formal groups $\widehat{E}$ and $\widehat{E'}$ respectively, as defined above, and assume that $e_1 < e$. Then,*

$$e' = \mu e, \quad \text{and} \quad e_1' = \mu e_1,$$

where $\mu = [K' : K] = 1$ or 2.

Proof. Since E and E' are isomorphic over F, it follows that they are also isomorphic over FK. Since E has good reduction over K, it also has good reduction over FK (see [12], VII, Proposition 5.4, part (b)). Thus, E' has good reduction over FK as well. By the properties of K' (see our comments at the beginning of Section 2) we know that $K' \subseteq FK$. Similarly, $K \subseteq FK'$. In particular, $FKK' = FK = FK'$.

Suppose that $K \neq K'$ and $e < e'$. Notice that

$$K \subsetneq KK' \subseteq FKK' = FK.$$

Thus, KK'/K is quadratic, and so is $K'/K \cap K'$. It follows that $K'/K \cap K'$ is a non-trivial (tamely) ramified quadratic extension of $K \cap K'$ and, since $p \geq 3$ and $L_\wp^{\mathrm{nr}} \subseteq K \cap K'$, there is a unique such extension of $K \cap K'$. Since we have assumed that $K \neq K'$, it follows that $K/K \cap K'$ is trivial, $K \subseteq K'$, and $K'/K = K'/K \cap K'$ is quadratic. Since $K \subsetneq K' \subseteq KK' \subseteq FK$, and FK/K is at most quadratic, it follows that $K' = FK$, as desired. This proves (1).

For (2), let $H = FK = FK'$, and assume that $e \leq e'$, as before. By part (1), either $K = K'$ and $e = e'$, or $K' = FK$ is quadratic over K and $e' = 2e$. Thus, $e' = \mu \cdot e$ with $\mu = [K' : K]$. Now, the

formulas in Theorem 3.3 applied to E say that $e_1 = \lambda = e/e(\wp|p) \cdot C$, where $C = C(j(E), \wp)$ is a constant that only depends on $j(E)$ and $\wp$. Let us apply Theorem 3.3 to E'/A':

$$\lambda' = e'/e(\wp|p) \cdot C(j(E'), \wp) = \mu e/e(\wp|p) \cdot C(j(E), \wp) = \mu\lambda,$$

where we have used the fact that $j(E) = j(E')$ because $E \cong_F E'$. Since $\lambda = e_1 < e$ by assumption, it follows that $\lambda' = \mu\lambda < \mu e = e'$. Hence, the theorem implies that $e_1' = \lambda' = \mu\lambda = \mu e_1$, as claimed. □

Lemma 4.11. *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 $\phi : E \to E'$ 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 $F(x(R)) = F(x(\phi(R)))$.*

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 [12], Ch. III, Prop. 3.1(b), the isomorphism $\phi : E \to E'$ 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) is 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). □

5. Formal groups and the valuation of torsion points

In this section we apply our previous results about the formal group of an elliptic curve with potential supersingular reduction to calculate the slopes in the Newton polygon of the multiplication-by-p map. In turn, the slopes will allow us to calculate the valuation of p^n-th torsion points in the formal group, and the ramification index in the extensions generated by these points.

Lemma 5.1. *Let E, K and ν be as above, so that E/K is an elliptic curve given by a minimal model with good supersingular reduction. Put $[p](X) = \sum_{i=1}^{\infty} s_i X^i$ and let $e = \nu(s_1) = \nu(p)$ and $e_1 = \nu(s_p)$. Let $T_1 \in E(\overline{K})[p]$ be a non-trivial p-torsion point, fix any sequence $\{T_n \in E[p^n] : [p]T_{n+1} = T_n\}$, and let t_n be the corresponding torsion points in $\widehat{E}(\mathcal{M})$, where $\mathcal{M}$ is the maximal ideal in the ring of integers of $\overline{K}$.*

(i) *$\nu(t_{n+1}) < \nu(t_n)$;*
(ii) *If $\nu(t_n) < \frac{ep}{p-1}$, then $\nu(t_{n+1}) < \frac{\nu(t_n)}{p}$;*
(iii) *If $\nu(t_m) < \min\{e, e_1\}$ for some $m \geq 1$, then for all $n \geq m$ we have*

$$\nu(t_n) = \frac{\nu(t_m)}{p^{2(n-m)}}.$$

In particular, the ramification index of $K(T_{n+1})/K(T_n)$ is p^2 for all $n \geq m$.

Proof. The theory of formal groups (see [12], VII, Proposition 2.2) shows that there is an isomorphism $t : E_1(\overline{K}) \cong \widehat{E}(\mathcal{M})$, where $\widehat{E}$ is the formal group associated to E. The isomorphism is given by $(x, y) \mapsto t((x, y)) = -x/y$. Since we are assuming that E/K has good supersingular reduction, all

torsion points with p-power order live in the kernel of reduction $E_1(\overline{K})$. Thus, $T_n \in E(\overline{K})[p^n] \subset E_1$, for $n = 1, 2, \ldots$, and we define $t_n = t(T_n)$.

Since E/K is good supersingular, the height of $\widehat{E}$ as a formal group is 2. As above, there are power series $f(X)$, $g(X)$ and $h(X)$ in $X \cdot A[[X]]$, with $f'(0) = g'(0) = h'(0) \in A^\times$, such that:

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

It follows that

$$\begin{aligned} \nu(t_n) = \nu([p](t_{n+1})) &\geq \min\{\nu(pf(t_{n+1})), \nu(\pi^{e_1} g(t_{n+1}^p)), \nu(h(t_{n+1}^{p^2}))\} \\ &= \min\{e + \nu(t_{n+1}), e_1 + p\nu(t_{n+1}), p^2\nu(t_{n+1})\} > \nu(t_{n+1}). \end{aligned} \tag{2}$$

It follows that $\nu(t_{n+1}) < \nu(t_n)$ as claimed in (i). Assume that $\nu(t_n) < ep/(p-1)$ or, equivalently, $e + \nu(t_n)/p > \nu(t_n)$. For a contradiction, suppose that $\nu(t_{n+1}) \geq \nu(t_n)/p$. By Eq. (2), this would imply $\nu(t_n) \geq \min\{e + \nu(t_n)/p, e_1 + \nu(t_n), p\nu(t_n)\} > \nu(t_n)$, a contradiction. This proves (ii).

We will prove (iii) using induction. Clearly, the base case $n = m$ is trivial. Now, suppose the equality is valid for some $n > m$, i.e., $\nu(t_n) = \nu(t_m)/p^{2(n-m)}$. In particular, $\nu(t_n) < \nu(t_m) < \min\{e, e_1\}$. Hence, the only possibility in Eq. (2) is that the minimum is attained with $p^2\nu(t_{n+1})$, and since this value is smaller than the other two, all inequalities are actually equalities. Thus, $\nu(t_n) = p^2\nu(t_{n+1})$. Hence,

$$\nu(t_{n+1}) = \frac{\nu(t_n)}{p^2} = \frac{\nu(t_m)}{p^{2(n-m)+2}} = \frac{\nu(t_m)}{p^{2(n+1-m)}}.$$

Thus, by the principle of mathematical induction, the equality is valid for all $n \geq m$. □

Lemma 5.2. *Let E/L be an elliptic curve with potential good supersingular reduction at a prime $\wp$. Let $K_E/L_\wp^{nr}$, A, π, e, and e_1 be as above, so that $[p](X) = pf(X) + \pi^{e_1} g(X^p) + h(X^{p^2})$, where $f(X)$, $g(X)$ and $h(X)$ are power series in $X \cdot A[[X]]$, with $f'(0) = g'(0) = h'(0) \in A^\times$. Then:*

1. *If $pe/(p+1) \leq e_1$, then $[p](X) = 0$ has $p^2 - 1$ roots of valuation $\frac{e}{p^2-1}$;*
2. *If $pe/(p+1) > e_1$, then $[p](X) = 0$ has $p - 1$ roots with valuation $\frac{e-e_1}{p-1}$ and $p^2 - p$ roots with valuation $\frac{e_1}{p(p-1)}$.*

Proof. This is shown in [10], §1.10 (pp. 271-272). Let N be the part of the Newton polygon of $[p](Z)$ that describes the roots of valuation > 0. Let $P_0 = (1, e)$, $P_1 = (p, e_1)$, and $P_2 = (p^2, 0)$. The slope of the segment P_0P_1 is $-(e - e_1)/(p - 1)$, while the slope of the segment P_0P_2 is $-e/(p^2 - 1)$. It follows from the theory of Newton polygons (see [10], p. 272) that:

1. If $pe/(p+1) \leq e_1$, then N is given by a single segment P_0P_2 of length $p^2 - 1$. Thus, there are $p^2 - 1$ roots of valuation $\frac{e}{p^2-1}$.
2. Otherwise, if $pe/(p+1) > e_1$, then N is given by two segments P_0P_1 and P_1P_2 of length $p - 1$ and $p^2 - p$, respectively. It follows that there are $p - 1$ roots with valuation $\frac{e-e_1}{p-1}$ and $p^2 - p$ roots with valuation $\frac{e_1}{p(p-1)}$.

□

We say that t is a primitive root of $[p^n](X) = 0$ if $[p^n](t) = 0$ but $[p^m](t) \neq 0$ for any $0 \leq m < n$.

Lemma 5.3. *With notation as in Lemma 5.2, let $n \geq 1$ be fixed.*

1. *If $pe/(p+1) \leq e_1$, then every primitive root of $[p^n](X) = 0$ has valuation $\frac{e}{p^{2(n-1)}(p^2-1)}$;*

(2) *If* $pe/(p+1) > e_1$, *then* $[p^n](X) = 0$ *has* $(p^2-p)p^{2(n-1)}$ *primitive roots with valuation* $\frac{e_1}{(p-1)p^{2n-1}}$. *Moreover, let* s *be the smallest non-negative integer such that* $e/e_1 \leq p^s(p+1)$. *Then,*

(a) *if* $n \leq s+1$, *there are* $(p-1)p^{2(n-1)}$ *primitive roots of valuation* $\frac{e-p^{n-1}e_1}{(p-1)p^{n-1}}$;

(b) *if* $n > s+1$, *there are* $(p-1)p^{2(n-1)}$ *primitive roots of valuation* $\frac{e-p^s e_1}{(p-1)p^{2(n-1)-s}}$.

Proof. Let t_n be a primitive root of $[p^n](X) = 0$. Then, $t_1 = [p^{n-1}](X)$ is a non-zero root of $[p](X) = 0$. By Lemma 5.2 there are three options according to the valuation of t_1.

(1) If $pe/(p+1) \leq e_1$, then the valuation of $t_1 \in \widehat{E}[p]$ is $e/(p^2-1)$. Thus,

$$\nu(t_1) = \frac{e}{p^2-1} < p(p-1)\frac{e}{p^2-1} = \frac{pe}{p+1} \leq \min\{e, e_1\}.$$

Hence, by Lemma 5.1,

$$\nu(t_n) = \frac{\nu(t_1)}{p^{2(n-1)}} = \frac{e}{p^{2(n-1)}(p^2-1)}.$$

(2) If $pe/(p+1) > e_1$, then the valuation of t_1 is $e_1/p(p-1)$ or $(e-e_1)/(p-1)$. Notice that in this case $e > pe/(p+1) > e_1$. If $\nu(t_1) = e_1/p(p-1) \leq \min\{e, e_1\}$, then by Lemma 5.1,

$$\nu(t_n) = \frac{\nu(t_1)}{p^{2(n-1)}} = \frac{e_1}{p^{2(n-1)+1}(p-1)} = \frac{e_1}{p^{2n-1}(p-1)}.$$

For the rest of the proof, let us assume that $\nu(t_1) = (e-e_1)/(p-1)$. We note that $\nu(t_1) < e$. Let us write $t_m = [p^{n-m}](t_n)$. In the proof of Lemma 5.1 we saw that

$$\nu(t_m) \geq \min\{e + \nu(t_{m+1}), e_1 + p\nu(t_{m+1}), p^2\nu(t_{m+1})\} > \nu(t_{m+1}),$$

for any $1 \leq m < n$. Since $\nu(t_m) > \nu(t_{m+1})$ for all m, and $\nu(t_1) < e$, it follows that the minimum cannot be $e + \nu(t_{m+1})$ for any $m \geq 1$. Thus,

$$\nu(t_m) \geq \min\{e_1 + p\nu(t_{m+1}), p^2\nu(t_{m+1})\},$$

and the inequality is an equality, unless $e_1 + p\nu(t_{m+1}) = p^2\nu(t_{m+1})$, i.e., $\nu(t_{m+1}) = e_1/(p^2-p)$. Thus, there are three options,

$$\nu(t_{m+1}) = \frac{\nu(t_m) - e_1}{p}, \text{ or } \frac{\nu(t_m)}{p^2}, \text{ or } \frac{e_1}{p^2-p},$$

according to whether the minimum is attained at $e_1 + p\nu(t_{m+1})$, at $p^2\nu(t_{m+1})$, or at $e_1 + p\nu(t_{m+1}) = p^2\nu(t_{m+1})$, respectively. The first option happens when $\nu(t_{m+1}) > e_1/(p^2-p)$, and the second option when $\nu(t_{m+1}) < e_1/(p^2-p)$. Equivalently, $\nu(t_{m+1}) = (\nu(t_m) - e_1)/p$ if $\nu(t_m) > pe_1/(p-1)$, and $\nu(t_{m+1}) = \nu(t_m)/p^2$ if $\nu(t_m) \leq pe_1/(p-1)$. Let s be the smallest non-negative integer such that $e/e_1 \leq p^s(p+1)$.

(a) We shall prove by induction that $\nu(t_n) = \frac{e-p^{n-1}e_1}{(p-1)p^{n-1}}$ for all $1 \leq n \leq s+1$. The base case of $n = 1$ follows from our assumtion that $\nu(t_1) = (e-e_1)/(p-1)$. Now suppose that $1 \leq n < s+1$, and $\nu(t_n) = \frac{e-p^{n-1}e_1}{(p-1)p^{n-1}}$. Since $n-1 < s$, it follows that $e > p^{n-1}(p+1)e_1$. Thus,

$$\nu(t_n) = \frac{e-p^{n-1}e_1}{(p-1)p^{n-1}} > \frac{p^{n-1}(p+1)e_1 - p^{n-1}e_1}{(p-1)p^{n-1}} = \frac{p^{n-1}pe_1}{(p-1)p^{n-1}} = \frac{pe_1}{p-1}.$$

By our previous remarks, this inequality implies that

$$\nu(t_{n+1}) = \frac{\nu(t_n) - e_1}{p} = \frac{\frac{e-p^{n-1}e_1}{(p-1)p^{n-1}} - e_1}{p} = \frac{e-p^n e_1}{(p-1)p^n}.$$

Thus, by the principle of mathematical induction, the result follows for all $1 \leq n \leq s+1$.

(b) Here we shall show by induction that $\nu(t_n) = \frac{e-p^s e_1}{(p-1)p^{2(n-1)-s}}$ for all $n \geq s+1$. The previous case shows that $\nu(t_{s+1}) = \frac{e-p^s e_1}{(p-1)p^s}$. Since $e \leq p^s(p+1)e_1$, it follows that

$$\nu(t_{s+1}) = \frac{e-p^s e_1}{(p-1)p^s} \leq \frac{p^s(p+1)e_1 - p^s e_1}{(p-1)p^s} = \frac{p^s p e_1}{(p-1)p^s} = \frac{pe_1}{p-1}.$$

By our previous remarks, this inequality implies that

$$\nu(t_{s+2}) = \frac{\nu(t_{s+1})}{p^2} = \frac{e-p^s e_1}{(p-1)p^{s+2}} = \frac{e-p^s e_1}{(p-1)p^{2(s+2-1)-s}}.$$

Now suppose that $n > s+1$ and $\nu(t_n) = \frac{e-p^s e_1}{(p-1)p^{2(n-1)-s}}$. Since $n > s+1$, it follows that $\nu(t_n) < \nu(t_{s+1}) \leq pe_1/(p-1)$. Therefore, our previous remarks show that

$$\nu(t_{n+1}) = \frac{\nu(t_n)}{p^2} = \frac{e-p^s e_1}{(p-1)p^{2(n-1)-s+2}} = \frac{e-p^s e_1}{(p-1)p^{2((n+1)-1)-s}},$$

as desired. Hence, the principle of mathematical induction shows that

$$\nu(t_n) = \frac{e-p^s e_1}{(p-1)p^{2(n-1)-s}}$$

for all $n \geq s+1$.

□

Example 5.4. Let $E/\mathbb{Q}$ be the elliptic curve with Cremona label "27a4", given by a Weierstrass equation $y^2 + y = x^3 - 30x + 63$. The curve E has additive reduction at $p = 3$, which turns out to be potential good supersingular reduction. In this case, the good reduction is first attained over a number field $K_0 = \mathbb{Q}(\alpha, \beta)$, where α and β are roots of the polynomials $x^4 - 3$ and $x^3 - 120x + 506$, respectively. The extension $K_0/\mathbb{Q}$ is of degree 12, totally ramified at $p = 3$. We define $K = K_0\mathbb{Q}_3^{\mathrm{nr}}$. In this particular case, we have $e = 12$, and we have also calculated $e_1 = 2$.

We have calculated (using Magma) the coordinates of torsion points T_1, T_2 and T_3 in E', respectively of order 3, 9 and 27, such that $[3]T_3 = T_2$, and $[3]T_2 = T_1$. There are two non-trivial 3-torsion points defined over K (this follows from the fact that E has a 3-torsion point defined over $\mathbb{Q}$), and we let T_1 be one of them. Let $F_3/\mathbb{Q}$ and $F_9/\mathbb{Q}$ be unique extensions of degrees 3 and 9 contained in $\mathbb{Q}(\zeta_{27})/\mathbb{Q}$. Then $T_2 \in E'(KF_3)$ and $T_3 \in E'(KF_9)$. If we let $t_i = -x(T_i)/y(T_i)$, we find that

$$\nu(t_1) = 5, \quad \nu(t_2) = 1, \quad \text{and} \quad \nu(t_3) = 1/9.$$

Notice that $3 \cdot 12/4 = 9 > 2 = e_1$, thus by Lemma 5.3, the formal group has $6 \cdot 3^{2(n-1)}$ primitive roots with valuation $\frac{2}{2 \cdot 3^{2n-1}} = \frac{1}{3^{2n-1}}$. Moreover, $12/2 = 6 \leq 3 \cdot 4$, so $s = 1$. Hence,

(1) if $n \leq 2$, there are $2 \cdot 3^{2(n-1)}$ primitive roots of valuation $\frac{12-3^{n-1}\cdot 2}{2\cdot 3^{n-1}}$;
(2) if $n > 2$, there are $2 \cdot 3^{2(n-1)}$ primitive roots of valuation $\frac{12-3\cdot 2}{2\cdot 3^{2(n-1)-1}} = \frac{1}{3^{2(n-1)-2}} = \frac{1}{3^{2n-4}}$.

In particular, there are precisely two points of 3-torsion in the formal group with valuation $(e - e_1)/(p-1) = (12-2)/2 = 5$ and t_1 is one of them (the rest of the 3-torsion points, 6 of them, have valuation $1/3$). Also, there are 18 points of 9-torsion in the formal group with valuation 1, and t_2 is one of them (the other 54 torsion points of order 9 have valuation $1/27$). Finally, there are 162 roots of 27-torsion with valuation $1/9$ and t_3 is one of them (the other 486 roots of order 27 have valuation $1/243$).

Example 5.5. Let $E = E_{121c2}$ defined over $\mathbb{Q}$. As we know $e = 3$ and $e_1 = 1$ for $p = 11$. Since $33/12 > 1$, it follows from Lemma 5.3 that $[11^n](X) = 0$ has $110 \cdot 11^{2(n-1)}$ primitive roots with valuation $\frac{1}{10 \cdot 11^{2n-1}}$, for all $n \geq 1$. Moreover, $e/e_1 = 3 \leq 12$ implies that $s = 0$, and so for all $n \geq 1$, there are $10 \cdot 11^{2(n-1)}$ primitive roots of valuation $\frac{1}{5 \cdot 11^{2(n-1)}}$. In particular, when $n = 1$, there are 110 roots with valuation $1/110$, and 10 roots with $1/5$.

Proposition 5.6. *Let E/L be an elliptic curve with potential good supersingular reduction at a prime p. Let K be the smallest extension of $L_\wp^{nr}$ such that E/K has good (supersingular) reduction at p, and let $e = \nu(p)$ and $e_1 = \nu(s_p)$ be defined as above.*

1. *If $pe/(p+1) \leq e_1$, then the ramification index in the extension $K(T_n)/K$ is divisible by $(p^2-1)p^{2(n-1)}/\gcd(e, (p^2-1)p^{2(n-1)})$, where $T_n \in E[p^n]$ is an arbitrary torsion point on E of exact order p^n.*
2. *If $pe/(p+1) > e_1$, then there are $(p^2-p)p^{2(n-1)}$ torsion points $T_n \in E[p^n]$ such that the ramification index in $K(T_n)/K$ is divisible by $(p-1)p^{2n-1}/\gcd(e_1, (p-1)p^{2n-1})$. Moreover, let s be the smallest non-negative integer such that $e/e_1 \leq p^s(p+1)$. Then,*
   (a) *if $n \leq s+1$, there are $(p-1)p^{2(n-1)}$ points $T_n \in E[p^n]$ such that the ramification index in $K(T_n)/K$ is divisible by $(p-1)p^{n-1}/\gcd(e - p^{n-1}e_1, (p-1)p^{n-1})$;*
   (b) *if $n > s+1$, there are $(p-1)p^{2(n-1)}$ points $T_n \in E[p^n]$ such that the ramification index in $K(T_n)/K$ is divisible by $(p-1)p^{2(n-1)-s}/\gcd(e - p^s e_1, (p-1)p^{2(n-1)-s})$.*

In all cases, there is a number $c = c(E/L, T, \wp)$ with $1 \leq c \leq e \leq 24e(\wp|p)$ such that if $T \in E[p^n]$ is of order p^n, then the ramification index in $K(T)/K$ is divisible by $\varphi(p^n)/\gcd(c, \varphi(p^n))$.

Proof. Let $T_n \in E[p^n]$ be an arbitrary point on $E(\overline{K})$ of exact order p^n, and write $T_i = [p^{n-i}]T_n$, for $i = 1, \ldots, n$. Also, write t_i for the corresponding torsion point in the formal group, i.e., $t_i = t(T_i) = -x(T_i)/y(T_i) \in \widehat{E}(\mathcal{M})$. The proposition now follows from Lemma 5.3. In the last statement, we simply pick $c = e$, e_1, $e - p^{n-1}e_1$, or $e - p^s e_1$. Notice that if $pe/(p+1) > e_1$, then $e > e_1$. Thus, in all cases, $1 \leq c \leq e$. □

The previous proposition has the following asymptotic consequence for the growth of ramification indices.

Corollary 5.7. *Let E/L be an elliptic curve with potential good supersingular reduction at a prime p. Let K be the smallest extension of $L_\wp^{nr}$ such that E/K has good (supersingular) reduction at p. Let $\{T_n \in E[p^n]\}_{n=1}^\infty$ be an arbitrary sequence of torsion points, such that T_n has exact order p^n. Then, there is an integer $m = m(E/K) \geq 1$ such that*

$$e(K(T_{n+1})/K) = e(K(T_n)/K) \cdot p^2,$$

for all $n \geq m$.

Proof. The statement follows directly from Proposition 5.6, by letting

$$m = \max\{s+1, \lceil(\nu_p(e)+2)/2\rceil, \lceil(\nu_p(e-p^s e_1)+s+2)/2\rceil\}$$

where $\lceil\cdot\rceil$ is the integer ceiling function. □

Remark 5.8. 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 $\iota : \overline{L} \hookrightarrow \overline{L}_\wp$ 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 $g = [K(T) : K]$.

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,*

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.*

Proof. Since $F(\eta)$ is a divisor of $F(\eta')$ (respectively, $F(\eta)$ is a divisor of $F_0(\eta')$) whenever $\eta \leq \eta'$, it suffices to show the theorem when $e(\wp|p) = \eta$. By Proposition 5.6 and Remark 5.8 it follows that $e(\mathfrak{P}|\wp)$ is divisible by one of the following quantities:

$$\frac{(p^2-1)p^{2(n-1)}}{\gcd((p^2-1)p^{2(n-1)}, e)}, \quad \text{or} \quad \frac{(p-1)p^{2n-1}}{\gcd((p-1)p^{2n-1}, e_1)},$$

$$\text{or} \quad \frac{(p-1)p^{n-1}}{\gcd((p-1)p^{n-1}, e - p^{n-1}e_1)} \quad \text{if } n \leq s+1,$$

$$\text{or} \quad \frac{(p-1)p^{2(n-1)-s}}{\gcd((p-1)p^{2(n-1)-s}, e - p^s e_1)} \quad \text{if } n > s+1,$$

where s is the smallest non-negative integer such that $e/e_1 \le p^s(p+1)$, so we define $c = e$, e_1, $e - p^{n-1}e_1$, or $e - p^s e_1$ accordingly, and it follows that $1 \le c \le e$, so the bounds on c follow from the discussion on the possible values of e at the beginning of Section 2. Hence, in all cases $e(\mathfrak{P}|\wp)$ is divisible by $(p-1)p^{n-1}/\gcd((p-1)p^{n-1}, c)$.

By Corollary 4.5, there is a constant $f(\eta, p)$ such that e, e_1, $e - p^{n-1}e_1$, and $e - p^s e_1$ are divisors of $f(\eta, p)$, so $c | f(\eta, p)$ as well. Moreover, $f(\eta, p)$ divides $F(\eta)$, and $f(\eta, p)$ divides $F_0(\eta)$ for $p > 3$. Hence, in all cases $e(\mathfrak{P}|\wp)$ is divisible by $\varphi(p^n)/\gcd(\varphi(p^n), F(\eta))$. This shows (1).

Let σ be the smallest non-negative integer such that $8\eta \le 2^\sigma$ (or such that $\eta \le 5^\sigma$, if $p > 3$). Since $e = e/e(\wp|p) \cdot e(\wp|p)$, and $e' = e/e(\wp|p)$ is ≤ 24 (resp. ≤ 6, if $p > 3$), then

$$e/e_1 \le 24\eta \le 3 \cdot 2^\sigma \le p^\sigma(p+1)$$

(resp. $e/e_1 \le 12\eta \le 6 \cdot 5^\sigma \le p^\sigma(p+1)$ if $p \ge 5$). Since s is smallest such that $p^s(p+1) \ge e/e_1$, it follows that $s \le \sigma$. Hence, if $n > \sigma + 1$, then $n > s + 1$ and $e(\mathfrak{P}|\wp)$ is divisible by one of

$$\frac{(p^2-1)p^{2(n-1)}}{\gcd((p^2-1)p^{2(n-1)}, c)}, \quad \text{or} \quad \frac{(p-1)p^{2n-1}}{\gcd((p-1)p^{2n-1}, c)}, \text{ or } \quad \frac{(p-1)p^{2(n-1)-s}}{\gcd((p-1)p^{2(n-1)-s}, c)},$$

or with c replaced by $F(\eta)$. Hence, in all cases $e(\mathfrak{P}|\wp)$ is divisible by the quantity

$$(p-1)p^{2(n-1)-s}/\gcd((p-1)p^{2(n-1)-s}, c).$$

This shows (2).

By Corollary 4.8, if $p > 3\eta \ge 3e(\wp|p)$, then e, e_1, $e - p^{n-1}e_1$, and $e - p^s e_1$ are not divisible by p. It follows that $e(\mathfrak{P}|\wp)$ is divisible by $(p-1)p^{n-1}/\gcd(p-1, c)$, and it is divisible by $(p-1)p^{2(n-1)-s}/\gcd(p-1, c)$ if $n > \sigma + 1$, and with c replaced by $F(\eta)$. This shows (3).

If $\eta = e(\wp|p) \le 1$ and $p > 3$, Corollary 4.5 says that e divides 4 or 6, and e_1, $e - e_1$, are divisors of 4 (note that $e/e_1 \le p + 1$ for all $p > 3$, so $s = 0$). Hence, $e(\mathfrak{P}|\wp)$ is divisible by one of

$$\frac{(p^2-1)p^{2(n-1)}}{\gcd(p^2-1, 6)}, \text{ or } \frac{(p^2-1)p^{2(n-1)}}{\gcd(p^2-1, 4)}, \text{ or } \frac{(p-1)p^{2n-1}}{\gcd(p-1, 4)}, \text{ or } \frac{(p-1)p^{2(n-1)}}{\gcd(p-1, 4)}.$$

It follows that $e(\mathfrak{P}|\wp)$ is divisible by $(p^2-1)p^{2(n-1)}/6$ or $(p-1)p^{2(n-1)}/\gcd(p-1, 4)$. If $d = 1$ and $p = 3$, then $e(\mathfrak{P}|\wp)$ is divisible by $\varphi(3^n)/\gcd(\varphi(3^n), c)$ where $1 \le c \le 12$. Since $\varphi(3^n) = 2 \cdot 3^{n-1}$, it is also divisible by $\varphi(3^n)/\gcd(\varphi(3^n), t)$ with $t = 6$ or 9. This shows (4) and concludes the proof of the theorem. □

Example 5.10. Let $E/\mathbb{Q}$ be the elliptic curve with Cremona label "27a4", given by a Weierstrass equation $y^2 + y = x^3 - 30x + 63$. We have seen in Example 5.4 that for this curve and $p = 3$, we have $e = 12$ and $e_1 = 2$. In particular $pe/(p+1) = 3 \cdot 12/4 = 9 > 2$ and Proposition 5.6 implies that, for all $n \ge 1$, there are $6 \cdot 3^{2n-2}$ points T_n in $E(\overline{\mathbb{Q}}_3)[3^n]$ such that the ramification index in $K(T_n)/K$ is divisible by $2 \cdot 3^{2n-1}/(\gcd(3^{2n-1} \cdot 2, 2)) = 3^{2n-1}$.

Let $T_i \in E[3^i]$ for $i = 1, 2, 3$ be the torsion points defined in Example 5.4. We also defined $t_i = -x(T_i)/y(T_i)$, and we found that $\nu(t_1) = 5$, $\nu(t_2) = 1$, and $\nu(t_3) = 1/9$. Since $\nu(t_3) < \min\{12, 2\} = 2$, Lemma 5.1 implies that for all $n \ge 3$, and all $T_n \in E[3^n]$ such that $[3^{n-3}](T_n) = T_3$ we have $\nu(t_n) = \frac{\nu(t_3)}{3^{2(n-3)}} = \frac{1}{3^{2n-4}}$. Thus, the ramification index of $K(T_n)/K$ is divisible by 3^{2n-4}, when $n \ge 3$.

In all cases, we find that, if T_n is any point of exact order 3^n and $n \ge 3$, then the ramification index of $K(T_n)/K$ is divisible either 3^{2n-1} or by 3^{2n-4}, so it is divisible by, at least, 3^{2n-4}. Thus,

Remark 5.8 implies that if $R \in E(\overline{\mathbb{Q}})$ is a point of exact order 3^n with $n \geq 3$, then the ramification index of any prime lying above 3 in the extension $\mathbb{Q}(R)/\mathbb{Q}$ is divisible by 3^{2n-4}.

Example 5.11. Let $E = E_{121c2}$ defined over $\mathbb{Q}$. As we know $e = 3$ and $e_1 = 1$ for $p = 11$. Since $33/12 > 1$, by Prop. 5.6, there are $110 \cdot 11^{2(n-1)}$ torsion points $T_n \in E[p^n]$ such that $c(E/\mathbb{Q}, T_n, 11) = e_1 = 1$ and, therefore, the ramification index in $\mathbb{Q}(T_n)/\mathbb{Q}$ is divisible by $10 \cdot 11^{2n-1}$. Moreover, $e/e_1 = 3 \leq 12$, so $s = 0$, and there are $10 \cdot 11^{2(n-1)}$ points $T_n \in E[p^n]$ such that $c(E/\mathbb{Q}, T_n, 11) = e - e_1 = 2$, and the ramification index in $\mathbb{Q}(T_n)/\mathbb{Q}$ is divisible by $5 \cdot 11^{2(n-1)}$ for all $n \geq 1$. In particular, if T_n is any point of order 11^n, then the ramification index at 11 in $\mathbb{Q}(T_n)/\mathbb{Q}$ is divisible by $5 \cdot 11^{2(n-1)}$ for all $n \geq 1$.

Let $F = \mathbb{Q}(\zeta_{11})$ be the 11th cyclotomic field, and let $\zeta = \zeta_{11}$ be a primitive 11th root of unity. Then, E has a point of exact order 11 defined over F, namely

$$\begin{aligned} T_1 = (&-22\zeta^9 - 11\zeta^7 - 11\zeta^6 - 11\zeta^5 - 11\zeta^4 - 22\zeta^2 + 17, \\ &-77\zeta^9 - 33\zeta^8 - 132\zeta^7 - 33\zeta^6 - 33\zeta^5 - 132\zeta^4 - 33\zeta^3 - 77\zeta^2 - 201). \end{aligned}$$

Moreover, notice that both $x(T_1)$ and $y(T_1)$ are fixed by complex conjugation and, therefore, T_1 is defined over $F^+ = \mathbb{Q}(\zeta_{11})^+$, the maximal real subfield of F. Moreover, one can verify that $\mathbb{Q}(T_1) = F^+$. Thus, the ramification index of 11 in $\mathbb{Q}(T_1)/\mathbb{Q}$ is 5, which is the smallest it can be, since it must be divisible by $5 \cdot 11^{2(n-1)}$ with $n = 1$.

We finish this section with a result on the behavior of ramification under quadratic twists.

Proposition 5.12. *Let E/L be an elliptic curve with potential supersingular reduction at a prime ideal $\wp$ above $p \geq 3$, and let $T_n \in E[p^n]$ be a point of exact order p^n. Let K be the smallest extension of $L_\wp^{nr}$ such that E/K has good reduction, let ν be a normalized valuation on K, and let $e = \nu(p)$ and $e_1 = \nu(s_p)$ defined as usual. Let E'/L be a quadratic twist of E, such that E and E are isomorphic over a quadratic extension F/L, and let K', ν', e', and e_1' be the analogous items attached to E'.*

1. *If F/L is unramified at $\wp$, then $e = e'$ and $e_1 = e_1'$, and the results of Proposition 5.6 apply equally to E or E'.*
2. *Otherwise, assume that F/L is ramified at $\wp$. If $K/L_\wp^{nr}$ contains a quadratic ramified extension, then $e = e'$ and $e_1 = e_1'$, and the results of Proposition 5.6 apply equally to E or E'.*
3. *Finally, assume that F/L is ramified at $\wp$, and assume further that $L(x(T_n))$ contains a quadratic extension H/L ramified at $\wp$. Let $T_n' \in E'[p^n]$ be the point on E' that corresponds to T_n on $E[p^n]$. Then, $L(T_n)/L$ and $L(T_n')/L$ have the same ramification properties for primes that lie above $\wp$.*

Proof. Part (1) is clear, since $FK = K$. For part (2), let $K_0/L_\wp^{\mathrm{nr}}$ be the quadratic extension contained in $K/L_\wp^{\mathrm{nr}}$. Then $FL_\wp^{\mathrm{nr}} = K_0$. Thus, $FK = K$ and, by Lemma 4.10, we have $K = K'$, and the result follows. Finally, for (3), we have $L(x(T_n)) = L(x(T_n'))$ by Lemma 4.11. Let us fix an embedding $\iota : \overline{L} \hookrightarrow \overline{L}_\wp$ and put $\mathcal{F}_n = \iota(L(T_n))$ and $\mathcal{F}_n' = \iota(L(T_n'))$. Since $p \geq 3$, it follows that $FL_\wp^{\mathrm{nr}} = HL_\wp^{\mathrm{nr}}$, therefore $FL_\wp^{\mathrm{nr}} \subseteq \mathcal{F}_n$, and $FL_\wp^{\mathrm{nr}} \subseteq \mathcal{F}_n'$. Since $E \cong_F E'$, it follows that

$$\mathcal{F}_n L_\wp^{\mathrm{nr}} = \iota(L(T_n))FL_\wp^{\mathrm{nr}} = \iota(L(T_n'))FL_\wp^{\mathrm{nr}} = \mathcal{F}_n' L_\wp^{\mathrm{nr}},$$

and the result follows. □

6. Examples from $X_0(p^n)$

In this last section, we discuss examples of elliptic curves with potential supersingular reduction that appear associated to non-cuspidal rational points on a modular curve $X_0(p^n)$ for some prime p and $n \geq 1$.

Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational cyclic isogeny ϕ of degree p^n. Then, the pair (E, C) with $C = \mathrm{Ker}(\phi)$ corresponds to a $\mathbb{Q}$-rational point on the modular curve $X_0(p^n)$. Conversely, following [1], each non-cuspidal $\mathbb{Q}$-rational point on $X_0(p^n)$ comes from such a pair $(E/\mathbb{Q}, \langle R \rangle)$, with $R \in E[p^n]$. The rational points on the modular curves $X_0(p^n)$ have been completely classified (see, for example, Section 9.1 and Tables 2, 3, and 4 of [5]). Here, in Table 2, we list 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 (and provide the Cremona labels for curves with the given j-invariant and least conductor). We remark here that $X_0(27)$, $X_0(11)$, $X_0(17)$, and $X_0(19)$ have genus 1, but only contain finitely many $\mathbb{Q}$-rational points.

Table 2: Elliptic curves with pot. supersingular reduction on $X_0(p^n)$ of genus ≥ 1

j-invariant	p	n	Cremona Label(s)	Good reduction over	e	e_1
$j = -2^{15} \cdot 3 \cdot 5^3$	3	3	27a2, 27a4	$\mathbb{Q}(\sqrt[4]{3}, \beta^3 - 120\beta + 506 = 0)$	12	2
$j = -11 \cdot 131^3$	11	1	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	1	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	1	361a1, 361a2	$\mathbb{Q}(\sqrt[4]{19})$	4	2
$j = -2^{18} \cdot 3^3 \cdot 5^3$	43	1	1849a1, 1849a2	$\mathbb{Q}(\sqrt[4]{43})$	4	2
$j = -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	67	1	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	1	26569a1, 26569a2	$\mathbb{Q}(\sqrt[4]{163})$	4	2

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 $n \geq 3$.*

Proof. With the notation of the statement of the theorem, fix a prime $\Omega_\wp$ of $\overline{\mathbb{Q}}$ that lies above $\wp$, and let $\iota_\wp : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ be the embedding associated to $\Omega_\wp$. We divide the j-invariants in three subsets:

- Let $j_0 = -2^{15} \cdot 3 \cdot 5^3$ and $p = 3$. Let $E/\mathbb{Q}$ be the elliptic curve with Cremona label "27a4". Then, we have worked out in Example 5.10 that, for all $n \geq 3$, the ramification index of $\mathbb{Q}_3(\iota(T_n))/\mathbb{Q}_3$ is divisible by 3^{2n-4}. Hence, the ramification of $\wp$ over p in the extension

$\mathbb{Q}(T_n)/\mathbb{Q}$ is also divisible by 3^{2n-4}. Since the smallest field extension of $\mathbb{Q}_3^{\mathrm{nr}}$ such that E acquires good reduction is given by $K = \mathbb{Q}_3^{\mathrm{nr}}(\sqrt[4]{3}, \beta^3 - 120\beta + 506 = 0)$ (see Table 2), it follows that $K/\mathbb{Q}_3^{\mathrm{nr}}$ contains the quadratic extension $\mathbb{Q}_3^{\mathrm{nr}}(\sqrt{3})/\mathbb{Q}_3^{\mathrm{nr}}$, and therefore, by Proposition 5.12, parts (1) and (2), any quadratic twist of $E/\mathbb{Q}$ shares the same ramification properties in the extension $\mathbb{Q}(T_n)/\mathbb{Q}$. Since any elliptic curve over $\mathbb{Q}$ with $j = j(E)$ is a quadratic twist of $E/\mathbb{Q}$ (by Lemma 4.11), we are done.

- Let j_0 be one of the j-invariants with $p = 11$, 19, 43, 67 or 163, and let $E/\mathbb{Q}$ be one of the elliptic curves with Cremona label as listed in Table 2. From the same table, we see that in all cases $e - e_1$ and e_1 are 1 or 2. If $E/\mathbb{Q}$ is replaced by a quadratic twist, then Lemma 4.10 says that the quantities (e, e_1) stay the same or are replaced by $(2e, 2e_1)$, and $2e-2e_1$ and $2e_1$ are 2 or 4. (Notice that, in fact, in [4], Cor. 4.6, we have shown that if E/L has potential supersingular reduction at $\wp$, with $e(\wp|p) = 1$, and $e_1 < e$, then $e - e_1$ and e_1 can only take the values $1, 2$, or 4). Moreover, in all cases $p \equiv 3 \bmod 4$, so $\gcd(p(p-1), 4) = \gcd(p(p-1), 4) = 2$. Also, in all cases it can be easily verified that $pe/(p+1) > e_1$ and, equivalently, $p(2e)/(p+1) > 2e_1$. Therefore, Proposition 5.6 implies that the ramification index in the extension $K(\iota(T_n))/K$ is divisible by $(p-1)p^{2n-2}/2$. Hence, by Remark 5.8, the ramification index of $\wp$ over p in the extension $\mathbb{Q}(T_n)/\mathbb{Q}$ is divisible by $(p-1)p^{2n-2}/2$ for any elliptic curve with $j = j_0$.

- Let j_0 be one of the two j-invariants with $p = 17$. Let $E/\mathbb{Q}$ be the elliptic curve with Cremona label "14450p1". Let T_n be a point of exact order 17^n on E. We claim that $\mathbb{Q}(x(T_n))$ contains $\mathbb{Q}(\sqrt{17})$. First notice that, if $T_1 = [p^{n-1}]T_n \in E[17]$, then $\mathbb{Q}(x(T_1)) \subseteq \mathbb{Q}(x(T_n))$ because the function $f = x \circ [17^{n-1}]$ is even, and therefore lies in the function field $\mathbb{Q}(x)$ (see [12], Cor. 2.3.1). The x-coordinate of T_1 is a root of $\psi_{17}(x)$, the 17th division polynomial of E. The division polynomial factors as $\psi_{17}(x) = s_1(x)s_2(x)$, where $s_1(x)$ and $s_2(x)$ have degrees 8 and 144 respectively. Let α_i be a root of $s_i(x)$, for $i = 1, 2$. We have verified with the software Magma that $\mathbb{Q}(\sqrt{17}) \subseteq \mathbb{Q}(\alpha_i)$ for both $i = 1$ and 2. Therefore, $\mathbb{Q}(\sqrt{17}) \subseteq \mathbb{Q}(x(T_1)) \subseteq \mathbb{Q}(x(T_n))$.

  Similarly, if we let $E'/\mathbb{Q}$ be the curve with label "14450p2", the 17th division polynomial factors as $\psi_{17}(x) = s_1(x)s_2(x)s_3(x)$ where the polynomials s_i have degrees 4, 4 and 136, respectively for $i = 1$, 2, and 3. Let α_i be a root of $s_i(x)$. We have also verified with the software Magma that $\mathbb{Q}(\sqrt{17}) \subseteq \mathbb{Q}(\alpha_i)$ for both $i = 1$, 2, and 3. Therefore, $\mathbb{Q}(\sqrt{17}) \subseteq \mathbb{Q}(x(T_1)) \subseteq \mathbb{Q}(x(T_n))$, for any $T_n \in E'$ of order 17^n.

  In particular, if $T_n \in E$ or E', parts (1) and (3) of our Proposition 5.12 imply that the ramification properties at p of $\mathbb{Q}(T_n)$ are invariant under quadratic twists, and therefore it suffices to show the theorem for E and E'. From Table 2 we see that, for E we have $(e - e_1, e_1) = (1, 2)$, and for E' we have $(e - e_1, e_1) = (2, 1)$. Hence, $\gcd(17 \cdot 16, e - e_1)$ and $\gcd(17 \cdot 16, e_1)$ are both ≤ 2. Moreover, in both cases $pe/(p+1) > e_1$ for $p = 17$. Hence, by Proposition 5.6 and Remark 5.8, we have that the ramification index of $\wp$ over (17) in the extension $\mathbb{Q}(T_n)/\mathbb{Q}$ is divisible by $16 \cdot 17^{2n-2}/2 = 8 \cdot 17^{2n-2}$, for all $n \geq 1$, as desired.

□

We conclude the paper with an example of an elliptic curve defined over a quadratic number field L, which appears as a non-cuspidal L-point on $X_0(13)(L)$.

Example 6.2. Let j_0 be a root of the polynomial

$$x^2 - 6896880000x - 567663552000000,$$

and let $L = \mathbb{Q}(j_0) = \mathbb{Q}(\sqrt{13})$. Let $p = 13$ and let $\wp = (\sqrt{13})$ be the ideal above p in $\mathcal{O}_L$. Let E/L be the elliptic curve with j-invariant equal to j_0. The curve E has complex multiplication by $\mathbb{Z}[\sqrt{-13}]$, i.e., $\mathrm{End}(E/\mathbb{C}) \cong \mathbb{Z}[\sqrt{-13}]$ and, in fact, all the endomorphisms are defined over $\mathbb{Q}(\sqrt{13}, i)$, see [13], Chapter 2, Theorem 2.2(b)). Since 13 ramifies in L, it follows from Deuring's criterion (see [3], Ch. 13, §4, Theorem 12) that the reduction of E at $\wp$ is potential supersingular. We choose a model for E/L given by

$$y^2 = x^3 + \frac{5231j_0 - 50692880808000}{3825792}x + \frac{-550711j_0 + 4485396184200000}{239112}.$$

The discriminant of this model is $\Delta_L = \frac{1354649517689000 0j_0 - 93429639900045292464000000}{29889}$ and $\nu_\wp(\Delta_L) = 0$. Hence, E/L has good supersingular reduction at $\wp$. In particular $K_E = L_\wp^{\mathrm{nr}}$ and $e = 2$. Since $p = 13 \equiv 1 \bmod 12$, we have $r(13) = s(13) = 0$, and we may use Theorem 3.3 to verify that $e_1 = 1$. Here $e(\wp|p) = 2$, and we know from Example 3.2 that $Q_{13}(T) = -349920T - 75582720$. One can verify (using Sage or Magma) that

$$\nu_\wp(Q_{13}(j_0)) = \nu_\wp(-349920j_0 - 75582720) = 1.$$

Thus,

$$\lambda = \nu_K(Q_{13}(j(E)) = \nu_\wp(Q_{13}(j_0)) = 1.$$

Since $1 = \lambda < 2 = e$, it follows from Theorem 3.3 that $e_1 = \lambda = 1$, as claimed.

Since $26/14 > 1$ and $e_1 = 1$, Proposition 5.6 and Remark 5.8 imply that there are $156 \cdot 13^{2(n-1)}$ torsion points $T_n \in E[p^n]$ such that the ramification index in $L(T_n)/L$ is divisible by $12 \cdot 13^{2n-1}$. Moreover, $2 \leq 14$ so $s = 0$, and $e - e_1 = 1$. Thus, there are $12 \cdot 13^{2(n-1)}$ points $T_n \in E[p^n]$ such that the ramification index in $L(T_n)/L$ is divisible by $12 \cdot 13^{2(n-1)}$.

References

[1] P. Deligne, M. Rapoport, *Les schémas de modules des courbes elliptiques*, in Modular Functions of One Variable II, Springer Lecture Notes in Mathematics 349 (1973), pp. 143-316. 6

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

[3] S. Lang, *Elliptic functions*, Second Edition, Springer-Verlag, New Tork, 1987. 6.2

[4] Á. Lozano-Robledo, *Formal groups of elliptic curves with potential good supersingular reduction*, Pacific Journal of Mathematics, 261 (2013), no. (1), 145-164. 1, 2, 2.5, 3, 3.3, 4, 6

[5] 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, 6

[6] Á. Lozano-Robledo, *Uniform boundedness in terms of ramification*, preprint. 1.4, 2

[7] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), no. 1-3, 437-449. 1.1

[8] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Inst. Hautes Etudes Sci. Publ. Math. (1964), No. 21, pp. 128. 3, 2

[9] P. Parent. *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. 506 (1999). 1.1

[10] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), pp. 259-331. 3, 2, 5

[11] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, Ann. of Math. 88 (1968), pp. 492 - 517. 2

[12] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 2nd Edition, New York, 2009. 2, 3.3, 4, 4, 5, 6

[13] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York. 6.2

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