# Ramification in the Division Fields of Elliptic Curves and an Application to Sporadic Points on Modular Curves

HANSON SMITH

Abstract. Consider an elliptic curve $E$ over a number field $K$ and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ lying above a prime $p$ of $\mathbb{Z}$. Suppose $E$ has supersingular reduction at $\mathfrak{p}$. Fix a positive integer $n$ and define $L$ to be a minimal extension of $K$ such that $E(L)$ has a point of exact order $p^n$. If $\mathfrak{p}$ is unramified over $p$, we show that $L/K$ is an extension of degree $p^{2n} - p^{2n-2}$ that is totally ramified over $\mathfrak{p}$. If $\mathfrak{p}$ is ramified over $p$, we are still able to show that $\varphi(p^n)$ properly divides $[L : \mathbb{Q}]$.

We apply our stronger bound to show that sporadic points on the modular curve $X_1(p^n)$ cannot correspond to elliptic curves that are supersingular at $\mathfrak{p}$ with $\mathfrak{p}$ unramified over $p$. Our methods are then generalized to $X_1(N)$ with $N$ composite. We also describe ramification at and away from $p$ in the full $p^n$-th division field $K(E[p^n])$. In the course of our investigation, we correct a theorem of Cassels.

## 1. Previous Work and Motivation

Before we formally introduce our results, we would like to motivate them by surveying previous work. Those immediately interested in our results are advised to proceed to Section 2.

Previous work in the area we consider has a variety of different thrusts. Division fields of elliptic curves have a strong analogy with cyclotomic fields. Motivated by this analogy, one can work to describe splitting, ramification, and inertia explicitly in division fields. To this end, Adelmann's book [1] provides a nice introduction culminating in criteria describing the decomposition of unramified primes in various division fields. In [23], Kraus completely describes the $p$-adic valuation of the different of the $p^{\text{th}}$ division field in terms of the $p$-adic valuation of $j(E)$ and the reduction type of $E$. With [3], Cali and Kraus describe the $p$-adic valuation of the different of the $l^{\text{th}}$ division field when $p \neq l$. Between these two papers, the differents of prime division fields have been completely described. In a recent paper [15], Freitas and Kraus fully classify the degree of $\mathbb{Q}_p(E[l])$ over $\mathbb{Q}_p$ when $l \neq p$.

In [22], Kida gives criteria for ramification in the division field $K(E[p^n])$ for all primes not equal to $p$. Kida also gives a criterion for wild ramification and, as an application, classifies quadratic fields with class number divisible by 3. If $E$ is an elliptic curve over $\mathbb{Q}$, González-Jiménez and Lozano-Robledo [16] classify and

---

*Date*: October 30, 2018.

2010 *Mathematics Subject Classification.* Primary 11G05, Secondary 14H52.

*Key words and phrases.* elliptic curves, torsion points, division fields, torsion fields, division polynomials, sporadic points, modular curves.

The author would like to thank Álvaro Lozano-Robledo for the helpful correspondence. The author would also like to thank Kate Stange for the patient advice and direction.

parametrize all division fields $\mathbb{Q}(E[n])$ that are contained within a cyclotomic field. In other words, they classify the division fields that have an abelian Galois group. In particular, they show this is only possible for $n = 2, 3, 4, 5, 6, 8$. Further, they describe all the Galois groups which occur. With [25], Lozano-Robledo constructs division fields with minimal ramification. That is, the author finds elliptic curves such that $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ and the ramification index above $p$ is exactly $\varphi(p^n)$. Informally speaking, these division fields have Galois groups that are as large as possible and ramification over $p$ that is as small as possible. Duke and Tóth's explicit computation of the Frobenius in [14] describes the splitting of primes not dividing $n$ or the discriminant of the elliptic curve in the division field $K(E[n])$. They then give an application to nonsolvable quintic extensions. In [7], Centeleghe works to find the structure of the Tate module $T_l(E)$ and uses this to give a criterion for whether a prime splits completely in the $n$-division field.

Describing $E(K)_{\text{tors}}$ is another motivation for the study at hand. Consider the following two questions.

*Question* 1.1. Fix a degree $d$ or a Galois group $G$ and suppose $K$ has that degree or that Galois group. What are the possibilities for the group $E(K)_{\text{tors}}$?

*Question* 1.2. Is there an upper bound for $|E(K)_{\text{tors}}|$ depending on $d$?

With [29] and [30] Mazur showed $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/N\mathbb{Z} \qquad \text{with } 1 \leq N \leq 10 \text{ or } N = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \qquad \text{with } 1 \leq N \leq 4.$$

This answers Question 1.1 when $d = 1$.

For $d = 2$, Kamienny, Kenku, and Momose (culminating with [21] and [20]) show that $E(K)_{\text{tors}}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/N\mathbb{Z} \qquad \text{with } 1 \leq N \leq 16 \text{ or } N = 18,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \qquad \text{with } 1 \leq N \leq 6,$$
$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3N\mathbb{Z} \qquad \text{with } 1 \leq N \leq 2,$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

The proofs of these results rely on carefully analyzing modular curves. In both the $d = 1$ and $d = 2$ case, there are infinite families of elliptic curves having each of the possible torsion subgroups. This means there are infinitely many points on the corresponding modular curve of the given degree. For $d \geq 3$, this is no longer the case. That is, there are modular curves with only finitely many degree $d$ points. For example, let $E$ be the elliptic curve with Cremona label 162b1. Najman [33] has shown

$$E\left(\mathbb{Q}(\zeta_9)^+\right) \cong \mathbb{Z}/21\mathbb{Z}.$$

However, it is known that only finitely many elliptic curves can have this torsion subgroup over a cubic field. See Jeon, Kim, and Schweizer's paper [19] for a list of the possible torsion subgroups that can occur for infinitely many elliptic curves over a cubic field. The point on the modular curve $X_1(21)$ corresponding to $E$ is an example of a *sporadic point*. Briefly, if $D$ is the minimal degree such that a curve $X$ has infinitely many points of degree $D$, then a sporadic point is any point with degree less than $D$.

Recently, Derickx, Etropolski, van Hoeij, Morrow, and Zureick-Brown have announced that $X_1(21)$ is the only modular curve with cubic sporadic points [11]. Combined with the work of Jeon, Kim, and Schweizer [19], this shows that when $[K : \mathbb{Q}] = 3$ then $E(K)_{\text{tors}}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/N\mathbb{Z} \qquad \text{for } 1 \leq N \leq 21 \text{ with } N \neq 17, 19,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \qquad \text{with } 1 \leq N \leq 7.$$

Thus, in order to answer Question 1.1 more generally, it seems likely we will need to have a better understanding of sporadic points on modular curves. To this end, Bourdon, Ejder, Liu, Odumodu, and Viray [2] have recently shown that, assuming Serre's uniformity conjecture, the number of sporadic $j$-invariants ($j$-invariants corresponding to sporadic points on some modular curve $X_1(N)$) in a given number field is finite.

Regarding Question 1.2, Merel [31] answered it in the affirmative. Namely, Merel showed that there is a uniform bound for $|E(K)_{\text{tors}}|$ that is independent of the curve $E/K$ and depends only on $d$. Further, Merel found that if $p$ divides $|E(K)_{\text{tors}}|$, then

$$p \leq d^{3d^2}.$$

Oesterlé later improved the bound to

$$p \leq \left(1 + 3^{\frac{d}{2}}\right)^2;$$

however, this work was unpublished. Thanks to the work of Derickx, a proof can now be found in [10, Appendix A]. Parent [34] showed that if $E$ has a point of order $p^n$, then

$$p^n \leq 129(5^d - 1)(3d)^6.$$

It is believed that the best possible bound on $|E(K)_{\text{tors}}|$ should be a polynomial in $d$. To this end Lozano-Robledo has conjectured [27]:

**Conjecture 1.3.** *There is a constant $C$ depending only on $d$ such that if $E$ has a point of order $p^n$, then*

$$\varphi(p^n) \leq C \cdot d.$$

Lozano-Robledo has made significant strides toward this conjecture by considering ramification in the fields of definition of $p^n$-torsion points. This investigation culminates in [27, Theorem 1.9]:

**Theorem 1.4.** *Fix a number field $L$ and suppose $E$ is defined over $L$. Further, suppose $p$ is odd and let $K$ be a finite extension of $L$ of degree $d$ over $\mathbb{Q}$. Then, there is a constant $C_L$, depending on $L$ such that if $p^n$ divides $|E(K)_{tors}|$, then*

$$\varphi(p^n) \leq C_L \cdot d.$$

In the case where $E$ has potential supersingular reduction, Lozano-Robledo has shown Conjecture 1.3 with $C = 24$. This work is initiated in [24] and completed in [26]. With Theorem 5.4, we will show that when $E$ has supersingular reduction we can take $C = 1$. More precisely, when $E$ has supersingular reduction at a prime above $p$, we show $\varphi(p^n)$ is a proper divisor of $d$.

## 2. Results

We begin by establishing some notation and conventions. Let $E$ be an elliptic curve over a number field $K$ and let $p \in \mathbb{Z}$ be a prime. Unless otherwise indicated, $\mathfrak{p}$ is a prime of $K$ lying over $p$ at which $E$ has good supersingular reduction. If $M$ is an extension of $K$ and $\mathfrak{p}_M$ is a prime of $M$ lying over $\mathfrak{p}$, then the ramification index of $\mathfrak{p}_M$ over $\mathfrak{p}$ will be denoted $e(\mathfrak{p}_M \mid \mathfrak{p})$.

Let $n$ be a positive integer. Generally, we will denote a point of exact order $p^n$ on $E$ by $P$. We call a minimal extension of $K$ over which $E$ has a point of order $p^n$ a *minimal $p^n$-torsion point field*. Fix a *minimal $p^n$-torsion point field* and denote it $L$. We also fix a prime of $L$ lying over $\mathfrak{p}$ and denote it $\mathscr{P}$. The *$p^n$-th division field* also known as the *$p^n$-th torsion field* is $K(E[p^n])$. We will denote this field by $T$. The field $T$ is the minimal extension of $K$ over which all points of $E$ of order $p^n$ are defined. Again, fix any prime of $T$ lying over $\mathscr{P}$, hence also over $\mathfrak{p}$, and denote it $\mathfrak{P}$. We summarize the situation:

$$\begin{array}{ccc}
T = K(E[p^n]) & & \mathfrak{P} \\
| & & | \\
L & & \mathscr{P} \\
| & & | \\
K & & \mathfrak{p} \\
| & & | \\
\mathbb{Q} & & p
\end{array}$$

Figure 1.

The local field obtained by completing $K$ at $\mathfrak{p}$ is denoted $K_{\mathfrak{p}}$. The normalized valuation is denoted $v_{\mathfrak{p}}$ and $\pi_{\mathfrak{p}}$ is a uniformizer. We mirror these conventions for $L$ and $T$. The ring of integers of a local or global field $M$ will be denoted $\mathcal{O}_M$ and the algebraic closure of a given field will be denoted $\overline{M}$. We use the notation $K(x(P))$ or $K_{\mathfrak{p}}(x(P))$ for the extension obtained by adjoining the $x$-coordinate of $P$, and the notation $K(P)$ or $K_{\mathfrak{p}}(P)$ for the extension obtained by adjoining both the $x$ and $y$-coordinates of $P$.

Please be aware that in Section 8 we will let $l$ be a prime and consider $l$-power division fields. In Section 8, $p$ is a prime distinct from $l$ and $\mathfrak{p}$ is a prime lying over $p$ at which $E$ has potential multiplicative reduction.

We are concerned with ramification in the extensions of $K$ obtained by adjoining torsion points of $E$. In Section 3 we will briefly review some facts about division polynomials, and in Section 4 we will revisit Cassels's paper [4]. Then, with Section 5 and Section 6 for the case when $p = 2$ and $n = 1$, we prove

**Theorem 2.1.** *The ramification index $e(\mathfrak{P} \mid p)$ is at least $p^{2n} - p^{2n-2}$, and the ramification index $e(\mathscr{P} \mid p)$ is properly divisible by $\varphi(p^n) = p^n - p^{n-1}$. Further, if $p$ is unramified in $K$, then $L/K$ is an extension of degree $p^{2n} - p^{2n-2}$ that is totally ramified at $\mathfrak{p}$. That is, if $e(\mathfrak{p} \mid p) = 1$, then $e(\mathscr{P} \mid \mathfrak{p}) = p^{2n} - p^{2n-2}$.*

In Section 7, we use our bound on $[L : K]$ when $p$ is unramified in $K$ along with an upper bound on the genus of the modular curve $X_1(N)$ to show the following:

**Theorem 2.2.** *Let $N > 12$ be a positive integer and write $N = \prod_{i=1}^{k} p_i^{e_i}$ for the prime factorization. Suppose that for each $p_i$ there exists a prime $\mathfrak{p}_i$ of $K$ at which $E$ is supersingular and with $e(\mathfrak{p}_i \mid p_i) = 1$. Then, $E$ does not correspond to a sporadic point on $X_1(N)$.*

After proving Theorem 2.2, we demonstrate how our methods can be generalized when one is interested in specific modular curves.

In Section 8, we change notation. Consider now the $l^n$-th division field $K(E[l^n])$. We turn our attention to primes $p$ distinct from $l$ at which $E$ has bad reduction that eventually resolves to split multiplicative reduction. We show:

**Theorem 2.3.** *Let $l$ be a prime in $\mathbb{Z}$ and suppose $\mathfrak{p}$ is a prime of $K$ not lying over $l$ for which $E$ has potential multiplicative reduction. Define $\Delta_{E,\min\mathfrak{p}}$ to be the discriminant of a model of $E$ that is minimal at $\mathfrak{p}$ and denote $v_l(v_{\mathfrak{p}}(\Delta_{E,\min\mathfrak{p}}))$ by $m$. Then the ramification indices of the primes of $K(E[l^n])$ lying above $\mathfrak{p}$ are $l^{n-m}$ if $E$ has multiplicative reduction at $\mathfrak{p}$ and either $2l^{n-m}$ or $l^{n-m}$ if $E$ has additive reduction at $\mathfrak{p}$.*

The methods we use throughout are rather classical. It is likely that many of our results are known, but to our knowledge they have not appeared in the literature. Moreover, our application to sporadic points on modular curves appears novel.

## 3. Background on Division Polynomials

Let $E$ be an elliptic curve over a number field $K$ with Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

One can define division polynomials, $\Psi_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]$, recursively starting with

$$\Psi_1 = 1,$$
$$\Psi_2 = 2y + a_1x + a_3,$$
$$\Psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$$
$$\Psi_4 = \Psi_2 \left(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\right),$$

and using the formulas

$$\Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3 \text{ for } m \geq 2 \text{ and}$$

$$\Psi_{2m}\Psi_2 = \Psi_{m-1}^2\Psi_m\Psi_{m+2} - \Psi_{m-2}\Psi_m\Psi_{m+1}^2 \text{ for } m \geq 3.$$

For a reference see [38, Exercise 3.7]. If $m$ is odd, we can write

$$\frac{1}{m}\Psi_m = \prod_P (x - x(P)), \tag{1}$$

where the product is over the non-trivial $m$-torsion points with distinct $x$-coordinates. If $m$ is even and not 2, we have

$$\frac{2}{m\Psi_2}\Psi_m = \prod_P (x - x(P)), \tag{2}$$

where now the product is over the non-trivial $m$-torsion points with distinct $x$-coordinates that are not 2-torsion points. Since $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, this definition makes it clear that when $m$ is odd $\Psi_m$ has degree $\dfrac{m^2-1}{2}$. The even division polynomials also have degree $\dfrac{m^2-1}{2}$ so long as we think of $y$ as having degree $\frac{3}{2}$ in $x$.

Equations (1) and (2) show that if $k \mid m$, then $\Psi_k \mid \Psi_m$. In general, $\Psi_m$ also includes roots that are $x$-coordinates of points with order dividing $m$ but not equal to $m$. We wish to consider points with order exactly $m$. Define a *primitive* $m$-torsion point to be a point with exact order $m$. We focus on the case when $m = p^n$. If $p = 2$, we require $n > 1$. We want a polynomial whose roots are exactly the distinct $x$-coordinates of primitive $p^n$-torsion points. To this end, we define the *primitive $p^n$-th division polynomial* to be

$$\Psi_{p^n,\text{prim}} = \frac{\Psi_{p^n}}{\Psi_{p^{n-1}}} = p\prod_P{}' (x - x(P)),$$

where the product is taken over the primitive $p^n$-torsion points with distinct $x$-coordinates. We note $\Psi_{p^n,\text{prim}}$ has degree $\frac{p^{2n}-p^{2n-2}}{2}$. Our results on ramification in the division fields of supersingular elliptic curves are obtained by an analysis of $\Psi_{p^n,\text{prim}}$, specifically the valuation of the constant coefficient.

**Lemma 3.1.** *Let $E$ be an elliptic curve over $K$ with supersingular reduction at $\mathfrak{p}$, a prime of $K$ lying above the odd prime $p$. Writing $c_0$ for the constant coefficient of $\Psi_{p^n}$, $v_{\mathfrak{p}}(c_0) = 0$ for all $n \in \mathbb{Z}^{>0}$.*

*Proof.* Write $k_{\mathfrak{p}}$ for the residue field at $\mathfrak{p}$. Choose $P \in E(\overline{k_{\mathfrak{p}}})$ with $x(P) = 0$. Note that $\alpha$ is a root of $\Psi_m$ if and only if points on $E$ with $x$-coordinates equal to $\alpha$ are $m$-torsion points. Thus $\Psi_{p^n}(0) = c_0 \equiv 0$ modulo $\mathfrak{p}$ if and only if $P$ has order dividing $p^n$. Since $E$ has supersingular reduction at $\mathfrak{p}$, all of the $p^n$-torsion points are in the kernel of reduction. Thus $P$ does not have order divisible by $p$. We conclude $v_{\mathfrak{p}}(c_0) = 0$ for all $n \in \mathbb{Z}^{>0}$. □

When $p = 2$, the proof of Lemma 3.1 goes through verbatim so long as we consider $\frac{\Psi_{2^n}}{\Psi_2}$ and exclude the $n = 1$ case.

**Lemma 3.2.** *Let $E$ be an elliptic curve over $K$ with supersingular reduction at $\mathfrak{p}$, a prime of $K$ dividing 2. Write $c_0$ for the constant coefficient of $\frac{\Psi_{2^n}}{\Psi_2}$, then $v_{\mathfrak{p}}(c_0) = 0$ for all $n \in \mathbb{Z}^{>1}$.*

Since $\Psi_{p^n,\mathrm{prim}} = \frac{\Psi_{p^n}}{\Psi_{p^{n-1}}}$, the valuations of the constant coefficients of $\Psi_{p^n}$ and $\Psi_{p^{n-1}}$ allow us to compute the valuation of the constant coefficient of $\Psi_{p^n,\mathrm{prim}}$. This, in conjunction with supersingular reduction, is enough to describe ramification in division fields and torsion point fields.

## 4. Cassels's Note on the Division Values of $\wp(u)$

We begin by quoting Theorem IV of [4], Cassels's note on the division values of the Weierstrass $\wp$-function.

**Theorem 4.1.** *Let $F$ be a number field and $E$ an elliptic curve over $F$. If $P = (x(P), y(P)) \in E(F)$ is a point of prime-power order $p^n$ with $p \neq 2$, then there is an integral ideal $\mathfrak{t} \subset \mathcal{O}_F$ such that $x(P)\mathfrak{t}^2$ and $y(P)\mathfrak{t}^3$ are integral and*

$$\mathfrak{t}^{\varphi(p^n)} \mid p \text{ for } p \neq 3, \tag{3}$$

$$\mathfrak{t}^{3^{2n}-3^{2n-2}} \mid 3 \text{ for } p = 3. \tag{4}$$

*When $P$ is not in the kernel of reduction, we take $\mathfrak{t} = \mathcal{O}_F$.*

Unfortunately, the second claim (4) is not technically correct. The second claim relies on the supposition that all the coefficients of $\Psi_{3^n,\mathrm{prim}}$, save for the constant term, are divisible by 3. The following example illustrates that this may not be the case.

*Example* 4.2. Consider the elliptic curve given by the Weierstrass equation

$$y^2 + y = x^3 - x^2 + 16x - 2.$$

This elliptic curve has Cremona label 5131a1 and has good ordinary reduction at 3. One computes

$$\Psi_{3,\mathrm{prim}}(x) = \Psi_3(x) = 3x^4 - 2^2x^3 + 2^5 \cdot 3x^2 - 3 \cdot 7x - 3 \cdot 83.$$

In particular, 3 divides the constant coefficient but not the coefficient of $x^3$.

Further, one can check that $\Psi_{3,\mathrm{prim}}$ is irreducible. Thus, for any primitive 3-torsion point $P$, the extensions $\mathbb{Q}(P)$ are isomorphic. Using SageMath [12], one finds that in $\mathcal{O}_{\mathbb{Q}(P)}$, the ideal (3) factors as $\mathfrak{a}^2 \cdot \mathfrak{b}^3$. Since there are some primitive 3-torsion points in the kernel of reduction, their denominators will be divisible by either $\mathfrak{a}$ or $\mathfrak{b}$. Thus claim (4) of Theorem 4.1 states that either $\mathfrak{a}^8 \mid 3$ or $\mathfrak{b}^8 \mid 3$. We can explicitly see that this is not the case.

With Theorem 5.4 we will show that, when $E$ is supersingular at one of the primes above $p$, (3) holds and *the divisibility is proper*. Further, if we suppose that there is a prime $\mathfrak{p} \subset \mathcal{O}_F$ at which $E$ is supersingular and with $e(\mathfrak{p} \mid p) = 1$, then Theorem 5.1 and Theorem 6.1 will show that (4) holds. We remark that although there is a corrigendum to Cassels's work [5], the error we describe is not rectified there.

## 5. Ramification in the Division Fields and Torsion Point Fields of Supersingular Elliptic Curves

In the case where $E$ has supersingular reduction, we can adapt Cassels's argument. We postpone the $p^n = 2$ case until Section 6. Note the ideas here are also present in Gupta's paper [17] for elliptic curves with complex multiplication and in Serre's article [36], where the $n = 1$ case was all that his purposes necessitated.

**Theorem 5.1.** *If $p = 2$, suppose $n > 1$. The ramification index $e(\mathfrak{P} \mid p)$ is at least $p^{2n} - p^{2n-2}$. Further, if $e(\mathfrak{p} \mid p) = 1$, then $[L : K] = p^{2n} - p^{2n-2}$ with $e(\mathscr{P} \mid \mathfrak{p}) = p^{2n} - p^{2n-2}$.*

*Proof.* Because $E$ has supersingular reduction at $\mathfrak{p}$, each $p^n$-torsion point $P \in E(T_{\mathfrak{P}})[p^n]$ is in the kernel of reduction modulo $\mathfrak{P}$. We see that each $x(P)$, considered as an element of $T_{\mathfrak{P}}$, has a power of $\pi_{\mathfrak{P}}$ in the denominator. Symbolically, $v_{\mathfrak{P}}(x(P)) < 0$.

For each primitive $p^n$-torsion point $P$, write $x(P) = \dfrac{P^*}{\pi_{\mathfrak{P}}^{m_P}}$ with $v_{\mathfrak{P}}(P^*) = 0$ and $m_P > 0$. Consider a Weierstrass equation for $E$ over $K$ evaluated at $P$

$$y(P)^2 + a_1\left(\frac{P_0}{\pi_{\mathfrak{P}}^{m_P}}\right)y(P) + a_3 y(P) = \left(\frac{P_0}{\pi_{\mathfrak{P}}^{m_P}}\right)^3 + a_2\left(\frac{P_0}{\pi_{\mathfrak{P}}^{m_P}}\right)^2 + a_4\left(\frac{P_0}{\pi_{\mathfrak{P}}^{m_P}}\right) + a_6. \quad (5)$$

Multiplying both sides of equation (5) by $\pi_{\mathfrak{P}}^{3m_P}$, we see that the $\mathfrak{P}$-adic valuation of the right hand side is 0. Considering the left hand side, $m_P$ must be even and $v_{\mathfrak{P}}(y(P)) = -\frac{3m_P}{2}$. Thus we may write $m_P = 2k_P$ with $k_P > 0$. Now $v_{\mathfrak{P}}(x(P)) = -2k_P$ and $v_{\mathfrak{P}}(y(P)) = -3k_P$.

From Lemmas 3.1 and 3.2, the constant coefficients of $\Psi_{p^{n-1}}$ and $\Psi_{p^n}$ both have valuation 0. Since

$$\Psi_{p^n} = \Psi_{p^n,\mathrm{prim}} \cdot \Psi_{p^{n-1}},$$

the constant coefficient, $c_0$, of $\Psi_{p^n,\mathrm{prim}}$ has valuation 0. Recall that

$$\frac{1}{p}\Psi_{p^n,\mathrm{prim}}(x) = \prod_P{}' (x - x(P)),$$

where the product is over the primitive $p^n$-torsion points with distinct $x$-coordinates. Thus, considering only the constant coefficient,

$$\frac{c_0}{p} = \frac{\prod' P^*}{\pi_{\mathfrak{P}}^{\sum' 2k_P}},$$

where again the sum and the products are over the primitive $p^n$-torsion points with distinct $x$-coordinates. Because there are $\dfrac{p^{2n}-p^{2n-2}}{2}$ primitive $p^n$-torsion points with distinct $x$-coordinates and since $k_P > 0$ for each primitive $P$,

$$\sum_P{}' 2k_P \geq p^{2n} - p^{2n-2}.$$

Thus $v_{\mathfrak{P}}(p) \geq p^{2n} - p^{2n-2}$ and $e(\mathfrak{P} \mid p) \geq p^{2n} - p^{2n-2}$.

Now suppose $e(\mathfrak{p} \mid p) = 1$. Regardless of the ramification of $p$ in $K$, the primitive $p^n$-th division polynomial has the shape

$$\Psi_{p^n,\mathrm{prim}} = px^{\frac{p^{2n}-p^{2n-2}}{2}} + \cdots + c_0.$$

Recall that $v_{\mathfrak{p}}(c_0) = 0$ and that all the roots of $\Psi_{p^n,\mathrm{prim}}$ have negative valuation over $T$.

We claim $\Psi_{p^n,\mathrm{prim}}$ is irreducible in $\mathcal{O}_{K_{\mathfrak{p}}}[x]$. Since $e(\mathfrak{p} \mid p) = 1$, one has $v_{\mathfrak{p}}(p) = 1$. By way of contradiction, suppose we have the non-trivial factorization $\Psi_{p^n,\mathrm{prim}} = (ax^d + \cdots + a_0)(bx^e + \cdots + b_0)$. Without loss of generality, $v_{\mathfrak{p}}(a) = 1$ and $v_{\mathfrak{p}}(b) = 0$. Since the roots of $\Psi_{p^n,\mathrm{prim}}$ have negative valuation, $v_{\mathfrak{p}}(b_0) < 0$. Considering that $v_{\mathfrak{p}}(c_0 = a_0 b_0) = 0$, one sees $v_{\mathfrak{p}}(a_0) > 0$. Thus, because $v_{\mathfrak{p}}(a) = 1$, $v_{\mathfrak{p}}\left(\frac{a_0}{a}\right) \geq 0$. However, since $\frac{a_0}{a}$ is a product of roots of $\Psi_{p^n,\mathrm{prim}}$, all of which have negative valuation over $T$, we have $v_{\mathfrak{p}}\left(\frac{a_0}{a}\right) < 0$. We have a contradiction. Hence $\Psi_{p^n,\mathrm{prim}}$ is irreducible.

As above, let $P$ be a primitive $p^n$-torsion point. Since $\Psi_{p^n,\mathrm{prim}}$ is irreducible, $K_{\mathfrak{p}}(x(P))$ is an extension of degree $\frac{p^{2n}-p^{2n-2}}{2}$. If $v$ is the normalized valuation of $K_{\mathfrak{p}}(x(P))$, one has $v(x(P)) = -1$ and $v(p) = \frac{p^{2n}-p^{2n-2}}{2}$. To see this, note that $v(x(P))$ must be negative since $P$ is in the kernel of reduction. However,

$$[K(x(P)) : K] = \frac{p^{2n}-p^{2n-2}}{2},$$

so $v(x(P))$ cannot be less than $-1$. The argument used with equation (5) shows that $v(x(P))$ must be even if $P$ is defined over $K_{\mathfrak{p}}(x(P))$. Hence $K_{\mathfrak{p}}(P)$ is a ramified quadratic extension of $K_{\mathfrak{p}}(x(P))$. Therefore $K_{\mathfrak{p}}(P)$ and $L_{\wp}$ coincide; the result follows. $\square$

To understand why $p$ must be unramified in $K$ to obtain $[L : K] = p^{2n} - p^{2n-2}$, it is useful to repurpose an example that can be found in Lozano-Robledo's papers [24] and [26]. We would like to illustrate that if $p$ is ramified, then $\Psi_{p^n,\mathrm{prim}}$ may be reducible.

*Example* 5.2. Let $E/\mathbb{Q}$ be the elliptic curve with Cremona label 121c2. The $j$-invariant is $-11 \cdot 131^3$ and the global minimal model over $\mathbb{Q}$ is

$$E: \quad y^2 + xy = x^3 + x^2 - 3632 + 82757.$$

At $p = 11$ the curve $E$ has bad additive reduction. Over $\mathbb{Q}(\sqrt[3]{11})$ the bad additive reduction resolves to good supersingular reduction and the curve has global minimal

model
$$E: \quad y^2 + \sqrt[3]{11}xy = x^3 + \sqrt[3]{11^2}x^2 + 3\sqrt[3]{11} + 2.$$

Using SageMath [12], one can compute the factorization
$$\Psi_{11,\mathrm{prim}} = 11\left(x^5 + \sqrt[3]{11^2}x^4 + 3\sqrt[3]{11}x^3 + 3x^2 - \frac{1}{\sqrt[3]{11^2}}\right)\left(x^{55} + \cdots + \frac{303271}{\sqrt[3]{11}}\right).$$

In particular, $\Psi_{11,\mathrm{prim}}$ is reducible and there is a degree 10 extension of $\mathbb{Q}(\sqrt[3]{11})$ over which $E$ has a point of exact order 11.

Informally speaking, this example shows that some $p^n$-torsion points are "more supersingular" than others, meaning the $x$-coordinates have a larger negative valuation. In general, not all $x$-coordinates of $p^n$-torsion points have the same valuation. For more general discussions of this phenomenon, the reader should consult [28] and [8]. In the proof of Theorem 5.4, we will show that $x$-coordinates of primitive $p^n$-torsion points that are multiples of one another have the same valuation.

For our application to sporadic points on modular curves, we would like to consider composite division fields. Luckily, ramification is quite controlled in division fields. Specifically, $\mathbb{Q}(E[p^n])$ is only ramified at $p$ and at primes for which $E$ has bad reduction. To see this one notes that reduction modulo $p$ is injective on $l$-power torsion for primes $l \neq p$ at which $E$ has good reduction. The utility of the following corollary will be seen in Section 7.

**Corollary 5.3.** *Let $N \in \mathbb{Z}^{>1}$. Factoring $N$ into primes, we write $N = \prod_{i=1}^{k} p_i^{n_i}$. Let $E$ be an elliptic curve over $\mathbb{Q}$ that has supersingular reduction at all the $p_i$. If $L$ is a minimal $N$-torsion point field, then any prime above $p_i$ in $L$ has ramification index $p_i^{2n_i} - p_i^{2n_i-2}$ and*
$$[L : \mathbb{Q}] = \prod_{i=1}^{k}\left(p_i^{2n_i} - p_i^{2n_i-2}\right).$$

We have stated Corollary 5.3 over $\mathbb{Q}$ for simplicity; however, the proof is valid over any number field $K$ in which the primes dividing $N$ are unramified. Note, we will establish the bound used when $v_2(N) = 1$ in Theorem 6.1.

*Proof.* Let $L_i$ be a minimal extension of $\mathbb{Q}$ containing a point of exact order $p_i^{n_i}$. If $p_i \neq p_j$, note that $p_j$ is unramified in $L_i$. Observe that the compositum of the $L_i$ for $1 \leq i \leq k$ is a minimal $N$-torsion point field.

For $i \neq j$, consider the compositum $L_iL_j$. The primes $p_i$ and $p_j$ have respective ramification indices $p_i^{2n_i} - p_i^{2n_i-2}$ and $p_j^{2n_j} - p_j^{2n_j-2}$. However, $p_i$ is unramified in $L_j$ and $p_j$ is unramified in $L_i$. One sees that $L_iL_j$ has degree $p_j^{2n_j} - p_j^{2n_j-2}$ over $L_i$ so as to attain the necessary ramification. The equivalent statement holds over $L_j$. Thus $L_iL_j$ has degree $\left(p_j^{2n_j} - p_j^{2n_j-2}\right)\left(p_i^{2n_i} - p_i^{2n_i-2}\right)$ over $\mathbb{Q}$. The situation is summarized in Figure 2. Repeating the above argument for each prime dividing $N$ we obtain the result. $\square$

$$\begin{tikzcd}[column sep=small] & L_iL_j \arrow[dl, dash, "p_j^{2n_j}-p_j^{2n_j-2}"'] \arrow[dr, dash, "p_i^{2n_i}-p_i^{2n_i-2}"] & \\ L_i \arrow[dr, dash, "p_i^{2n_i}-p_i^{2n_i-2}"'] & & L_j \arrow[dl, dash, "p_j^{2n_j}-p_j^{2n_j-2}"] \\ & \mathbb{Q} & \end{tikzcd}$$

FIGURE 2.

**Theorem 5.4.** *As above, if $p = 2$ assume $n > 1$. We make no assumptions regarding the ramification of $p$ in $K$. Then, the ramification index $e(\mathcal{P} \mid p)$ is properly divisible by $\varphi(p^n)$. In particular, $[L : \mathbb{Q}]$ is properly divisible by $\varphi(p^n)$.*

*Proof.* Fix a primitive $p^n$-torsion point in $P \in E(L)$. Immediately, we have $\varphi(p^n)$ other primitive $p^n$-torsion points in $E(L)$, since $[j]P$ is a primitive $p^n$-torsion point if $j$ is relatively prime to $p$. This yields at least $\dfrac{\varphi(p^n)}{2}$ roots of $\Psi_{p^n,\mathrm{prim}}$ in $L$. For ease of notation, denote $[j]P$ by $P_j$. Similarly to the proof of Theorem 5.1, each $P_j$ can be written $\left(\dfrac{P_j^*}{\pi_{\mathcal{P}}^{2k_{P_j}}}, \dfrac{P_{j,y}^*}{\pi_{\mathcal{P}}^{3k_{P_j}}}\right)$ with $v_{\mathcal{P}}(P_j^*) = v_{\mathcal{P}}(P_{j,y}^*) = 0$. Let $\hat{E}(\pi_{\mathcal{P}}\mathcal{O}_{L_{\mathcal{P}}})$ be the formal group associated to $E$ over $L_{\mathcal{P}}$. Denoting the kernel of reduction by $E_1(L_{\mathcal{P}})$, we have an isomorphism

$$\Theta : E_1(L_{\mathcal{P}}) \to \hat{E}(\pi_{\mathcal{P}}\mathcal{O}_{L_{\mathcal{P}}}),$$

given by $(x, y) \mapsto -x/y$. One can consult [38, Chapter IV] for a reference. We see $\Theta(P_j) = P_{j,y}^* \pi_{\mathcal{P}}^{k_{P_j}} / P_j^*$. Hence $v_{\mathcal{P}}(\Theta(P_j)) = k_{P_j}$. Denote $\Theta(P)$ by $z$ and note $z \in \mathcal{P}$. The multiplication by $j$ map in $\hat{E}$, denoted $[j]_{\hat{E}}$, has the form

$$[j]_{\hat{E}}(z) = jz + (\text{terms of degree 2 and higher}).$$

Thus if $\gcd(j, p) = 1$, then $k_P = v_{\mathcal{P}}(z) = v_{\mathcal{P}}([j]_{\hat{E}}(z)) = k_{P_j}$. Therefore, the $x$-coordinates of all the multiples of $P$ that are primitive $p^n$-torsion points have the same valuation.

Now consider the polynomial

$$\chi(x) = \prod_{\substack{0<j<p^n \\ \gcd(j,p)=1}} (x - x(P_j)),$$

where the product is taken over $1 \le j < p^n$ with $j$ relatively prime to $p$. By construction, $\chi(x)$ is the product of the linear factors of $\Psi_{p^n,\mathrm{prim}}$ that are coming from multiples of $P$. The constant coefficient of $\chi(x)$ is

$$\prod_{\substack{0<j<p^n \\ \gcd(j,p)=1}} \frac{P_j^*}{\pi_{\mathcal{P}}^{2k_{P_j}}} = \prod_{\substack{0<j<p^n \\ \gcd(j,p)=1}} \frac{P_j^*}{\pi_{\mathcal{P}}^{\varphi(p^n)k_P}},$$

since $k_P = k_{P_j}$ for any $j$ relatively prime to $p$. We may factor $\Psi_{p^n,\mathrm{prim}}$

$$\frac{1}{p}\Psi_{p^n,\mathrm{prim}} = \chi(x)\omega(x), \tag{6}$$

where $\omega(x)$ is the product of all the $x$-coordinates of primitive $p^n$-torsion points that are not multiples of $P$. From equation (6), one sees that the constant coefficient of $\chi(x)$ is a proper divisor of $\frac{c_0}{p}$, where $c_0$ is the constant coefficient of $\Psi_{p^n,\mathrm{prim}}$. Recall, from Lemma 3.1 or Lemma 3.2, $v_{\wp}(c_0) = 0$. Thus $p$ is divisible by $\pi_{\wp}^{k_P\varphi(p^n)}$. Further, $\pi_{\wp}^{k_P\varphi(p^n)}$ divides a proper factor of $p$, since the constant coefficient of $\omega(x)$ will also have some factor of $p$ in the denominator. □

*Remark* 5.5. From real uniformization [37, Corollary V.2.3.1], the group $E(\mathbb{R})$ contains at least $\varphi(p^n)$ primitive $p^n$-torsion points. Let $P \in E(\mathbb{R})[p^n]$ be primitive. When $K$ admits a real embedding, $K(P)$ also admits a real embedding. Recall, the Weil pairing shows that $\mu_{p^n} \subset T$. Hence, when $K$ admits a real embedding, $L$ is always properly contained in $T$. The obvious exception to this is when $p^n = 2$. Since $-1$ is the primitive 2nd root of unity, there is no obstruction to $T$ being embedded in $\mathbb{R}$.

## 6. The $p^n = 2$ Case

To begin, suppose

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

is an elliptic curve with good supersingular reduction at a prime $\mathfrak{p} \subset K$ lying above 2. Recall,

$$\Psi_2 = 2y + a_1x + a_3.$$

Squaring and substituting for $y^2$, we obtain

$$\Psi_2^2 = 4x^3 + (4a_2 + a_1^2)x^2 + (4a_4 + 2a_1a_3)x + 4a_6 + a_3^2.$$

We may write

$$\frac{1}{4}\Psi_2^2 = \prod_P (x - x(P)),$$

where the product is over the three non-trivial 2-torsion points. Over $\overline{\mathbb{F}_2}$ the unique supersingular elliptic curve is

$$E_{\mathrm{sup}} : y^2 + y = x^3.$$

See [38, Chapter V.4] for a reference. Thus, the reduction of $E$ mod $\mathfrak{p}$ admits a change of coordinates over $\overline{\mathbb{F}_2}$ to $E_{\mathrm{sup}}$. Recall, the admissible changes of coordinates have the form

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + u^2sx' + t,$$

where $r, s, t \in \overline{\mathbb{F}_2}$ and $u \in \overline{\mathbb{F}_2}^*$. Also recall, $ua_1' = a_1 + 2s$ and $u^3a_3' = a_3 + ra_1 + 2t$. We see $a_1'$ and $a_1$ are either both 0 or both non-zero. Considering $E_{\mathrm{sup}}$, we have $a_1 \equiv 0$ modulo $\mathfrak{p}$. Hence, $a_3 \not\equiv 0$ modulo $\mathfrak{p}$. Therefore we can see, rather explicitly, that the constant coefficient of $\Psi_2$, hence also of $\Psi_2^2$, has $\mathfrak{p}$-adic valuation 0. Alternatively, we could mirror the argument in Lemma 3.1 with $\Psi_2^2$ to obtain $v_{\mathfrak{p}}(a_3) = 0$. This, in conjunction with supersingular reduction, is enough for our result.

**Theorem 6.1.** *If $e(\mathfrak{p} \mid 2) = 1$, then $[L : K]$ is an extension of degree 3 with $e(\mathscr{P} \mid \mathfrak{p}) = 3$. Further, the ramification index $e(\mathfrak{P} \mid 2)$ is at least 3 regardless of the ramification of $p$ in $K$.*

*Proof.* Let $P$ be a primitive 2-torsion point in $E(L)$. As before, write

$$P = \left( \frac{P^*}{\pi_{\mathscr{P}}^{2k_P}}, \frac{P_y^*}{\pi_{\mathscr{P}}^{3k_P}} \right),$$

with $v_{\mathscr{P}}(P^*) = v_{\mathscr{P}}(P_y^*) = 0$. Note $P$ satisfies $\Psi_2$, so we have

$$0 = 2\frac{P_y^*}{\pi_{\mathscr{P}}^{3k_P}} + a_1 \frac{P^*}{\pi_{\mathscr{P}}^{2k_P}} + a_3.$$

Recall, $v_{\mathfrak{p}}(a_1) \geq 1$. Since $v_{\mathfrak{p}}(2) = 1$, the fraction $\frac{a_1}{2}$ has non-negative $\mathfrak{p}$-adic valuation. Hence, $v_{\mathscr{P}}(\frac{a_1}{2}) \geq 0$. Reorganizing,

$$-a_3 = \frac{2}{\pi_{\mathscr{P}}^{3k_P}} \left( P_y^* + \frac{a_1}{2} \pi_{\mathscr{P}}^{k_P} P^* \right).$$

We see $v_{\mathscr{P}}(-a_3) = v_{\mathscr{P}}(P_y^* + \frac{a_1}{2}\pi_{\mathscr{P}}^{k_P} P^*) = 0$. Hence, $v_{\mathscr{P}}(2) = 3k_P$.

To see that $[L : K] \leq 3$, let $\alpha$ be a root of $\Psi_2^2$. We claim $K(\alpha)$ contains a primitive 2-torsion point. Let $P$ be the primitive 2-torsion point with $x$-coordinate $x(P) = \alpha$. The $y$-coordinate, $y(P)$, satisfies

$$\Psi_2(\alpha, y(P)) = 2y(P) + a_1\alpha + a_3 = 0.$$

We have $y(P) = \dfrac{-a_1\alpha - a_3}{2} \in K(\alpha)$. Therefore, $[L : K] = 3$ with $e(\mathscr{P} \mid \mathfrak{p}) = 3$.

Considering $\Psi_2^2$ and using an argument very similar to that used in the proof of Theorem 5.1 yields the result for $e(\mathfrak{P} \mid 2)$. ∎

The analogue of Theorem 5.4 is not particularly troublesome.

## 7. An Application to Sporadic Points on Modular Curves

Our exposition follows Sutherland's notes, "Torsion Subgroups of Elliptic Curves over Number Fields" [39]. Let $K$ be a number field. The *$K$-gonality*, $\gamma_K(X)$, of a curve $X/K$ is the minimum degree among all dominant morphisms $\phi : X \to \mathbb{P}^1_K$. Recall, a dominant morphism is a morphism with dense image. We are interested in the $\mathbb{Q}$-gonality of the modular curve $X_1(N)$. For ease, we will denote $\gamma_{\mathbb{Q}}(X_1(N))$ by $\gamma(X_1(N))$. Another definition we will need is the degree of a point. If $Q \in X_1(N)$ is a point, define the *degree* of $Q$ to be the least degree of a number field $K$ such that $Q$ is defined over $K$.

Given a dominant morphism $\phi : X_1(N) \to \mathbb{P}^1_{\mathbb{Q}}$ of degree $d$, one can construct infinitely many points of $X_1(N)$ defined over number fields of degree $d$. As an example, let $[a, 1] \in \mathbb{P}^1_{\mathbb{Q}}$. In some affine neighborhood containing $[a, 1]$, $\phi$ is given by $[f(x_1, \ldots, x_m), g(x_1, \ldots, x_m)]$ where $f$ and $g$ are homogeneous polynomials of degree

$d$. Solving $f(x_1, 1, \ldots, 1) = a$ and $g(x_1, 1, \ldots, 1) = 1$, we obtain a degree $d$ extension of $\mathbb{Q}$ over which a point in $\phi^{-1}([a, 1])$ is defined.

Continuing, let $g(X_1(N))$ be the genus of $X_1(N)$ and define $\delta(X_1(N))$ to be the smallest positive integer $k$ such that there are infinitely many points of degree $k$ on $X_1(N)$. From the above example, one has $\delta(X_1(N)) \le \gamma(X_1(N))$. A point on $X_1(N)$ of degree strictly less than $\delta(X_1(N))$ is called a *sporadic point.* Non-cuspidal sporadic points on $X_1(N)$ correspond to finite families of elliptic curves with a point of order $N$ defined over a number field of "small" degree. Let $\mathfrak{h}$ be a Weber function for $E$. Recall, a *Weber function* is a map

$$\mathfrak{h} : E \to E/\operatorname{Aut}(E) \cong \mathbb{P}^1.$$

Except for $j$-invariants 0 and 1728, taking the $x$-coordinate of a point is a Weber function. The degree of a point $x \in X_1(N)(\overline{\mathbb{Q}})$ corresponding to an isomorphism class of an elliptic curve $E$ and a marked point $P$ of order $N$ is $[\mathbb{Q}(j(E), \mathfrak{h}(P)) : \mathbb{Q}]$. For a reference, see [13, Chapter 7.6].

Now suppose $N > 12$ so that $g(X_1(N)) > 1$. For the modular curve $X_1(N)$ we have the bounds

$$\delta(X_1(N)) \le \gamma(X_1(N)) \le g(X_1(N)) \le \frac{N^2 - 1}{24}. \tag{7}$$

To see that the gonality is bounded above by the genus, consult [35, appendix A]. A reference for the upper bound on the genus is [32, chapter 4].

We apply our work in Sections 5 and 6 to show:

**Theorem 7.1.** *Let $N \in \mathbb{Z}^{>12}$, and write $N = \prod_{i=1}^{k} p_i^{n_i}$ for the factorization of $N$ into primes. Let $E$ be an elliptic curve defined over a number field $K$ in which there is a prime $\mathfrak{p}_i$ above each $p_i$ at which $E$ has supersingular reduction and with $e(\mathfrak{p}_i \mid p_i) = 1$. Then, $E$ does not correspond to a sporadic point on $X_1(N)$.*

*Proof.* If $L$ is a minimal extension of $K$ over which $E$ has a point of exact order $N$, then Corollary 5.3 shows $[L : K] = \prod_{i=1}^{k} \left(p_i^{2n_i} - p_i^{2n_i - 2}\right)$. Suppose for the moment that $j(E) \neq 0, 1728$. If $P \in E(L)$ is a point of exact order $N$, we have

$$[K(\mathfrak{h}(P), j(E)) : \mathbb{Q}] \ge \frac{1}{2} \prod_{i=1}^{k} \left(p_i^{2n_i} - p_i^{2n_i - 2}\right).$$

Taking the two leading terms we obtain

$$\frac{1}{2} \prod_{i=1}^{k} \left(p_i^{2n_i} - p_i^{2n_i - 2}\right) \ge \frac{1}{2} N^2 - \frac{1}{2} \sum_{i}^{k} \frac{N^2}{p_i^2}. \tag{8}$$

Let $P(s)$ be the the prime zeta function, $\sum_{p \text{ prime}} p^{-s}$. The value of $P(s)$ has been computed for various $s$. For $s = 2$, $P(2) \approx 0.45225$. More relevant to our goals, $P(2) < 0.45225$. The decimal expansion of $P(2)$ is sequence A085548 in the OEIS [18].

In order to show that $E$ does not correspond to a sporadic point on the modular curve $X_1(N)$, we wish to show $[K(\mathfrak{h}(P), j(E)) : \mathbb{Q}] \geq g(X_1(N))$, since $g(X_1(N)) \geq \delta(X_1(N))$. Recall, we have the bound $g(X_1(N)) \leq \dfrac{N^2-1}{24} < \dfrac{N^2}{24}$. Hence, using equation (8), our problem is implied by the middle inequality of

$$[K(\mathfrak{h}(P), j(E)) : \mathbb{Q}] \geq \frac{1}{2}N^2 - \frac{1}{2}\sum_i^k \frac{N^2}{p_i^2} \geq \frac{N^2}{24} \geq g(X_1(N)).$$

Thus, it is enough to show

$$\sum_i^k \frac{N^2}{p_i^2} \leq \frac{11}{12}N^2.$$

The result is obtained by the following string of inequalities:

$$\sum_i^k \frac{N^2}{p_i^2} < N^2 \sum_{p \text{ prime}}^{\infty} \frac{1}{p^2} < N^2(0.45225) < \frac{11}{12}N^2.$$

For $j$-invariants 0 and 1728, one conducts the same analysis as above, but with an additional factor of $\frac{1}{3}$ or $\frac{1}{2}$ respectively. In these cases, it boils down to showing

$$\sum_i^k \frac{N^2}{p_i^2} \leq \frac{3}{4}N^2$$

and

$$\sum_i^k \frac{N^2}{p_i^2} \leq \frac{5}{6}N^2$$

respectively. □

*Remark* 7.2. Being supersingular at some prime above a large prime dividing $N$ is a relatively strong constraint. In [9, page 57], Derickx and van Hoeij mention that one can obtain $\delta(X_1(N)) \leq \dfrac{11N^2}{840}$. If one uses this upper bound and conducts a finer analysis of $\prod_{i=1}^k \left(p_i^{2n_i} - p_i^{2n_i-2}\right)$, then one can deal with more general situations where $E$ may not have supersingular reduction at any of the primes of $K$ lying above some of the primes dividing $N$. In these cases one should consult Lozano-Robledo's paper [27] for bounds to replace $p^{2n} - p^{2n-2}$ when $E$ has ordinary or bad reduction.

*Example* 7.3. As an example of how one might deal with non-supersingular primes, suppose $E$ does not have supersingular reduction at any of the primes above 2. Note $j$-invariants 0 and 1728 are supersingular at 2. Consider $N = 2N_0$ where $N_0$ is odd. The degree of the smallest extension of $K$ over which $E$ has a point $P$ of order $N$ is at least $N_0^2 - \sum_i^k \frac{N_0^2}{p_i^2}$. Hence $[K(\mathfrak{h}(P), j(E)) : \mathbb{Q}] \geq \frac{1}{2}N_0^2 - \frac{1}{2}\sum_i^k \frac{N_0^2}{p_i^2}$. We wish to show that

$$\frac{N^2-1}{24} = \frac{4N_0^2-1}{24} < \frac{N_0^2}{6} \le \frac{1}{2}N_0^2 - \frac{1}{2}\sum_i^k \frac{N_0^2}{p_i^2}.$$

This amounts to showing $\frac{1}{2}\sum_i^k \frac{1}{p_i^2} \le \frac{1}{3}$. Using that $\sum_{p \text{ prime}}^{\infty} \frac{1}{p^2} < 0.45225$, the inequality is clear. Thus we have shown that, if $v_2(N) = 1$, sporadic points on $X_1(N)$ cannot correspond to elliptic curves that are supersingular at at least one unramified prime above each of the odd primes dividing $N$.

## 8. Ramification in $K(E[l^n])$ away from $l$.

**We change notation in this section.** As before $E$ will be an elliptic curve over a number field $K$. However, let $l$ be a prime, and consider the $l^n$-th division field $K(E[l^n])$. We would like to reserve $p$ for primes not equal to $l$ at which $E$ has bad reduction. Suppose $\mathfrak{p}$ is a prime of $K$ lying over $p$ for which $E$ has potential multiplicative reduction. In other words, the bad reduction of $E$ at $\mathfrak{p}$ eventually resolves to split multiplicative reduction. Similarly to before, we denote $K(E[l^n])$ by $T$ and let $\mathfrak{P}$ be a prime of $T$ above $\mathfrak{p}$. Other than these changes, we keep the previous conventions.

Before we begin our investigation into the ramification of primes away from $l$ in $T$, we remark that our methods are quite well-known. Our proof revolves around the fact that if $E$ has split multiplicative reduction at $\mathfrak{p}$, then

$$T_{\mathfrak{P}} \subseteq K_{\mathfrak{p}}\left(\mu_{l^n}, q^{1/l^n}\right)$$

where $q$ is the Tate parameter for $E$ over $K_{\mathfrak{p}}$. This has been noted by numerous authors, especially when $n = 1$. However, the case we describe here does not appear, to our knowledge, in the literature.

**Theorem 8.1.** *Denote the discriminant of a model of $E$ that is minimal at $\mathfrak{p}$ by $\Delta_{E,\min\mathfrak{p}}$. Define $m := v_l\left(v_{\mathfrak{p}}\left(\Delta_{E,\min\mathfrak{p}}\right)\right)$. In other words, $m$ is $l$-adic valuation of the number of components of the special fiber of the Néron model. Then $e(\mathfrak{P} \mid \mathfrak{p})$ is $l^{n-m}$ if $E$ has multiplicative reduction at $\mathfrak{p}$, while $e(\mathfrak{P} \mid \mathfrak{p})$ is either $2l^{n-m}$ or $l^{n-m}$ if $E$ has additive reduction at $\mathfrak{p}$.*

Intuitively speaking, the ramification index of $\mathfrak{p}$ in $T$ is just enough so that $l^n$ divides $v_{\mathfrak{P}}(\Delta_{E,\min\mathfrak{p}})$. This is what one would expect, since when $l^n$ divides $v_{\mathfrak{P}}(\Delta_{E,\min\mathfrak{p}})$, the group of components of the special fiber of the Néron model has an order that can accommodate a subgroup of order $l^n$.

*Proof.* From $\mathfrak{p}$-adic uniformization, there exists a $\mathfrak{p}$-adic analytic isomorphism

$$\Phi : E(K_{\mathfrak{p}}) \cong K_{\mathfrak{p}}^*/q^{\mathbb{Z}},$$

with $q \in K_{\mathfrak{p}}^*$ and $v_{\mathfrak{p}}(q) = v_{\mathfrak{p}}(\Delta_{E,\min\mathfrak{p}}) > 0$. See [37, Theorem V.3.1] for a reference. Considering $T_{\mathfrak{P}}$, one sees $\Phi$ extends to $\Phi' : E(T_{\mathfrak{P}}) \cong T_{\mathfrak{P}}^*/q^{\mathbb{Z}}$ with $v_{\mathfrak{P}}(q) = v_{\mathfrak{P}}(\Delta_{E,\min\mathfrak{p}}) > 0$.

We investigate the image of $E[l^n]$. Part of the $l^n$-torsion maps to $\mu_{l^n} \subset T_{\mathfrak{P}}^*$; however, this only accounts for half the story since $E[l^n] \cong \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$. An $l^n$-torsion point in $T_{\mathfrak{P}}^*/q^{\mathbb{Z}}$ satisfies either $x^{l^n} - 1$ or $x^{l^n} - q^t$ for some $t \in \mathbb{Z}$. As $\mu_{l^n}$ accounts for the roots of $x^{l^n} - 1$, there is some $u \in T_{\mathfrak{P}}^*$ that is a root of $x^{l^n} - q^t$. We note that $u$ generates the other half of the $l^n$-torsion and $v_{\mathfrak{P}}(u) > 0$.

Henceforth make the following identifications:

$$P \in E[l^n] \sim (1,0) \in \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z} \sim u \in T_{\mathfrak{P}}^*/q^{\mathbb{Z}}$$

and

$$Q \in E[l^n] \sim (0,1) \in \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z} \sim \zeta_{l^n} \in T_{\mathfrak{P}}^*/q^{\mathbb{Z}}.$$

Since $\zeta_{l^n}$ and $u$ form a basis for the $l^n$-torsion of $T_{\mathfrak{P}}^*/q^{\mathbb{Z}}$, it is clear every element of $T_{\mathfrak{P}}^*$ that reduces to $u^k \in T_{\mathfrak{P}}^*/q^{\mathbb{Z}}$ with $1 \leq k < l^n$ has non-zero valuation. In other words, if $1 \leq k < l^n$, then no element of $\mathcal{O}_{T_{\mathfrak{P}}}^*$ can reduce to $u^k \in T_{\mathfrak{P}}^*/q^{\mathbb{Z}}$.

Now let $E_0(T_{\mathfrak{P}})$ be the points of $E(T_{\mathfrak{P}})$ with non-singular reduction. From the theory of Néron models, we have the following isomorphisms:

$$E(T_{\mathfrak{P}})/E_0(T_{\mathfrak{P}}) \cong T_{\mathfrak{P}}^*/q^{\mathbb{Z}}\mathcal{O}_{T_{\mathfrak{P}}}^* \cong \mathbb{Z}/v_{\mathfrak{P}}(q)\mathbb{Z} = \mathbb{Z}/v_{\mathfrak{P}}(\Delta_{E,\min\mathfrak{p}})\mathbb{Z}. \tag{9}$$

For a reference, see [37, Chapter IV]. We see that the image of $u$ generates a subgroup of order $l^n$ in $\mathbb{Z}/v_{\mathfrak{P}}(q)\mathbb{Z}$. In order to accommodate this subgroup of order $l^n$ in $\mathbb{Z}/v_{\mathfrak{P}}(q)\mathbb{Z}$, the valuation $v_{\mathfrak{p}}$ must have ramification index at least $l^{n-m}$ .

To see that $l^{n-m}$ is the largest possible ramification index, note $K_{\mathfrak{p}}(\zeta_{l^m})$ is an unramified extension of $K_{\mathfrak{p}}$. Further, $K_{\mathfrak{p}}(\zeta_{l^n})^*/q^{\mathbb{Z}}$ has a subgroup isomorphic to $\mathbb{Z}/l^n\mathbb{Z}$. Recalling that $\pi_{\mathfrak{p}}$ denotes a uniformizer for $K_{\mathfrak{p}}$, we write $q = z\pi_{\mathfrak{p}}^{l^m s}$, where $v_{\mathfrak{p}}(z) = 0$ and $\gcd(s,l) = 1$. Consider $f(x) = x^{l^n} - z$, and let $z^{\frac{1}{l^n}}$ be a root. We claim $K_{\mathfrak{p}}\left(\zeta_{l^m}, z^{1/l^n}\right)$ is an unramified extension of $K_{\mathfrak{p}}$.

It is clear that $K_{\mathfrak{p}}\left(\zeta_{l^m}, z^{1/l^n}\right)$ is the splitting field of $f(x)$, as the roots of $f(x)$ are $\zeta_{l^n}^i z^{1/l^n}$ for $0 \leq i < l^n$. Using the Vandermonde determinant, the discriminant of $f$ is

$$\begin{aligned}(-1)^{\frac{l^n(l^n-1)}{2}} \prod_{i\neq j}\left(\zeta_{l^n}^i z^{\frac{1}{l^n}} - \zeta_{l^n}^j z^{\frac{1}{l^n}}\right) &= (-1)^{\frac{l^n(l^n-1)}{2}} z^{\frac{l^n-1}{2}} \prod_{i\neq j}\left(\zeta_{l^n}^i - \zeta_{l^n}^j\right) \\ &= z^{\frac{l^n-1}{2}} \prod_{k=1}^{n} \operatorname{disc}(\phi_{l^k}(x)),\end{aligned}$$

where $\operatorname{disc}(\phi_{l^k}(x))$ is the discriminant of the $l^k$-th cyclotomic polynomial. Since $\prod_{k=1}^{n} \operatorname{disc}(\phi_{l^k}(x))$ is a power of $l$ and $z$ is a unit in $K_{\mathfrak{p}}$, the discriminant of $f$ is not divisible by $p$. Thus the extension is unramified.

Now let $\pi_{\mathfrak{p}}^{1/l^{n-m}}$ be a root of $x^{l^{n-m}} - \pi_{\mathfrak{p}}$ and define

$$W_{\mathfrak{p}} := K_{\mathfrak{p}}\left(\zeta_{l^n}, z^{1/l^n}, \pi_{\mathfrak{p}}^{1/l^{n-m}}\right).$$

Note $W_\mathfrak{p}$ is ramified over $K_\mathfrak{p}$ of degree $l^{n-m}$. We have built $W_\mathfrak{p}$ so that $x^{l^n} - q$ splits completely. To see this, observe the roots of $x^{l^n} - q$ are $\zeta_{l^m}^i z^{1/l^n} \pi_\mathfrak{p}^{s/l^{n-m}}$ with $0 \le i < l^n$.

By construction $W_\mathfrak{p}^*/q^\mathbb{Z}$ has a subgroup isomorphic to $\mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$. Thus by equation (9), replacing $T_\mathfrak{P}$ with $W_\mathfrak{p}$, the group $E(W_\mathfrak{p})$ contains all the $l^n$-torsion. Since $v_\mathfrak{p}$ has ramification index $l^{n-m}$ in $W_\mathfrak{p}$, identifying $T_\mathfrak{P}$ with a subfield of $W_\mathfrak{p}$, we see $v_\mathfrak{p}$ has at most ramification index $l^{n-m}$ in $T_\mathfrak{P}$. Hence $T_\mathfrak{P}$ has ramification index $l^{n-m}$ over $K_\mathfrak{p}$.

Note that if $E$ has non-split multiplicative or additive reduction at $p$, the above argument holds after first passing to a quadratic extension, $K'_\mathfrak{p}$, over which $E$ will have split multiplicative reduction. If $E$ has non-split multiplicative reduction over $K_\mathfrak{p}$, then $K'_\mathfrak{p}$ is an unramified quadratic extension. We observe that $K'_\mathfrak{p}(E[l^n])$ and $T_\mathfrak{P}$ have the same ramification indices over $K_\mathfrak{p}$. Likewise, if $E$ has additive reduction over $K_\mathfrak{p}$, then $K'_\mathfrak{p}$ is a ramified quadratic extension. We observe that the ramification index of $K'_\mathfrak{p}(E[l^n])$ over $K_\mathfrak{p}$ divides $2[T_\mathfrak{P} : K_\mathfrak{p}]$ and is at least $[T_\mathfrak{P} : K_\mathfrak{p}]$. ☐

In cases where $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_k/\mathfrak{p}\mathcal{O}_K$, we can use the theory of cyclotomic extensions to describe inertia. Note that the ideas below give a lower bound on inertia when $\mathfrak{p}$ has inertia degree greater than 1 over $p$.

**Corollary 8.2.** *Let $\mathfrak{p} \subset K$ be a prime at which $E$ has multiplicative reduction. Suppose $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_k/\mathfrak{p}\mathcal{O}_K$. Then the residue degree of $\mathfrak{p}$ in $T$ is the smallest $f$ such that $p^f \equiv 1$ modulo $l^n$.*

*Proof.* Adjoining a root of $x^{l^{n-m}} - \pi_\mathfrak{p}$ to $K_\mathfrak{p}(\zeta_{l^n})$ is a totally ramified extension and corresponds to a trivial extension of residue fields. Thus any extension of the residue field is coming from adjoining a primitive $l^n$-th root of unity. From the theory of cyclotomic fields, the residue degree is the smallest $f$ such that $p^f \equiv 1$ modulo $l^n$. For a reference, see [6, Chapter III]. ☐

*Remark* 8.3. Let $\mathfrak{l}$ be a prime of $K$ lying above $l$. When $E$ has multiplicative reduction at $\mathfrak{l}$, we can parrot the proof of Theorem 8.1 to show that $l$ has ramification index divisible by $\varphi(l^n)$ in $K(E[l^n])$. One can attempt to use these ideas to obtain a lower bound for the ramification in a minimal $l^n$-torsion point field $L$. This works well unless $l^n$ divides $m = v_l(v_\mathfrak{l}(\Delta_{E,\min \mathfrak{l}}))$.

## References


[1] C. Adelmann. *The decomposition of primes in torsion point fields*, volume 1761 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2001. ISBN 3-540-42035-5. URL https://doi.org/10.1007/b80624.

[2] A. Bourdon, Ö. Ejder, Y. Liu, F. Odumodu, and B. Viray. On the level of modular curves that give rise to sporadic $j$-invariants. *ArXiv e-prints*, Aug. 2018.

[3] E. Cali and A. Kraus. Sur la $p$-différente du corps des points de $l$-torsion des courbes elliptiques, $l \neq p$. *Acta Arith.*, 104(1):1–21, 2002. ISSN 0065-1036. doi: 10.4064/aa104-1-1. URL https://doi.org/10.4064/aa104-1-1.

[4] J. W. S. Cassels. A note on the division values of $\wp(u)$. *Proc. Cambridge Philos. Soc.*, 45:167–172, 1949.

[5] J. W. S. Cassels. Corrigendum: "A note on the division values of $\wp(u)$". *Proc. Cambridge Philos. Soc.*, 71:431, 1972.

[6] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, 2010. London Mathematical Society, London. ISBN 978-0-95027-342-6. Papers from the conference held at the University of Sussex, Brighton, September 1–17, 1965, Including a list of errata.

[7] T. G. Centeleghe. Integral Tate modules and splitting of primes in torsion fields of elliptic curves. *Int. J. Number Theory*, 12(1):237–248, 2016. ISSN 1793-0421. doi: 10.1142/S1793042116500147. URL https://doi.org/10.1142/S1793042116500147.

[8] R. F. Coleman. Classical and overconvergent modular forms. *Invent. Math.*, 124(1-3):215–241, 1996. ISSN 0020-9910. doi: 10.1007/s002220050051. URL https://doi.org/10.1007/s002220050051.

[9] M. Derickx and M. van Hoeij. Gonality of the modular curve $X_1(N)$. *J. Algebra*, 417:52–71, 2014. ISSN 0021-8693. doi: 10.1016/j.jalgebra.2014.06.026. URL https://doi.org/10.1016/j.jalgebra.2014.06.026.

[10] M. Derickx, S. Kamienny, W. Stein, and M. Stoll. Torsion points on elliptic curves over number fields of small degree. *ArXiv e-prints*, July 2017.

[11] M. Derickx, D. Zureick-Brown, A. Etropolski, M. van Hoeij, and J. Morrow. Unreleased. 2018. URL http://www.mathcs.emory.edu/~dzb/slides/DZB-SERMON-cubic-torsion.pdf.

[12] T. S. Developers. *SageMath, the Sage Mathematics Software System (Version 7.3)*, 2016. http://www.sagemath.org.

[13] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. ISBN 0-387-23229-X.

[14] W. Duke and A. Tóth. The splitting of primes in division fields of elliptic curves. *Experiment. Math.*, 11(4):555–565 (2003), 2002. ISSN 1058-6458. URL http://projecteuclid.org/euclid.em/1057864664.

[15] N. Freitas and A. Kraus. On the degree of the $p$-torsion field of elliptic curves over $\mathbb{Q}\_\ell$ for $\ell \neq p$. *ArXiv e-prints*, Apr. 2018.

[16] E. González-Jiménez and Á. Lozano-Robledo. Elliptic curves with abelian division fields. *Math. Z.*, 283(3-4):835–859, 2016. ISSN 0025-5874. URL https://doi.org/10.1007/s00209-016-1623-z.

[17] R. Gupta. Ramification in the Coates-Wiles tower. *Invent. Math.*, 81 (1):59–69, 1985. ISSN 0020-9910. doi: 10.1007/BF01388772. URL https://doi.org/10.1007/BF01388772.

[18] C. Hilliard. *A085548 Decimal expansion of the prime zeta function at 2*. URL https://oeis.org/A085548.

[19] D. Jeon, C. H. Kim, and A. Schweizer. On the torsion of elliptic curves over cubic number fields. *Acta Arith.*, 113(3):291–301, 2004. ISSN 0065-1036. doi: 10.4064/aa113-3-6. URL https://doi.org/10.4064/aa113-3-6.

[20] S. Kamienny. Torsion points on elliptic curves and $q$-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992. ISSN 0020-9910. doi: 10.1007/BF01232025. URL https://doi.org/10.1007/BF01232025.

[21] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988. ISSN 0027-7630. doi: 10.1017/S0027763000002816. URL https://doi.org/10.1017/S0027763000002816.

[22] M. Kida. Ramification in the division fields of an elliptic curve. *Abh. Math. Sem. Univ. Hamburg*, 73:195–207, 2003. ISSN 0025-5858. doi: 10.1007/BF02941276. URL http://dx.doi.org/10.1007/BF02941276.

[23] A. Kraus. Sur la $p$-différente du corps des points de $p$-torsion des courbes elliptiques. *Bull. Austral. Math. Soc.*, 60(3):407–428, 1999. ISSN 0004-9727. doi: 10.1017/S0004972700036595. URL https://doi.org/10.1017/S0004972700036595.

[24] Á. Lozano-Robledo. Formal groups of elliptic curves with potential good supersingular reduction. *Pacific J. Math.*, 261(1):145–164, 2013. ISSN 0030-8730. doi: 10.2140/pjm.2013.261.145. URL https://doi.org/10.2140/pjm.2013.261.145.

[25] Á. Lozano-Robledo. Division fields of elliptic curves with minimal ramification. *Rev. Mat. Iberoam.*, 31(4):1311–1332, 2015. ISSN 0213-2230. doi: 10.4171/RMI/870. URL https://doi.org/10.4171/RMI/870.

[26] Á. Lozano-Robledo. Ramification in the division fields of elliptic curves with potential supersingular reduction. *Res. Number Theory*, 2:Art. 8, 25, 2016. ISSN 2363-9555. URL https://doi.org/10.1007/s40993-016-0040-z.

[27] Á. Lozano-Robledo. Uniform boundedness in terms of ramification. *Res. Number Theory*, 4(1):4:6, 2018. ISSN 2363-9555. doi: 10.1007/s40993-018-0095-0. URL https://doi.org/10.1007/s40993-018-0095-0.

[28] J. Lubin. Canonical subgroups of formal groups. *Trans. Amer. Math. Soc.*, 251:103–127, 1979. ISSN 0002-9947. doi: 10.2307/1998685. URL https://doi.org/10.2307/1998685.

[29] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977. ISSN 0073-8301. URL http://www.numdam.org/item?id=PMIHES_1977__47__33_0.

[30] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978. ISSN 0020-9910. doi: 10.1007/BF01390348. URL https://doi.org/10.1007/BF01390348.

[31] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996. ISSN 0020-9910. doi: 10.1007/s002220050059. URL https://doi.org/10.1007/s002220050059.

[32] T. Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006. ISBN 978-3-540-29592-1; 3-540-29592-5. Translated from the 1976 Japanese original by Yoshitaka Maeda.

[33] F. Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. *Math. Res. Lett.*, 23(1):245–272,

2016. ISSN 1073-2780. doi: 10.4310/MRL.2016.v23.n1.a12. URL https://doi.org/10.4310/MRL.2016.v23.n1.a12.

[34] P. Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999. ISSN 0075-4102. doi: 10.1515/crll.1999.009. URL https://doi.org/10.1515/crll.1999.009.

[35] B. Poonen. Gonality of modular curves in characteristic $p$. *Math. Res. Lett.*, 14 (4):691–701, 2007. ISSN 1073-2780. doi: 10.4310/MRL.2007.v14.n4.a14. URL https://doi.org/10.4310/MRL.2007.v14.n4.a14.

[36] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972. ISSN 0020-9910. URL https://doi.org/10.1007/BF01405086.

[37] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. ISBN 0-387-94328-5. doi: 10.1007/978-1-4612-0851-8. URL http://dx.doi.org/10.1007/978-1-4612-0851-8.

[38] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. ISBN 978-0-387-09493-9. doi: 10.1007/978-0-387-09494-6. URL https://doi.org/10.1007/978-0-387-09494-6.

[39] A. Sutherland. Torsion subgroups of elliptic curves over number fields. 2012. URL https://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf.

Department of Mathematics, University of Colorado, Campus Box 395, Boulder, Colorado 80309-0395

*E-mail address*: hanson.smith@colorado.edu