Ramification in Division Fields and Sporadic Points on Modular Curves

HANSON SMITH

Abstract. Consider an elliptic curve E over a number field K. Suppose that E has supersingular reduction at some prime $\mathfrak{p}$ of K lying above the rational prime p and that $E(K)$ has a point of exact order p^n. To describe the minimum necessary ramification at $\mathfrak{p}$, we completely classify the valuations of the p^n-torsion points of E by the valuation of a coefficient of the p^{th} division polynomial. In particular, if E does not have a canonical subgroup at $\mathfrak{p}$, we show that $\mathfrak{p}$ has ramification index at least $p^{2n} - p^{2n-2}$ over p.

We apply this bound to show that sporadic points on the modular curve $X_1(p^n)$ cannot correspond to supersingular elliptic curves without a canonical subgroup. Our methods are generalized to $X_1(N)$ with N composite.

The goal of this paper is to fully describe the valuations of the coordinates of p^n-torsion points of supersingular elliptic curves via the valuation of the coefficient of $x^{(p^2-p)/2}$ in the p^{th} division polynomial (Theorem 5.3 and Corollary 5.4) and to use this description to preclude certain supersingular elliptic curves to corresponding to sporadic points on the modular curve $X_1(N)$ (Theorems 2.2 and 7.1).

1. Previous Work and Motivation

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 great 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^{th} division field in terms of the p-adic valuation of $j(E)$ and the reduction type of E. With [6], Cali and Kraus describe the p-adic valuation of the different of the l^{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 [17], 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. González-Jiménez and Lozano-Robledo, in [18], classify all elliptic curves $E/\mathbb{Q}$ such that the division field $\mathbb{Q}(E[n])$ is contained in a cyclotomic field. In other words, they classify the $E/\mathbb{Q}$ with 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, Lozano-Robledo finds elliptic curves such that $\operatorname{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}) \cong \operatorname{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ 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 [16] 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 [8], 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.

Date: September 7, 2020.

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.

With our work, we will describe the valuations of the coordinates of a point in $E[p^n]$ when E has supersingular reduction at some prime above p. This description depends only on the valuation of a certain coefficient of the p^{th} division polynomial, Ψ_p. As an immediate consequence, we obtain the minimum necessary ramification for the existence of such a point.

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

Question 1.1. Let K be a field of fixed degree d (resp. fixed Galois group G). What are the possibilities for the group $E(K)_{\text{tors}}$ as we vary E?

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

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

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

This answers Question 1.1 when $d = 1$ (resp. G is trivial).

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:

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

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 (and j-invariant $-1 \cdot 2^{-3} \cdot 3^2 \cdot 5^6$). Najman [32] has shown

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

However, it is known that only finitely many isomorphism classes of 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*[1]. 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 shown that $X_1(21)$ is the only modular curve with a cubic sporadic point [13]. In fact, they show that the only cubic sporadic point is the one corresponding to Najman's curve. Combined with the work of Jeon, Kim, and Schweizer [19], this shows that if $[K : \mathbb{Q}] = 3$, then $E(K)_{\text{tors}}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/N\mathbb{Z} \quad \text{for } 1 \leq N \leq 21 \text{ with } N \neq 17, 19,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad \text{with } 1 \leq N \leq 7.$$

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 [4] have made an insightful investigation of sporadic j-invariants. Among the many results in [4], they have shown that, assuming Serre's uniformity conjecture, the number of

[1] Sporadic points are also called *unexpected points* or *exceptional points* in the literature.

sporadic j-invariants (j-invariants corresponding to a sporadic point on a modular curve $X_1(N)$ for some $N > 0$) 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 [12, Appendix A]. Parent [33] 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 such that if E has a point of exact order p^n over a number field of degree d, 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]. We take the same approach as Lozano-Robledo to understand the multiplication-by-p map in the formal group. For the most part Theorem 5.3 agrees with [26, Lemma 5.3]; however, we find a phenomenon similar in some respects to the canonical subgroup can occur for p^n-torsion, with $n > 1$. Thus, with Theorem 5.3, we essentially reprove [26, Lemma 5.3] and make a correction in a certain case. We note that this correction does not affect the main result of [26].

Acknowledgments

The author would like to thank Álvaro Lozano-Robledo for the helpful correspondence, Katherine Stange for the advice, direction, and patience, and Alex Braat for discovering a false claim in an earlier version of this paper. The author is also indebted to David Grant for kindly pointing out [5] and for suggesting more focus on the formal group. This research was partially supported by NSF-CAREER CNS-1652238 under the supervision of PI Dr. Katherine E. Stange.

2. Results

We begin by establishing some notation and conventions along with our setup. These will hold unless otherwise specified. Let E be an elliptic curve over a number field K and $P \in E(K)$ a point of exact order p^n. Let $\mathfrak{p}$ be a prime of K lying over $p \in \mathbb{Z}$ at which E has good supersingular reduction. We can adjoin all the p^n-torsion points of E to K to obtain the full p^n-th division field[2],

[2]This field is also commonly called the p^n-th *torsion field* in the literature.

$K(E[p^n])$. Write $\mathfrak{P}$ for a prime of $K(E[p^n])$ lying over $\mathfrak{p}$. We will be studying the ramification of $\mathfrak{p}$, and to a lesser extent $\mathfrak{P}$, over p.

Definition 2.1. Let $e_{\mathfrak{p}}$ denote the ramification index of $\mathfrak{p}$ over p and $e_{\mathfrak{P}}$ the ramification index of $\mathfrak{P}$ over p.

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

FIGURE 1.

The ring of integers of K is $\mathcal{O}_K$, and the local field obtained by completing K at $\mathfrak{p}$ is denoted $K_{\mathfrak{p}}$. The valuation is denoted v, since p will be clear from context, and is normalized so that $v(p) = 1$. We let $\pi_{\mathfrak{p}}$ be a uniformizer. The residue field of $K_{\mathfrak{p}}$ at $\mathfrak{p}$ is denoted $k_{\mathfrak{p}}$. As is common, the algebraic closure of a given field will be denoted with an overbar, e.g., $\overline{k_{\mathfrak{p}}}$.

Our work is primarily concerned with using ramification above p to bound the degree of K. We accomplish this by analyzing the formal group. In Section 3 we will briefly review some facts about division polynomials, and in Section 4 we will revisit Cassels's paper [7] to motivate our work. In Section 5, we completely classify the valuations of p^n-torsion elements of the formal group in the supersingular case. This classification involves the *canonical subgroup*, a distinguished subgroup of $E[p]$ that lifts the kernel of Frobenius; see Definition 5.1. As a consequence of Theorem 5.3 we obtain

Theorem 2.2. *Minimal values for $e_{\mathfrak{p}}$ and $e_{\mathfrak{P}}$ can be determined from the valuation of a coefficient of the p^{th} division polynomial. The minimal values are*

$$e_{\mathfrak{P}} \geq p^{2n} - p^{2n-2} \qquad \textit{and} \qquad e_{\mathfrak{p}} > \varphi(p^n) = p^n - p^{n-1}. \tag{1}$$

Further, if E does not have a canonical subgroup at $\mathfrak{p}$, then

$$p^{2n} - p^{2n-2} \mid e_{\mathfrak{p}}. \tag{2}$$

If E has a canonical subgroup at $\mathfrak{p}$, then $e_{\mathfrak{P}} > p^{2n} - p^{2n-2}$.

Another consequence of our work is that if E is defined over a number field with a supersingular prime below $\mathfrak{p}$ that is unramified over p, then E cannot have a canonical subgroup at $\mathfrak{p}$. Hence Equation (2) holds.

Corollary 2.2 and other straightforward consequences of Section 5 are the subject of Section 6. In Section 7, we use ramification to show that, on $X_1(p^n)$, a subset of the supersingular locus is disjoint from the sporadic locus:

Theorem 2.3. *Let L be a number field and E/L be an elliptic curve that is supersingular at some prime $\mathfrak{p}$ of $\mathcal{O}_L$ above p. Suppose that E does not have a canonical subgroup at $\mathfrak{p}$, then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$.*

Understanding ramification also provides a similar, though slightly weaker result for $X_1(N)$, with N composite; this is the content of Theorem 7.1. After proving these theorems, we demonstrate via some examples how our methods can be generalized when one is interested in specific modular curves.

The methods we use in Section 5 follow a very similar vein to Lozano-Robledo's methods in [26], though we focus more heavily on division polynomials, so the flavor is somewhat different. It is possible that some of our results are known in various guises, but to our knowledge they have not appeared in the literature as they are stated here. Moreover, our application to sporadic points on modular curves appears novel.

3. Background on Division Polynomials

Keeping the same assumptions on E as in Section 2, we write a 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

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

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 [35, Exercise 3.7]. If m is odd, we can write

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

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

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

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, Ψ_m has degree $\frac{m^2-1}{2}$. The even division polynomials also have degree $\frac{m^2-1}{2}$, so long as we think of y as having degree $\frac{3}{2}$ in x.

It is convenient to have the valuations of the constant coefficients of various division polynomials.

Lemma 3.1. *Keep the same assumptions as in Section 2. If p is an odd prime, write c_0 for the constant coefficient of Ψ_{p^n} and if $p = 2$, write c_0 for the constant coefficient of $\Psi_2\Psi_{2^n}$, then $v\left(c_0\right) = 0$.*

Proof. Assume p is odd and choose some $Q \in E\left(\overline{k_\mathfrak{p}}\right)$ with $x(Q) = 0$. Note that α is a root of Ψ_{p^n} if and only if points on E with x-coordinates equal to α are p^n-torsion points. Thus $\Psi_{p^n}(0) = c_0 \equiv 0$ modulo $\mathfrak{p}$ if and only if Q 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 Q does not have order dividing p^n and $v_\mathfrak{p}(c_0) = 0$. For $p = 2$, repeat the above, but replace Ψ_{p^n} with $\Psi_2\Psi_{2^n}$. □

Note that since $\Psi_{p^n}/\Psi_{p^{n-1}}$ has leading coefficient p, the p-adic valuations of the distinct x-coordinates of points of exact order p^n sum to negative one. That is, letting $E\left[=p^n\right]$ denote the points of exact order p^n,

$$\sum_{P \in E[=p^n]/\pm} v\left(x(P)\right) = -1. \tag{3}$$

The exception to Equation (3) is when $p^n = 2$, then the valuations of the roots of Ψ_2^2 is

$$\sum_{P \in E[=2]} v\left(x(P)\right) = -2. \tag{4}$$

Remark 3.2. Without referencing the formal group, we can already use Lemma 3.1 to obtain some of our results. Let E be an elliptic curve over a number field K with an unramified prime $\mathfrak{p}$ over p at which E is supersingular. To employ a "reciprocal Eisenstein" trick, consider the polynomial

$$x^{-\frac{p^2-1}{2}}\Psi_p\left(x^{-1}\right) \in K_{\mathfrak{p}}[x].$$

Since $\mathfrak{p}$ is unramified and Ψ_p has leading coefficient p, one can show this polynomial is Eisenstein. Hence, with some additional consideration of the y-coordinate, adjoining a point of exact order p to $K_{\mathfrak{p}}$ is a totally ramified extension of degree p^2-1. For p^n-torsion, we can employ this same trick with

$$x^{-\frac{p^{2n}-p^{2n-2}}{2}}\frac{\Psi_{p^n}}{\Psi_{p^{n-1}}}\left(x^{-1}\right).$$

Though this result is significantly weaker than Theorem 5.3, it is actually all that is necessary to prove Theorem 7.1.

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

We begin by quoting Theorem IV of [7], Cassels's note on the division values of the Weierstrass $\wp$-function.

Theorem 4.1. *Let F be a number field and $E_{A,B}: \quad y^2 = x^3 - Ax - B$ an elliptic curve over F is short Weierstrass form with $A, B \in \mathcal{O}_F$. 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*

$$\mathfrak{t}^{\varphi(p^n)} \mid p \text{ for } p \neq 3, \tag{5}$$

$$\mathfrak{t}^{3^{2n}-3^{2n-2}} \mid 3 \text{ for } p = 3. \tag{6}$$

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

In an earlier version of this paper, the author believed that there was a mistake in Theorem 4.1; however, Cassels's result is explicitly for elliptic curves in short Weierstrass form and does not hold for an arbitrary elliptic curve in generalized Weierstrass form.

If $\mathfrak{p}$ is a prime of F above 3 and $E_{A,B}$ has good reduction at $\mathfrak{p}$, then $E_{A,B}$ is supersingular at $\mathfrak{p}$. See [38, pg. 103]. Explicitly, one has

$$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2.$$

Since $\mu = v\left(c_{\frac{9-3}{2}} = 0\right) = \infty$, we see (via Theorem 5.3) that there is no canonical subgroup. Hence the result.

With Theorem 5.3 we will show that, when an elliptic curve E is supersingular at one of the primes above p, then (5) holds and *the divisibility is proper*. In other words, the ramification above p is greater than $\phi(p^n)$. Further, if $\mu \geq \frac{p}{p+1}$, then (6) will hold.

5. Analyzing the Formal Group

In this section we elaborate on Lemma 4.7 of [5] and Lemma 5.3 of [26] to suit our application. All the facts used here regarding formal groups can be found in [35, Chapter IV]. For the case when the ramification index above p is 1, see Serre's landmark paper [34]; the endnote in Section 1.11 alludes to the direction we take here.

We recall our setup. Unless otherwise noted, in this section $P \in E(K)$ will be a point with exact order p^n, with $n \geq 1$, on an elliptic curve E that is supersingular at some prime $\mathfrak{p} \subset \mathcal{O}_K$ lying above the odd prime p; for the caveat with $p = 2$, see Remark 5.7. As before, v is the valuation associated to $\mathfrak{p}$, normalized so that $v(p) = 1$.

Let $F_E \in K_{\mathfrak{p}}[\![S,T]\!]$ denote the formal group law of E over $K_{\mathfrak{p}}$. Let $\pi_{\mathfrak{p}}$ be a uniformizer at $\mathfrak{p}$; the set of elements of the ideal $(\pi_{\mathfrak{p}})$ becomes a group under F_E and will be denoted $\hat{E}$. If $\beta \in \hat{E}$, the map $\beta \mapsto (x(\beta), y(\beta))$ yields an injection from $\hat{E}$ into $E(K_{\mathfrak{p}})$. Conversely, if $(x,y) \in E(K_{\mathfrak{p}})$ is in the kernel of reduction, then $(x,y) \mapsto \frac{-x}{y} \in \hat{E}$ yields an inverse, so that $\hat{E}$ is isomorphic to the kernel of reduction modulo $\pi_{\mathfrak{p}}$. If Q is in the kernel of reduction, write $\hat{Q}$ for the image of Q in $\hat{E}$, i.e., $\frac{-x(Q)}{y(Q)}$. We will often just use $+$ to denote addition in $\hat{E}$. The reader may find it useful to recall the following identity for moving between valuations of roots of division polynomials and of elements of the formal group:

$$v(x(Q)) = -2v\left(\hat{Q}\right).$$

Consider $E[p^n]$. Since E is supersingular, $E[p^n] \cong \hat{E}[p^n]$. We will conflate these groups when context makes our meaning clear. Recall $E[=p^n]$ is the set of points of exact order p^n. Multiplication by an integer relatively prime to p is an automorphism of $\hat{E}[p]$. Choosing a basis $\{B_1, B_2\}$, the action of $(\mathbb{Z}/p\mathbb{Z})^*$ has $p+1$ orbits:

$$\langle B_1 \rangle, \langle B_1 + B_2 \rangle, \ldots, \langle B_1 + [p-1]B_2 \rangle, \langle B_2 \rangle.$$

We label the orbits C_0 through C_p. Excluding the identity, we notice $v\left(\hat{Q}\right)$ is the same for all $\hat{Q}$ in a given orbit.

We have two possibilities: In one case, $v\left(\hat{Q}\right)$ is the same for all $\hat{Q} \in \hat{E}[=p]$. In the other case, $v\left(\hat{R}\right) > v\left(\hat{Q}\right)$ for all $\hat{R}$ in some orbit C_i and all $\hat{Q}$ in some other orbit C_j. We notice $v\left(\hat{S}\right) = v\left(\hat{Q}\right)$ if $\hat{S}$ is in any orbit C_k with $k \neq i$. This is because $\hat{S} = [l]\hat{R} + [m]\hat{Q}$ for some $l, m \in \mathbb{Z}/p\mathbb{Z}$ with $m \neq 0$, and $F_E(S,T) = S + T + (\text{terms of degree } \geq 2)$.

Definition 5.1. The orbit C_i along with the identity is called the *canonical subgroup*[3]. That is, if there exists $\hat{R} \in \hat{E}[=p]$ such that $v\left(\hat{R}\right) > v\left(\hat{Q}\right)$ for some $\hat{Q} \in \hat{E}[=p]$, then the orbit $\left\langle \hat{R} \right\rangle$ is the canonical subgroup and denoted C_{can}.

Imprecisely speaking, we could say elliptic curves with a canonical subgroup are less supersingular since, like ordinary elliptic curves, they also have a distinguished subgroup of order p that is a canonical lift of the kernel of Frobenius. For more general discussions of canonical subgroups, the reader should consult [28] and [10]. Lubin's article [28], in particular, has a number of nice examples.

We are primarily concerned with the fact that elements in the canonical subgroup have larger valuations (equivalently, the fact that x-coordinates of points in C_{can} have smaller valuations). In this section, we will show that there can be a similar phenomenon in certain fibers $[p]^{-1}\hat{Q}$, where $\hat{Q} \in \hat{E}\left[=p^{n-1}\right]$. Specifically, there may be a set of p elements in $[p]^{-1}\hat{Q}$ with larger valuations; see Figure 5. If $\hat{W}$ is one such element, the others all have the form $\hat{W} + \hat{R}$ with $\hat{R} \in C_{\text{can}}$. Moreover, the subgroup of $\hat{E}[p^n]$ generated by any such $\hat{W}$ is exactly the set of elements of order dividing p^n with larger valuation; see Remark 5.5.

For $p > 2$, define $\mu := v\left(c_{\frac{p^2-p}{2}}\right)$, where

$$\Psi_p(x) = px^{p^2-1} + c_{p^2-2}x^{p^2-2} + \cdots + c_1 x + c_0$$

is the p^{th} division polynomial. For $p = 2$, define $\mu := v\left(a_1^2 + 4a_2\right)/2$. With $p = 2$, the following discussion needs to be augmented slightly since x-coordinates of points in $E[=2]$ are distinct; see

[3]The nomenclature comes from the fact that such a subgroup is a canonical lifting of the kernel of Frobenius.

Remark 5.7. Returning to the discussion at hand, label the distinct x-coordinates of points in $E[=p]$ as $x_1, \ldots, x_{\frac{p^2-1}{2}}$. Notice

$$c_{\frac{p^2-p}{2}} = p \sum_{1 \le i_1 < i_2 < \cdots < i_{\frac{p-1}{2}} \le \frac{p^2-1}{2}} x_{i_1} \cdots x_{i_{\frac{p-1}{2}}}. \tag{7}$$

If there is a canonical subgroup, there is a distinct summand on the right-hand side of (7) with smallest valuation (recall, we multiply valuations by -2 to move between $\hat{E}$ and x-coordinates of points on E). Namely, the summand with smallest valuation is the product of the $\frac{p-1}{2}$ distinct x-coordinates of points in C_{can}. Hence, if we have a canonical subgroup, $-(1-\mu)$ is the sum of the valuations of all the distinct x-coordinates of points that are in C_{can}. We see the valuation of the x-coordinate of a point in C_{can} is $\frac{-2(1-\mu)}{p-1}$. Hence, the valuation of the x-coordinate of a point that is not in C_{can} is $\frac{-2\mu}{p^2-p}$. Note, μ is defined to correspond to valuations in $\hat{E}$. Thus, if $P \in C_{\text{can}}$, then $v\left(\hat{P}\right) = \frac{1-\mu}{p-1}$, and if $P \notin C_{\text{can}}$, then $v\left(\hat{P}\right) = \frac{\mu}{p^2-p}$.

A classical criterion of Deuring [14] states that $E : y^2 = f(x)$ is supersingular at $\mathfrak{p}$ if and only if the coefficient of x^{p-1} in $f(x)^{\frac{p-1}{2}}$ vanishes modulo $\mathfrak{p}$. One may be curious how the coefficient $c_{\frac{p^2-p}{2}}$ is related to Deuring's coefficient. Thanks to Debry [11], we know that they are in fact equal. Thus, for such E, we could just as well define μ to be the valuation of Deuring's coefficient.

Many authors (such as [5], [26], [28], [34]) prefer to work directly with the multiplication-by-p power series, $[p]T$, as opposed to the division polynomial. In this case, the valuation of the coefficient of T^p in $[p]T$ indicates whether or not there is a canonical subgroup. Following [5], we have called this valuation μ. The coefficient of T^p is the sum of distinct products of p^2-p elements of $\hat{E}[=p]$. If there is a canonical subgroup, μ is the sum of the valuations of the p^2-p elements that are not in C_{can}. As such, $\mu < \frac{p}{p+1}$. Conversely, if there is not a canonical subgroup, $\mu \ge \frac{p}{p+1}$. Since all elements of $\hat{E}[=p]$ have the same valuation in this case, Equation (7) shows the valuation of each element must be $\frac{1}{p^2-1}$.

Before we state the main theorem of this section, it may be useful to actually "see" a canonical subgroup. To this end, we revisit a nice example that can be found in Lozano-Robledo's papers [24] and [26].

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 $\mathbb{Q}\left(\sqrt[3]{11}\right)$ 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 [15], one can compute the factorization

$$\begin{aligned}\Psi_{11} &= 11x^{60} + \cdots + 195530917\sqrt[3]{11}x^{55} + \cdots - 7312712\sqrt[3]{11}x - 303271 \\ &= 11\left(x^5 + \sqrt[3]{11^2}x^4 + 3\sqrt[3]{11}x^3 + 3x^2 - \frac{1}{\sqrt[3]{11^2}}\right)\left(x^{55} + \cdots + \frac{303271}{\sqrt[3]{11}}\right).\end{aligned}$$

The valuation of the coefficient of x^{55} is $\frac{1}{3}$, so $\mu = \frac{1}{3}$. From the factorization above, we see that the sum of the valuations of the five distinct x-coordinates of 11-torsion points in the canonical subgroup is $-\frac{2}{3} = -(1-\mu)$. Figures 2 and 3 illustrate the various Newton polygons associated to the 11-torsion on this elliptic curve. The polygons are constructed by taking the lower convex hull of the points $(i, v(c_i))$, where c_i is the coefficient of x^i or T^i. We can visualize the canonical subgroup in its various guises as the side of the Newton polygon with steepest slope. Figure 2 is labeled specifically referring to our Ψ_{11}, while Figure 3 is labeled generally to help clarify the larger discussion.

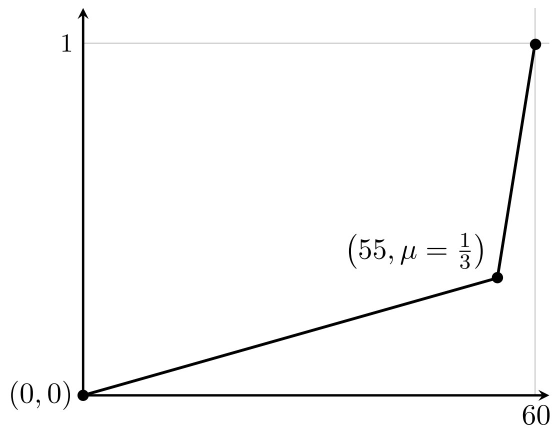

FIGURE 2. The Newton polygon for the polynomial $\Psi_{11} = 11 \prod_{P \in E[=11]/\pm} (x - x(P))$

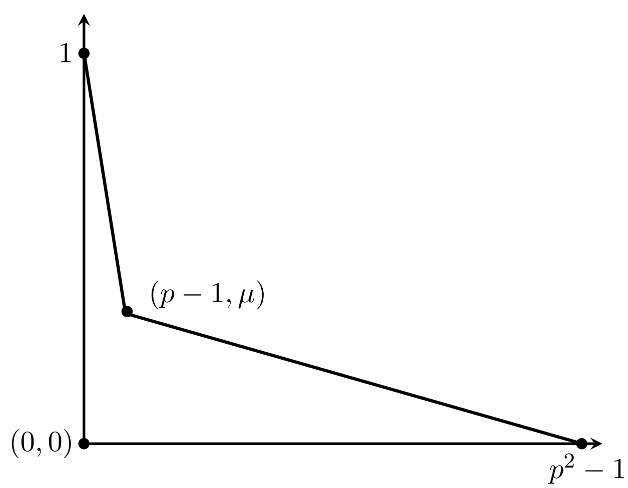

FIGURE 3. The Newton polygon for the polynomial $\prod_{\hat{P} \in \hat{E}[=11]} T - \hat{P}$

Of particular import to our work in Section 7 is that there is a degree 10 extension of $\mathbb{Q}\left(\sqrt[3]{11}\right)$ over which E has a point of exact order 11. If we did not have a canonical subgroup at 11, an extension of at least degree 40 (degree $120 = 11^2 - 1$ over $\mathbb{Q}$) would be needed to ensure the requisite ramification for an 11-torsion point.

With a way to visualize things, we are ready for the main theorem of the section. Some of the expressions in the theorem below are not fully simplified. This is deliberate and intended to make it easier for the reader to better understand how the values are obtained.

Theorem 5.3. *Keep the same notation as above and recall $P \in E\,[=p^n]$. If $\mu \geq \frac{p}{p+1}$, then there is no canonical subgroup at $\mathfrak{p}$ and*

$$v\left(\hat{P}\right) = \frac{1}{p^{2n} - p^{2n-2}}. \tag{8}$$

Otherwise, $0 < \mu < \frac{p}{p+1}$ *and there is a canonical subgroup at* $\mathfrak{p}$*. In this case, if* $\left[p^{n-1}\right] P \notin C_{\text{can}}$*, then*

$$v\left(\hat{P}\right) = \frac{\mu}{p^{2n-2}\left(p^2 - p\right)}. \tag{9}$$

If $\left[p^{n-1}\right] P \in C_{\text{can}}$*, then there are a number of cases: First, if* $n = 1$*,*

$$v\left(\hat{P}\right) = \frac{1-\mu}{p-1}. \tag{10}$$

For $n > 1$*, if there is a smallest non-negative integer* m *such that* $v\left(\left[p^m\right]\hat{P}\right) = \frac{\mu}{p^2-p}$*, then*

$$v\left(\hat{P}\right) = \frac{\mu}{p^{2m}(p^2 - p)}. \tag{11}$$

If no such integer exists, then let $s \in \mathbb{Z}^{\geq 0}$ *be the smallest integer such that* $\mu \geq \frac{1}{p^s(p+1)}$*. If* $n > s+1$*, then*

$$v\left(\hat{P}\right) = \frac{1 - p^s\mu}{p^{2n-s-2}(p-1)}. \tag{12}$$

Otherwise,

$$v\left(\hat{P}\right) = \frac{1 - p^{n-1}\mu}{p^{n-1}(p-1)}. \tag{13}$$

Write $\hat{Q} := [p]\hat{P}$*. In the last case, there are* p *elements in* $[p]^{-1}\hat{Q}$ *of valuation* $\frac{1-p^{n-1}\mu}{p^{n-1}(p-1)}$ *and* $p^2 - p$ *elements of valuation* $\frac{\mu}{p^2-p}$*.*

If we change perspectives slightly, we obtain

Corollary 5.4. *If* $n \leq s+1$*, then there are* $p^{n-1}(p-1)$ *elements of* $\hat{E}\left[=p^n\right]$ *above* C_{can} *with valuation* $\frac{1-p^{n-1}\mu}{p^{n-1}(p-1)}$ *and, for all* $2 \leq j \leq n$*, there are* $p^{2(n-j)}(p^2-p)p^{j-2}(p-1)$ *elements with valuation* $\frac{\mu}{p^{2(n-j)}(p^2-p)}$*.*

If $n > s+1$*, then there are* $p^{2(n-s-1)}p^s(p-1)$ *elements of* $\hat{E}\left[=p^n\right]$ *above* C_{can} *with valuation* $\frac{1-p^s\mu}{p^{2(n-s-1)}p^s(p-1)}$ *and, for all* $2 \leq j \leq s+1$*, there are* $p^{2(n-j)}(p^2-p)p^{j-2}(p-1)$ *elements with valuation* $\frac{\mu}{p^{2(n-j)}(p^2-p)}$*.*

In either case, there are exactly $p^{2(n-1)}(p^2-p)$ *elements of* $\hat{E}\left[=p^n\right]$ *that are not above* C_{can}*. Each of these elements has valuation* $\frac{\mu}{p^{2(n-1)}(p^2-p)}$*.*

Among other things, Theorem 5.3 and Corollary 5.4 show that the phenomenon of having subsets of larger valuation is not just relegated to the p-torsion. In certain fibers $[p]^{-1}\hat{Q}$, with $\hat{Q} \in \hat{E}\left[=p^{n-1}\right]$ and $v\left(\hat{Q}\right) = \frac{1-p^{n-2}\mu}{p^{n-2}(p-1)}$, there exists a subset of size p whose elements have larger valuation than the other elements of the fiber. Namely, the p elements all have valuation $\frac{1-p^{n-1}\mu}{p^{n-1}(p-1)}$, while the other elements have valuation $\frac{\mu}{p^2-p}$. Further, these elements of large valuation all differ by an element of C_{can}. However, at a certain level (specifically, when $n > s+1$), the phenomenon stops and all valuations in a given fiber are the same and obtained by simply dividing by p^2. This behavior is all totally determined by the valuation of a coefficient of the polynomial Ψ_p.

We note, that if one wishes for the valuations of x-coordinates of p^n-torsion points of E, they need only multiply the equations in Theorem 5.3 by -2.

Proof. First, Lemma 3.1 shows $\mu > 0$. We proceed by induction on n. The base case, including Equation (10), is established by the discussion immediately preceding Example 5.2.

For the induction step, suppose we have our result for all $k < n$. Define $Q := [p]P$, and consider the power series $[p]T - \hat{Q}$ in $K_{\mathfrak{p}}[\![T]\!]$. If α is a root of $[p]T - \hat{Q}$ in $\overline{K_{\mathfrak{p}}}$, e.g., $\alpha = \hat{P} = -\frac{x(P)}{y(P)}$, then we see $v([p]\alpha) = v\left(\hat{Q}\right)$. Because the height of the formal group is 2, we have $[p]T = pf(T) + \pi_{\mathfrak{p}}^{\mu} g\left(T^p\right) + h\left(T^{p^2}\right)$, where f, g, and h are power series without constant coefficients and with $f'(0), g'(0), h'(0) \in K_{\mathfrak{p}}^*$.

Recall $v\left(\hat{Q}\right) < 1$ by hypothesis. If $v([p]\alpha) \geq v(p\alpha) = 1 + v(\alpha)$, then $v(\alpha) \leq v\left(\hat{Q}\right) - 1 < 0$. We have a contradiction, since $\alpha \in (\pi_{\mathfrak{p}})$. Thus $v([p]\alpha) < v(p\alpha)$ and

$$v([p]\alpha) \geq \min\left(v\left(\pi_{\mathfrak{p}}^{\mu}\alpha^p\right), v\left(\alpha^{p^2}\right)\right) = \min\left(\mu + pv(\alpha), p^2 v(\alpha)\right). \tag{14}$$

Using $v(\alpha) < v\left(\left[p^{n-1}\right]\alpha\right) = \frac{1}{p^2-1}$, a short computation with (14) yields Equation (8).

Generally, suppose $[p^m]\alpha = \hat{R}$ with $0 < m < n$ and $v\left(\hat{R}\right) \leq \frac{\mu}{p^2-p}$. If $\mu + pv(\alpha) \leq p^2 v(\alpha)$, then $v(\alpha) \geq \frac{\mu}{p^2-p} \geq v\left(\hat{R}\right)$ and we have a contradiction. Thus, if $[p^m]\alpha = \hat{R}$, then $v(\alpha) = \frac{1}{p^{2m}} v\left(\hat{R}\right)$. This gives us Equations (9) and (11).

We turn our attention to establishing Equations (12) and (13), so we assume $\mu < \frac{p}{p+1}$. Consider $\alpha \in [p]^{-1}\hat{Q}$, where $\hat{Q} \in \hat{E}\left[=p^{n-1}\right]$ has valuation $\frac{1-p^{n-2}\mu}{p^{n-2}(p-1)}$. Suppose $\mu \geq \frac{1}{p^{n-2}(p+1)}$ and, for a contradiction, take the case that $\mu + pv(\alpha) \leq p^2 v(\alpha)$. Using $v\left(\hat{Q}\right) \leq \frac{1}{p^{n-3}(p^2-1)}$, we obtain

$$\frac{1}{p^{n-1}(p^2-1)} \leq \frac{\mu}{p^2-p} \leq v(\alpha) \leq \frac{v\left(\hat{Q}\right)}{p^2} \leq \frac{1}{p^{n-1}(p^2-1)}.$$

Unless $\mu = \frac{1}{p^{n-2}(p+1)}$, we have a contradiction. In any case, using (14), we obtain Equation (12). To rephrase, if $\mu \geq \frac{1}{p^{n-2}(p+1)}$, then the valuations of p^k-th roots of $\hat{Q}$ are obtained by dividing $v\left(\hat{Q}\right)$ by p^{2k}.

Suppose $\mu < \frac{1}{p^{n-2}(p+1)}$ and $v\left(\hat{Q}\right) = \frac{1-p^{n-2}\mu}{p^{n-2}(p-1)}$. For a contradiction suppose $v(\alpha) = \frac{1}{p^2} v\left(\hat{Q}\right) = \frac{1-p^{n-2}\mu}{p^n(p-1)}$. Using the upper bound on μ, we compute

$$\mu + p\left(\frac{1-p^{n-2}\mu}{p^n(p-1)}\right) < \frac{1}{p^{n-3}(p^2-1)} < p^2\left(\frac{1-p^{n-2}\mu}{p^n(p-1)}\right).$$

Hence $\mu + pv(\alpha) < p^2 v(\alpha)$ and $v([p]\alpha) = \mu + pv(\alpha)$. This contradicts our hypothesis that $v(\alpha) = \frac{1}{p^2} v\left(\hat{Q}\right)$. Therefore $\mu + pv(\alpha) \leq p^2 v(\alpha)$ for all $\alpha \in [p]^{-1}\hat{Q}$.

For at least one $\alpha \in [p]^{-1}\hat{Q}$, we will have $v([p]\alpha) = \mu + pv(\alpha)$. If this was not the case, then $v(\alpha) > \frac{1}{p^2} v\left(\hat{Q}\right)$ for every $\alpha \in [p]^{-1}\hat{Q}$. Hence $\sum_{\alpha \in [p]^{-1}\hat{Q}} v(\alpha) > v\left(\hat{Q}\right)$. However the elements of $[p]^{-1}\hat{Q}$ are exactly the roots of $[p]T - \hat{Q}$ and the valuation of the constant coefficient is $v\left(\hat{Q}\right)$. Thus there exist $\alpha \in [p]^{-1}\hat{Q}$ with $v(\alpha) = \frac{1-p^{n-1}\mu}{p^{n-1}(p-1)}$. Considering sums of the form $\alpha + \hat{S}$ with $\hat{S} \in \hat{E}[p]$, we see that there are p elements in $[p]^{-1}\hat{Q}$ with valuation $\frac{1-p^{n-1}\mu}{p^{n-1}(p-1)}$ and $p^2 - p$ with valuation $\frac{\mu}{p^2-p}$. □

Corollary 5.4 is established by a straightforward count.

Remark 5.5. Suppose $\hat{W} \in \hat{E}\left[=p^n\right]$ is an element of large valuation, i.e., $v(\hat{W}) = \frac{1-p^{n-1}\mu}{p^{n-1}(p-1)}$. As a porism of Theorem 5.3, the subgroup of $\hat{E}\left[p^n\right]$ generated by $\hat{W}$ is exactly the set of elements of $\hat{E}\left[p^n\right]$ with large valuation. In other words, $\langle\hat{W}\rangle$ is C_{can} and every element above C_{can} with valuation $\frac{1-p^k\mu}{p^k(p-1)}$, where $1 \leq k \leq n-1$.

Example 5.6. Consider the elliptic curve $E : y^2 + \sqrt[5]{3}xy + y = x^3 + \sqrt[5]{3}x^2 + 2x$ over $\mathbb{Q}\left(\sqrt[5]{3}\right)$. This curve has good supersingular reduction at $\left(\sqrt[5]{3}\right)$, the lone prime above 3. We can compute $\Psi_3 = 3x^4 + \left(\sqrt[5]{3^2} + 4\sqrt[5]{3}\right)x^3 + \left(3\sqrt[5]{3} + 12\right)x^2 + 3x - \sqrt[5]{3} - 4$. Thus $\mu = v\left(\sqrt[5]{3^2} + 4\sqrt[5]{3}\right) = \frac{1}{5} < \frac{1}{3+1}$.

There are 36 distinct x-coordinates of points in $E[=9]$. By Theorem 5.3, there are 27 with $v(x(P)) = -\frac{\mu}{27} = -\frac{1}{135}$, there are 6 with $v(x(P)) = -\frac{\mu}{3} = -\frac{1}{15}$, and 3 with $v(x(P)) = \frac{3\mu-1}{3} = -\frac{2}{15}$. Thus in $\frac{\Psi_9}{9\Psi_3}$, the coefficient of x^{33} should have valuation $3\mu - 1 = -\frac{2}{5}$ and the coefficient of x^{27} should have valuation $\mu - 1 = -\frac{4}{5}$. A computation verifies this.

Shifting to thinking about elements of the formal group, Figure 5 shows the fiber $[p]^{-1}\hat{Q}$ where $\hat{Q} \in C_{\text{can}}$. We see there are three elements of larger valuation $\frac{1}{15}$ and six elements of smaller valuation $\frac{1}{30}$.

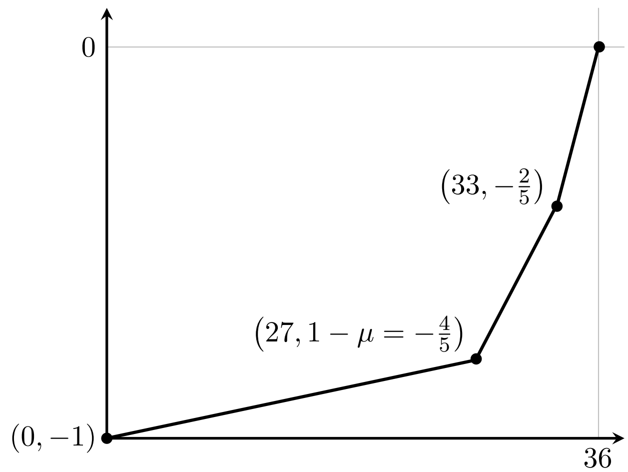

FIGURE 4. The Newton polygon for the polynomial $\Psi_9/\left(9\Psi_3\right)$

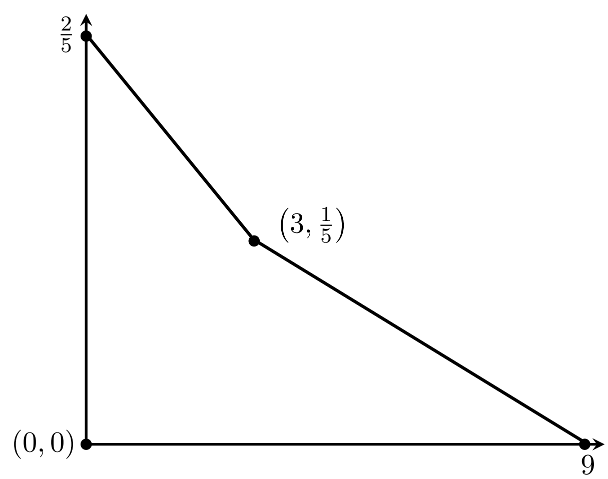

FIGURE 5. The fiber above an element of C_{can}

Remark 5.7. Consider now the case that $p = 2$. Our work above with the formal group carries through almost verbatim, but there is a slight caveat for division polynomials. The roots of $\psi_2 =$

$2y+a_1x+a_3$ are not the distinct x-coordinates of the non-trivial 2-torsion points. Instead we must take

$$\Psi_2^2 = 4x^3 + \left(4a_2 + a_1^2\right)x^2 + (4a_4 + 2a_1a_3)x + 4a_6 + a_3^2 = 4 \cdot \prod_{P \in E[=2]} (x - x(P)).$$

Now $\sum_{P\in E[=2]} v_2(x(P)) = -2$ instead of -1. However, summing over distinct x-coordinates does not introduce a factor of 2 as the x-coordinates of the points in $E[=2]$ are all distinct. Similarly to above, we wish to isolate the coefficient of $\frac{1}{4}\Psi_2^2$ that captures the canonical subgroup if it exists. We see $\eta := v_2\left(\frac{1}{4}\left(4a_2 + a_1^2\right)\right)$ is the valuation of the x-coordinate of the single point in the canonical subgroup, if there is one. The corresponding element of $\hat{E}$ has valuation $-\frac{\eta}{2}$. The constant coefficient of $[2]T/T$ is 2, hence $\mu = 1 + \frac{\eta}{2} = v_2\left(4a_2 + a_1^2\right)/2$.

6. Ramification in Division Fields

Theorem 2.2 is a quick consequence of our work in Section 5:

Proof of Theorem 2.2. Equations (1) and (2) are implied directly by Theorem 5.3. A computation with maximal values of μ, shows $e_{\mathfrak{P}} > p^{2n} - p^{2n-2}$ when there is a canonical subgroup. $\square$

Theorem 5.3 can also be used, in conjunction with a lack of ramification, to preclude the existence of a canonical subgroup.

Corollary 6.1. *No elliptic curve defined over $\mathbb{Q}$ has a canonical subgroup at any prime. More generally, no elliptic curve that is supersingular at $\mathfrak{p}$, some unramified prime over p, has a canonical subgroup at $\mathfrak{p}$.*

Proof. We consider μ, and note $0 < \mu < \frac{p}{p+1}$ is required for a canonical subgroup. The existence of such a valuation requires ramification. $\square$

We remark that isogenies of degree coprime to p also preserve the existence or nonexistence of canonical subgroups.

For a positive integer m, define a *minimal m-torsion point field* of an elliptic curve over a number field to be an extension of minimal degree such that the elliptic curve has a point of order m over that extension. The following corollary describes where ramification in a composite level torsion point field is coming from. It will be used in Section 7.

Corollary 6.2. *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*

$$[L:\mathbb{Q}] = \prod_{i=1}^{k}\left(p_i^{2n_i} - p_i^{2n_i-2}\right).$$

Though we have stated Corollary 6.2 over $\mathbb{Q}$, it is valid over any number field in which there is at least one unramified, supersingular prime over each prime dividing N.

Proof. Let L_i be a minimal $p_i^{n_i}$-torsion point field. If $p_i \neq p_j$, then p_j is unramified in L_i. Observe that the compositum of all the L_i is a minimal N-torsion point field.

For $i \neq j$, consider the compositum L_iL_j. Since elliptic curves with supersingular reduction over $\mathbb{Q}$ cannot have a canonical subgroup, the prime p_i has a ramification index divisible by $p_i^{2n_i} - p_i^{2n_i-2}$ and likewise, p_j a ramification index divisible by $p_j^{2n_j} - p_j^{2n_j-2}$. However, p_i is unramified in L_j and p_j is unramified in L_i. One sees that L_iL_j has degree at least $p_j^{2n_j} - p_j^{2n_j-2}$ over L_i so as to attain the necessary ramification. Considering $\Psi_{p_j^{n_j}}$, the degree is also at most $p_j^{2n_j} - p_j^{2n_j-2}$. The equivalent statement holds over L_j. Thus L_iL_j has degree $\left(p_j^{2n_j} - p_j^{2n_j-2}\right) \cdot \left(p_i^{2n_i} - p_i^{2n_i-2}\right)$ over $\mathbb{Q}$. The situation is summarized in Figure 6. Repeating the above argument for each prime dividing N we obtain the result. $\square$

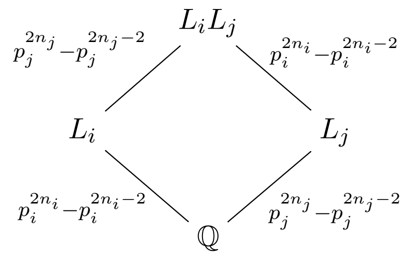

FIGURE 6. Degrees of Minimal Torsion Point Fields

7. An Application to Sporadic Points on Modular Curves

Our brief exposition follows [36]. 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 will employ an upper bound on 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 $x \in X_1(N)$ is a point, define the *degree* of x to be the degree of the residue field at x over $\mathbb{Q}$. If x corresponds to the data of an elliptic curve E and a point $P \in E[=N]$, then the degree of x is $[\mathbb{Q}(j(E), \mathfrak{h}(P)) : \mathbb{Q}]$, where $\mathfrak{h} : E \to E/\operatorname{Aut}(E) \cong \mathbb{P}^1$ is a Weber function for E.

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 by taking preimages. Define $\delta(X_1(N))$ to be the smallest positive integer k such that there are infinitely many points of degree k on $X_1(N)$. One sees $\delta(X_1(N)) \leq \gamma(X_1(N))$. 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.

Now suppose $N > 12$ so that $g(X_1(N)) > 1$. Using [37], we have the bound

$$\delta(X_1(N)) \leq \gamma(X_1(N)) \leq \frac{11N^2}{840}. \tag{15}$$

We apply our work in Section 5 to show Theorem 2.3, which we restate for convenience.

Theorem 2.3. *Let L be a number field and E/L be an elliptic curve that is supersingular at some prime $\mathfrak{p}$ of $\mathcal{O}_L$ above p. Suppose that E does not have a canonical subgroup at $\mathfrak{p}$, then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$.*

In what follows, we have to take special care for the CM j-invariants 0 and 1728. One should consult [9] for a thorough study of sporadic CM points on modular curves. The specific case of the least degree of CM points on $X_1(p^n)$ is treated in Section 6 of [2].

Proof. From ramification, the minimal possible degree over $\mathbb{Q}$ of an extension where an elliptic curve with j-invariant equal to $j(E)$ has a point P of exact order p^n is $\frac{1}{24}\left(p^{2n} - p^{2n-2}\right)$, where the factor $\frac{1}{24}$ comes from possibly needing to resolve bad additive reduction. For $p = 2$, resolving bad additive reduction may require an extension of degree 24; for $p = 3$, an extension of degree 12; and for $p > 3$, an extension of degree 6. See [25, Section 2].

First we contend with $j(E) \neq 0, 1728$. Here $[\mathbb{Q}(j(E), \mathfrak{h}(P)) : \mathbb{Q}] \geq \frac{1}{48}\left(p^{2n} - p^{2n-2}\right)$, since $|\operatorname{Aut}(E)| = 2$. The result follows after a brief comparison with Equation (15).

When $j(E) = 0$, then $|\operatorname{Aut}(E)| = 6$ and when $j(E) = 1728$, then $|\operatorname{Aut}(E)| = 4$. In these cases, if we suppose $p > 3$, then the minimal possible degree over $\mathbb{Q}$ of an extension where E has a point of exact order p^n is $\frac{1}{6}\left(p^{2n} - p^{2n-2}\right)$. Now $[\mathbb{Q}(j(E), \mathfrak{h}(P)) : \mathbb{Q}] \geq \frac{1}{36}\left(p^{2n} - p^{2n-2}\right)$, and our previous comparison with Equation (15) yields the result.

Take $j(E) = 0$ and $p = 2$. The elliptic curve $E_2 :\ y^2 + y = x^3$ is defined over $\mathbb{Q}$, has j-invariant 0, and has good supersingular reduction at 2. Hence, if we have another elliptic curve over some number field with j-invariant 0 and bad additive reduction at 2, we can make a degree $|\operatorname{Aut}(E)| = 6$ extension so that the isomorphism between the curve with bad reduction and E_2 is defined and thereby resolve the bad additive reduction. Thus the minimal possible degree over $\mathbb{Q}$ of an extension where an elliptic curve with j-invariant 0 has a point of exact order 2^n is $\frac{1}{6}\left(2^{2n} - 2^{2n-2}\right)$. Therefore, $[\mathbb{Q}(0, \mathfrak{h}(P)) : \mathbb{Q}] \geq \frac{1}{36}\left(2^{2n} - 2^{2n-2}\right)$, and the result follows.

Take $j(E) = 1728$ and $p = 3$. Similarly to the above argument, the elliptic curve $E_3 :\ y^2 = x^3 - x$ has j-invariant 1728 and good supersingular reduction at 3. Thus we can resolve bad additive reduction at 3 by making a degree $|\operatorname{Aut}(E)| = 4$ extension to define the isomorphism with E_3. We have $[\mathbb{Q}(1728, \mathfrak{h}(P)) : \mathbb{Q}] \geq \frac{1}{16}\left(3^{2n} - 3^{2n-2}\right)$, and the result follows.

When $j(E) = 1728$ and $p = 2$ and when $j(E) = 0$ and $p = 3$, the techniques we have been employing run aground. Appealing to [9, Theorem 3.4], which the authors state is a special case of [2, Theorem 7.1] and [3, Theorem 7.2], we find the least degree of a point on $X_1(2^n)$ corresponding to an elliptic curve with CM by $\mathbb{Z}[i]$ is 2^{2n-4} and the least degree of a point on $X_1(3^n)$ corresponding to an elliptic curve with CM by $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is 3^{2n-3}. Respectively, these results apply to j-invariants 1728 and 0. Comparing with Equation (15) finishes the proof. $\square$

We can also restrict sporadic points for composite level:

Theorem 7.1. *Let $N > 12$ be a positive integer*[4] *not divisible by 6 and write $N = \prod_{i=1}^{k} p_i^{n_i}$ for the prime factorization. Suppose that $E/\mathbb{Q}$ has good supersingular reduction at each p_i, then $j(E)$ does not correspond to a sporadic point on $X_1(N)$.*

Proof. Corollary 6.2 shows the degree of a minimal extension over which E has a point of exact order N is $\prod_{i=1}^{k}\left(p_i^{2n_i} - p_i^{2n_i-2}\right)$. If E' is an elliptic curve over a number field K with $j(E') = j(E)$ and $E'(K)[=N] \neq \emptyset$, then there is an extension of degree at most six over which $E' \cong E$. As E has a point of exact order N over this extension, we see $[K : \mathbb{Q}] \geq \frac{1}{6}\prod_{i=1}^{k}\left(p_i^{2n_i} - p_i^{2n_i-2}\right)$.

Hence

$$[\mathbb{Q}(\mathfrak{h}(P), j(E)) : \mathbb{Q}] \geq \frac{1}{6} \cdot \frac{1}{6}\prod_{i=1}^{k}\left(p_i^{2n_i} - p_i^{2n_i-2}\right) \geq \frac{1}{36}N^2 - \frac{1}{36}\sum_{i}^{k}\frac{N^2}{p_i^2}, \tag{16}$$

where we simply take the two leading terms for the last inequality.

We wish to show $[\mathbb{Q}(\mathfrak{h}(P), j(E)) : \mathbb{Q}] \geq \frac{11N^2}{840}$. Hence, via (16), our problem is implied by $\frac{1}{36}N^2 - \frac{1}{36}\sum_{i=1}^{k}\frac{N^2}{p_i^2} \geq \frac{11N^2}{840}$. Thus, it is enough to show

$$\frac{37}{2520} \geq \frac{70}{2520}\sum_{i=1}^{k}\frac{1}{p_i^2}. \tag{17}$$

The prime zeta function evaluated at 2 is approximately .45225; see https://oeis.org/A085548. Thus the right-hand side of (17) is strictly less than $\frac{35}{2520}$, say, and our result follows. $\square$

[4]For $1 \leq N \leq 12$, the curve $X_1(N)$ has $\mathbb{Q}$-gonality 1 and hence no sporadic points.

Example 7.2. As an example of how one might deal with non-supersingular primes, suppose $E/\mathbb{Q}$ does not have supersingular reduction at any of the primes above 2 or 3. Note j-invariants 0 and 1728 are supersingular at 2 and 3. Take $N = 6N_0$, where $\gcd(6, N_0) = 1$ and $N_0 > 1$, and suppose E has good supersingular reduction at all the primes dividing N_0. The degree of the smallest extension of K over which E has a point P of order N is at least $N_0^2 - \sum_{i=1}^k \frac{N_0^2}{p_i^2}$. Hence, accounting for quadratic twists with bad additive reduction, we wish to show that $\frac{1}{2}N_0^2 - \frac{1}{2}\sum_{i=1}^k \frac{N_0^2}{p_i^2} \geq \frac{11N^2}{840} = \frac{11N_0^2}{140}$. This amounts to showing $\frac{59}{70} \approx 0.84286 \geq \sum_{i=1}^k \frac{1}{p_i^2}$. Using the a rough estimate with the prime zeta function as above, the inequality is clear.

Though we have shown that sporadic points on $X_1(6N_0)$ do not correspond to rational elliptic curves with good supersingular reduction at the prime divisors of N_0, the point of this example is to show that being supersingular at some primes dividing the level is an obstacle to corresponding to a sporadic point.

In Example 7.2, we needed a lack of ramification at at least one of the primes above each of the primes dividing N_0 in order to preclude a canonical subgroup. The following example shows that, with or without a canonical subgroup, it is difficult for supersingular elliptic curves to correspond to sporadic points.

Example 7.3. Let $p \leq 17$ be a prime and let E be an elliptic curve over a quadratic field that has good supersingular reduction (with or without a canonical subgroup) at a prime above p. Combining Theorem 2.3 and a computation with $\mu = \frac{1}{2}$ similar to what we have done above, we can see that $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$.

To elaborate on the computation, Theorem 2.3 covers the case where E does not have a canonical subgroup. Thus we must deal with the case where $\mu = \frac{1}{2}$. Here we have a canonical subgroup, but we have no elements of larger valuation at higher levels. In other words, if $\hat{P}$ is a p^n-torsion element with $n > 1$, then the valuation of $\hat{P}$ is obtained by dividing the valuation of $[p]\hat{P}$ by p^2. The valuation of any $\hat{P} \in C_{\text{can}}$ is $\frac{1}{2(p-1)}$, and the computation reduces to showing $\frac{1}{4} \cdot \frac{1}{2} \cdot 2(p-1)$ is greater than $\frac{11p^2}{840}$. Here we have the factor of $\frac{1}{4}$ for potentially needing to resolve bad additive reduction and the factor of $\frac{1}{2}$ for the Weber function quotienting by $\mathrm{Aut}(E)$. We are making use of the fact that if E'/L is another elliptic curve with $j(E') = j(E)$, then we can make a quadratic extension to define E and another quadratic extension so $E' \cong E$ in order to resolve bad additive reduction.

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 and P. L. Clark. Torsion points and isogenies on CM elliptic curves. *arXiv e-prints*, art. arXiv:1906.07121, June 2019.

[3] A. Bourdon and P. L. Clark. Torsion points and Galois representations on CM elliptic curves. *Pacific J. Math.*, 305(1):43–88, 2020. ISSN 0030-8730. doi: 10.2140/pjm.2020.305.43. URL https://doi.org/10.2140/pjm.2020.305.43.

[4] A. Bourdon, Ö. Ejder, Y. Liu, F. Odumodu, and B. Viray. On the level of modular curves that give rise to isolated j-invariants. *Adv. Math.*, 357:106824, 33, 2019. ISSN 0001-8708. doi: 10.1016/j.aim.2019.106824. URL https://doi.org/10.1016/j.aim.2019.106824.

[5] J. Boxall and D. Grant. Singular torsion points on elliptic curves. *Math. Res. Lett.*, 10(5-6): 847–866, 2003. ISSN 1073-2780. doi: 10.4310/MRL.2003.v10.n6.a11. URL https://doi.org/10.4310/MRL.2003.v10.n6.a11.

[6] 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.

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

[8] 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.

[9] P. L. Clark, T. Genau, P. Pollack, and F. Saia. The least degree of a CM point on a modular curve. URL http://pollack.uga.edu/least_CM_degree.pdf.

[10] 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.

[11] C. Debry. Beyond two criteria for supersingularity: coefficients of division polynomials. *J. Théor. Nombres Bordeaux*, 26(3):595–606, 2014. ISSN 1246-7405. URL http://jtnb.cedram.org/item?id=JTNB_2014__26_2_595_0.

[12] 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.

[13] M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow, and D. Zureick-Brown. Sporadic Cubic Torsion. *arXiv e-prints*, art. arXiv:2007.13929, July 2020.

[14] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941. ISSN 0025-5858. doi: 10.1007/BF02940746. URL https://doi.org/10.1007/BF02940746.

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

[16] 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.

[17] 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.

[18] 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.

[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] 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.

[33] 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.

[34] 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.

[35] 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.

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

[37] M. van Hoeij and H. Smith. A Divisor Formula and a Bound on the $\mathbb{Q}$-gonality of the Modular Curve $X_1(N)$. *arXiv e-prints*, art. arXiv:2004.13644, Apr. 2020.

[38] L. C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2003. ISBN 1-58488-365-0. Number theory and cryptography.

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

Email address: hanson.smith@colorado.edu or hansonsmith101@gmail.com