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 $p$ of $K$ lying above the rational prime $p$. 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. This classification corrects an error in earlier work of Lozano-Robledo. As an application, we find the minimum necessary ramification at $p$ in order for $E$ to have a point of exact order $p^n$. Using this bound we show that sporadic points on the modular curve $X_1(p^n)$ cannot correspond to supersingular elliptic curves without a canonical subgroup. We generalize our methods to $X_1(N)$ with $N$ composite.

Keywords: Elliptic curves, Torsion points, Division fields, Torsion fields, Division polynomials, Sporadic points, Modular curves

Mathematics Subject Classification: Primary 11G05, Secondary 14H52

Contents

1 Introduction and Results .................................. 1
2 Previous work and motivation ............................... 3
3 Background on division polynomials ............................ 5
4 Valuations of the $p^n$-torsion points of the formal group ................. 6
   4.1 Setup and basics .................................... 6
   4.2 Main theorem ..................................... 9
5 Ramification in division fields ................................ 14
6 An application to sporadic points on modular curves ................... 16
References ............................................ 18

1 Introduction and Results

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 (Lemma 4.8 and Theorem 4.6) and to use this description to preclude certain supersingular elliptic curves from corresponding to sporadic points on the modular curve $X_1(N)$ (Theorems 1.1 and 6.1).

Before describing the results more precisely, we establish our setup along with some notation. These conventions will hold unless otherwise specified. Let $E$ be an elliptic curve over a number field $K$ with $P \in E(K)$ a point of exact order $p^n$. Let $p$ 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 $K(E[p^n])$. Write $\mathfrak{P}$ for a prime of $K(E[p^n])$ lying over $p$. We will be studying the ramification of $p$, and to a lesser extent $\mathfrak{P}$, over $p$. Let $e_p$ denote the ramification index of $p$ over $p$ and $e_{\mathfrak{P}}$ the ramification index of $\mathfrak{P}$ over $p$.

The ring of integers of $K$ is $\mathcal{O}_K$ and the local field obtained by completing $K$ at $p$ is denoted $K_p$. The valuation is denoted $v$, since $p$ will be clear from context, and it is normalized so that $v(p) = 1$. **Warning:** This normalization is distinct from much of the other literature in this area. We have chosen it, however, because we believe it makes the proofs more clean and straightforward. We let $\pi_p$ be a uniformizer; i.e., $\pi_p$ generates the maximal ideal of the valuation ring of $K_p$. The residue field of $K_p$ at $p$ is denoted $k_p$. As is common, the algebraic closure of a given field will be denoted with an overbar, e.g., $\overline{k_p}$.

Section 4 states and establishes the main result, a complete classification of the valuations of $p^n$-torsion elements of the formal group of $E$. This classification involves the *canonical subgroup*, a distinguished subgroup of $E[p]$ that lifts the kernel of Frobenius, as well as *higher-level canonical subgroups*; see Definitions 4.1 and 4.4. This complete classification is also the subject of [31, Lemma 5.3]. There is a significant error in the proposed valuations and the proof thereof in [31, Lemma 5.3]. Our work corrects this.

We use our classification to obtain a lower bound for ramification above $p$ which in turn gives a lower bound for the degree of $K$:

**Theorem 1.1** Minimal values for $e_p$ and $e_{\mathfrak{P}}$ can be determined from the valuation of a coefficient of the $p$th division polynomial. The minimal values are

$$e_{\mathfrak{P}} \geq p^{2n} - p^{2n-2} \quad \text{and} \quad e_p > \psi(p^n) = p^n - p^{n-1}. \quad (1)$$

Further, if $E$ does not have a canonical subgroup at $p$, then

$$(p^{2n} - p^{2n-2}) \mid e_p. \quad (2)$$

If $E$ has a canonical subgroup at $p$, 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 $p$ that is unramified over $p$, then $E$ cannot have a canonical subgroup at $p$. Hence Eq. (2) holds.

Theorem 1.1 and other consequences of Sect. 4 are the subject of Sect. 5. In Sect. 6, we use ramification to show that on $X_1(p^n)$ a subset of the supersingular locus is disjoint from the sporadic locus:

```
\[ K(E[p^n]) \quad \mathfrak{P} \]
\[ K \quad p \]
\[ \mathbb{Q} \quad p \]
```

**Fig. 1** Number fields and their respective primes in our setup
Theorem 1.2  Let $L$ be a number field and $E/L$ be an elliptic curve that is supersingular at some prime $p$ of $\mathcal{O}_L$ above $p$. If $E$ does not have a canonical subgroup at $p$, 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 result for $X_1(N)$ with $N$ composite; this is the content of Theorem 6.1. After proving these theorems, we demonstrate how our methods can be generalized when one is interested in specific modular curves via some examples.

Previous work has addressed the valuations of the $p^n$-torsion points of an elliptic curve that is supersingular or potentially supersingular at a prime above $p$; see Lemma 4.7 of [6] and §1.10–1.11 of [39]. However, these investigations do not pursue a complete classification of the valuations and are not focused on the importance of the canonical subgroup. As mentioned above, the classification in Lemma 5.3 of [31] contains an error and is not correct. Example 4.9 explicitly shows how our work corrects this error. Fortunately, it seems that the main results of [31] will still hold. Indeed, the valuations from Theorem 4.6 and [31, Lemma 5.3] that correspond to the least possible ramification agree. However, a more delicate argument may be necessary to reestablish Theorem 1.2 of [31]. This will be discussed more formally in a future corrigendum of [31] by the author and Lozano-Robledo.

Another feature of our description is it presents a natural and concrete example of the phenomenon of higher-level canonical subgroups described in more general and abstract contexts in [7, 12, 13, 21]. See Definition 4.4.

2 Previous work and motivation

Previous work in the area we consider has a variety of different thrusts. We quickly survey three distinct lines of research where our classification of the valuations of the coordinates of $p^n$-torsion points of supersingular elliptic curves has consequences.

Division fields of elliptic curves have a strong analogy with cyclotomic fields, the $\mathbb{G}_m$ division fields. Motivated by this analogy, one can work to describe splitting, ramification, and inertia explicitly in division fields of elliptic curves. To this end, Adelmann’s book [1] provides a nice introduction culminating in criteria describing the decomposition of unramified primes in various division fields. An abbreviated list of other relevant work in this area includes [8, 9, 18–20, 26, 28, 30, 41].

Given an arbitrary elliptic curve $E$ over some number field $K$, one wishes to have a description of the torsion subgroup $E(K)_{\text{tors}}$. This is another motivation for the study at hand. With [34] and [35], Mazur described $E(\mathbb{Q})_{\text{tors}}$. When $[K : \mathbb{Q}] = 2$, Kamienny, Kenku, and Momose (culminating with [23] and [25]) describe $E(K)_{\text{tors}}$.

The proofs of these results rely on carefully analyzing modular curves. In the cases discussed above, 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. When $[K : \mathbb{Q}] \geq 3$ this is no longer the case. That is, writing $d = [K : \mathbb{Q}]$, 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 [37] 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 et al.’s paper [22] 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.\footnote{Sporadic points are also called unexpected points or exceptional points in the literature.} 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 of the form $X_1(N)$ with a cubic sporadic point [15]. In fact, they show that the only cubic sporadic point is the one corresponding to Najman’s curve. Combined with the work of Jeon et al. [22], this classifies the possible groups $E(K)_{\text{tors}}$ when $[K : \mathbb{Q}] = 3$.

Thus, in order to understand $E(K)_{\text{tors}}$ when the degree of $K$ is greater than 3, it seems likely we will need to have a better understanding of sporadic points on modular curves. To this end, Bourdon et al. [3] have made an insightful investigation of sporadic $j$-invariants ($j$-invariants corresponding to a sporadic point on a modular curve $X_1(N)$ for some $N > 0$). Among the many results in [3], they have shown that, assuming Serre’s uniformity conjecture, the number of sporadic $j$-invariants in a given number field is finite. The interested reader should also consult the recent papers [4] and [5].

Finally, one can ask about bounds on the size of the torsion subgroup in terms of the degree $d$. Merel [36] 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

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

however, this work was unpublished. Thanks to the work of Derickx, a proof can now be found in [16, Appendix A]. Parent [38] 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 $d$. Indeed, Lozano-Robledo has conjectured [32]:

**Conjecture 2.1** 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

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

In [32], Lozano-Robledo makes significant strides toward this conjecture by considering ramification in the fields of definition of $p^n$-torsion points.

In the case where $E$ has potential supersingular reduction, the results of [29] and [31] show Conjecture 2.1 with $C = 24$. Theorem 1.1 shows that when $E$ is supersingular with no canonical subgroup, then $\varphi(p^n) \cdot (p^n + p^{n-1}) = p^{2n} - p^{2n-2} \leq d$, and Theorem 4.6 gives minimal ramification in all other cases of supersingular reduction.
3 Background on division polynomials

As in Sect. 1, we let $E/K$ be an elliptic curve with a point $P \in E(K)$ or exact order $p^n$, and we suppose $p$ is a prime of $K$ of residue characteristic $p$ at which $E$ has good supersingular reduction. Write

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$ 

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

$$\Psi_1 = 1, \quad \Psi_2 = 2y + a_1 x + a_3, \quad \Psi_3 = 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8,$$

$$\Psi_4 = \Psi_2 \left( 2x^6 + b_2 x^5 + 5b_4 x^4 + 10b_6 x^3 + 10b_8 x^2 + (b_2 b_8 - b_4 b_6) x + (b_4 b_8 - b_6^2) \right),$$

and using the formulas

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

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

For a reference see [40, 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

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

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 $\Psi_m$ 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 understand how division polynomials behave after reduction.

**Lemma 3.1** As above, let $E/k$ be an elliptic curve such that $E$ has good supersingular reduction at a prime $p$ of $K$ lying over $p$. If $p$ is an odd prime, write $c_0$ for the constant coefficient of $\Psi_p$. If $p = 2$, write $c_0$ for the constant coefficient of $\Psi_2 \Psi_2$. Then

$$\Psi_p(x) \equiv c_0 \not\equiv 0 \mod p \quad \text{if } p \text{ is odd, and } \Psi_2 \Psi_2(x) \equiv c_0 \not\equiv 0 \mod p \quad \text{if } p = 2.$$ 

In particular, $\nu(c_0) = 0$.

**Proof** Write $\hat{E}$ for the reduction of $E$ at $p$. Suppose $p$ is odd for the moment. Recalling $k_p$ is the residue field at $p$, suppose that $\Psi_p(x)$ does not reduce to a non-zero constant in $k_p[x]$. Hence $\Psi_p(x)$ has a root in $\overline{k_p}$ and thus there is a non-identity point on $\hat{E}/\overline{k_p}$ of order dividing $p^n$. This contradicts our assumption that $\hat{E}$ is supersingular. For $p = 2$, repeat the above, but replace $\Psi_p$ with $\Psi_2 \Psi_2$.

When $p^n \neq 2$, we can use Lemma 3.1 and the fact that $\Psi_p / \Psi_{p-1}$ has leading coefficient $p$ to see that the valuations of the distinct $x$-coordinates of points of exact order $p^n$ sum to $-1$. That is, letting $E[=p^n]$ denote the points of exact order $p^n$,

$$\sum_{P \in E[=p^n]/\pm} \nu(x(P)) = -1. \quad (3)$$
When \( p^n = 2 \), the sum of the valuations of the roots of \( \Psi_2 \) is
\[
\sum_{P \in E[2]} v(x(P)) = -2 \tag{4}
\]

**Remark 3.2** Without referencing the formal group, we can already use Lemma 3.1 to obtain partial results. Let \( E \) be an elliptic curve over a number field \( K \) with an unramified prime \( p \) over \( p \) at which \( E \) is supersingular. To employ a “reciprocal Eisenstein” trick, consider the polynomial
\[
x - \frac{p^{n-1}}{2} \Psi_p \left( x^{-1} \right) \in K_p[x].
\]
Since \( p \) is unramified and \( \Psi_p \) 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 \( K_p \) is a totally ramified extension of degree \( p^2 - 1 \). For \( p^n \)-torsion, we can employ this same trick with
\[
x - \frac{p^{n-1}}{2} \Psi_p \left( x^{-1} \right) \in K_p[x].
\]
Though this result is significantly weaker than Theorem 4.6, it is actually all that is necessary to prove Theorem 6.1.

**4 Valuations of the \( p^n \)-torsion points of the formal group**

In this section we will fully describe the valuations of the \( p^n \)-torsion points of an elliptic curve that is supersingular at a prime above \( p \). All the facts used here regarding formal groups can be found in [40, Chap. IV].

**4.1 Setup and basics**

Unless otherwise noted, in this section \( P \in E(K) \) will be a point of exact order \( p^n \) with \( n \geq 1 \) on an elliptic curve \( E/K \) that is supersingular at some prime \( p \subset \mathcal{O}_K \) lying above the odd prime \( p \); for the caveat with \( p = 2 \), see Remark 4.2. As before, \( v \) is the valuation associated to \( p \), normalized so that \( v(p) = 1 \). Recall, \( E[=p^n] \) denotes the set of points of exact order \( p^n \).

Let \( F_E \in K_p[[S, T]] \) denote the formal group law of \( E \) over \( K_p \). Let \( \pi_p \) be a uniformizer at \( p \); the set of elements of the ideal \( (\pi_p) \) 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 \( E(K_p) \). Conversely, if \( (x, y) \in E(K_p) \) 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 \( \pi_p \).

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:
\[
v(x(Q)) = -2v(\hat{Q}).
\]

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. Multiplication by an integer relatively prime to \( p \) is an automorphism of \( E[p] \). 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 $v(\hat{Q})$ is the same for all $\hat{Q}$ in a given orbit.

We have two possibilities: In one case, $v(\hat{Q})$ is the same for all $\hat{Q} \in \hat{E}[-p]$. In the other case, $v(\hat{R}) > v(\hat{Q})$ for all $\hat{R}$ in one orbit $C_j$ and all $\hat{Q}$ in some other orbit $C_j$. We notice $v(\hat{S}) = v(\hat{Q})$ 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 4.1** The orbit $C_i$ along with the identity is called the **canonical subgroup**. That is, if there exists $\hat{R} \in \hat{E}[-p]$ such that $v(\hat{R}) > v(\hat{Q})$ for some $\hat{Q} \in \hat{E}[-p]$, then the orbit $\langle \hat{R} \rangle$ is the canonical subgroup and denoted $C_{\text{can}}$. We have made this definition for $\hat{E}$, but since $E[p^n] \cong \hat{E}[p^n]$ it is also natural to refer to the canonical subgroup of $E$ as the image of $C_{\text{can}}$ under this isomorphism.

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 [33] and [11].

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 $C_{\text{can}}$ have smaller valuations). In this section, we will explicitly show that there can be a similar phenomenon at higher levels and describe exactly when and to what extent it happens. Specifically, in certain fibers $[p]^{-1}\hat{Q}$ with $\hat{Q} \in \hat{E}[-p^{-1}]$ there may be a set of $p$ elements with larger valuations. For an example see Fig. 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. We call this the **level-$n$ canonical subgroup**; see Definition 4.4.

For $p > 2$, define

$$
\mu := v\left(c_{\frac{p-1}{2}}\right), \quad \text{where} \quad \Psi_p(x) = px^{\frac{p^2-1}{4}} + c_{\frac{p-1}{2}}x^{\frac{p^2-3}{4}} + \cdots + c_1x + c_0.
$$

(5)

For $p = 2$, define $\mu := v(a_1^2 + 4a_2)/2$. With $p = 2$, the following discussion needs to be augmented slightly since $x$-coordinates of points in $E[=2]$ are distinct; see Remark 4.2.

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

$$
\frac{c_{\frac{p-1}{2}}}{2^\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} p \sum_{1 \leq i_1 < i_2 < \cdots < i_{\frac{p-1}{2}} \leq \frac{p-1}{2}} x_{i_1} \cdots x_{i_{\frac{p-1}{2}}}.
$$

(6)

If there is a canonical subgroup, there is a distinct summand on the right-hand side of (6) with smallest valuation. (Recall that we multiply valuations by $-2$ to move between $\hat{E}$ and $x$-coordinates of points on $E$.) Indeed the summand with smallest valuation is the product of the $\frac{p-1}{2}$ distinct $x$-coordinates of points in $C_{\text{can}}$. Hence, if we have a canonical subgroup, $-\mu$ is the sum of the valuations of all distinct $x$-coordinates of points that are in $C_{\text{can}}$. We see the valuation of the $x$-coordinate of a point in $C_{\text{can}}$ is $-\frac{2(1-\mu)}{p-1}$. Hence, from Eq. (3), the valuation of the $x$-coordinate of a point that is not in $C_{\text{can}}$ is $-\frac{2\mu}{p^2-p}$.

---

2The nomenclature comes from the fact that such a subgroup is a canonical lifting of the kernel of Frobenius. For a detailed explanation of this lifting, see the introduction of [24].
Note, $\mu$ is defined to correspond to valuations in $\hat{E}$. Thus, if $P \in C_{\text{can}}$, then $v(\hat{P}) = \frac{1 - \mu}{p - \sqrt{1}}$, and if $P \notin C_{\text{can}}$, then $v(\hat{P}) = \frac{-\mu}{p - \sqrt{1}}$.

A classical criterion of Deuring [17] states that $E : y^2 = f(x)$ is supersingular at $p$ if and only if the coefficient of $x^{p-1}$ in $f(x)^{\frac{p-1}{2}}$ vanishes modulo $p$. One may be curious how the coefficient $c_{\frac{p-1}{2}}$ is related to Deuring’s coefficient. Thanks to Deby [14], we know that they are in fact equal. Thus, for such $E$, we could just as well define $\mu$ to be the valuation of Deuring’s coefficient.

Many authors 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 [6], we have called this valuation $\mu$. 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, $\mu$ is the sum of the valuations of the $p^2 - p$ elements that are not in $C_{\text{can}}$. As such, $\mu < \frac{p}{p+1}$. Conversely, if there is not a canonical subgroup, $\mu \geq \frac{p}{p-1}$. Since all elements of $\hat{E}[=p]$ have the same valuation in this case, Eq. (6) shows the valuation of each element must be $\frac{1}{p+1}$.

**Remark 4.2** Consider now the case that $p = 2$. Our discussion of the formal group above is the same, 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

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

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 $\frac{1}{2} \Psi_2^2$ that captures the canonical subgroup if it exists. We see $\eta := v_2(\frac{1}{2}(4a_2 + a_1^2))$ 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 $-\frac{3}{2}$. The constant coefficient of $[2]T/T$ is 2, hence $\mu = 1 + \frac{\eta}{2} = v_2(4a_2 + a_1^2)/2$. Example 4.10 makes Theorem 4.6 explicit in the $p = 2$ case.

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 [29] and [31].

**Example 4.3** 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

$$E : y^2 + xy = x^3 + x^2 - 3632x + 82,757.$$ 

At $p = 11$ the curve $E$ has bad additive reduction. Over $\mathbb{Q}(\sqrt[4]{11})$ the bad additive reduction resolves to good supersingular reduction and the curve has global minimal model

$$E : y^2 + \sqrt[4]{11}xy = x^3 + \sqrt[3]{11^2}x^2 + 3\sqrt[4]{11}x + 2.$$ 

Using SageMath [43], one can compute the factorization

$$\Psi_{11} = 11x^{60} + \cdots + 195,530, 917\sqrt[4]{11}x^{55} + \cdots - 7, 312, 712\sqrt[4]{11}x - 303, 271.$$
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 \( \Psi_1 \), while Fig. 3 is labeled generally to help clarify the larger discussion.

Of particular import to our work in Sect. 6 is that there is a degree 10 extension of \( \mathbb{Q}(\sqrt[3]{11}) \) 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.

### 4.2 Main theorem

Echoing [13] and [12], we make the following definition.

**Definition 4.4** Suppose that \( \frac{1}{p^{n-2}(p+1)} < \mu < \frac{1}{p^{n-2}(p+1)} \) and that \( \hat{W} \in \hat{E}[\equiv p^n] \) is an element with valuation \( v(\hat{W}) = \frac{1-p^{n-1}\mu}{p^{n-1}(p+1)} \). We define the level-\( n \) canonical subgroup to be the subgroup of \( \hat{E}[p^n] \) generated by \( \hat{W} \).

**Remark 4.5** As a porism of Lemma 4.8, we will see that the subgroup of \( \hat{E}[p^n] \) generated by \( \hat{W} \) is exactly the set of elements of \( \hat{E}[p^n] \) with large valuations. In other words, \( \langle \hat{W} \rangle \) is \( C_{\text{can}} \) and every element above \( C_{\text{can}} \) with valuation \( \frac{1-p^k\mu}{p^{k+1}(p+1)} \) for \( 1 \leq k \leq n-1 \). Moreover, \( \langle \hat{W} \rangle = \langle \hat{R} \rangle \) for any \( \hat{R} \in \hat{E}[\equiv p^n] \) with \( v(\hat{R}) = \frac{1-p^{n-1}\mu}{p^{n-1}(p+1)} \). The work below shows such a distinguished subgroup exists if and only if \( \mu < \frac{1}{p^{n-1}(p+1)} \); otherwise, the valuations behave more uniformly in the fibers.
With a way to visualize things and some terminology, we are ready for the main theorem. Some of the expressions below are not fully simplified. This is deliberate and intended to make it easier for the reader to see how the values are obtained.

**Theorem 4.6** Let $E/K$ be an elliptic curve with supersingular reduction at a prime $p$ of $K$. Write $p$ for the residue characteristic of $p$. Let $\mu$ be the valuation of the coefficient of $x^{p^2-p}$ in $\Psi_{p}(x)$ if $p$ is odd and $v_2(4a_2 + a_1^2)/2$ as in Remark 4.2 if $p = 2$.

If $\mu \geq \frac{p}{p+1}$, then there is no canonical subgroup at $p$ and every element of $\hat{E}[=p^n]$ has valuation $\frac{v_2(\hat{P})}{p^n - 1} - 1$.

If $\mu < \frac{p}{p+1}$, there is a (level-1) canonical subgroup at $p$. Suppose this is the case and let $s$ be the smallest non-negative integer such that $\mu \geq \frac{1}{p^s(p+1)}$. The last level for which there is a canonical subgroup is $s + 1$. If $n \leq s + 1$, then there are $p^{n-1}(p-1)$ elements of $\hat{E}[=p^n]$ above $C_{\mathrm{can}}$ with valuation $\frac{1}{p^n-1(p^s-1)}\mu$ 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 $\frac{1}{p^{2(n-j)}(p^2 - p)}\mu$.

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

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

We can state a rougher but easier to digest consequence:

**Corollary 4.7** Let $P \in E(K)$ be a point of exact order $p^n$. If $[p]\hat{P}$ is not in the (possibly non-existent) level-$(n-1)$ canonical subgroup or if $\mu \geq \frac{1}{p^{n-1}(p+1)}$, then

\[ v(\hat{P}) = \frac{1}{p^2}v([p]\hat{P}). \]

Otherwise, $v(\hat{P})$ has valuation

\[ \frac{1 - p^{n-1}\mu}{p^{n-1}(p-1)} \quad \text{or} \quad \frac{\mu}{p^2 - p}. \]
depending, respectively, on whether or not \( \hat{P} \) is in the level-\( n \) canonical subgroup.

We now state the fundamental lemma of the section. Theorem 4.6 is a quick consequence of this lemma.

**Lemma 4.8** Keep the same notation as above and recall \( P \in E(\mathbb{F}_p^n) \). If \( \mu \geq \frac{p}{p+1} \), then there is no canonical subgroup at \( \mathfrak{p} \) and

\[
v (\hat{P}) = \frac{1}{p^{2n} - p^{2n-2}}. \tag{7}
\]

Otherwise, \( 0 < \mu < \frac{p}{p+1} \) and there is a (level-1) canonical subgroup at \( \mathfrak{p} \). Suppose this is the case and let \( s \) be the smallest non-negative integer such that \( \mu \geq \frac{1}{p^{s+1}} \). The last level for which there is a canonical subgroup is \( s + 1 \). If \( [p^{\mu-1}]P \notin \mathcal{C}_{\text{can}} \), then

\[
v (\hat{P}) = \frac{\mu}{p^{2n-2}(p^2 - p)}. \tag{8}
\]

\( p^{n-1} \mathcal{C} \in \mathcal{C}_{\text{can}} \) then there are a number of cases: First, if \( n = 1 \),

\[
v (\hat{P}) = 1 - \frac{\mu}{p - 1}. \tag{9}
\]

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

\[
v (\hat{P}) = \frac{\mu}{p^{2m}(p^2 - p)}. \tag{10}
\]

If no such integer exists, then two cases remain. If \( n > s + 1 \), then there is no level-\( n \) canonical subgroup and

\[
v (\hat{P}) = \frac{1 - p^s \mu}{p^n(p - 1)} = \frac{1 - p^s \mu}{p^{2n-s-2}(p - 1)}. \tag{11}
\]

Otherwise, there is a level-\( n \) canonical subgroup and \( \hat{P} \) is an element of it. The valuation is

\[
v (\hat{P}) = \frac{1 - p^{n-1} \mu}{p^{n-1}(p - 1)}. \tag{12}
\]

Write \( \hat{Q} = [p]P \). 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 \( \frac{\mu}{p^2 - p} \).

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 Lemma 4.8 and Theorem 4.6 by \(-2\).

**Proof of Lemma 4.8** First, Lemma 3.1 shows \( \mu > 0 \). We proceed by induction on \( n \). The base case, including Eq. (9), is established by the discussion immediately preceding Example 4.3.

For the induction step, suppose we have our result for all \( k < n \). Define \( \hat{Q} = [p]P \), and consider the power series \([p]T - \hat{Q} \in K_p[[T]]\). If \( \alpha \) is a root of \([p]T - \hat{Q} \in K_p\), e.g., \( \alpha = \hat{P} = \frac{\alpha([p]T)}{y([p]T)} \), then we see \( v([p]\alpha) = v(\hat{Q}) \). Let \( e \) be the exponent of \( \pi_p \) in \( p \) so that \( v(\pi_p) = \frac{1}{e} \). Because the height of the formal group is 2, we have

\[
[p]T = p\hat{f}(T) + \pi_p^e \hat{g}(T^p) + h\left(T^{p^2}\right), \tag{13}
\]

where \( \hat{f}, \hat{g}, \) and \( h \) are power series without constant coefficients and with \( \hat{f}'(0), \hat{g}'(0), h'(0) \in K_p^e \).
Recall \( v(\hat{Q}) < 1 \) by hypothesis. If \( v([p]α) ≥ v(\alpha) = 1 + v(α) \), then \( v(α) ≤ v(\hat{Q}) − 1 < 0 \). We have a contradiction since \( α \) is in the maximal ideal of the valuation ring of \( \hat{K}_p \). Thus \( v([p]α) < v(\alpha) \) and

\[
v([p]α) ≥ \min \left( v \left( \frac{p^α}{p^\mu} \right), v \left( \alpha^p \right) \right) = \min (\mu + pv(α), p^2v(α))
\]

with equality when there is a unique minimum. Using \( v(α) < v([p^{n−1}]α) = \frac{1}{p−1} \), a short computation with (14) yields Eq. (7).

Suppose now that \( [p^{n}]α = \hat{S} \) with \( 0 < m < n \) and \( v(\hat{S}) ≤ \frac{1}{p^{−1}} \). If \( \mu + pv(α) ≤ p^2v(α) \), then \( v(α) ≥ \frac{\mu}{p^2}p ≥ v(\hat{S}) \) and we have a contradiction. Thus \( v(α) = \frac{1}{p^{m}}v(\hat{S}) \). This gives us Eqs. (8) and (10).

We turn our attention to establishing Eq. (11), so we assume \( \frac{1}{p^{n−2}(p+1)} ≤ \mu < \frac{p}{p+1} \). We will begin with the case where there is a level-\((n − 1)\) canonical subgroup. From the induction hypotheses and previously established equations, we have that \( α \in [p]−1\hat{Q} \) where \( \hat{Q} ∈ \hat{E} \) has valuation \( \frac{1−p^{n−1}−\mu}{p^{n−2}(p−1)} \). For a contradiction, take the case that \( \mu + pv(α) ≤ p^2v(α) \). Using \( v(\hat{Q}) ≤ \frac{1}{p^{−1}(p−1)} \), we obtain

\[
\frac{1}{p^{n−1}(p−1)} \leq \frac{\mu}{p^2−p} ≤ v(α) ≤ \frac{v(\hat{Q})}{p^2} ≤ \frac{1}{p^{n−1}(p−1)}
\]

Unless \( \mu = \frac{1}{p^{n−1}(p+1)} \), we have a contradiction. Regardless of whether \( \mu = \frac{1}{p^{n−1}(p+1)} \) and \( \mu + pv(α) = p^2v(α) \) or \( \mu + pv(α) > p^2v(α) \), we see that \( v(α) = \frac{v(\hat{Q})}{p^2} \). Thus there is no level-\( n \) canonical subgroup. Since \( \mu + pv(α) ≥ p^2v(α) \), Eq. (14) shows that the valuations of the various \( p \)-power roots of \( α \) are obtained by dividing by \( p^2 \). To rephrase, if \( \mu ≥ \frac{1}{p^{−1}(p+1)} \) and \( k ∈ \mathbb{Z}_{>0} \), then the valuations of \( p^k \)-th roots of \( \hat{Q} \) are obtained by dividing \( v(\hat{Q}) \) by \( p^2k \).

If there is not a level-\((n − 1)\) canonical subgroup, then from the induction hypotheses and previously established equations, \( [p^{n−(s+1)}]α \) is in the level \((s+1)\)-canonical subgroup and has valuation \( \frac{1−p^{n−s}}{p^{s+1}(p−1)} \). Moreover, the conclusions above apply to \( [p^{n−(s+1)}]α \). Thus \( v(α) = \frac{1}{p^{n−(s+1)}} \cdot v([p^{n−(s+1)}]α) = \frac{1−p^s}{p^{s+1}(p−1)} \), and we have established Eq. (11).

Finally, we focus on Eq. (12). Suppose \( \mu < \frac{1}{p^{n−1}(p+1)} \) and \( v(\hat{Q}) = \frac{1−p^{n−2}−\mu}{p^{n−2}(p−1)} \). For a contradiction suppose \( v(α) = \frac{1}{p^2}v(\hat{Q}) = \frac{1−p^{n−2}−\mu}{p^{n−2}(p−1)} \). Using the upper bound on \( μ \), we compute

\[
\mu + pv(α) = \mu + p \left( \frac{1−p^{n−2}−\mu}{p^{n−2}(p−1)} \right) = p^2v(α).
\]

Hence \( \mu + pv(α) < p^2v(α) \) and \( v([p]α) = \mu + pv(α) \). This contradicts our hypothesis that \( v(α) = \frac{1}{p^2}v(\hat{Q}) \). Therefore \( μ + pv(α) ≤ p^2v(α) \) for all \( α \in [p]−1\hat{Q} \).

For at least one \( α \in [p]−1\hat{Q} \), we will have \( μ + pv(α) = v(\hat{Q}) \). If this was not the case, then Eq. (14) implies that for each \( α \in [p]−1\hat{Q} \) one would have \( μ + pv(α) = p^2v(α) \) and \( v(α) < \frac{1}{p^2}v(\hat{Q}) \). Hence \( \sum_{α \in [p]−1\hat{Q}} v(α) < v(\hat{Q}) \). However the elements of \([p]−1\hat{Q}\) are exactly the roots of \([p]T − \hat{Q}\) in the formal group and the valuation of the constant coefficient is \( v(\hat{Q}) \). Thus, with this contradiction, we see that there exists \( α \in [p]−1\hat{Q} \) with \( v(α) = \frac{1}{p^{n−1}(p−1)} \). Considering sums of the form \( α + \hat{S} \) with \( \hat{S} \in \hat{E}[p] \), we see that there are \( p \) elements in \([p]−1\hat{Q}\) with valuation \( \frac{1−p^{n−1}}{p^{n−1}(p−1)} \) and \( p^2 − p \) with valuation \( \frac{μ}{p−1} \). The \( p \) elements with larger valuation are the part of the level-\( n \) canonical subgroup that is above \( \hat{Q} \).

Theorem 4.6 is immediate after counting the \( p^n \)-torsion points of various valuations.
Example 4.9 Consider the elliptic curve $E : y^2 + \sqrt[3]{3}xy + y = x^3 + \sqrt[3]{3}x^2 + 2x$ over $\mathbb{Q}(\sqrt[3]{3})$. This curve has good supersingular reduction at $(\sqrt[3]{3})$, the lone prime above 3. We can compute
\[
\Psi_3 = 3x^4 + (\sqrt[3]{3}^2 + 4\sqrt[3]{3})x^3 + (3\sqrt[3]{3} + 12)x^2 + 3x - \sqrt[3]{3} - 4.
\]
Thus $\mu = v(\sqrt[3]{3}^2 + 4\sqrt[3]{3}) = \frac{1}{5} < \frac{1}{3^2}$ and $E$ has a level-2 canonical subgroup at the prime $(\sqrt[3]{3})$.

There are 36 distinct $x$-coordinates of points in $E[= 9]$. By Theorem 4.6, there are 27 with $v(x(P)) = -\frac{\mu}{27} = -\frac{1}{115}$, there are 6 with $v(x(P)) = -\frac{\mu}{3} = -\frac{1}{15}$, and 3 with $v(x(P)) = 3\sqrt[3]{3} - 1 = -\frac{1}{13}$. These 3 with smallest valuation correspond to the level-2 canonical subgroup. Thus in $\Psi_9$, 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, Fig. 5 shows the fiber $p^{-1} \hat{Q}$ where $\hat{Q} \in C_{can}$. We see there are three elements of larger valuation $\frac{1}{13}$ and six elements of smaller valuation $\frac{1}{30}$.

This example confirms that [31, Lemma 5.3] is not correct. To translate the notation of [31] to our notation, one needs to divide by $e$ and note that $\frac{c_1}{e} = \mu$. Lemma 5.3 claims there should be 27 distinct $x$-coordinates of valuation $-\frac{\mu}{27} = -\frac{1}{115}$ and 9 distinct $x$-coordinates of valuation $\frac{3\sqrt[3]{3} - 1}{13} = -\frac{1}{13}$. If this were the case, then the coefficient of $x^{27}$ would have valuation $-\frac{6}{5}$ and not $-\frac{4}{5}$.

Example 4.10 To see an example with a level-2 canonical subgroup but no level-3 canonical subgroup and to confirm our work with $p = 2$, consider the curve
\[
E : y^2 + \sqrt[2]{2}xy + y = x^3 + x^2 + x \quad \text{over} \quad \mathbb{Q}(\sqrt[2]{2}).
\]
We compute $\mu = v_2(4 + \sqrt[2]{2})/2 = \frac{1}{4}$. Thus $s = 1$ and there will be a level-2 canonical subgroup but not a level-3 canonical subgroup. The valuation of the coefficient of $x^2$ in $\Psi_2^2/4$ shows the valuation of the $x$-coordinate of the lone point in the level-1 canonical subgroup is $-\frac{3}{2}$ as expected.
Moving to level 2, the coefficient of $x^5$ in $\Psi_4/2\Psi_2$ has valuation $-\frac{1}{2}$. This corresponds to the $x$-coordinate shared by the two 4-torsion points in the level-2 canonical subgroup. There should be two 4-torsion points above the level-1 canonical subgroup that are not in the level-2 canonical subgroup and share an $x$-coordinate with valuation $-\frac{1}{4}$. Accordingly, the coefficient of $x^4$ in $\Psi_4/2\Psi_2$ has valuation $-\frac{3}{4} = -\frac{1}{2} - \frac{1}{4}$.

We do not have a level-3 canonical subgroup, and Theorem 4.6 tells us that there should be four 8-torsion $x$-coordinates with valuation $-\frac{1}{8}$ and four 8-torsion $x$-coordinates with valuation $-\frac{1}{16}$. We confirm that the coefficient of $x^{20}$ in $\Psi_8/2\Psi_4$ has valuation $-\frac{1}{2} = 4 \cdot (-\frac{1}{8})$ and the coefficient of $x^{16}$ has valuation $-\frac{3}{4} = 4 \cdot (-\frac{1}{8}) + 4 \cdot (-\frac{1}{16})$.

### 5 Ramification in division fields

Theorem 1.1 is a quick consequence of our work in Section 4:

**Proof of Theorem 1.1** First note that with our normalization, the denominators of the valuations in Theorem 4.6 and Lemma 4.8 provide bounds on ramification. Equation (2) is immediate from Eq. (7). Since this covers the case where there is no canonical subgroup, we can assume $0 < \mu < \frac{p}{p+1}$. The claim that $e_P \geq p^{2n} - p^{2n-2}$ in Eq. (1) can be seen by considering Eq. (8) and noting $\frac{p^{2n-2}(p^2-p)}{p^{2n-2}(p^2-p)} < \frac{1}{p^{n-1}(p+1)}$. Equality comes from the case where there is no canonical subgroup, so $e_P > p^{2n} - p^{2n-2}$ when there is a canonical subgroup.

Finally, $e_p > \varphi(p^n)$ is established by a straightforward case-by-case analysis. We will detail the case where $P$ is in the level-$n$ canonical subgroup since this is perhaps the most novel. By hypothesis $n-1 \leq s$ and $\mu < \frac{1}{p^{n-1}(p+1)}$. Hence $p^{n-1}\mu < \frac{p}{p+1}$ and $1 - p^{n-1}\mu < 1$. Thus

$$
\nu(\hat{P}) = \frac{1 - p^{n-1}\mu}{p^{n-1}(p-1)} < \frac{1}{p^{n-1}(p-1)} = \frac{1}{\varphi(p^n)}.
$$

\[ \Box \]

Theorem 4.6 can also be used, in conjunction with a lack of ramification, to preclude the existence of a canonical subgroup.
Corollary 5.1  No elliptic curve defined over $\mathbb{Q}$ with supersingular reduction at a rational prime $p$ has a canonical subgroup at $p$. More generally, no elliptic curve that is supersingular at $p$, some unramified prime over $p$, has a canonical subgroup at $p$.

Proof  Notice $0 < \mu < \frac{p}{p+1}$ 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.

The following corollary describes ramification in fields where there is a torsion point of composite order. It will be used in Sect. 6.

Corollary 5.2  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 over all the $p_i$. If $L$ is a number field over which $E$ has a point of exact order $N$, then any prime above $p_i$ in $L$ has ramification index divisible by $p_i^{2n_i} - p_i^{2n_i - 2}$ and

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

Though we have stated Corollary 5.2 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 $P \in E(L)$ be a point of exact order $N$ and write $P_i = [N/p_i^{n_i}]P$. Define $L_i = \mathbb{Q}(P_i)$ and note $L_i \subset L$. Since elliptic curves with supersingular reduction over $\mathbb{Q}$ cannot have a canonical subgroup, Theorem 4.6 shows $\nu_{p_i}(\hat{P}_i) = \frac{1}{p_i^{2n_i} - p_i^{2n_i - 2}}$. Because the degree of $\Psi_{p_i, n_i}$ is $\frac{1}{2}(p_i^{2n_i} - p_i^{2n_i - 2})$, we see $[L_i : \mathbb{Q}] = p_i^{2n_i} - p_i^{2n_i - 2}$ with $p_i$ totally ramified. Moreover, if $p_j \neq p_i$, then $p_j$ is unramified in $L_i$.

We consider the compositum $L_iL_j \subset L$, and we repeat our argument comparing ramification and the degree of a division polynomial to see $[L_iL_j : L_i] = p_i^{2n_j} - p_i^{2n_j - 2}$ with each of the primes above $p_j$ being totally ramified over $L_i$. Thus $L_iL_j$ has degree $(p_i^{2n_j} - p_i^{2n_j - 2}) \cdot (p_i^{2n_i} - p_i^{2n_i - 2})$ over $\mathbb{Q}$ and $p_h$ is unramified in $L_iL_j$ if $h \neq i, j$. The situation is summarized in Fig. 6. Iterating the above argument, we obtain $L_1 \cdots L_k \subset L$ and the result. $\square$
6 An application to sporadic points on modular curves

Our brief exposition follows [42]. 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 $X_1(N)$. If $x \in X_1(N)$ is a closed 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 $[\mathbb{Q}(j(E), h(P)) : \mathbb{Q}]$, where $h : E \to E/\text{Aut}(E) \cong \mathbb{P}^1$ is a Weber function for $E$.

Given a dominant morphism $\phi : X_1(N) \to \mathbb{P}^1_K$ 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 $\delta(X_1(N)) \leq \gamma_\mathbb{Q}(X_1(N))$. A point on $X_1(N)$ of degree strictly less than $\delta(X_1(N))$ is called a sporadic point. In other words, if $x \in X_1(N)$ is sporadic if there are only finitely many points $y \in X_1(N)$ with $\deg(y) \leq \deg(x)$. A non-cuspidal sporadic point on $X_1(N)$ corresponds to an elliptic curve with a point of order $N$ defined over a number field of “small” degree. The interested reader should consult [3] for a more thorough exposition of sporadic points on curves.

Now suppose $N > 12$ so that $g(X_1(N)) > 1$. Using [44], we have the bound

$$\delta(X_1(N)) \leq \gamma_\mathbb{Q}(X_1(N)) \leq \frac{11N^2}{840}. \quad (15)$$

We apply our work in Sect. 4 to show Theorem 1.2, which we restate for convenience.

**Theorem 1.2.** Let $L$ be a number field and $E/L$ be an elliptic curve that is supersingular at some prime $p$ of $\mathcal{O}_L$ above $p$. Suppose that $E$ does not have a canonical subgroup at $p$, 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 [10] 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 Sect. 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 $\frac{1}{24}(p^{2n} - p^{2n-2})$, 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 [27].

First we contend with $j(E) \neq 0, 1728$. Here

$$[\mathbb{Q}(j(E), h(P)) : \mathbb{Q}] \geq \frac{1}{48} (p^{2n} - p^{2n-2}),$$

since $|\text{Aut}(E)| = 2$. The result follows after a brief comparison with Eq. (15).

When $j(E) = 0$, then $|\text{Aut}(E)| = 6$ and when $j(E) = 1728$, then $|\text{Aut}(E)| = 4$. 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 $\frac{1}{6}(p^{2n} - p^{2n-2})$. Now

$$[\mathbb{Q}(j(E), h(P)) : \mathbb{Q}] \geq \frac{1}{36} (p^{2n} - p^{2n-2}),$$

and our previous comparison with Eq. (15) yields the result.

We are left with the four special cases where we have the CM $j$-invariants 0 and 1728 and the primes 2 and 3. Though our work can make some headway in a couple of these cases, it is easier and more coherent to appeal to the results in Sect. 6 of [2].
From Theorem 6.1 of [2], we obtain the following bounds. Recall that \( p^n > 12 \). For \( j(E) = 1728 \), the least degree of a corresponding point on \( X_1(2^n) \) is \( 2^{2n-4} \), and on \( X_1(3^n) \) it is \( 2 \cdot 3^{2n-2} \). For \( j(E) = 0 \), the least degree of a corresponding point on \( X_1(2^n) \) is \( 2^{2n-3} \), and on \( X_1(3^n) \) it is \( 3^{2n-3} \). Comparing with Eq. (15) finishes the proof.

We can also restrict sporadic points for composite level:

**Theorem 6.1** Let \( N > 12 \) be a positive integer\(^3\) not divisible by 6 and write \( N = \prod_{i=1}^{k} p_i^{n_i} \) for the prime factorization. If \( E/\mathbb{Q} \) has good supersingular reduction at each \( p_i \), then \( j(E) \) does not correspond to a sporadic point on \( X_1(N) \).

Corollary 5.2 shows the minimal degree of an extension over which \( E \) has a point of exact order \( N \) is \( \prod_{i=1}^{k} (p_i^{2n_i} - p_i^{2n_i-2}) \). If \( E' \) is an elliptic curve over a number field \( K \) with \( j(E') = j(E) \) and \( E'(K) = \mathbb{N} \), then there is an extension of degree at most six over which \( E' \approx E \). As \( E \) has a point of exact order \( N \) over this extension, we see \( [K : \mathbb{Q}] \geq \frac{1}{6} \prod_{i=1}^{k} (p_i^{2n_i} - p_i^{2n_i-2}) \).

Hence

\[
[\mathbb{Q}(b(P), j(E)) : \mathbb{Q}] \geq \frac{1}{6} \prod_{i=1}^{k} (p_i^{2n_i} - p_i^{2n_i-2}) \geq \frac{1}{36} N^2 - \frac{1}{36} \sum_{i=1}^{k} \frac{N_i^2}{p_i^{2n_i-2}},
\]

(16)

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

We wish to show \( [\mathbb{Q}(b(P), j(E)) : \mathbb{Q}] \geq \frac{11N^2}{840} \). Hence, via (16), our problem is implied by

\[
\frac{11}{36} N^2 - \frac{1}{36} \sum_{i=1}^{k} \frac{N_i^2}{p_i^{2n_i-2}} \geq \frac{11N^2}{840}.
\]

Thus, it is enough to show

\[
\frac{37}{2520} \geq \frac{70}{2520} \sum_{i=1}^{k} \frac{1}{p_i^{2n_i-2}}.
\]

The prime zeta function evaluated at 2 is approximately 0.45225; see sequence https://oeis.org/A085548 in the OEIS. Eq. (17) follows.

**Example 6.2** 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 \( N_0^2 - \sum_{i=1}^{k} \frac{N_i^2}{p_i^{2n_i-2}} \). Hence, accounting for quadratic twists with bad additive reduction, we wish to show that

\[
\frac{11}{70} N_0^2 - \frac{1}{2} \sum_{i=1}^{k} \frac{N_i^2}{p_i^{2n_i-2}} \geq \frac{11N^2}{740}.
\]

This amounts to showing

\[
\frac{79}{70} \geq \sum_{i=1}^{k} \frac{1}{p_i^{2n_i-2}}.
\]

Using 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 6.2, 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

\[\text{By work of Mazur, Kamienny, Kenku, and Momose surveyed in Sect. 2, there are non-cuspidal sporadic points on } X_1(N) \text{ for } 1 \leq N \leq 12.\]
example shows that, with or without a (level-1) canonical subgroup, it is difficult for supersingular elliptic curves to correspond to sporadic points.

**Example 6.3** 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 1.2 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 1.2 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 do not have higher-level canonical subgroups. In particular, 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 $\frac{1}{np^n - 1}$, and the computation reduces to showing $\frac{1}{2} \cdot \frac{1}{2} \cdot 2(p - 1)$ is greater than $\frac{11p^2}{100}$. 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 $\text{Aut}(E)$. 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.

**Acknowledgements**
The author would like to thank Álvaro Lozano-Robledo for the helpful correspondence and discussions, Katherine Stange for the advice and direction, and Alex Braat for discovering a false claim in an earlier version of this paper. The author is also indebted to David Grant for the insightful conversations and suggestions. Finally, the author is immensely grateful to the anonymous referees for the detailed comments, helpful feedback, and thoughtful criticism. This paper is much improved because of their work. This research was partially supported by NSF-CAREER CNS-1652238 under the supervision of PI Dr. Katherine E. Stange.

**Data Availability** Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Received: 5 February 2022 Accepted: 11 January 2023 Published online: 2 February 2023

**References**

1. Adelmann, C.: The Decomposition of Primes in Torsion Point Fields. Lecture Notes in Mathematics, vol. 1761. Springer, Berlin (2001)
2. Bourdon, A., Clark, P.L.: Torsion points and isogenies on CM elliptic curves. J. Lond. Math. Soc. (2) 102(2), 580–622 (2020)
3. Bourdon, A., Ejder, O., Liu, Y., Odumodu, F., Viray, B.: On the level of modular curves that give rise to isolated $j$-invariants. Adv. Math. 357, 106824 (2019)
4. Bourdon, A., Gill, D.R., Reuse, J., Watson, L.D.: Odd degree isolated points on $X_1(n)$ with rational $j$-invariant (2020)
5. Bourdon, A., Filipp, N.: Sporadic points of odd degree on $X_1(n)$ coming from $\mathbb{Q}$-curves (2021)
6. Boxall, J., Grant, D.: Singular torsion points on elliptic curves. Math. Res. Lett. 10(5–6), 847–866 (2003)
7. Buzzard, K.: Analytic continuation of overconvergent eigenforms. J. Am. Math. Soc. 16(1), 29–55 (2003)
8. Cali, E., Kraus, A.: Sur la $p$-différente du corps des points de $t$-torsion des courbes elliptiques, $j \neq p$. Acta Arith. 104(1), 1–21 (2002)
9. Centeleghe, T.G.: Integral Tate modules and splitting of primes in torsion fields of elliptic curves. Int. J. Number Theory 12(1), 237–248 (2016)
10. Clark, P.L., Genao, T., Pollack, P., Saia, F.: The least degree of a CM point on a modular curve. J. Lond. Math. Soc. 105(2), 825–883 (2022)
11. Coleman, R.F.: Classical and overconvergent modular forms. Invent. Math. 124(1–3), 215–241 (1996)
12. Conrad, B.: Higher-level canonical subgroups in abelian varieties (2006). http://virtualmath1.stanford.edu/~conrad/papers/subgppaper.pdf
13. Conrad, B.: Modular curves and rigid-analytic spaces. Pure Appl. Math. Q. 2(1), Special Issue: In honor of John H. Coates. Part 1), 29–110 (2006)
14. Deby, C.: Beyond two criteria for supersingularity: coefficients of division polynomials. J. Théor. Nr. Bords 26(3), 595–606 (2014)
15. Derickx, M., Etropolski, A., van Hoeij, M., Morrow, J.S., Zureick-Brown, D.: Sporadic cubic torsion. Algebra Number Theory 15(7), 1837–1864 (2021)
16. Derickx, M., Kamienny, S., Stein, W., Stoll, M.: Torsion points on elliptic curves over number fields of small degree. ArXiv e-prints (July 2017)
17. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hans. Univ. 14, 197–272 (1941)
18. Duke, W., Tóth, Á.: The splitting of primes in division fields of elliptic curves. Exp. Math. (2002) 11(4), 555–565 (2003)
19. Freitas, N., Kraus, A.: On the degree of the $p$-torsion field of elliptic curves over $\mathbb{Q}_p$ for $p \neq p$. Acta Arith. 195(1), 13–55 (2020)
20. González-Jiménez, E., Lozano-Robledo, Å.: Elliptic curves with abelian division fields. Math. Z. 283(3-4), 835–859 (2016)
21. Gouvea, F.Q.: Arithmetic of $p$-adic Modular Forms. Lecture Notes in Mathematics, vol. 1304. Springer, Berlin (1988)
22. Jeon, D., Kim, C.H., Schweizer, A.: On the torsion of elliptic curves over cubic number fields. Acta Arith. 113(3), 291–301 (2004)
23. Kamienny, S.: Torsion points on elliptic curves and $q$-coefficients of modular forms. Invent. Math. 109(2), 221–229 (1992)
24. Katz, N.M.: $p$-adic properties of modular schemes and modular forms. In: Modular Functions of One Variable, III (Proceedings of the International Summer School, University of Antwerp, Antwerp, 1972), Lecture Notes in Mathematics, vol. 350, pp. 69–190. Springer, Berlin (1973)
25. Kenku, M.A., Momose, F.: Torsion points on elliptic curves defined over quadratic fields. Nagoya Math. J. 109, 125–149 (1988)
26. Kida, M.: Ramification in the division fields of an elliptic curve. Abh. Math. Sem. Univ. Hamburg 73, 195–207 (2003)
27. Kraus, A.: Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. Manuscr. Math. 69(4), 353–385 (1990)
28. Kraus, A.: Sur la $p$-différente du corps des points de $p$-torsion des courbes elliptiques. Bull. Aust. Math. Soc. 60(3), 407–428 (1999)
29. Lozano-Robledo, Á.: Formal groups of elliptic curves with potential good supersingular reduction. Pac. J. Math. 261(1), 145–164 (2013)
30. Lozano-Robledo, Á.: Division fields of elliptic curves with minimal ramification. Rev. Mat. Iberoam. 31(4), 1311–1332 (2015)
31. Lozano-Robledo, Á.: Ramification in the division fields of elliptic curves with potential supersingular reduction. Res. Number Theory 2, 8 (2016)
32. Lubin, J.: Canonical subgroups of formal groups. Trans. Am. Math. Soc. 251, 103–127 (1979)
33. Mazur, B.: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. (1977) 47, 33–186 (1978)
34. Mazur, B.: Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math. 44(2), 129–162 (1978)
35. Merel, L.: Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math. 124(1–3), 437–449 (1996)
36. Najman, F.: Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. Math. Res. Lett. 23(1), 245–272 (2016)
37. Parent, P.: Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. J. Reine Angew. Math. 506, 85–116 (1999)
38. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. 15(4), 259–331 (1972)
39. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 106, 2nd edn. Springer, Dordrecht (2009)
40. Smith, H.: Non-monogenic division fields of elliptic curves. J. Number Theory 228, 174–187 (2021)
41. Sutherland, A.: Torsion subgroups of elliptic curves over number fields (2012)
42. The Sage Developers: SageMath, the Sage Mathematics Software System (Version 9.1). The Sage Developers (2020). http://www.sagemath.org
43. van Hoeij, M., Smith, H.: A divisor formula and a bound on the $Q$-gonality of the modular curve $X_1(N)$. Res. Number Theory 7(2), 22 (2021)

Publisher’s Note
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightholder(s). Author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.