Ramification in Division Fields and Sporadic Points on Modular Curves

Hanson Smith

University of Connecticut
1. Summary

2. Context

3. Valuations of Points

4. Proof Ideas

5. Application to Sporadic Points on $X_1(N)$
Summary
Let $E$ be an elliptic curve over a number field $K$ with good supersingular reduction at some prime $p$ living above the rational prime $p$. 

\[^{1}\text{Normalize so that } v_p(p) = 1.\]
Let $E$ be an elliptic curve over a number field $K$ with good supersingular reduction at some prime $p$ living above the rational prime $p$. Suppose $P \in E(K)$ is a point of exact order $p^n$. 

$^1$Normalize so that $v_p(p) = 1$. 

Ramification Result
Let $E$ be an elliptic curve over a number field $K$ with good supersingular reduction at some prime $p$ living above the rational prime $p$. Suppose $P \in E(K)$ is a point of exact order $p^n$. Then we precisely classify the possible valuations of the $x$- and $y$-coordinates of $P$ in terms of the valuation of the coefficient of $x^{p^2-p}$ in the $p$th division polynomial of $E$.

\[ v_p(p) = 1. \]
Let \( E \) be an elliptic curve over a number field \( K \) with good supersingular reduction at some prime \( p \) living above the rational prime \( p \). Suppose \( P \in E(K) \) is a point of exact order \( p^n \). Then we precisely classify the possible valuations of the \( x \)- and \( y \)-coordinates of \( P \) in terms of the valuation of the coefficient of \( x^{\frac{p^2-p}{2}} \) in the \( p \)th division polynomial of \( E \).

Call this valuation\(^1\) \( \mu \). If \( \mu \geq \frac{p}{p+1} \), then all the \( x \)-coordinates of \( p^n \)-torsion points have the same valuation, which is

\[
\frac{-2}{p^{2n} - p^{2n-2}} = -2 \cdot \frac{1}{p^{2(n-1)}(p^2 - 1)}.
\]

\(^1\)Normalize so that \( v_p(p) = 1 \).
Let $E$ be an elliptic curve that is supersingular at some prime above $p$ with $\mu \geq \frac{p}{p+1}$, then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$. 
Let $E$ be an elliptic curve that is supersingular at some prime above $p$ with $\mu \geq \frac{p}{p+1}$, then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$.

In other words, $E$ does not have a $p^n$-torsion point over a number field of especially small degree.
Let $N > 12$ be a positive integer not divisible by 6 and write $N = \prod_{i=1}^{k} p_i^{e_i}$ for the prime factorization. Suppose $E/\mathbb{Q}$ has good supersingular reduction at each $p_i$, then $j(E)$ does not correspond to a sporadic point on $X_1(N)$. 
Being supersingular at primes dividing $N$ can be an obstruction to having an $N$-torsion point defined over a number field of particularly low degree.
Context
Previous work in this area comes in a couple of different flavors:

- Firstly, in analogy with cyclotomic fields we can ask about the arithmetic structure of fields obtained by adjoining some or all of the $N$-division points of an elliptic curve.

- We can also ask about the possible torsion structures for elliptic curves over a number field with a given Galois group or degree.
Previous work in this area comes in a couple of different flavors:

- Firstly, in analogy with cyclotomic fields we can ask about the arithmetic structure of fields obtained by adjoining some or all of the $N$-division points of an elliptic curve.

- We can also ask about the possible torsion structures for elliptic curves over a number field with a given Galois group or degree.

Mazur’s Theorem +: [Mazur, 1977], [Mazur, 1978]; [Kenku and Momose, 1988], [Kamienny, 1992]; [Jeon et al., 2004], [Najman, 2016], [Derickx et al., 2020].

Valuations of Points
Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $p$ and write $[p]T$ for the multiplication-by-$p$ map.
Let \( \hat{E} \) denote the formal group of an elliptic curve that is supersingular at \( p \) and write \( [p] T \) for the multiplication-by-\( p \) map.

In “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques,” Serre recognized that the Newton polygon associated to \( [p] T \) could have two forms in the supersingular case.
Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $p$ and write $[p]T$ for the multiplication-by-$p$ map.

In “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques,” Serre recognized that the Newton polygon associated to $[p]T$ could have two forms in the supersingular case.

It could have one side (one-slope case) corresponding to all $p$-torsion elements in $\hat{E}$ having the same valuation,
Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $p$ and write $[p]T$ for the multiplication-by-$p$ map.

In “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques,” Serre recognized that the Newton polygon associated to $[p]T$ could have two forms in the supersingular case.

It could have one side (one-slope case) corresponding to all $p$-torsion elements in $\hat{E}$ having the same valuation, or it could have two sides (two-slope case), corresponding to a subgroup of $\hat{E}[p]$ of order $p$ having larger valuation.
Notice \( \mu \) is the valuation of the coefficient corresponding to sums of products of \( p^2 - p \) roots.

**Figure 1:** The Newton polygon for the polynomial \( \prod_{\hat{P} \in \hat{E}[=p]} (T - \hat{P}) \).
The One-Slope Case

Figure 2: The Newton polygon for the polynomial

\[ \prod_{\hat{\rho} \in \hat{E}[=p]} (T - \hat{P}) \]
In the ‘two-slope case’ people say that $E$ has a canonical subgroup at $p$. This is because the subgroup of $\hat{E}$ with larger valuation is a canonical lift of the kernel of Frobenius. This subgroup is very important to those who study overconvergent modular forms and well-studied in that context.
Recall, $\mu$ is the valuation of the coefficient of $x^{p^2/p}$ in the $p^{\text{th}}$ division polynomial. Equivalently, it is the valuation of the coefficient of $T^p$ in $[p]T$. When there is a canonical subgroup, then you can think of $\mu$ as the sum of the valuations of elements of $\hat{E}[=p]$ that are not in the canonical subgroup.

If $\mu < p^{2/p} + 1$, then there is a canonical subgroup. The elements that are not in it have valuation $\mu p^{-2}$ and the elements that are in it have valuation $1/\mu p^{1/p}$.
Recall, $\mu$ is the valuation of the coefficient of $x^{\frac{p^2-p}{2}}$ in the $p^{\text{th}}$ division polynomial. Equivalently, it is the valuation of the coefficient of $T^p$ in $[p]T$. When there is a canonical subgroup, then you can think of $\mu$ as the sum of the valuations of elements of $\hat{E}[=p]$ that are not in the canonical subgroup.

If $\mu \geq \frac{p}{p+1}$, then there is no canonical subgroup and all the elements in $\hat{E}[=p]$ have the same valuation, which is $\frac{1}{p^2-1}$. 
Recall, $\mu$ is the valuation of the coefficient of $x^{\frac{p^2-p}{2}}$ in the $p$th division polynomial. Equivalently, it is the valuation of the coefficient of $T^p$ in $[p] T$. When there is a canonical subgroup, then you can think of $\mu$ as the sum of the valuations of elements of $\hat{E}[= p]$ that are not in the canonical subgroup.

If $\mu \geq \frac{p}{p+1}$, then there is no canonical subgroup and all the elements in $\hat{E}[= p]$ have the same valuation, which is $\frac{1}{p^2-1}$.

If $\mu < \frac{p}{p+1}$, then there is a canonical subgroup. The elements that are not in it have valuation $\frac{\mu}{p^2-p}$ and the elements that are in it have valuation $\frac{1-\mu}{p-1}$. 
What about $p^n$-torsion when $n > 1$?
What about $p^n$-torsion when $n > 1$?

First off, if there is no canonical subgroup, we “just divide by $p^2$.” So a 125-torsion element has valuation $\frac{1}{5^4(5^2-1)}$. 

\begin{align*}
25\text{-tors} & \downarrow [5] \\
5\text{-tors} & \downarrow [5] \\
5\text{-tors} & \downarrow [5] \\
\frac{1}{5^2(5^2-1)} & \\
\frac{1}{5^2-1} & 
\end{align*}
What about $p^n$-torsion when $n > 1$?

First off, if there is no canonical subgroup, we “just divide by $p^2$. “ So a 125-torsion element has valuation $\frac{1}{5^4(5^2-1)}$.

Even when there is a canonical subgroup, for points that are not above it we still divide by $p^2$. 
What about $p^n$-torsion when $n > 1$?

First off, if there is no canonical subgroup, we “just divide by $p^2$.” So a 125-torsion element has valuation $\frac{1}{5^4(5^2-1)}$.

Even when there is a canonical subgroup, for points that are not above it we still divide by $p^2$. So a 125-torsion element $\hat{P}$ such that $[5^2]\hat{P}$ is not in the canonical subgroup has valuation $\frac{\mu}{5^4(5^2-5)}$. 
Interestingly, we have a phenomenon that is similar to the canonical subgroup in some ways occurring for higher power torsion.
Interestingly, we have a phenomenon that is similar to the canonical subgroup in some ways occurring for higher power torsion. When $\mu$ is small enough, then in the fibers over ($p^{th}$ roots of) elements in the canonical subgroup, $[p]^{-1} \hat{Q}$, there is a subset of $p$-elements with larger valuation.
For $n > 1$, let $s \in \mathbb{Z}_{\geq 0}$ be the smallest integer such that $\mu \geq \frac{1}{p^s(p+1)}$. If $n \leq s + 1$, then either

$$v_p\left(\hat{P}\right) = \frac{1 - p^{n-1}\mu}{p^{n-1}(p - 1)} \quad \text{or} \quad v_p\left(\hat{P}\right) = \frac{\mu}{p^{2m}(p^2 - p)},$$

where $m$ is the smallest non-negative integer such that $v_p\left([p^m] \hat{P}\right) = \frac{\mu}{p^2 - p}$. 

(1)
For \( n > 1 \), let \( s \in \mathbb{Z}^{\geq 0} \) be the smallest integer such that \( \mu \geq \frac{1}{p^s(p+1)} \). If \( n \leq s + 1 \), then either

\[
\nu_p \left( \hat{P} \right) = \frac{1 - p^{n-1} \mu}{p^{n-1}(p - 1)} \quad \text{or} \quad \nu_p \left( \hat{P} \right) = \frac{\mu}{p^{2m}(p^2 - p)},
\]

(1)

where \( m \) is the smallest non-negative integer such that \( \nu_p \left( [p^m] \hat{P} \right) = \frac{\mu}{p^2 - p} \). If \( n > s + 1 \), then either

\[
\nu_p \left( \hat{P} \right) = \frac{1 - p^s \mu}{p^{2n-s-2}(p - 1)} \quad \text{or} \quad \nu_p \left( \hat{P} \right) = \frac{\mu}{p^{2m}(p^2 - p)},
\]

(2)

where \( m \) is as above.
Proof Ideas
Main Idea

Stare at the power series for the multiplication-by-$p$ map in the formal group of $E$ at $p$ for a long time. Because $E$ is supersingular at $p$ this is equivalent to staring at the $p^{\text{th}}$ division polynomial.
Main Idea

Stare at the power series for the multiplication-by-$p$ map in the formal group of $E$ at $p$ for a long time. Because $E$ is supersingular at $p$ this is equivalent to staring at the $p^{\text{th}}$ division polynomial.

Let $\pi_p$ be a uniformizer at $p$. The multiplication-by-$p$ map has the form

$$[p]T = pf(T) + \pi_p^\mu g(T^p) + h\left(T^{p^2}\right),$$

where $f$, $g$, and $h$ are power series without constant coefficients and with $f'(0), g'(0), h'(0)$ all units.

After a little work we see that we must compare $pv(\hat{P}) + \mu$ and $p^2v(\hat{P})$ where $\hat{P}$ is the image of a point of $E[=p^n]$ in the formal group. We also have that the minimum of these two values is greater than or equal to $\hat{Q}$, where $Q \in E[=p^{n-1}]$. 

Ramification in Division Fields and Sporadic Points on Modular Curves
Application to Sporadic Points on $X_1(N)$
The work above gives the minimal ramification necessary to have a $p^n$-torsion point in terms of the valuation of a coefficient of the $p^\text{th}$ division polynomial. This yields a lower bound on the degree of a field over which a $p^n$-torsion point is defined.
The work above gives the minimal ramification necessary to have a $p^n$-torsion point in terms of the valuation of a coefficient of the $p^\text{th}$ division polynomial. This yields a lower bound on the degree of a field over which a $p^n$-torsion point is defined.

So to preclude sporadic points on $X_1(p^n)$, compare the lower bound with have with an upper bound on the $\mathbb{Q}$-gonality of the modular curve $X_1(p^n)$. 
The work above gives the minimal ramification necessary to have a $p^n$-torsion point in terms of the valuation of a coefficient of the $p^\text{th}$ division polynomial. This yields a lower bound on the degree of a field over which a $p^n$-torsion point is defined.

So to preclude sporadic points on $X_1(p^n)$, compare the lower bound with an upper bound on the $\mathbb{Q}$-gonality of the modular curve $X_1(p^n)$. There is also some dotting of i’s and crossing of t’s with additive reduction resolving to good supersingular reduction and Weber functions.
Let $E$ be an elliptic curve that is supersingular at some prime above $p$ with no canonical subgroup ($\mu \geq \frac{p}{p+1}$), then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$. 
Let $E$ be an elliptic curve that is supersingular at some prime above $p$ with no canonical subgroup ($\mu \geq \frac{p}{p+1}$), then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$.

Elliptic curves with a canonical subgroup are “less supersingular” because, like ordinary elliptic curves, they have a canonical lift of the kernel of Frobenius. Hence, if one was willing to speak imprecisely (which I always am), we could say that the most supersingular elliptic curves do not correspond to sporadic points.

The decomposition of primes in torsion point fields, volume 1761 of Lecture Notes in Mathematics.
Springer-Verlag, Berlin.


Sur la $p$-différente du corps des points de $l$-torsion des courbes elliptiques, $l \neq p$.


**Sporadic Cubic Torsion.**

*arXiv e-prints.*


**Torsion points on elliptic curves over number fields of small degree.**

*ArXiv e-prints.*


**The splitting of primes in division fields of elliptic curves.**


**On the degree of the** $p$-**torsion field of elliptic curves over** $\mathbb{Q}_\ell$
**for** $\ell \neq p$.

*ArXiv e-prints.*


**Elliptic curves with abelian division fields.**


**On the torsion of elliptic curves over cubic number fields.**

**Torsion points on elliptic curves and q-coefficients of modular forms.**  

**Torsion points on elliptic curves defined over quadratic fields.**  

**Sur la p-différente du corps des points de p-torsion des courbes elliptiques.**  

**Uniform boundedness in terms of ramification.**


**Modular curves and the Eisenstein ideal.**


**Rational isogenies of prime degree (with an appendix by D. Goldfeld).**


**Bornes pour la torsion des courbes elliptiques sur les corps de nombres.**


**Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$.**


Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres.

Ramification in Division Fields and Sporadic Points on Modular Curves

Hanson Smith

University of Connecticut
1. Summary

2. Context

3. Valuations of Points

4. Proof Ideas

5. Application to Sporadic Points on $X_1(N)$
Summary
Let $E$ be an elliptic curve over a number field $K$ with good supersingular reduction at some prime $p$ living above the rational prime $p$.

\[P \in E(K)\] is a point of exact order $p^n$. Then we precisely classify the possible valuations of the $x$- and $y$-coordinates of $P$ in terms of the valuation of the coefficient of $x^{p^2}y^{p^2}$ in the $p$th division polynomial of $E$.

Call this valuation $\nu_{p^2}$. If $\nu_{p^2} = p^2 + 1$, then the $x$-coordinates of $p^n$-torsion points have the same valuation, which is $2p^2n = 2 \cdot 1\cdot (p^21)$.  

\(^1\)Normalize so that $v_p(p) = 1$. 

1. Ramification in Division Fields and Sporadic Points on Modular Curves
Let $E$ be an elliptic curve over a number field $K$ with good supersingular reduction at some prime $p$ living above the rational prime $p$. Suppose $P \in E(K)$ is a point of exact order $p^n$. 

\[1\text{ Normalize so that } v_p(p) = 1.\]
Let $E$ be an elliptic curve over a number field $K$ with good supersingular reduction at some prime $p$ living above the rational prime $p$. Suppose $P \in E(K)$ is a point of exact order $p^n$. Then we precisely classify the possible valuations of the $x$- and $y$-coordinates of $P$ in terms of the valuation of the coefficient of $x^{\frac{p^2-p}{2}}$ in the $p^{th}$ division polynomial of $E$.

\footnote{Normalize so that $v_p(p) = 1$.}
Let $E$ be an elliptic curve over a number field $K$ with good supersingular reduction at some prime $p$ living above the rational prime $p$. Suppose $P \in E(K)$ is a point of exact order $p^n$. Then we precisely classify the possible valuations of the $x$- and $y$-coordinates of $P$ in terms of the valuation of the coefficient of $x^{p^2 - p^2}$ in the $p^{\text{th}}$ division polynomial of $E$.

Call this valuation\(^1\) $\mu$. If $\mu \geq \frac{p}{p+1}$, then all the $x$-coordinates of $p^n$-torsion points have the same valuation, which is

$$\frac{-2}{p^{2n} - p^{2n-2}} = -2 \cdot \frac{1}{p^{2(n-1)}(p^2 - 1)}.$$  

\(^1\)Normalize so that $v_p(p) = 1$.  

Hanson Smith

Ramification in Division Fields and Sporadic Points on Modular Curves
Let $E$ be an elliptic curve that is supersingular at some prime above $p$ with $\mu \geq \frac{p}{p+1}$, then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$. 
Let $E$ be an elliptic curve that is supersingular at some prime above $p$ with $\mu \geq \frac{p}{p+1}$, then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$.

In other words, $E$ does not have a $p^n$-torsion point over a number field of especially small degree.
Let $N > 12$ be a positive integer not divisible by 6 and write $N = \prod_{i=1}^{k} p_i^{e_i}$ for the prime factorization. Suppose $E/\mathbb{Q}$ has good supersingular reduction at each $p_i$, then $j(E)$ does not correspond to a sporadic point on $X_1(N)$. 
Moral

Being supersingular at primes dividing $N$ can be an obstruction to having an $N$-torsion point defined over a number field of particularly low degree.
Context
Previous work in this area comes in a couple of different flavors:

• Firstly, in analogy with cyclotomic fields we can ask about the arithmetic structure of fields obtained by adjoining some or all of the $N$-division points of an elliptic curve.
Previous work in this area comes in a couple of different flavors:

- Firstly, in analogy with cyclotomic fields we can ask about the arithmetic structure of fields obtained by adjoining some or all of the $N$-division points of an elliptic curve.

- We can also ask about the possible torsion structures for elliptic curves over a number field with a given Galois group or degree.
Some Previous Work

**Arithmetic of Torsion Fields:** [Duke and Tóth, 2002]; [Adelmann, 2001]; [Kraus, 1999], [Cali and Kraus, 2002], [Freitas and Kraus, 2018]; [González-Jiménez and Lozano-Robledo, 2016].

**Mazur’s Theorem +:** [Mazur, 1977], [Mazur, 1978]; [Kenku and Momose, 1988], [Kamienny, 1992]; [Jeon et al., 2004], [Najman, 2016], [Derickx et al., 2020].

**Uniform Boundedness +:** [Merel, 1996]; Oesterlé’s proof: [Derickx et al., 2017, Appendix A]; [Parent, 1999]; [Lozano-Robledo, 2018].
Valuations of Points
Let \( \hat{E} \) denote the formal group of an elliptic curve that is supersingular at \( p \) and write \([p] T\) for the multiplication-by-\( p \) map.
Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $p$ and write $[p]T$ for the multiplication-by-$p$ map.

In “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques,” Serre recognized that the Newton polygon associated to $[p]T$ could have two forms in the supersingular case.
Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $p$ and write $[p]T$ for the multiplication-by-$p$ map.

In “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques,” Serre recognized that the Newton polygon associated to $[p]T$ could have two forms in the supersingular case.

It could have one side (one-slope case) corresponding to all $p$-torsion elements in $\hat{E}$ having the same valuation,
Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $p$ and write $[p]T$ for the multiplication-by-$p$ map.

In “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques,” Serre recognized that the Newton polygon associated to $[p]T$ could have two forms in the supersingular case.

It could have one side (one-slope case) corresponding to all $p$-torsion elements in $\hat{E}$ having the same valuation, or it could have two sides (two-slope case), corresponding to a subgroup of $\hat{E}[p]$ of order $p$ having larger valuation.
The Two-Slope Case

Notice $\mu$ is the valuation of the coefficient corresponding to sums of products of $p^2 - p$ roots.

Figure 1: The Newton polygon for the polynomial $\prod_{\hat{P} \in \hat{E}[=p]} (T - \hat{P})$.
The One-Slope Case

Figure 2: The Newton polygon for the polynomial
$$\prod_{\hat{P} \in \mathcal{E}[\equiv p]} (T - \hat{P})$$
In the ‘two-slope case’ people say that $E$ has a *canonical subgroup* at $p$. This is because the subgroup of $\hat{E}$ with larger valuation is a canonical lift of the kernel of Frobenius. This subgroup is very important to those who study overconvergent modular forms and well-studied in that context.
Recall, $\mu$ is the valuation of the coefficient of $x^{\frac{p^2-p}{2}}$ in the $p^{\text{th}}$ division polynomial. Equivalently, it is the valuation of the coefficient of $T^p$ in $[p]T$. When there is a canonical subgroup, then you can think of $\mu$ as the sum of the valuations of elements of $\hat{E}[=p]$ that are not in the canonical subgroup.

If $\mu \geq p^2-p$, then there is no canonical subgroup and all the elements in $\hat{E}[=p]$ have the same valuation, which is $\frac{1}{p^2-p}$.

If $\mu < p^2-p$, then there is a canonical subgroup. The elements that are not in it have valuation $\frac{\mu}{p^2-p}$ and the elements that are in it have valuation $\frac{1}{\mu}$. 

Hanson Smith

Ramification in Division Fields and Sporadic Points on Modular Curves
Recall, $\mu$ is the valuation of the coefficient of $x^{\frac{p^2-p}{2}}$ in the $p^{th}$ division polynomial. Equivalently, it is the valuation of the coefficient of $T^p$ in $[p]T$. When there is a canonical subgroup, then you can think of $\mu$ as the sum of the valuations of elements of $\hat{E}[/=p]$ that are not in the canonical subgroup.

If $\mu \geq \frac{p}{p+1}$, then there is no canonical subgroup and all the elements in $\hat{E}[/=p]$ have the same valuation, which is $\frac{1}{p^2-1}$. 
Recall, $\mu$ is the valuation of the coefficient of $x^{\frac{p^2-p}{2}}$ in the $p^{\text{th}}$ division polynomial. Equivalently, it is the valuation of the coefficient of $T^p$ in $[p]T$. When there is a canonical subgroup, then you can think of $\mu$ as the sum of the valuations of elements of $\hat{E} [= p]$ that are not in the canonical subgroup.

If $\mu \geq \frac{p}{p+1}$, then there is no canonical subgroup and all the elements in $\hat{E} [= p]$ have the same valuation, which is $\frac{1}{p^2-1}$.

If $\mu < \frac{p}{p+1}$, then there is a canonical subgroup. The elements that are not in it have valuation $\frac{\mu}{p^2-p}$ and the elements that are in it have valuation $\frac{1-\mu}{p-1}$.
What about $p^n$-torsion when $n > 1$?
What about $p^n$-torsion when $n > 1$?

First off, if there is no canonical subgroup, we “just divide by $p^2$.” So a 125-torsion element has valuation $\frac{1}{5^4(5^2-1)}$. 
What about $p^n$-torsion when $n > 1$?

First off, if there is no canonical subgroup, we “just divide by $p^2$.” So a 125-torsion element has valuation $\frac{1}{5^4(5^2-1)}$.

Even when there is a canonical subgroup, for points that are not above it we still divide by $p^2$. 
What about \( p^n \)-torsion when \( n > 1 \)?

First off, if there is no canonical subgroup, we “just divide by \( p^2 \).” So a 125-torsion element has valuation \( \frac{1}{5^4(5^2-1)} \).

Even when there is a canonical subgroup, for points that are not above it we still divide by \( p^2 \). So a 125-torsion element \( \hat{P} \) such that \([5^2]\hat{P}\) is not in the canonical subgroup has valuation \( \frac{\mu}{5^4(5^2-5)} \).
Interestingly, we have a phenomenon that is similar to the canonical subgroup in some ways occurring for higher power torsion.
Interestingly, we have a phenomenon that is similar to the canonical subgroup in some ways occurring for higher power torsion. When $\mu$ is small enough, then in the fibers over ($p^{\text{th}}$ roots of) elements in the canonical subgroup, $[p]^{-1}\hat{Q}$, there is a subset of $p$-elements with larger valuation.
For $n > 1$, let $s \in \mathbb{Z}^{\geq 0}$ be the smallest integer such that $\mu \geq \frac{1}{p^s(p+1)}$. If $n \leq s + 1$, then either

$$v_p \left( \hat{P} \right) = \frac{1 - p^{n-1} \mu}{p^{n-1}(p - 1)} \quad \text{or} \quad v_p \left( \hat{P} \right) = \frac{\mu}{p^{2m}(p^2 - p)},$$

(1)

where $m$ is the smallest non-negative integer such that $v_p \left( [p^m] \hat{P} \right) = \frac{\mu}{p^2 - p}$. 

---

Hanson Smith

Ramification in Division Fields and Sporadic Points on Modular Curves
For \( n > 1 \), let \( s \in \mathbb{Z}^{\geq 0} \) be the smallest integer such that \( \mu \geq \frac{1}{p^s(p+1)} \). If \( n \leq s + 1 \), then either

\[ v_p \left( \hat{P} \right) = \frac{1 - p^{n-1}\mu}{p^{n-1}(p-1)} \quad \text{or} \quad v_p \left( \hat{P} \right) = \frac{\mu}{p^{2m}(p^2 - p)}, \tag{1} \]

where \( m \) is the smallest non-negative integer such that \( v_p \left( [p^m] \hat{P} \right) = \frac{\mu}{p^2 - p} \). If \( n > s + 1 \), then either

\[ v_p \left( \hat{P} \right) = \frac{1 - p^s\mu}{p^{2n-s-2}(p-1)} \quad \text{or} \quad v_p \left( \hat{P} \right) = \frac{\mu}{p^{2m}(p^2 - p)}, \tag{2} \]

where \( m \) is as above.
Proof Ideas
Main Idea

Stare at the power series for the multiplication-by-$p$ map in the formal group of $E$ at $p$ for a long time. Because $E$ is supersingular at $p$ this is equivalent to staring at the $p^{th}$ division polynomial.
Main Idea

Stare at the power series for the multiplication-by-$p$ map in the formal group of $E$ at $p$ for a long time. Because $E$ is supersingular at $p$ this is equivalent to staring at the $p^{\text{th}}$ division polynomial.

Let $\pi_p$ be a uniformizer at $p$. The multiplication-by-$p$ map has the form

$$[p] T = pf(T) + \pi_p g(T^p) + h(T^{p^2}),$$

where $f$, $g$, and $h$ are power series without constant coefficients and with $f'(0)$, $g'(0)$, $h'(0)$ all units.

After a little work we see that we must compare $pv(\hat{P}) + \mu$ and $p^2 v(\hat{P})$ where $\hat{P}$ is the image of a point of $E[= p^n]$ in the formal group. We also have that the minimum of these two values is greater than or equal to $\hat{Q}$, where $Q \in E[= p^{n-1}]$. 
Application to Sporadic Points on $X_1(N)$
The work above gives the minimal ramification necessary to have a $p^n$-torsion point in terms of the valuation of a coefficient of the $p^\text{th}$ division polynomial. This yields a lower bound on the degree of a field over which a $p^n$-torsion point is defined.
The work above gives the minimal ramification necessary to have a $p^n$-torsion point in terms of the valuation of a coefficient of the $p^{th}$ division polynomial. This yields a lower bound on the degree of a field over which a $p^n$-torsion point is defined.

So to preclude sporadic points on $X_1(p^n)$, compare the lower bound with an upper bound on the $\mathbb{Q}$-gonality of the modular curve $X_1(p^n)$. 
The work above gives the minimal ramification necessary to have a $p^n$-torsion point in terms of the valuation of a coefficient of the $p^\text{th}$ division polynomial. This yields a lower bound on the degree of a field over which a $p^n$-torsion point is defined.

So to preclude sporadic points on $X_1(p^n)$, compare the lower bound with an upper bound on the $\mathbb{Q}$-gonality of the modular curve $X_1(p^n)$. There is also some dotting of i’s and crossing of t’s with additive reduction resolving to good supersingular reduction and Weber functions.
Let $E$ be an elliptic curve that is supersingular at some prime above $p$ with no canonical subgroup ($\mu \geq \frac{p}{p+1}$), then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$. The elliptic curves with a canonical subgroup are "less supersingular" because, like ordinary elliptic curves, they have a canonical lift of the kernel of Frobenius. Hence, if one was willing to speak imprecisely (which I always am), we could say that the most supersingular elliptic curves do not correspond to sporadic points.
Let $E$ be an elliptic curve that is supersingular at some prime above $p$ with no canonical subgroup ($\mu \geq \frac{p}{p+1}$), then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$.

Elliptic curves with a canonical subgroup are “less supersingular” because, like ordinary elliptic curves, they have a canonical lift of the kernel of Frobenius. Hence, if one was willing to speak imprecisely (which I always am), we could say that the most supersingular elliptic curves do not correspond to sporadic points.

The decomposition of primes in torsion point fields, volume 1761 of Lecture Notes in Mathematics.
Springer-Verlag, Berlin.


Sur la $p$-différente du corps des points de $l$-torsion des courbes elliptiques, $l \neq p$.


Sporadic Cubic Torsion.


Torsion points on elliptic curves over number fields of small degree.

ArXiv e-prints.


The splitting of primes in division fields of elliptic curves.


**On the degree of the $p$-torsion field of elliptic curves over $\mathbb{Q}_\ell$ for $\ell \neq p$.**

*ArXiv e-prints.*


**Elliptic curves with abelian division fields.**


**On the torsion of elliptic curves over cubic number fields.**


**Torsion points on elliptic curves and \( q \)-coefficients of modular forms.**


**Torsion points on elliptic curves defined over quadratic fields.**


**Sur la \( p \)-différente du corps des points de \( p \)-torsion des courbes elliptiques.**


Uniform boundedness in terms of ramification.


Modular curves and the Eisenstein ideal.


Rational isogenies of prime degree (with an appendix by D. Goldfeld).


**Bornes pour la torsion des courbes elliptiques sur les corps de nombres.**


**Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$.**


Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres.