Ramification in Division Fields and Sporadic Points on Modular Curves

Hanson Smith

University of Connecticut

Table of contents

Summary

Ramification Result

Let E be an elliptic curve over a number field K with good supersingular reduction at some prime $\mathfrak{p}$ living above the rational prime p.

[1]Normalize so that $v_{\mathfrak{p}}(p) = 1$.

Ramification Result

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

[1] Normalize so that $v_{\mathfrak{p}}(p) = 1$.

Ramification Result

Let E be an elliptic curve over a number field K with good supersingular reduction at some prime $\mathfrak{p}$ 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.

[1] Normalize so that $v_{\mathfrak{p}}(p) = 1$.

Ramification Result

Let E be an elliptic curve over a number field K with good supersingular reduction at some prime $\mathfrak{p}$ 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] μ. 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 $v_{\mathfrak{p}}(p) = 1$.

Sporadic Points: Prime Power Level

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 $n > 0$.

Sporadic Points: Prime Power Level

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.

Sporadic Points: Composite Level

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

Division/Torsion Fields

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.

Division/Torsion Fields

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

Canonical Subgroups

$P = (x, y) \rightsquigarrow -\frac{x}{y} \in \hat{E}$

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

Canonical Subgroups

Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $\mathfrak{p}$ 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.

Canonical Subgroups

Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $\mathfrak{p}$ 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,

Canonical Subgroups

Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $\mathfrak{p}$ 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 μ is the valuation of the coefficient corresponding to sums of products of $p^2 - p$ roots.

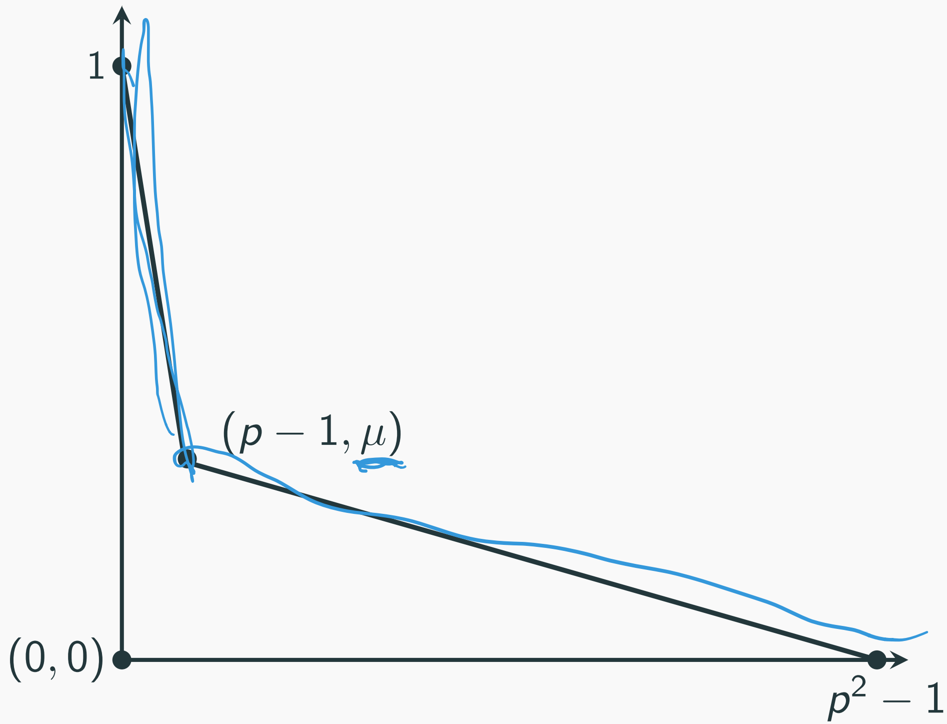


Figure 1: The Newton polygon for the polynomial $\prod_{\hat{P} \in \hat{E}[=p]} (T - \hat{P})$

The One-Slope Case

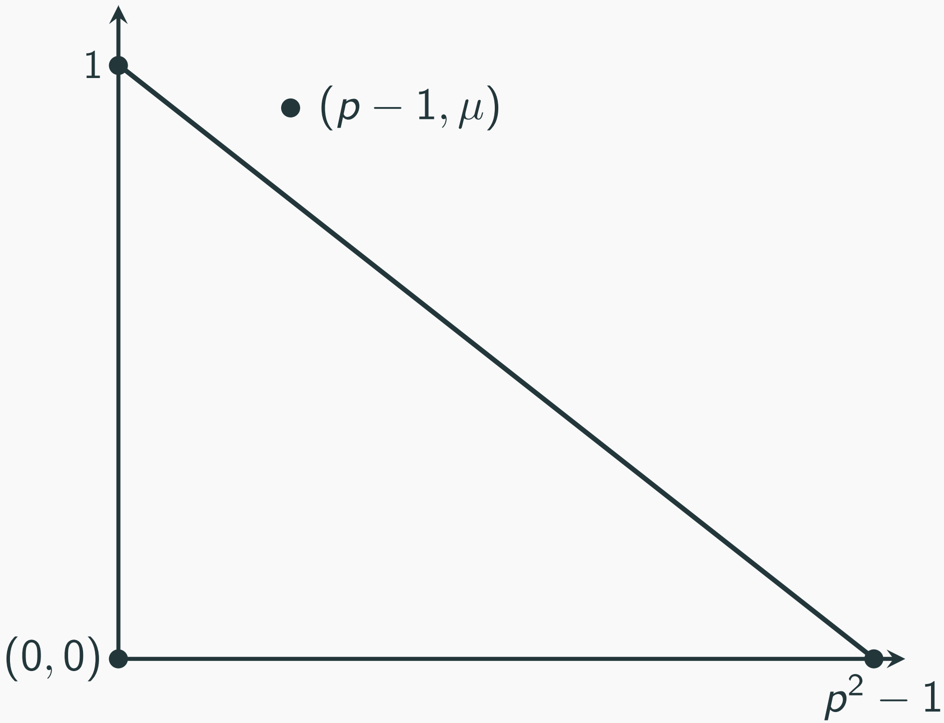


Figure 2: The Newton polygon for the polynomial $\prod_{\hat{P} \in \hat{E}[=p]} (T - \hat{P})$

Canonical Subgroups

In the ‘two-slope case’ people say that E has a *canonical subgroup* at $\mathfrak{p}$. 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.

Valuations and Canonical Subgroups

Recall, μ 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 μ as the sum of the valuations of elements of $\hat{E}[=p]$ that are **not** in the canonical subgroup.

Valuations and Canonical Subgroups

Recall, μ 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 μ 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 $\frac{1}{p^2-1}$.

Valuations and Canonical Subgroups

Recall, μ 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 μ 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 $\frac{1-\mu}{p-1}$.

p^n-Torsion

What about p^n-torsion when $n > 1$?

p^n-Torsion

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 $\frac{1}{5^4(5^2-1)}$.

$\vdots$

25-tors $\qquad \frac{1}{5^2(5^2-1)}$

$\big\downarrow [5]$

5-tors $\qquad \frac{1}{5^2-1}$

p^n-Torsion

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.

p^n-Torsion

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 $\frac{1}{5^4(5^2-1)}$.

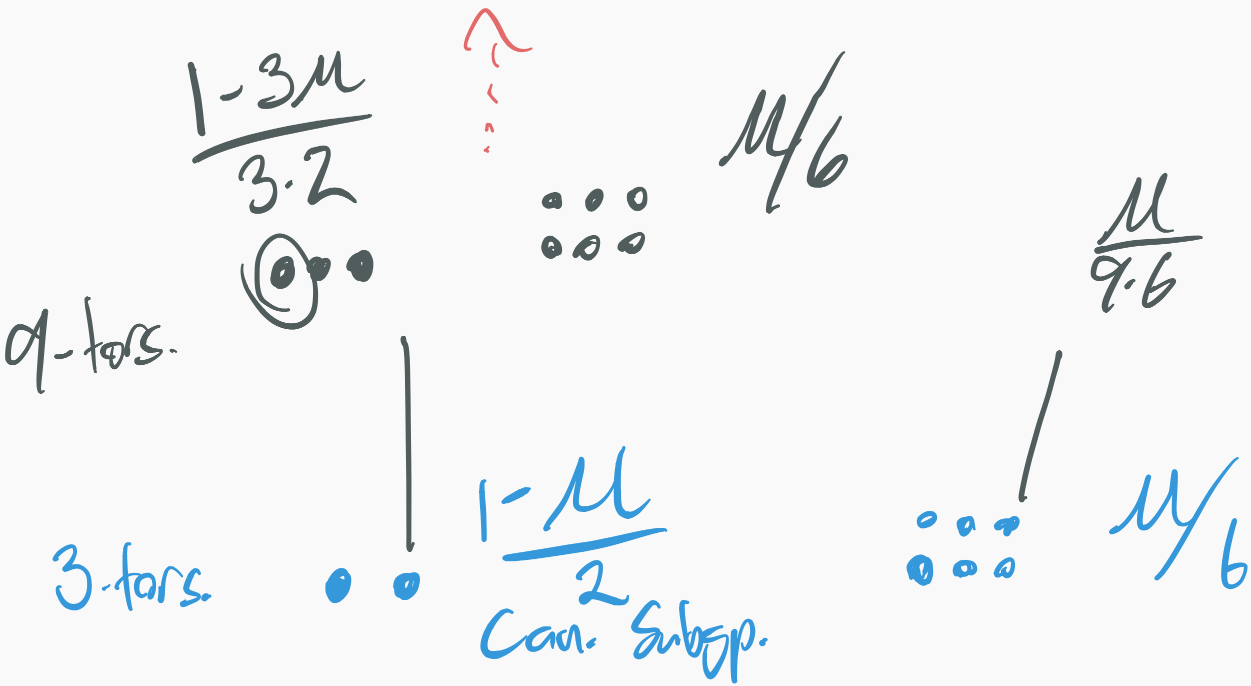
Even when there is a canonical subgroup, for points that are not above it we still divide by p^2. So a 125-torsion element $\hat{P}$ such that $[5^2]\hat{P}$ is not in the canonical subgroup has valuation $\frac{\mu}{5^4(5^2-5)}$.

Higher Order Subset of Larger Valuation

Interestingly, we have a phenomenon that is similar to the canonical subgroup in some ways occurring for higher power torsion.

Higher Order Subset of Larger Valuation

Interestingly, we have a phenomenon that is similar to the canonical subgroup in some ways occurring for higher power torsion. When μ 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.



Partial Theorem Statement

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

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

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

Partial Theorem Statement

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

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

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

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

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 $\mathfrak{p}$ for a long time. Because E is supersingular at $\mathfrak{p}$ 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 $\mathfrak{p}$ for a long time. Because E is supersingular at $\mathfrak{p}$ this is equivalent to staring at the p^{th} division polynomial.

Let $\pi_{\mathfrak{p}}$ be a uniformizer at $\mathfrak{p}$. The multiplication-by-p map has the form

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

where f, g, and h are power series without constant coefficients and with $f'(0), g'(0), h'(0)$ 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 $X_1(N)$

Degrees of Minimal p^n-Torsion Fields

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.

Degrees of Minimal p^n-Torsion Fields

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 have with an upper bound on the $\mathbb{Q}$-gonality of the modular curve $X_1(p^n)$.

Degrees of Minimal p^n-Torsion Fields

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 have 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.

Prime Power Level Sporadic Points

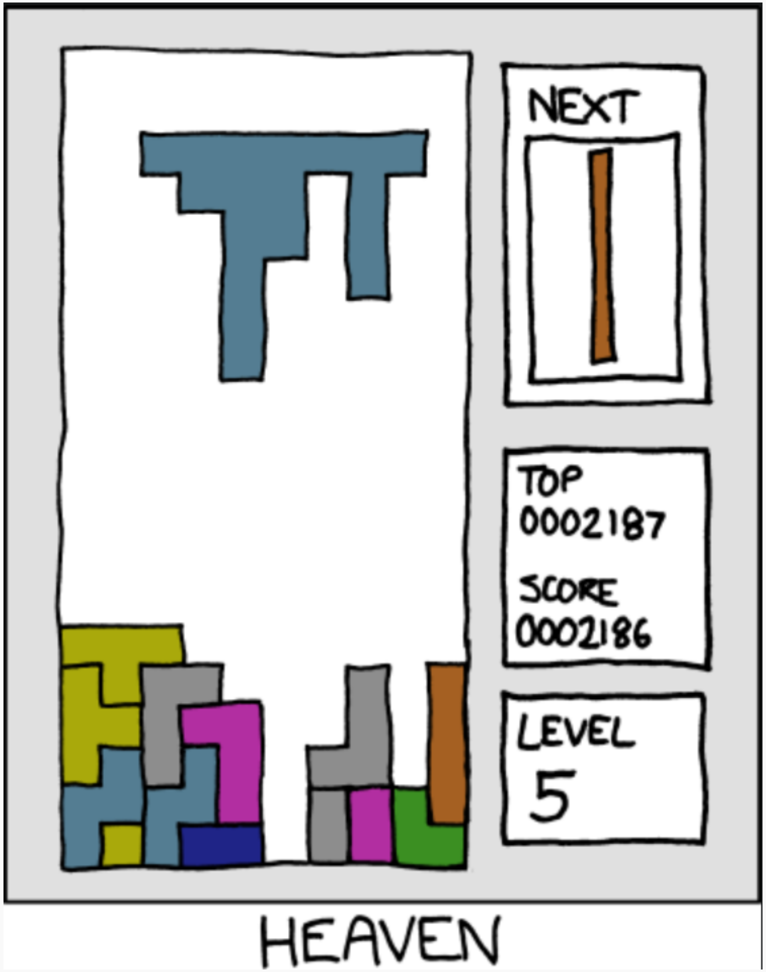
Let E be an elliptic curve that is supersingular at some prime above p with no canonical subgroup ($\mu \geq \frac{p}{p+1}$), then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$.

Prime Power Level 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.

https://xkcd.com/888/



References i

Adelmann, C. (2001).

The decomposition of primes in torsion point fields, volume 1761 of Lecture Notes in Mathematics.

Springer-Verlag, Berlin.

Cali, E. and Kraus, A. (2002).

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

Acta Arith., 104(1):1–21.

Derickx, M., Etropolski, A., van Hoeij, M., Morrow, J. S., and Zureick-Brown, D. (2020).

Sporadic Cubic Torsion.

arXiv e-prints.

Derickx, M., Kamienny, S., Stein, W., and Stoll, M. (2017).

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

ArXiv e-prints.

Duke, W. and Tóth, A. (2002).

The splitting of primes in division fields of elliptic curves.

Experiment. Math., 11(4):555–565 (2003).

References iii

Freitas, N. and Kraus, A. (2018).

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

ArXiv e-prints.

González-Jiménez, E. and Lozano-Robledo, Á. (2016).

Elliptic curves with abelian division fields.

Math. Z., 283(3-4):835–859.

Jeon, D., Kim, C. H., and Schweizer, A. (2004).

On the torsion of elliptic curves over cubic number fields.

Acta Arith., 113(3):291–301.

Kamienny, S. (1992).

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

Invent. Math., 109(2):221–229.

Kenku, M. A. and Momose, F. (1988).

Torsion points on elliptic curves defined over quadratic fields.

Nagoya Math. J., 109:125–149.

Kraus, A. (1999).

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

Bull. Austral. Math. Soc., 60(3):407–428.

References v

Lozano-Robledo, Á. (2018).

Uniform boundedness in terms of ramification.

Res. Number Theory, 4(1):4:6.

Mazur, B. (1977).

Modular curves and the Eisenstein ideal.

Inst. Hautes Études Sci. Publ. Math., (47):33–186 (1978).

Mazur, B. (1978).

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

Invent. Math., 44(2):129–162.

References vi

Merel, L. (1996).

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

Invent. Math., 124(1-3):437–449.

Najman, F. (2016).

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

Math. Res. Lett., 23(1):245–272.

Parent, P. (1999).

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

J. Reine Angew. Math., 506:85–116.

Ramification in Division Fields and Sporadic Points on Modular Curves

Hanson Smith

University of Connecticut

Table of contents

Summary

Ramification Result

Let E be an elliptic curve over a number field K with good supersingular reduction at some prime $\mathfrak{p}$ living above the rational prime p.

[1] Normalize so that $v_{\mathfrak{p}}(p) = 1$.

Ramification Result

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

[1] Normalize so that $v_{\mathfrak{p}}(p) = 1$.

Ramification Result

Let E be an elliptic curve over a number field K with good supersingular reduction at some prime $\mathfrak{p}$ 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.

[1] Normalize so that $v_{\mathfrak{p}}(p) = 1$.

Ramification Result

Let E be an elliptic curve over a number field K with good supersingular reduction at some prime $\mathfrak{p}$ 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] μ. 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 $v_{\mathfrak{p}}(p) = 1$.

Sporadic Points: Prime Power Level

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 $n > 0$.

Sporadic Points: Prime Power Level

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.

Sporadic Points: Composite Level

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

Division/Torsion Fields

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.

Division/Torsion Fields

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

Canonical Subgroups

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

Canonical Subgroups

Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $\mathfrak{p}$ 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.

Canonical Subgroups

Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $\mathfrak{p}$ 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,

Canonical Subgroups

Let $\hat{E}$ denote the formal group of an elliptic curve that is supersingular at $\mathfrak{p}$ 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 μ is the valuation of the coefficient corresponding to sums of products of $p^2 - p$ roots.

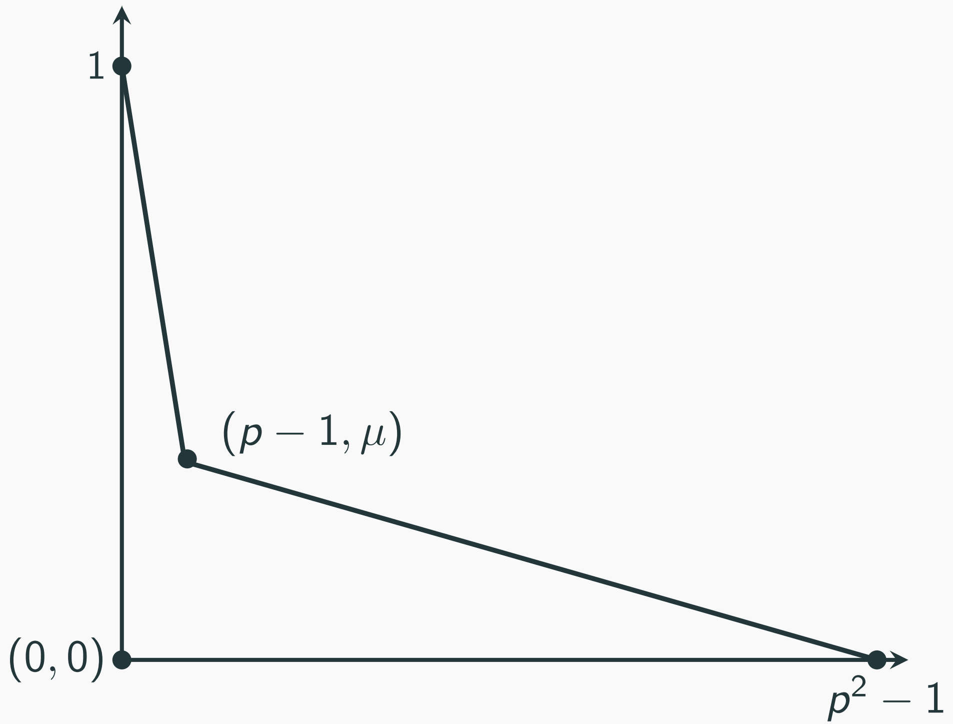


Figure 1: The Newton polygon for the polynomial $\prod_{\hat{P} \in \hat{E}[=p]} (T - \hat{P})$

The One-Slope Case

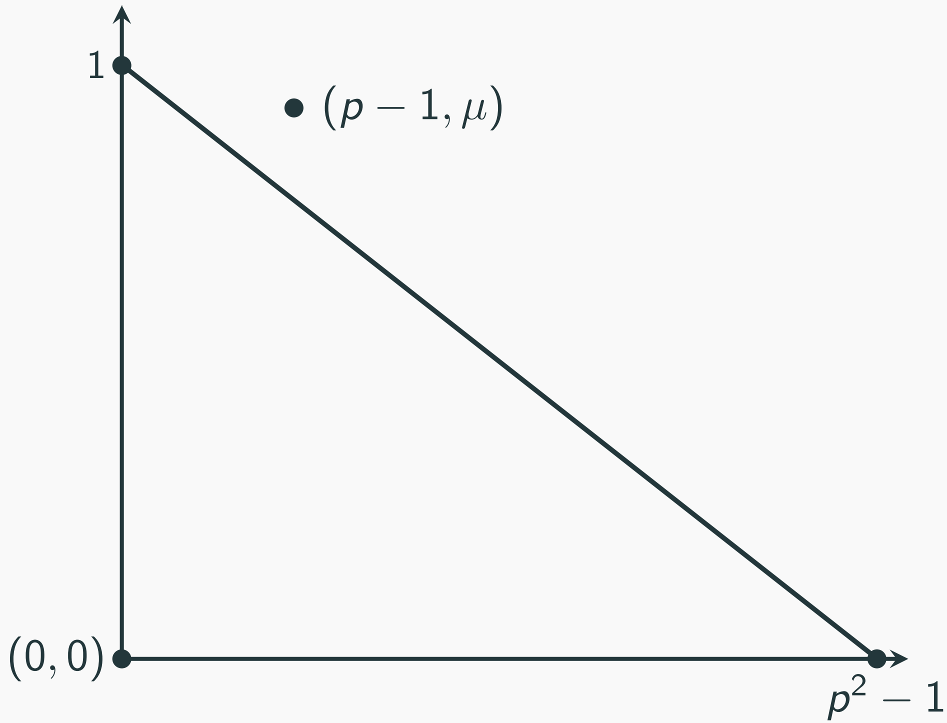


Figure 2: The Newton polygon for the polynomial $\prod_{\hat{P}\in\hat{E}[=p]}(T-\hat{P})$

Canonical Subgroups

In the ‘two-slope case’ people say that E has a *canonical subgroup* at $\mathfrak{p}$. 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.

Valuations and Canonical Subgroups

Recall, μ 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 μ as the sum of the valuations of elements of $\hat{E}[=p]$ that are **not** in the canonical subgroup.

Valuations and Canonical Subgroups

Recall, μ 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 μ 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 $\frac{1}{p^2-1}$.

Valuations and Canonical Subgroups

Recall, μ 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 μ 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 $\frac{1-\mu}{p-1}$.

p^n-Torsion

What about p^n-torsion when $n > 1$?

p^n-Torsion

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 $\frac{1}{5^4(5^2-1)}$.

p^n-Torsion

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.

p^n- Torsion

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 $\frac{\mu}{5^4(5^2-5)}$.

Higher Order Subset of Larger Valuation

Interestingly, we have a phenomenon that is similar to the canonical subgroup in some ways occurring for higher power torsion.

Higher Order Subset of Larger Valuation

Interestingly, we have a phenomenon that is similar to the canonical subgroup in some ways occurring for higher power torsion. When μ 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.

Partial Theorem Statement

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

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

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

Partial Theorem Statement

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

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

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

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

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 $\mathfrak{p}$ for a long time. Because E is supersingular at $\mathfrak{p}$ 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 $\mathfrak{p}$ for a long time. Because E is supersingular at $\mathfrak{p}$ this is equivalent to staring at the p^{th} division polynomial.

Let $\pi_{\mathfrak{p}}$ be a uniformizer at $\mathfrak{p}$. The multiplication-by-p map has the form

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

where f, g, and h are power series without constant coefficients and with $f'(0), g'(0), h'(0)$ 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 $Q \in E[=p^{n-1}]$.

Application to Sporadic Points on $X_1(N)$

Degrees of Minimal p^n-Torsion Fields

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.

Degrees of Minimal p^n-Torsion Fields

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 have with an upper bound on the $\mathbb{Q}$-gonality of the modular curve $X_1(p^n)$.

Degrees of Minimal p^n-Torsion Fields

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 have 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.

Prime Power Level Sporadic Points

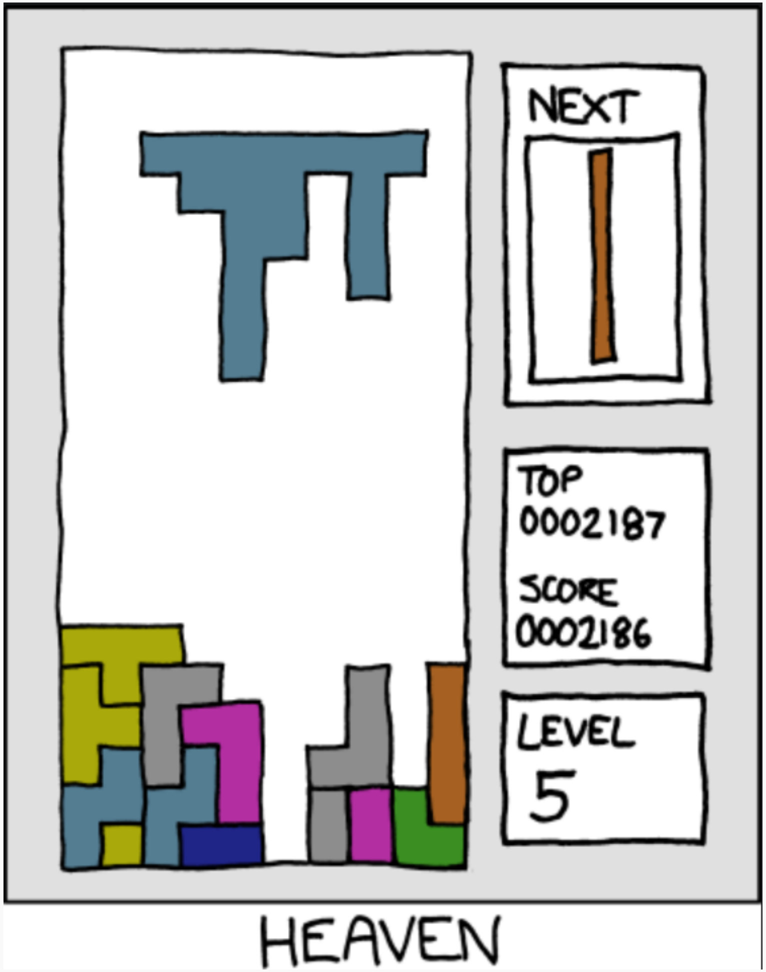
Let E be an elliptic curve that is supersingular at some prime above p with no canonical subgroup ($\mu \geq \frac{p}{p+1}$), then $j(E)$ does not correspond to a sporadic point on $X_1(p^n)$ for any $n > 0$.

Prime Power Level 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.

https://xkcd.com/888/



References i

Adelmann, C. (2001).

The decomposition of primes in torsion point fields, volume 1761 of Lecture Notes in Mathematics.

Springer-Verlag, Berlin.

Cali, E. and Kraus, A. (2002).

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

Acta Arith., 104(1):1–21.

References ii

Derickx, M., Etropolski, A., van Hoeij, M., Morrow, J. S., and Zureick-Brown, D. (2020).

Sporadic Cubic Torsion.

arXiv e-prints.

Derickx, M., Kamienny, S., Stein, W., and Stoll, M. (2017).

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

ArXiv e-prints.

Duke, W. and Tóth, A. (2002).

The splitting of primes in division fields of elliptic curves.

Experiment. Math., 11(4):555–565 (2003).

Freitas, N. and Kraus, A. (2018).

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

ArXiv e-prints.

González-Jiménez, E. and Lozano-Robledo, Á. (2016).

Elliptic curves with abelian division fields.

Math. Z., 283(3-4):835–859.

Jeon, D., Kim, C. H., and Schweizer, A. (2004).

On the torsion of elliptic curves over cubic number fields.

Acta Arith., 113(3):291–301.

Kamienny, S. (1992).

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

Invent. Math., 109(2):221–229.

Kenku, M. A. and Momose, F. (1988).

Torsion points on elliptic curves defined over quadratic fields.

Nagoya Math. J., 109:125–149.

Kraus, A. (1999).

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

Bull. Austral. Math. Soc., 60(3):407–428.

References v

Lozano-Robledo, Á. (2018).

Uniform boundedness in terms of ramification.

Res. Number Theory, 4(1):4:6.

Mazur, B. (1977).

Modular curves and the Eisenstein ideal.

Inst. Hautes Études Sci. Publ. Math., (47):33–186 (1978).

Mazur, B. (1978).

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

Invent. Math., 44(2):129–162.

Merel, L. (1996).

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

Invent. Math., 124(1-3):437–449.

Najman, F. (2016).

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

Math. Res. Lett., 23(1):245–272.

References vii

Parent, P. (1999).

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

J. Reine Angew. Math., 506:85–116.