Ramification in the Division Fields of Supersingular Elliptic Curves and Sporadic Points on Modular Curves

Hanson Smith

University of Colorado, Boulder
1. Motivating Questions and Previous Work

2. The Main Results

3. Proof Ideas

4. Further Questions
Motivating Questions and Previous Work
**Question 1:** Let $E$ be an elliptic curve defined over a number field $K$ of degree $d$ over $\mathbb{Q}$. What are the possibilities for the torsion subgroup of $E$ over $K$, $E(K)_{\text{tors}}$?
A Couple of Questions

**Question 1:** Let $E$ be an elliptic curve defined over a number field $K$ of degree $d$ over $\mathbb{Q}$. What are the possibilities for the torsion subgroup of $E$ over $K$, $E(K)_{\text{tors}}$?

**Question 2:** Is there an upper bound for $|E(K)_{\text{tors}}|$ depending on $d$?
Mazur showed $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups:

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

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad \text{with } 1 \leq N \leq 4.$$

This answers Question 1 when $d = 1$. 
For $d = 2$, Kamienny, Kenku, and Momose show $E(K)_{\text{tors}}$ is isomorphic to one of the following groups:

- $\mathbb{Z}/N\mathbb{Z}$ with $1 \leq N \leq 16$ or $N = 18$,
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ with $1 \leq N \leq 6$,
- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3N\mathbb{Z}$ with $1 \leq N \leq 2$,
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. 
Elliptic curves with a marked point of order $N$ are parametrized by points on the modular curve $X_1(N)$. 
Elliptic curves with a marked point of order $N$ are parametrized by points on the modular curve $X_1(N)$.

The answers we have for $d = 1$ and 2 come from analyzing modular curves. Each of the possibilities for $E(K)_{\text{tors}}$ with $d = 1$ and 2 occur for infinitely many $\mathbb{C}$-isomorphism classes of elliptic curves.
Elliptic curves with a marked point of order $N$ are parametrized by points on the modular curve $X_1(N)$.

The answers we have for $d = 1$ and 2 come from analyzing modular curves. Each of the possibilities for $E(K)_{\text{tors}}$ with $d = 1$ and 2 occur for infinitely many $\mathbb{C}$-isomorphism classes of elliptic curves.

For $d = 3$, the situation is more subtle.
Jeon, Kim, and Schweizer have shown that the torsion subgroups of elliptic curves over cubic fields that occur infinitely often are:

\[ \mathbb{Z}/N\mathbb{Z} \quad \text{for } 1 \leq N \leq 20 \text{ with } N \neq 17, 19, \]

\[ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad \text{with } 1 \leq N \leq 7. \]
Jeon, Kim, and Schweizer have shown that the torsion subgroups of elliptic curves over cubic fields that occur infinitely often are:

\[ \mathbb{Z}/N\mathbb{Z} \quad \text{for } 1 \leq N \leq 20 \text{ with } N \neq 17, 19, \]

\[ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad \text{with } 1 \leq N \leq 7. \]

Consider the elliptic curve

\[ E : y^2 + xy + y = x^3 - x^2 - 5x + 5 \]
Jeon, Kim, and Schweizer have shown that the torsion subgroups of elliptic curves over cubic fields that occur infinitely often are:

\[ \mathbb{Z}/N\mathbb{Z} \] for \( 1 \leq N \leq 20 \) with \( N \neq 17, 19, \)

\[ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \] with \( 1 \leq N \leq 7. \)

Consider the elliptic curve

\[ E : y^2 + xy + y = x^3 - x^2 - 5x + 5 \]

Najman has shown

\[ E(\mathbb{Q}(\zeta_9)^+) \cong \mathbb{Z}/21\mathbb{Z}. \]
The *degree* of a point $P$ on a modular curve $X_1(N)$ is the degree of the smallest field of definition of $P$. Najman's curve corresponds to a sporadic point on the modular curve $X_1(21)$. 
The degree of a point $P$ on a modular curve $X_1(N)$ is the degree of the smallest field of definition of $P$.

We say $P$ is sporadic if there are only finitely many points on $X_1(N)$ with degree less than or equal to $P$. 

Najman's curve corresponds to a sporadic point on the modular curve $X_1(21)$. 
The degree of a point $P$ on a modular curve $X_1(N)$ is the degree of the smallest field of definition of $P$.

We say $P$ is sporadic if there are only finitely many points on $X_1(N)$ with degree less than or equal to $P$.

Najman’s curve corresponds to a sporadic point on the modular curve $X_1(21)$. 

Recently and independently, Derickx and Etropolski, van Hoeij, Morrow and Zureick-Brown have announced that $X_1(21)$ is the only modular curve with a cubic sporadic point.
Recently and independently, Derickx and Etropolski, van Hoeij, Morrow and Zureick-Brown have announced that $X_1(21)$ is the only modular curve with a cubic sporadic point.

Combined with the aforementioned work this shows that when $[K : \mathbb{Q}] = 3$, then $E(K)_{\text{tors}}$ is isomorphic to one of the following groups:

\[ \mathbb{Z}/N\mathbb{Z} \quad \text{for } 1 \leq N \leq 21 \text{ with } N \neq 17, 19, \]

\[ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad \text{with } 1 \leq N \leq 7. \]
Question 2:

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

Merel showed that there is a constant $B(d)$ such that $|E(K)_{\text{tors}}| \leq B(d)$ and if $p$ divides $|E(K)_{\text{tors}}|$, then $p \leq d^{3d^2}$.

Oesterlé improved the bound in unpublished work to $p \leq (1 + 3d^2)^2$.

Parent showed that if $E(K)$ has a point of exact order $p^n$, then $p^n \leq 129(5d - 1)(3d)^6$. 
Question 2: Is there an upper bound for $|E(K)_\text{tors}|$ depending on $d$?

Merel showed that there is a constant $B(d)$ such that $|E(K)_\text{tors}| \leq B(d)$ and if $p$ divides $|E(K)_\text{tors}|$, then

$$p \leq d^{3d^2}.$$
Question 2: Is there an upper bound for $|E(K)_{tors}|$ depending on $d$?

Merel showed that there is a constant $B(d)$ such that $|E(K)_{tors}| \leq B(d)$ and if $p$ divides $|E(K)_{tors}|$, then

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

Oesterlé improved the bound in unpublished work to

$$p \leq (1 + 3^\frac{d}{2})^2.$$
Question 2: Is there an upper bound for $|E(K)_{\text{tors}}|$ depending on $d$?

Merel showed that there is a constant $B(d)$ such that $|E(K)_{\text{tors}}| \leq B(d)$ and if $p$ divides $|E(K)_{\text{tors}}|$, then

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

Oesterlé improved the bound in unpublished work to

$$p \leq (1 + 3^{\frac{d}{2}})^2.$$  

Parent showed that if $E(K)$ has a point of exact order $p^n$, then

$$p^n \leq 129(5^d - 1)(3d)^6.$$
Conjecture: The bound $B(d)$ should be polynomial in $d$. More specifically, there is a constant $C$ independent of $d$ such that $|E(K)_{tors}| \leq C \cdot d \log \log d$. 

Motivated by Flexor and Oesterl´e, Lozano-Robledo had the idea of attacking this conjecture using ramification. Using this idea Lozano-Robledo has shown:

Suppose $E$ has CM by a maximal order and let $K$ be a number field of degree $d$. If $E(K)$ has a point of order $p^n$, then $\phi(p^n) \leq 12d$.

Let $p$ be an odd prime. Consider a fixed number field $K$ and let $E$ be an elliptic curve over $K$. If $L$ is a finite extension of $K$ with degree $d$ over $\mathbb{Q}$ and $E(L)$ has a point of order $p^n$, then there is a constant $C_K$ depending on $K$ such that $\phi(p^n) \leq C_K \cdot d$.
**Conjecture:** The bound $B(d)$ should be polynomial in $d$. More specifically, there is a constant $C$ independent of $d$ such that $|E(K)_{\text{tors}}| \leq C \cdot d \log \log d$.

Motivated by Flexor and Oesterlé, Lozano-Robledo had the idea of attacking this conjecture using ramification. Using this idea Lozano-Robledo has shown:
**Conjecture:** The bound $B(d)$ should be polynomial in $d$. More specifically, there is a constant $C$ independent of $d$ such that $|E(K)_{\text{tors}}| \leq C \cdot d \log \log d$.

Motivated by Flexor and Oesterlé, Lozano-Robledo had the idea of attacking this conjecture using ramification. Using this idea Lozano-Robledo has shown:

Suppose $E$ has CM by a maximal order and let $K$ be a number field of degree $d$. If $E(K)$ has a point of order $p^n$, then $\varphi(p^n) \leq 12d$. 
**Conjecture:** The bound $B(d)$ should be polynomial in $d$. More specifically, there is a constant $C$ independent of $d$ such that $|E(K)_{tors}| \leq C \cdot d \log \log d$.

Motivated by Flexor and Oesterlé, Lozano-Robledo had the idea of attacking this conjecture using ramification. Using this idea Lozano-Robledo has shown:

Suppose $E$ has CM by a maximal order and let $K$ be a number field of degree $d$. If $E(K)$ has a point of order $p^n$, then $\varphi(p^n) \leq 12d$.

Let $p$ be an odd prime. Consider a fixed number field $K$ and let $E$ be an elliptic curve over $K$. If $L$ is a finite extension of $K$ with degree $d$ over $\mathbb{Q}$ and $E(L)$ has a point of order $p^n$, then there is a constant $C_K$, depending on $K$, such that

$$\varphi(p^n) \leq C_K \cdot d.$$
Supersingular Case

When $E$ has supersingular reduction at a prime of $K$ lying above $p$, Lozano-Robledo has produced even stronger bounds.
Supersingular Case

When $E$ has supersingular reduction at a prime of $K$ lying above $p$, Lozano-Robledo has produced even stronger bounds.

As before let $E$ be an elliptic curve over a number field $K$ of degree $d$ over $\mathbb{Q}$. Suppose that $E(K)$ has a point of exact order $p^n$ and suppose $E$ is supersingular at a prime of $K$ lying above $p$. 

\[
\phi(p^n) \leq \begin{cases} 
24d & \text{if } p = 2, \\
12d & \text{if } p = 3, \\
6d & \text{if } p > 3.
\end{cases}
\]

When $E$ is defined over a subfield of $K$ in which $p$ is unramified these bounds are strengthened.
Supersingular Case

When $E$ has supersingular reduction at a prime of $K$ lying above $p$, Lozano-Robledo has produced even stronger bounds.

As before let $E$ be an elliptic curve over a number field $K$ of degree $d$ over $\mathbb{Q}$. Suppose that $E(K)$ has a point of exact order $p^n$ and suppose $E$ is supersingular at a prime of $K$ lying above $p$.

Lozano-Robledo shows

$$\varphi(p^n) \leq \begin{cases} 
24d & \text{if } p = 2, \\
12d & \text{if } p = 3, \\
6d & \text{if } p > 3.
\end{cases}$$

Supersingular Case

When \( E \) has supersingular reduction at a prime of \( K \) lying above \( p \), Lozano-Robledo has produced even stronger bounds.

As before let \( E \) be an elliptic curve over a number field \( K \) of degree \( d \) over \( \mathbb{Q} \). Suppose that \( E(K) \) has a point of exact order \( p^n \) and suppose \( E \) is supersingular at a prime of \( K \) lying above \( p \).

Lozano-Robledo shows

\[
\varphi(p^n) \leq \begin{cases} 
24d & \text{if } p = 2, \\
12d & \text{if } p = 3, \\
6d & \text{if } p > 3.
\end{cases}
\]

When \( E \) is defined over a subfield of \( K \) in which \( p \) is unramified these bounds are strengthened.
The Main Results
Let $E$ be an elliptic curve over a number field $K$ and let $L$ be the minimal extension of $K$ such that $E(L)$ has a point of order $p^n$. Suppose further that $E$ has supersingular reduction at a prime $p$ of $K$ lying above $p$, where $p$ is odd. Then we show:

- The ramification indices (over $p$) of the primes above $p$ in $L$ are properly divisible by $\varphi(p^n)$. In particular, $\varphi(p^n)$ divides $[L:K]$ properly.
- If $p$ has ramification index 1 over $p$, then $p$ has ramification index $p^2n - p^2n - 2$ in $L$. Hence, $[L:K] = p^2n - p^2n - 2$. 


Let $E$ be an elliptic curve over a number field $K$ and let $L$ be the minimal extension of $K$ such that $E(L)$ has a point of order $p^n$. Suppose further that $E$ has supersingular reduction at a prime $p$ of $K$ lying above $p$, where $p$ is odd. Then we show:

The ramification indices (over $p$) of the primes above $p$ in $L$ are properly divisible by $\varphi(p^n)$. In particular, $\varphi(p^n)$ divides $[L : \mathbb{Q}]$ properly.
Let $E$ be an elliptic curve over a number field $K$ and let $L$ be the minimal extension of $K$ such that $E(L)$ has a point of order $p^n$. Suppose further that $E$ has supersingular reduction at a prime $p$ of $K$ lying above $p$, where $p$ is odd. Then we show:

The ramification indices (over $p$) of the primes above $p$ in $L$ are properly divisible by $\varphi(p^n)$. In particular, $\varphi(p^n)$ divides $[L : \mathbb{Q}]$ properly.

If $p$ has ramification index 1 over $p$, then $p$ has ramification index $p^{2n} - p^{2n-2}$ in $L$. Hence, $[L : K] = p^{2n} - p^{2n-2}$. 
Sporadic Points?

Recall, the degree of a point \( P \) on a modular curve \( X_{1}(N) \) is the degree of the minimal field of definition of \( P \).

A point \( P \) is sporadic if there are only finitely many points on \( X_{1}(N) \) of degree less than or equal to \( P \).

The \( Q \)-gonality of the curve \( X_{1}(N) \) is the minimal degree of a dominant \( X_{1}(N) \rightarrow \mathbb{P}^{1}_{Q} \) morphism.

A degree \( d \) map to \( \mathbb{P}^{1}_{Q} \) allows one to construct infinitely many points of degree \( d \).

Necessarily, a sporadic point must have degree less than the \( Q \)-gonality of a curve.

Using bounds on the genera of modular curves we have \( Q \)-gonality of \( X_{1}(N) \leq N^2 - \frac{1}{24} \).

Since \( p^2 \cdot n - p^2 \cdot n - \frac{1}{2} \geq p^2 \cdot n - \frac{1}{24} \), sporadic points on \( X_{1}(p^2 \cdot n) \) cannot correspond to elliptic curves that are supersingular at an unramified prime above \( p \).
Sporadic Points?

Recall, the *degree* of a point $P$ on a modular curve $X_1(N)$ is the degree of the minimal field of definition of $P$.

A point $P$ is sporadic if there are only finitely many points on $X_1(N)$ of degree less than or equal to $P$.

The $Q$-gonality of the curve $X_1(N)$ is the minimal degree of a dominant morphism $X_1(N) \to P^1_Q$.

A degree $d$ map to $P^1_Q$ allows one to construct infinitely many points of degree $d$.

Necessarily, a sporadic point must have degree less than the $Q$-gonality of a curve.

Using bounds on the genera of modular curves we have $Q$-gonality of $X_1(N) \leq N^2 - \frac{1}{24}$.

Since $p^2_n - p^2_n - 2 \geq p^2_n - 1$, sporadic points on $X_1(p^n)$ cannot correspond to elliptic curves that are supersingular at an unramified prime above $p$. 
Recall, the degree of a point $P$ on a modular curve $X_1(N)$ is the degree of the minimal field of definition of $P$. A point $P$ is sporadic if there are only finitely many points on $X_1(N)$ of degree less than or equal to $P$. A degree $d$ map to $P_1$ allows one to construct infinitely many points of degree $d$. Necessarily, a sporadic point must have degree less than the $Q$-gonality of a curve. Using bounds on the genera of modular curves we have $Q$-gonality of $X_1(N) \leq N^2 - 1/24$. Since $p^2-n-p^2-n-2^2 \geq p^2-n-1/24$, sporadic points on $X_1(p^n)$ cannot correspond to elliptic curves that are supersingular at an unramified prime above $p$. 
Sporadic Points?

Recall, the *degree* of a point $P$ on a modular curve $X_1(N)$ is the degree of the minimal field of definition of $P$. A point $P$ is *sporadic* if there are only finitely many points on $X_1(N)$ of degree less than or equal to $P$. The $\mathbb{Q}$-*gonality* of the curve $X_1(N)$ is the minimal degree of a dominant morphism $X_1(N) \to \mathbb{P}^1_\mathbb{Q}$.

Since $p_n^2 - p_n^2 - 2 \geq p_n^2 - 1$, sporadic points on $X_1(p_n)$ cannot correspond to elliptic curves that are supersingular at an unramified prime above $p$. 

13
Sporadic Points?

Recall, the *degree* of a point $P$ on a modular curve $X_1(N)$ is the degree of the minimal field of definition of $P$. A point $P$ is *sporadic* if there are only finitely many points on $X_1(N)$ of degree less than or equal to $P$. The $\mathbb{Q}$-*gonality* of the curve $X_1(N)$ is the minimal degree of a dominant morphism $X_1(N) \to \mathbb{P}^1_{\mathbb{Q}}$. A degree $d$ map to $\mathbb{P}^1_{\mathbb{Q}}$ allows one to construct infinitely many points of degree $d$. 

Necessarily, a sporadic point must have degree less than the $\mathbb{Q}$-gonality of a curve. Using bounds on the genera of modular curves we have $\mathbb{Q}$-gonality of $X_1(N) \leq N^2 - 12$. Since $p^2 n - p^2 n - 2 \geq p^2 n - 12$, sporadic points on $X_1(p^n)$ cannot correspond to elliptic curves that are supersingular at an unramified prime above $p$. 

\begin{align*}
\end{align*}
Recall, the degree of a point $P$ on a modular curve $X_1(N)$ is the degree of the minimal field of definition of $P$. A point $P$ is sporadic if there are only finitely many points on $X_1(N)$ of degree less than or equal to $P$. The $\mathbb{Q}$-gonality of the curve $X_1(N)$ is the minimal degree of a dominant morphism $X_1(N) \to \mathbb{P}^1_{\mathbb{Q}}$. A degree $d$ map to $\mathbb{P}^1_{\mathbb{Q}}$ allows one to construct infinitely many points of degree $d$. Necessarily, a sporadic point must have degree less than the $\mathbb{Q}$-gonality of a curve.
Recall, the *degree* of a point $P$ on a modular curve $X_1(N)$ is the degree of the minimal field of definition of $P$. A point $P$ is *sporadic* if there are only finitely many points on $X_1(N)$ of degree less than or equal to $P$.

The $\mathbb{Q}$-*gonality* of the curve $X_1(N)$ is the minimal degree of a dominant morphism $X_1(N) \to \mathbb{P}^1_\mathbb{Q}$. A degree $d$ map to $\mathbb{P}^1_\mathbb{Q}$ allows one to construct infinitely many points of degree $d$. Necessarily, a sporadic point must have degree less than the $\mathbb{Q}$-gonality of a curve. Using bounds on the genera of modular curves we have

$$\text{Q-gonality of } X_1(N) \leq \frac{N^2 - 1}{24}.$$
Sporadic Points?

Recall, the *degree* of a point $P$ on a modular curve $X_1(N)$ is the degree of the minimal field of definition of $P$. A point $P$ is *sporadic* if there are only finitely many points on $X_1(N)$ of degree less than or equal to $P$. The $\mathbb{Q}$-*gonality* of the curve $X_1(N)$ is the minimal degree of a dominant morphism $X_1(N) \to \mathbb{P}_\mathbb{Q}^1$. A degree $d$ map to $\mathbb{P}_\mathbb{Q}^1$ allows one to construct infinitely many points of degree $d$. Necessarily, a sporadic point must have degree less than the $\mathbb{Q}$-gonality of a curve. Using bounds on the genera of modular curves we have

$$\text{Q-gonality of } X_1(N) \leq \frac{N^2 - 1}{24}.$$ 

Since $\frac{p^{2n} - p^{2n-2}}{2} \geq \frac{p^{2n} - 1}{24}$, sporadic points on $X_1(p^n)$ cannot correspond to elliptic curves that are supersingular at an unramified prime above $p$. 


Proof Ideas
Write a Weierstrass equation for $E$, $E$:

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

We define the $N$-th division polynomial $\Psi_N$, recursively starting with $\Psi_1 = 1$, $\Psi_2 = 2y + a_1 x + a_3$, $\Psi_3 = 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8$, $\Psi_4 \Psi_2 = 2x^6 + b_2 x^5 + 5b_4 x^4 + 10b_6 x^3 + 10b_8 x^2 + (b_2 b_8 - b_4 b_6)x + (b_4 b_8 - b_2 b_6)$, and using the formulas $\Psi_{2m}^{m+1} = \Psi_{m+2} \Psi_{3m} - \Psi_{m+1} \Psi_{3m} + 1$ for $m \geq 2$, $\Psi_{2m+1}^{m+1} \Psi_{2m+1} = \Psi_{m+2} \Psi_{m+1} \Psi_{m+2} - 2 \Psi_{m+1} \Psi_{m+1} \Psi_{2m} + \Psi_{m+2} \Psi_{2m} + 1$ for $m \geq 3$. 

14
Write a Weierstrass equation for $E$,

$$E : \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$
Write a Weierstrass equation for $E$,

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

We define the $N$-th division polynomial, $\Psi_N$, recursively starting with $\Psi_1 = 1$,
Write a Weierstrass equation for $E$,

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

We define the $N$-th division polynomial, $\Psi_N$, recursively starting with

$\Psi_1 = 1,$  

$\Psi_2 = 2y + a_1 x + a_3,$
Write a Weierstrass equation for $E$,

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

We define the $N$-th division polynomial, $\Psi_N$, recursively starting with

$\psi_1 = 1,$

$\psi_2 = 2y + a_1 x + a_3,$

$\psi_3 = 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8,$
Write a Weierstrass equation for $E$, 

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

We define the $N$-th division polynomial, $\Psi_N$, recursively starting with 

$\Psi_1 = 1,$

$\Psi_2 = 2y + a_1 x + a_3,$

$\Psi_3 = 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8,$

$$\frac{\psi_4}{\psi_2} = 2x^6 + b_2 x^5 + 5b_4 x^4 + 10b_6 x^3 + 10b_8 x^2 + (b_2 b_8 - b_4 b_6) x + (b_4 b_8 - b_6^2).$$
Write a Weierstrass equation for $E$,

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

We define the $N$-th division polynomial, $\Psi_N$, recursively starting with

$\Psi_1 = 1,$

$\Psi_2 = 2y + a_1 x + a_3,$

$\Psi_3 = 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8,$

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

and using the formulas

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

$$\Psi_{2m+1} \Psi_2 = \Psi_{m-1} \Psi_m \Psi_{m+2} - \Psi_{m-2} \Psi_m \Psi_{m+1}^2 \quad \text{for } m \geq 3.$$
The $N$-th division polynomial, $\Psi_N$, encodes the distinct $x$-coordinates of the $N$-torsion points of $E$. 

More precisely, $\Psi_N(x) = N \cdot \prod_{P} (x - x(P))$, where the product is over the $N$-torsion points with distinct $x$-coordinates excluding the identity of $E$. 

We see the degree of $\Psi_N$ is $N^2 - 1/2$. 


The $N$-th division polynomial, $\Psi_N$, encodes the distinct $x$-coordinates of the $N$-torsion points of $E$.

More precisely,

$$\Psi_N(x) = N \cdot \prod_P (x - x(P)),$$

where the product is over the $N$-torsion points with distinct $x$-coordinates excluding the identity of $E$. 
The $N$-th division polynomial, $\Psi_N$, encodes the distinct $x$-coordinates of the $N$-torsion points of $E$.

More precisely,

$$\Psi_N(x) = N \cdot \prod_{P} (x - x(P)),$$

where the product is over the $N$-torsion points with distinct $x$-coordinates excluding the identity of $E$.

We see the degree of $\Psi_N$ is $\frac{N^2 - 1}{2}$. 
We are interested in $L$, the minimal field of definition of a $p^n$-torsion point of $E$. 
We are interested in \( L \), the minimal field of definition of a \( p^n \)-torsion point of \( E \).

We call a point of exact order \( p^n \) \textit{primitive} and we define the \textit{primitive} \( p^n \)-th division polynomial to be

\[
\Psi_{p^n, \text{prim}}(x) = \frac{\Psi_{p^n}(x)}{\Psi_{p^{n-1}}(x)} = p \cdot \prod'_P (x - x(P)),
\]

where the product is over the primitive \( p^n \)-torsion points with distinct \( x \)-coordinates.
Primitive Division Polynomials

We are interested in $L$, the minimal field of definition of a $p^n$-torsion point of $E$.

We call a point of exact order $p^n$ primitive and we define the primitive $p^n$-th division polynomial to be

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

where the product is over the primitive $p^n$-torsion points with distinct $x$-coordinates

We see the degree of $\Psi_{p^n, \text{prim}}$ is $\frac{p^{2n} - 1}{2} - \frac{p^{2n-2} - 1}{2} = \frac{p^{2n} - p^{2n-2}}{2}$. 
For the sake of exposition, suppose $E$ is defined over $\mathbb{Q}$. If we adjoin a root of $\Psi_{p^n,\text{prim}}$ to $\mathbb{Q}$, then we have a subfield of $L$. However, each $p^n$-torsion point $P$ is in the kernel of reduction so $x(P)$ necessarily has negative valuation. Clearing denominators in the Weierstrass equation, the valuation of $x(P)$ must be even.
Valuations and the Kernel of Reduction

For the sake of exposition, suppose $E$ is defined over $\mathbb{Q}$. If we adjoin a root of $\Psi_{p^n,\text{prim}}$ to $\mathbb{Q}$, then we have a subfield of $L$.

Using that $x$-coordinates of primitive $p^n$-torsion points are roots of $\Psi_{p^n,\text{prim}}$, we can shown that the $p$-adic valuation, $v_p$, of the constant coefficient of $\Psi_{p^n,\text{prim}}$ is zero.
For the sake of exposition, suppose $E$ is defined over $\mathbb{Q}$. If we adjoin a root of $\Psi_{p^n,\text{prim}}$ to $\mathbb{Q}$, then we have a subfield of $L$.

Using that $x$-coordinates of primitive $p^n$-torsion points are roots of $\Psi_{p^n,\text{prim}}$, we can shown that the $p$-adic valuation, $\nu_p$, of the constant coefficient of $\Psi_{p^n,\text{prim}}$ is zero. However, each $p^n$-torsion point $P$ is in the kernel of reduction so $x(P)$ necessarily has negative valuation.
For the sake of exposition, suppose $E$ is defined over $\mathbb{Q}$. If we adjoin a root of $\Psi_{p^n,\text{prim}}$ to $\mathbb{Q}$, then we have a subfield of $L$.

Using that $x$-coordinates of primitive $p^n$-torsion points are roots of $\Psi_{p^n,\text{prim}}$, we can shown that the $p$-adic valuation, $v_p$, of the constant coefficient of $\Psi_{p^n,\text{prim}}$ is zero. However, each $p^n$-torsion point $P$ is in the kernel of reduction so $x(P)$ necessarily has negative valuation. Clearing denominators in the Weierstrass equation, the valuation of $x(P)$ must be even.
Consider $\mathbb{Q}_p$ and let $v_p$ be the normalized valuation.
Consider $\mathbb{Q}_p$ and let $\nu_p$ be the normalized valuation.

Suppose we have a factorization

$$\Psi_{p^n,\text{prim}} = (ax^e + \cdots + a_0)(bx^f + \cdots + b_0)$$

with $\nu_p(a) = 0$ and $\nu_p(b) = 1$, say.
Consider $\mathbb{Q}_p$ and let $v_p$ be the normalized valuation.

Suppose we have a factorization

$$\Psi_{p^n, \text{prim}} = (ax^e + \cdots + a_0)(bx^f + \cdots + b_0)$$

with $v_p(a) = 0$ and $v_p(b) = 1$, say.

One has $v_p(a_0) < 0$, hence $v_p(b_0) > 0$. 

Consider $\mathbb{Q}_p$ and let $\nu_p$ be the normalized valuation.

Suppose we have a factorization

$$\Psi_{p^n, \text{prim}} = (ax^e + \cdots + a_0)(bx^f + \cdots + b_0)$$

with $\nu_p(a) = 0$ and $\nu_p(b) = 1$, say.

One has $\nu_p(a_0) < 0$, hence $\nu_p(b_0) > 0$.

However, $\nu_p\left(\frac{b_0}{b}\right) = \nu_p(b_0) - 1 < 0$. 

Consider $\mathbb{Q}_p$ and let $v_p$ be the normalized valuation.

Suppose we have a factorization

$$\Psi_{p^n, \text{prim}} = (ax^e + \cdots + a_0)(bx^f + \cdots + b_0)$$

with $v_p(a) = 0$ and $v_p(b) = 1$, say.

One has $v_p(a_0) < 0$, hence $v_p(b_0) > 0$.

However, $v_p\left(\frac{b_0}{b}\right) = v_p(b_0) - 1 < 0$.

With this contradiction, we see $\Psi_{p^n, \text{prim}}$ is irreducible.
Further Questions
What about good ordinary reduction?
Further Questions

What about good ordinary reduction?

Can we generalize to abelian varieties? A first case is hyperelliptic Jacobians.
Thank you for listening. Please send me an email at hanson.smith@colorado.edu if you have any questions that aren’t answered here. A preprint should be on my website soon.