Sporadic torsion

David Zureick-Brown
Anastassia Etropolski (Emory University)
Jackson Morrow (Emory University)

Emory University
Slides available at http://www.mathcs.emory.edu/~dzb/slides/

SERMON XXIX,
Harrisonburg, VA

April 2-3, 2016
Mazur’s Theorem

Theorem (Mazur, 1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups.

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

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 4.$$
Mazur’s Theorem

Theorem (Mazur, 1978)

Let \( E/\mathbb{Q} \) be an elliptic curve. Then \( E(\mathbb{Q})_{\text{tors}} \) is isomorphic to one of the following groups.

\[
\mathbb{Z}/N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 10 \text{ or } N = 12,
\]

\[
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 4.
\]

More precisely, let

- \( Y_1(N) \) be the curve parameterizing \((E, P)\), where \( P \) is a point of exact order \( N \) on \( E \), and let
Mazur’s Theorem

Theorem (Mazur, 1978)

Let \( E/\mathbb{Q} \) be an elliptic curve. Then \( E(\mathbb{Q})_{\text{tors}} \) is isomorphic to one of the following groups.

\[
\mathbb{Z}/N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 10 \text{ or } N = 12,
\]

\[
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 4.
\]

More precisely, let

- \( Y_1(N) \) be the curve parameterizing \((E, P)\), where \( P \) is a point of exact order \( N \) on \( E \), and let
- \( Y_1(M, N) \) (with \( M \mid N \)) be the curve parameterizing \( E/K \) such that \( E(K)_{\text{tors}} \) contains \( \mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z} \).
Mazur’s Theorem

Theorem (Mazur, 1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups.

- $\mathbb{Z}/N\mathbb{Z}$, for $1 \leq N \leq 10$ or $N = 12$,
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$, for $1 \leq N \leq 4$.

More precisely, let

- $Y_1(N)$ be the curve parameterizing $(E, P)$, where $P$ is a point of exact order $N$ on $E$, and let
- $Y_1(M, N)$ (with $M \mid N$) be the curve parameterizing $E/K$ such that $E(K)_{\text{tors}}$ contains $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$.

Then $Y_1(N)(\mathbb{Q}) \neq \emptyset$ and $Y_1(2, 2N)(\mathbb{Q}) \neq \emptyset$ iff $N$ are as above.
Example (\(N = 9\))

\[ E(K) \cong \mathbb{Z}/9\mathbb{Z} \] if and only if there exists \(t \in K\) such that \(E\) is isomorphic to

\[ y^2 + (t - rt + 1)xy + (rt - r^2 t)y = x^3 + (rt - r^2 t)x^2 \]

where \(r\) is \(t^2 - t + 1\). The torsion point is \((0, 0)\).
Modular curves

Example \( (N = 9) \)

\[ E(K) \cong \mathbb{Z}/9\mathbb{Z} \text{ if and only if there exists } t \in K \text{ such that } E \text{ is isomorphic to } \]

\[ y^2 + (t - rt + 1)xy + (rt - r^2 t)y = x^3 + (rt - r^2 t)x^2 \]

where \( r \) is \( t^2 - t + 1 \). The torsion point is \((0, 0)\).

Example \( (N = 11) \)

\[ E(K) \cong \mathbb{Z}/11\mathbb{Z} \text{ correspond to } a, b \in K \text{ such that } \]

\[ a^2 + (b^2 + 1)a + b; \]

in which case \( E \) is isomorphic to

\[ y^2 + (s - rs + 1)xy + (rs - r^2 s)y = x^3 + (rs - r^2 s)x^2 \]

where \( r \) is \( ba + 1 \) and \( s \) is \(-b + 1\).
Let $X_1(N)$ and $X_1(M, N)$ be the smooth compactifications of $Y_1(N)$ and $Y_1(M, N)$. 
Let $X_1(N)$ and $X_1(M, N)$ be the smooth compactifications of $Y_1(N)$ and $Y_1(M, N)$. We can restate the results of Mazur’s Theorem as follows.
Let $X_1(N)$ and $X_1(M, N)$ be the smooth compactifications of $Y_1(N)$ and $Y_1(M, N)$. We can restate the results of Mazur’s Theorem as follows.

- $X_1(N)$ and $X_1(2, 2N)$ have genus 0 for exactly the $N$ appearing in Mazur’s Theorem. (So in particular, there are infinitely many $E/\mathbb{Q}$ with such torsion structure.)
Let $X_1(N)$ and $X_1(M, N)$ be the smooth compactifications of $Y_1(N)$ and $Y_1(M, N)$. We can restate the results of Mazur’s Theorem as follows.

- $X_1(N)$ and $X_1(2, 2N)$ have genus 0 for exactly the $N$ appearing in Mazur’s Theorem. (So in particular, there are infinitely many $E/\mathbb{Q}$ with such torsion structure.)
- If $g(X_1(N))$ (resp. $g(X_1(2, 2N))$) is greater than 0, then $X_1(N)(\mathbb{Q})$ (resp. $X_1(2, 2N)(\mathbb{Q})$) consists only of cusps.
Rational Points on $X_1(N)$ and $X_1(2, 2N)$

Let $X_1(N)$ and $X_1(M, N)$ be the smooth compactifications of $Y_1(N)$ and $Y_1(M, N)$. We can restate the results of Mazur’s Theorem as follows.

- $X_1(N)$ and $X_1(2, 2N)$ have genus 0 for **exactly** the $N$ appearing in Mazur’s Theorem. (So in particular, there are **infinitely many** $E/\mathbb{Q}$ with such torsion structure.)
- If $g(X_1(N))$ (resp. $g(X_1(2, 2N))$) is greater than 0, then $X_1(N)(\mathbb{Q})$ (resp. $X_1(2, 2N)(\mathbb{Q})$) consists only of cusps.

So, in a sense, the simplest thing that could happen does happen for these modular curves.
Theorem (Merel, 1996)

For every integer \( d \geq 1 \), there is a constant \( N(d) \) such that for all \( K/\mathbb{Q} \) of degree at most \( d \) and all \( E/K \),

\[
\#E(K)_{\text{tors}} \leq N(d).
\]
Higher Degree Torsion Points

Theorem (Merel, 1996)

For every integer \( d \geq 1 \), there is a constant \( N(d) \) such that for all \( K/\mathbb{Q} \) of degree at most \( d \) and all \( E/K \),

\[
\#E(K)_{\text{tors}} \leq N(d).
\]

Problem

Fix \( d \geq 1 \). Classify all groups which can occur as \( E(K)_{\text{tors}} \) for \( K/\mathbb{Q} \) of degree \( d \). Which of these occur infinitely often?
The Quadratic Case

Theorem (Kamienny-Kenku-Momose, 1980’s)

Let $E$ be an elliptic curve over a quadratic number field $K$. Then $E(K)_{\text{tors}}$ is one of the following groups.

- $\mathbb{Z}/N\mathbb{Z}$, for $1 \leq N \leq 16$ or $N = 18$,
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$, for $1 \leq N \leq 6$,
- $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z}$, for $1 \leq N \leq 2$, or
- $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. 

In particular, the corresponding curves $X_1(M, N)$ all have $g \leq 2$, which guarantees that they have infinitely many quadratic points.
The Quadratic Case

Theorem (Kamienny-Kenku-Momose, 1980’s)

Let $E$ be an elliptic curve over a quadratic number field $K$. Then $E(K)_{\text{tors}}$ is one of the following groups.

\[ \mathbb{Z}/N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 16 \text{ or } N = 18, \]
\[ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 6, \]
\[ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 2, \text{ or} \]
\[ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \]

In particular, the corresponding curves $X_1(M, N)$ all have $g \leq 2$, which guarantees that they have infinitely many quadratic points.
Example \((N = 9)\)

\[ E(K) \cong \mathbb{Z}/9\mathbb{Z} \] if and only if there exists \(t \in K\) such that \(E\) is isomorphic to

\[ y^2 + (t - rt + 1)xy + (rt - r^2 t)y = x^3 + (rt - r^2 t)x^2 \]

where \(r\) is \(t^2 - t + 1\). The torsion point is \((0, 0)\).
Modular curves

Example \((N = 9)\)

\[ E(K) \cong \mathbb{Z}/9\mathbb{Z} \] if and only if there exists \(t \in K\) such that \(E\) is isomorphic to

\[ y^2 + (t - rt + 1)xy + (rt - r^2 t)y = x^3 + (rt - r^2 t)x^2 \]

where \(r\) is \(t^2 - t + 1\). The torsion point is \((0, 0)\).

Example \((N = 11)\)

\[ E(K) \cong \mathbb{Z}/11\mathbb{Z} \] correspond to \(a, b \in K\) such that

\[ a^2 + (b^2 + 1)a + b; \]

in which case \(E\) is isomorphic to

\[ y^2 + (s - rs + 1)xy + (rs - r^2 s)y = x^3 + (rs - r^2 s)x^2 \]

where \(r\) is \(ba + 1\) and \(s\) is \(-b + 1\).
Let $X/\mathbb{Q}$ be a curve.

- If $X$ admits a degree $d = [K : \mathbb{Q}]$ map to $\mathbb{P}^1_{\mathbb{Q}}$, then $X(K)$ is infinite.
Let $X/\mathbb{Q}$ be a curve.

- If $X$ admits a degree $d = [K : \mathbb{Q}]$ map to $\mathbb{P}^1_{\mathbb{Q}}$, then $X(K)$ is infinite.
- More precisely, if $D$ is a divisor of degree $d$ on $X$ and $\dim |D| \geq 1$, then $D$ parameterizes an infinite family of effective degree $d$ divisors.
Let $X/\mathbb{Q}$ be a curve.

- If $X$ admits a degree $d = [K : \mathbb{Q}]$ map to $\mathbb{P}^1_\mathbb{Q}$, then $X(K)$ is infinite.
- More precisely, if $D$ is a divisor of degree $d$ on $X$ and $\dim |D| \geq 1$, then $D$ parameterizes an infinite family of effective degree $d$ divisors.

**Question**

If $Y_1(M, N)(K) \neq \emptyset$, are all of the points coming from the existence of such divisors?
Expected $K$-Rational Points

Let $X/\mathbb{Q}$ be a curve.

- If $X$ admits a degree $d = [K : \mathbb{Q}]$ map to $\mathbb{P}^1_\mathbb{Q}$, then $X(K)$ is infinite.
- More precisely, if $D$ is a divisor of degree $d$ on $X$ and $\dim |D| \geq 1$, then $D$ paramaterizes an infinite family of effective degree $d$ divisors.

**Question**

If $Y_1(M, N)(K) \neq \emptyset$, are all of the points coming from the existence of such divisors?

If not, we call these outliers **sporadic** points.
Theorem (Jeon-Kim-Schweizer, 2004)

Let $E$ be an elliptic curve over a cubic number field $K$. Then the subgroups which arise as $E(K)_{\text{tors}}$ infinitely often are exactly the following.

$$\mathbb{Z}/N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 20, \ N \neq 17, 19, \text{ or}$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 7.$$
Theorem (Jeon-Kim-Schweizer, 2004)

Let \( E \) be an elliptic curve over a cubic number field \( K \). Then the subgroups which arise as \( E(K)_{\text{tors}} \) infinitely often are exactly the following.

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

\[
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 7.
\]

Theorem (Najman, 2014)

There is an elliptic curve \( E/\mathbb{Q} \) whose torsion subgroup over a cubic field is \( \mathbb{Z}/21\mathbb{Z} \).
Sporadic Cubic Points
The only torsion subgroups which appear for an elliptic curve over a cubic field are

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

\[ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 7. \]
Classification of Cubic Torsion

Theorem (Etropolski–Morrow–ZB, Derickx)

The only torsion subgroups which appear for an elliptic curve over a cubic field are

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

\[ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 7. \]

In other words, there is only one cubic sporadic point.
Theorem (Etropolski–Morrow–ZB, Derickx)

The only torsion subgroups which appear for an elliptic curve over a cubic field are

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

\[ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad \text{for } 1 \leq N \leq 7. \]

In other words, there is only one cubic sporadic point.

Remark

Parent showed that the largest prime that can divide \( E(K)_{\text{tors}} \) in the cubic case is \( p = 13 \).
Let $X$ be either of $X_1(N)$ or $X_1(2,2N)$. 

Get lucky
Let $X$ be either of $X_1(N)$ or $X_1(2, 2N)$.
For almost all $N$ we need to consider, $\text{rk } J_X(\mathbb{Q}) = 0$. 
Let $X$ be either of $X_1(N)$ or $X_1(2,2N)$.

For almost all $N$ we need to consider, $\text{rk } J_X(\mathbb{Q}) = 0$. 
Let $X^{(d)} := X^d / S_d$ denote the $d$th symmetric power of $X$. Note that degree $d$ points of $X$ are $\mathbb{Q}$-points of $X^{(d)}$. 
Let $X^{(d)} := X^d / S_d$ denote the $d$th symmetric power of $X$. Note that degree $d$ points of $X$ are $\mathbb{Q}$-points of $X^{(d)}$.

For a finite set $S$ of primes of good reduction, we have the following commutative diagram.

$$
\begin{array}{ccc}
X^{(d)}(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) \\
\downarrow & & \downarrow \alpha \\
\prod_{p \in S} X(\mathbb{F}_q) & \overset{\beta}{\longrightarrow} & \prod_{p \in S} J(\mathbb{F}_p)
\end{array}
$$

We want to choose $S$ so that, once we remove any known rational points, the images of $\alpha$ and $\beta$ are disjoint.
Let $X^{(d)} := X^d / S_d$ denote the $d$th symmetric power of $X$. Note that degree $d$ points of $X$ are $\mathbb{Q}$-points of $X^{(d)}$.

For a finite set $S$ of primes of good reduction, we have the following commutative diagram.

$$
\begin{array}{ccc}
X^{(d)}(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) \\
\downarrow & & \downarrow \alpha \\
\prod_{p \in S} X(\mathbb{F}_q) & \overset{\beta}{\longrightarrow} & \prod_{p \in S} J(\mathbb{F}_p)
\end{array}
$$

We want to choose $S$ so that, once we remove any known rational points, the images of $\alpha$ and $\beta$ are disjoint.
Let $Y = X_1(33)$. Then $g(Y) = 21$ and $\gamma_Y = 10$. 
An Example

- Let $Y = X_1(33)$. Then $g(Y) = 21$ and $\gamma_Y = 10$.
- $J_Y(\mathbb{Q})$ contains a subgroup of order $2 \cdot 3 \cdot 5 \cdot 11 \cdot 61 \cdot 421$. 
Let $Y = X_1(33)$. Then $g(Y) = 21$ and $\gamma_Y = 10$. 

$J_Y(\mathbb{Q})$ contains a subgroup of order $2 \cdot 3 \cdot 5 \cdot 11 \cdot 61 \cdot 421$. 

We sieve using the map $f : X_1(33) \to X_0(33)$. 

mod 7: $(m, n)$ is either $(0, 3)$, $(2, 2)$, $(5, 8)$, or $(7, 7)$.

mod 13: $(m, n)$ is either $(1, 1)$, $(1, 4)$, $(3, 3)$, $(4, 7)$, $(6, 6)$, $(6, 9)$, $(8, 8)$, or $(9, 2)$. 

David Zureick-Brown (Emory University)
An Example

- Let $Y = X_1(33)$. Then $g(Y) = 21$ and $\gamma_Y = 10$.
- $J_Y(\mathbb{Q})$ contains a subgroup of order $2 \cdot 3 \cdot 5 \cdot 11 \cdot 61 \cdot 421$.
- We sieve using the map $f : X_1(33) \to X_0(33)$.
- $g(X_0(33)) = 2$ and $J_0(33)(\mathbb{Q}) \simeq \mathbb{Z}/10 \times \mathbb{Z}/10 = \langle D_1, D_2 \rangle$. 

An Example

- Let $Y = X_1(33)$. Then $g(Y) = 21$ and $\gamma_Y = 10$.
- $J_Y(\mathbb{Q})$ contains a subgroup of order $2 \cdot 3 \cdot 5 \cdot 11 \cdot 61 \cdot 421$.
- We sieve using the map $f : X_1(33) \rightarrow X_0(33)$.
- $g(X_0(33)) = 2$ and $J_0(33)(\mathbb{Q}) \cong \mathbb{Z}/10 \times \mathbb{Z}/10 = \langle D_1, D_2 \rangle$.
- Write $P - 3Q = mD_1 + nD_2$ in $J_0(33)$. 

mod 7: $\ (m, n)$ is either $(0, 3)$, $(2, 2)$, $(5, 8)$, or $(7, 7)$.

mod 13: $\ (m, n)$ is either $(1, 1)$, $(1, 4)$, $(3, 3)$, $(4, 7)$, $(6, 6)$, $(6, 9)$, $(8, 8)$, or $(9, 2)$. 

David Zureick-Brown (Emory University)  Sporadic torsion  April 2-3, 2016  14 / 14
Let $Y = X_1(33)$. Then $g(Y) = 21$ and $\gamma_Y = 10$.

$J_Y(\mathbb{Q})$ contains a subgroup of order $2 \cdot 3 \cdot 5 \cdot 11 \cdot 61 \cdot 421$.

We sieve using the map $f : X_1(33) \to X_0(33)$.

$g(X_0(33)) = 2$ and $J_0(33)(\mathbb{Q}) \simeq \mathbb{Z}/10 \times \mathbb{Z}/10 = \langle D_1, D_2 \rangle$.

Write $P - 3Q = mD_1 + nD_2$ in $J_0(33)$.

mod $7$: $(m, n)$ is either $(0, 3)$, $(2, 2)$, $(5, 8)$, or $(7, 7)$.
Let $Y = X_1(33)$. Then $g(Y) = 21$ and $\gamma_Y = 10$.

$J_Y(\mathbb{Q})$ contains a subgroup of order $2 \cdot 3 \cdot 5 \cdot 11 \cdot 61 \cdot 421$.

We sieve using the map $f : X_1(33) \to X_0(33)$.

$g(X_0(33)) = 2$ and $J_0(33)(\mathbb{Q}) \simeq \mathbb{Z}/10 \times \mathbb{Z}/10 = \langle D_1, D_2 \rangle$.

Write $P - 3Q = mD_1 + nD_2$ in $J_0(33)$.

mod 7: $(m, n)$ is either $(0, 3), (2, 2), (5, 8), \text{ or } (7, 7)$.

mod 13: $(m, n)$ is either $(1, 1), (1, 4), (3, 3), (4, 7), (6, 6), (6, 9)$ $(8, 8), \text{ or } (9, 2)$. 
Let $Y = X_1(33)$. Then $g(Y) = 21$ and $\gamma_Y = 10$.

$J_Y(\mathbb{Q})$ contains a subgroup of order $2 \cdot 3 \cdot 5 \cdot 11 \cdot 61 \cdot 421$.

We sieve using the map $f: X_1(33) \to X_0(33)$.

$g(X_0(33)) = 2$ and $J_0(33)(\mathbb{Q}) \simeq \mathbb{Z}/10 \times \mathbb{Z}/10 = \langle D_1, D_2 \rangle$.

Write $P - 3Q = mD_1 + nD_2$ in $J_0(33)$.

mod 7: $(m, n)$ is either $(0, 3), (2, 2), (5, 8)$, or $(7, 7)$.

mod 13: $(m, n)$ is either $(1, 1), (1, 4), (3, 3), (4, 7), (6, 6), (6, 9), (8, 8)$, or $(9, 2)$. 