Families of Sporadic Points on Modular Curves

Abbey Bourdon, Wake Forest University
Filip Najman, University of Zagreb

May 12, 2021
Theorem (Mordell-Weil)

Let $E$ be an elliptic curve defined over a number field $F$. Then there is a finite abelian group $E(F)_{\text{tors}}$ and nonnegative integer $r$ such that

$$E(F) \cong E(F)_{\text{tors}} \times \mathbb{Z}^r.$$ 

**Question:** If I consider *all* elliptic curves defined over *all* number fields $F$ of a fixed degree, what groups arise as $E(F)_{\text{tors}}$?

This list is *finite* for number fields of fixed degree by Merel (1996).
Torsion Subgroups of Elliptic Curves

**Theorem (Mazur, 1977)**

For $E/\mathbb{Q}$, the group $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following:

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

**Theorem (Kenku-Momose, 1988, Kamienny, 1992)**

Let $F$ be a quadratic field. For $E/F$, the group $E(F)_{\text{tors}}$ is isomorphic to one of the following:

- $\mathbb{Z}/m\mathbb{Z}$, $1 \leq m \leq 18$, $m \neq 17$
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$, $1 \leq m \leq 6$
- $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}$, $1 \leq m \leq 2$
- $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
Theorem (Derickx, Etropolski, van Hoeij, Morrow, Zureick-Brown, 2020)

Let $F$ be a cubic field. For $E/F$, the group $E(F)_{\text{tors}}$ is isomorphic to one of the following:

- $\mathbb{Z}/m\mathbb{Z}$, $1 \leq m \leq 16$ or $m = 18, 20, 21$
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$, $1 \leq m \leq 7$

There exist infinitely many $\overline{\mathbb{Q}}$-isomorphism classes for each such torsion subgroup except for $\mathbb{Z}/21\mathbb{Z}$. In this case, the base change of the elliptic curve 162b1 to $\mathbb{Q}(\zeta_9)^+$ is the unique elliptic curve over a cubic field with $\mathbb{Z}/21\mathbb{Z}$-torsion.

This example was first identified by Najman (2012).
$X_1(N)/\mathbb{Q}$: Non-cuspidal points parametrize pairs $(E, P)/ \sim$

**Definition**
We say a closed point $x \in X_1(N)$ is **sporadic** if there are only finitely many points of degree at most $\deg(x)$.

A non-cuspidal sporadic point on $X_1(N)$ corresponds to an elliptic curve with a rational point of order $N$ defined over a number field of “unusually low degree.”

**Example (Najman, 2012)**
The elliptic curve 162b1 has a point $P$ of order 21 over $\mathbb{Q}(\zeta_9)^+$. 

$\implies [E, P] \in X_1(21)$ is a sporadic point of degree 3
Sporadic vs. Isolated

**Definition**
We say a closed point \( x \in X_1(N) \) is **sporadic** if there are only finitely many points of degree at most \( \deg(x) \).

**Definition**
More generally, a closed point of degree \( d \) is **isolated** if it does not belong to an infinitely family of degree \( d \) points parametrized by \( \mathbb{P}^1 \) or a positive-rank abelian subvariety of the Jacobian.

- A curve \( C \) over a number field has infinitely many degree \( d \) points iff there is a degree \( d \) point on \( C \) that is *not* isolated.
- \( x \) sporadic \( \implies \) \( x \) isolated, but converse does not hold.
- There are only finitely many isolated points on \( C \).

*Faltings (’94), Frey (’94), B., Ejder, Liu, Odumodu, Viray (’19)*
Sporadic Points: CM Elliptic Curves

We say an elliptic curve $E$ over a number field $F$ has complex multiplication (CM) if $\text{End}_F(E) \cong \mathcal{O}$, an order in an imaginary quadratic field $K$.

**Theorem (Clark, Genao, Pollack, Saia, 2019)**

For all $N \geq 721$, the curve $X_1(N)$ has a sporadic CM point.

**Theorem (B., Ejder, Liu, Odumodu, Viray - BELOV, 2019)**

Let $E$ be a CM elliptic curve. Then $E$ corresponds to a sporadic point on infinitely many modular curves of the form $X_1(N)$.

So every CM $j$-invariant is a “sporadic $j$-invariant.”
Searching for non-CM Sporadic Points

**Definition**

We say a closed point $x \in X_1(N)$ is **sporadic** if there are only finitely many points of degree at most $\deg(x)$.

- If $x = [E, P] \in X_1(N)$, then the degree of $x$ is the degree of the residue field $\mathbb{Q}(x)$.

- Suppose $j(E) \neq 0, 1728$. Fix a model of $E/\mathbb{Q}(j(E))$ and let $P = (x_0, y_0)$. Then $\mathbb{Q}(x) \cong \mathbb{Q}(j(E), x_0)$.

**Question:** Is $x$ more likely to be sporadic if $j(x) = j(E) \in \mathbb{Q}$?
Examples of Sporadic Points on Modular Curves

**Table:** Least Known Degree of Non-cuspidal Sporadic Point $x \in X_1(N)$

<table>
<thead>
<tr>
<th>Curve</th>
<th>$\deg(x)$</th>
<th>$\deg(j(x))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1(21)$</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>$X_1(28)$</td>
<td>5</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(29)$</td>
<td>9</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(30)$</td>
<td>5</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(31)$</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>$X_1(33)$</td>
<td>7</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(34)$</td>
<td>8</td>
<td>1,2,4</td>
</tr>
<tr>
<td>$X_1(35)$</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>$X_1(36)$</td>
<td>7</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(37)$</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

Derickx, van Hoeij (2014)
Examples of Sporadic Points on Modular Curves

Table: Least Known Degree of Non-cuspidal Sporadic Point $x \in X_1(N)$

<table>
<thead>
<tr>
<th>Curve</th>
<th>$\deg(x)$</th>
<th>$\deg(j(x))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1(21)$</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>$X_1(28)$</td>
<td>5</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(29)$</td>
<td>9</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(30)$</td>
<td>5</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(31)$</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>$X_1(33)$</td>
<td>7</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(34)$</td>
<td>8</td>
<td>1,2,4 ← has CM</td>
</tr>
<tr>
<td>$X_1(35)$</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>$X_1(36)$</td>
<td>7</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(37)$</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

Derickx, van Hoeij (2014)
Examples of Sporadic Points on Modular Curves

<table>
<thead>
<tr>
<th>Curve</th>
<th>$\deg(x)$</th>
<th>$\deg(j(x))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1(21)$</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>$X_1(28)$</td>
<td>5</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(29)$</td>
<td>9</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(30)$</td>
<td>5</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(31)$</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>$X_1(33)$</td>
<td>7</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(34)$</td>
<td>8</td>
<td>$1,2,4 \leftarrow$ has CM</td>
</tr>
<tr>
<td>$X_1(35)$</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>$X_1(36)$</td>
<td>7</td>
<td>same as $\deg(x)$</td>
</tr>
<tr>
<td>$X_1(37)$</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

**Question (BELOV, 2019)**

Are there only finitely many non-cuspidal, non-CM sporadic (resp., isolated) points in $\bigcup_{N \in \mathbb{Z}^+} X_1(N)$ with rational $j$-invariant?
### Examples of Sporadic Points on Modular Curves

<table>
<thead>
<tr>
<th>Curve</th>
<th>$\text{deg}(x)$</th>
<th>$\text{deg}(j(x))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1(21)$</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>$X_1(28)$</td>
<td>5</td>
<td>same as $\text{deg}(x)$</td>
</tr>
<tr>
<td>$X_1(29)$</td>
<td>9</td>
<td>same as $\text{deg}(x)$</td>
</tr>
<tr>
<td>$X_1(30)$</td>
<td>5</td>
<td>same as $\text{deg}(x)$</td>
</tr>
<tr>
<td>$X_1(31)$</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>$X_1(33)$</td>
<td>7</td>
<td>same as $\text{deg}(x)$</td>
</tr>
<tr>
<td>$X_1(34)$</td>
<td>8</td>
<td>1,2,4</td>
</tr>
<tr>
<td>$X_1(35)$</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>$X_1(36)$</td>
<td>7</td>
<td>same as $\text{deg}(x)$</td>
</tr>
<tr>
<td>$X_1(37)$</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

**Question (BELOV, 2019)**

Are there only finitely many $j \in \mathbb{Q}$ equal to $j(x)$ for a sporadic (resp., isolated) point $x \in \bigcup_{N \in \mathbb{Z}^+} X_1(N)$?
Serre’s Uniformity Conjecture

$K =$ number field
$E/K =$ elliptic curve

For any prime $p$, we have the mod $p$ Galois representation:

$$\rho_{E,p} : \text{Gal}(\overline{K}/K) \to \text{Aut}(E[p]) \cong \text{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Open Image Theorem (Serre, 1972)

If $E/K$ is non-CM, then there exists $C = C(E)$ such that $\rho_{E,p}$ is surjective if $p > C$.

- Can we take $C$ to depend only on $K$? On $[K : \mathbb{Q}]$?
  
  **Guess:** $C = 37$ if $K = \mathbb{Q}$.

- In the case where $K = \mathbb{Q}$, this assumption has become known as **Serre’s Uniformity Conjecture**.
Observation: If $\rho_{E,p}$ is surjective, $E$ will not give a sporadic point on $X_1(p)$.

\[ x = [E, P] \in X_1(p) \]

\[ \deg(x) \geq \frac{1}{2}(p^2 - 1) \geq \gon_Q(X_1(p)) \]

\[ \implies x \text{ is not sporadic.} \]
Theorem (BELOV, 2019)

Assuming Serre’s Uniformity Conjecture, there are only finitely many elliptic curves with rational $j$-invariant giving rise to a sporadic (or isolated) point in \( \bigcup_{N \in \mathbb{Z}^+} X_1(N) \).

- The set of “sporadic $j$-invariants” in $\mathbb{Q}$ contains $-3^2 \cdot 5^6 / 2^3$, $-7 \cdot 11^3$, and all CM $j$-invariants.
A Finiteness Result

**Theorem (BELOV, 2019)**

Assuming Serre’s Uniformity Conjecture, there are only finitely many elliptic curves with rational $j$-invariant giving rise to a sporadic (or isolated) point in $\bigcup_{N \in \mathbb{Z}^+} X_1(N)$.

- B., Gill, Rouse, Watson (2020) show that 162b1 is the unique non-CM elliptic curve with rational $j$-invariant giving rise to a sporadic point of odd degree on any modular curve of the form $X_1(N)$.

- There is one additional non-CM elliptic curve with rational $j$-invariant corresponding to an isolated point of odd degree. Specifically, 338.e2 gives an isolated point of degree 9 on $X_1(28)$. 
What about $\mathbb{Q}$-curves?

**Definition**

A $\mathbb{Q}$-curve is an elliptic curve isogenous (over $\overline{\mathbb{Q}}$) to its Galois conjugates.

**Examples:**

- Any CM elliptic curve.
- Any elliptic curve $E$ with $j(E) \in \mathbb{Q}$.
- Any elliptic curve isogenous to a $\mathbb{Q}$-curve.

**Question (B., Najman, 2021)**

Do there exist only finitely many non-CM $\mathbb{Q}$-curves giving rise to sporadic points on *any* modular curve of the form $X_1(N)$?
What about $\mathbb{Q}$-curves?

Definition

A $\mathbb{Q}$-curve is an elliptic curve isogenous (over $\overline{\mathbb{Q}}$) to its Galois conjugates.

Examples:

- Any CM elliptic curve.
- Any elliptic curve $E$ with $j(E) \in \mathbb{Q}$.
- Any elliptic curve isogenous to a $\mathbb{Q}$-curve.

Question (B., Najman, 2021)

Do there exist only finitely many non-CM $\mathbb{Q}$-curves giving rise to sporadic points on any modular curve of the form $X_1(N)$?
Theorem (B., Najman, 2021)

Suppose that all $\mathbb{Q}$-curves corresponding to sporadic points on $X_1(p^2)$ lie in finitely many $\mathbb{Q}$-isogeny classes, as $p$ varies through all primes. Then Serre’s Uniformity Conjecture holds.

- Suppose $E/\mathbb{Q}$ is non-CM and has $\text{im } \rho_{E,p} = C_{ns}^+(p)$ for $p > 37$.
  $\implies F = \mathbb{Q}(E[p])$ has degree $2(p^2 - 1)$

- $E$ has two independent $p$-isogenies over $F$.
  $\implies E$ is $F$-isogenous to $\mathbb{Q}$-curve $E'$ which possesses a rational cyclic $p^2$-isogeny

- Show $E'$ has a point of order $p^2$ in degree at most $2p(p^2 - 1)$.
  $\implies$ Sporadic by Abramovich (’96) for $p$ sufficiently large.
Theorem (B., Najman, 2021)

Let \( p \) be a prime number. If \( x \in X_1(p^k) \) is a sporadic point of odd degree corresponding to a \( \mathbb{Q} \)-curve \( E \), then \( E \) has complex multiplication. Moreover, for any prime \( p \equiv 3 \pmod{4} \) and \( k \) sufficiently large, there exist sporadic CM points of odd degree on \( X_1(p^k) \).

- In fact there are infinitely many non-isomorphic CM elliptic curves producing sporadic points on \( X_1(p^k) \) of odd degree.
Theorem (B., Najman, 2021)

Let $x \in X_1(N)$ be a sporadic point of odd degree corresponding to a non-CM $\mathbb{Q}$-curve $E$. Then there exists a finite set of rational numbers $\mathcal{J} \subseteq \mathbb{Q}$ such that $E$ is $\overline{\mathbb{Q}}$-isogenous to an elliptic curve with $j$-invariant in $\mathcal{J}$.

- $\mathcal{J}$ is nonempty as it contains $-3^2 \cdot 5^6/2^3$.
- Work in progress: Identify $\mathcal{J}$ explicitly.
Theorem (Cremona, Najman, 2020)

Let $E$ be a non-CM $\mathbb{Q}$-curve defined over a number field $F$. If either $\mathbb{Q}(j(E))$ has odd degree, or more generally if $\mathbb{Q}(j(E))$ has no quadratic subfields, then $E$ is isogenous over $F$ to an elliptic curve with rational $j$-invariant.
Proof Strategy: $p \neq 3$

1. If $x = [E, P] \in X_1(N)$ is a point of odd degree where $E$ is a non-CM $\mathbb{Q}$-curve, then $N = 2^a p^b$ for $p \in \{3, 5, 7, 11, 13\}$ or else $E$ is in the isogeny class of one of finitely many elliptic curves over $\mathbb{Q}$.

2. If $x$ is sporadic and $p \neq 3$, then use the isogeny $\varphi : E \to E'$ where $j(E') \in \mathbb{Q}$ to show $E'$ (or another curve $\mathbb{Q}$-isogenous to $E'$) would possess a point of order $2p$ or $4p$ in unusually low degree.

3. Show this point of order $2p$ or $4p$ in unusually low degree cannot exist.
Proof Strategy: $p \neq 3$

1. If $x = [E, P] \in X_1(N)$ is a point of odd degree where $E$ is a non-CM $\mathbb{Q}$-curve, then $N = 2^a p^b$ for $p \in \{3, 5, 7, 11, 13\}$ or else $E$ is in the isogeny class of one of finitely many elliptic curves over $\mathbb{Q}$.

2. If $x$ is sporadic and $p \neq 3$, then use the isogeny $\varphi : E \rightarrow E'$ where $j(E') \in \mathbb{Q}$ to show $E'$ (or another curve $\mathbb{Q}$-isogenous to $E'$) would possess a point of order $2p$ of $4p$ in unusually low degree.

3. Show this point of order $2p$ or $4p$ in unusually low degree cannot exist.
Proof Strategy: \( p = 3 \)

1. If \( x = [E, P] \in X_1(N) \) is a point of odd degree where \( E \) is a non-CM \( \mathbb{Q} \)-curve, then \( N = 2^a p^b \) for \( p \in \{3, 5, 7, 11, 13\} \) or else \( E \) is in the isogeny class of one of finitely many elliptic curves over \( \mathbb{Q} \).

2. If \( x \) is sporadic and \( p = 3 \), then use the isogeny \( \varphi : E \to E' \) where \( j(E') \in \mathbb{Q} \) to show \( E' \) (or another curve \( \mathbb{Q} \)-isogenous to \( E' \)) would have unusual \( 2 \cdot 3^k \) entanglement. That is, an elliptic curve \( E'' \) that is \( \mathbb{Q} \)-isogenous to \( E' \) would have no rational point of order 2, restricted 3-adic image, and \( \mathbb{Q}(E''[2]) \subseteq \mathbb{Q}(E''[27]) \).

3. Such an \( E'' \) would correspond to a rational point on one of 10 modular curves \( X_H \), all of which have genus at least 2.
Summary

**Question (B., Najman, 2021)**

Do there exist only finitely many non-CM $\mathbb{Q}$-curves giving rise to sporadic points on *any* modular curve of the form $X_1(N)$?

- Finiteness of $\overline{\mathbb{Q}}$-isogeny classes would imply Serre’s Uniformity Conjecture and holds for sporadic points of odd degree.

**Questions:**

1. Can there exist infinitely many distinct non-CM $\mathbb{Q}$-curves within a single isogeny class which produce sporadic points?
2. Can there exist infinitely many sporadic points above a single non-CM $j$-invariant in $\mathbb{Q}$?
3. What progress can be made for sporadic points of even degree?
Thank you!
Suppose $P_0 \in C(k)$ and $x \in C$ is a closed point of degree $d$.

$$\Phi_d : \text{Sym}^d C \to \text{Jac}(C)$$

$$x = P_1 + P_2 + \cdots + P_d \mapsto [P_1 + \cdots + P_d - dP_0]$$

If $C$ has infinitely many closed points of degree $d$, then one of the following is true:

- $\Phi_d(x) = \Phi_d(y)$ for distinct $y \in (\text{Sym}^d C)(k)$. $\exists f \in k(C)^\times$ with $\text{div}(f) = x - y$, and $f : C \to \mathbb{P}^1$ has degree $d$.

- $\Phi_d$ is injective on degree $d$ points. By Faltings (’94), there must be an infinite family of degree $d$ points parametrized by a positive rank abelian subvariety of $\text{Jac}(C)$.
Isolated Points

\[ \Phi_d : \text{Sym}^d \, C \to \text{Jac}(C) \]

\[ x = P_1 + P_2 + \cdots + P_d \mapsto [P_1 + \cdots + P_d - dP_0] \]

**Definition**

1. A closed point \( x \in C \) of degree \( d \) is **\( \mathbb{P}^1 \)-parametrized** if there exists distinct \( y \in (\text{Sym}^d \, C)(k) \) such that \( \Phi_d(x) = \Phi_d(y) \).

2. A closed point \( x \in C \) of degree \( d \) is **AV-parametrized** if there exists a positive rank abelian subvariety \( A \subset \text{Jac}(C) \) such that \( \Phi_d(x) + A \subset \text{im}(\Phi_d) \).

3. A closed point \( x \in C \) of degree \( d \) is **isolated** if it is neither \( \mathbb{P}^1 \)-parametrized nor AV-parametrized.