Torsion groups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$ for $|d| < 800$

Barinder S. Banwait, Maarten Derickx

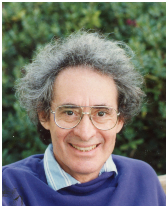
Boston University

Modular curves and Galois representations
Zagreb, Croatia
Thursday 21st September 2023 Link to slides:

https://tinyurl.com/quadratic-torsion

Introduction

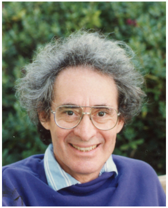
Mazur's Torsion Theorem



Barry C. Mazur

Mazur's Torsion Theorem

Theorem (Mazur, 1977)

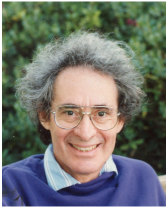


Barry C. Mazur

Mazur's Torsion Theorem

Theorem (Mazur, 1977)

$E(\mathbb{Q})_{tors}$ is one of the following 15 groups:



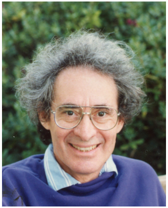
Barry C. Mazur

Mazur's Torsion Theorem

Theorem (Mazur, 1977)

$E(\mathbb{Q})_{tors}$ is one of the following 15 groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, &\qquad 1 \leq N \leq 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, &\qquad 1 \leq N \leq 4. \end{aligned}$$



Barry C. Mazur

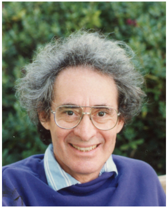
Mazur's Torsion Theorem

Theorem (Mazur, 1977)

$E(\mathbb{Q})_{tors}$ is one of the following 15 groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, &\qquad 1 \leq N \leq 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, &\qquad 1 \leq N \leq 4. \end{aligned}$$

Moreover, each group occurs infinitely often.



Barry C. Mazur

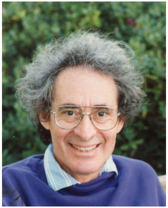
Mazur's Torsion Theorem

Theorem (Mazur, 1977)

$E(\mathbb{Q})_{tors}$ is one of the following 15 groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, &\qquad 1 \le N \le 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, &\qquad 1 \le N \le 4. \end{aligned}$$

Moreover, each group occurs infinitely often.



Barry C. Mazur

This was conjectured by Beppo Levi in 1908 (in his Rome ICM address), then again by Andrew Ogg in 1970.

Kamienny-Kenku-Momose Torsion Theorem

Sheldon Kamienny

Monsur A. Kenku

Fumiyuki Momose

Kamienny-Kenku-Momose Torsion Theorem

Theorem (Kamienny-Kenku-Momose, 1992)

Sheldon Kamienny

Monsur A. Kenku

Fumiyuki Momose

Kamienny-Kenku-Momose Torsion Theorem

Theorem (Kamienny-Kenku-Momose, 1992)

For K a quadratic field, $E(K)_{tors}$ is one of the following 26 groups:

Sheldon Kamienny

Monsur A. Kenku

Fumiyuki Momose

Kamienny-Kenku-Momose Torsion Theorem

Theorem (Kamienny-Kenku-Momose, 1992)

For K a quadratic field, $E(K)_{tors}$ is one of the following 26 groups:

$$\begin{array}{rl} \mathbb{Z}/N\mathbb{Z} & 1 \leq N \leq 16 \text{ or } N = 18 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} & 1 \leq N \leq 6 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z} & 1 \leq N \leq 2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \end{array}$$

Sheldon Kamienny

Monsur A. Kenku

Fumiyuki Momose

Kamienny-Kenku-Momose Torsion Theorem

Theorem (Kamienny-Kenku-Momose, 1992)

For K a quadratic field, $E(K)_{tors}$ is one of the following 26 groups:

$$\begin{array}{rl} \mathbb{Z}/N\mathbb{Z} & 1 \leq N \leq 16 \text{ or } N = 18 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} & 1 \leq N \leq 6 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z} & 1 \leq N \leq 2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \end{array}$$

Moreover, as K varies, each group occurs infinitely often.

Sheldon Kamienny

Monsur A. Kenku

Fumiyuki Momose

What about over particular quadratic fields?

What about over particular quadratic fields?

Question (Motivating question of the talk, v1)

What about over particular quadratic fields?

Question (Motivating question of the talk, v1)

For a fixed quadratic field, what possible groups arise as $E(K)_{tors}$?

What about over particular quadratic fields?

Question (Motivating question of the talk, v1)

For a fixed quadratic field, what possible groups arise as $E(K)_{tors}$*?*

i.e. which of the 26 groups from the KKM classification arise for a particular K?

Quadratic Cyclotomic fields

Filip Najman

Quadratic Cyclotomic fields

Filip Najman

Theorem (Najman, 2011)

1. *Let E be an elliptic curve over $\mathbb{Q}(i)$.*

Quadratic Cyclotomic fields

Filip Najman

Theorem (Najman, 2011)

1. *Let E be an elliptic curve over $\mathbb{Q}(i)$. Then $E(\mathbb{Q}(i))_{tors}$ is isomorphic to one of the groups from Mazur's theorem,*

Quadratic Cyclotomic fields

Filip Najman

Theorem (Najman, 2011)

1. *Let E be an elliptic curve over $\mathbb{Q}(i)$. Then $E(\mathbb{Q}(i))_{tors}$ is isomorphic to one of the groups from Mazur's theorem, or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.*

Quadratic Cyclotomic fields

Filip Najman

Theorem (Najman, 2011)

1. *Let E be an elliptic curve over $\mathbb{Q}(i)$. Then $E(\mathbb{Q}(i))_{tors}$ is isomorphic to one of the groups from Mazur's theorem, or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.*
2. *Let E be an elliptic curve over $\mathbb{Q}(\sqrt{-3})$.*

Quadratic Cyclotomic fields

Filip Najman

Theorem (Najman, 2011)

1. *Let E be an elliptic curve over $\mathbb{Q}(i)$. Then $E(\mathbb{Q}(i))_{tors}$ is isomorphic to one of the groups from Mazur's theorem, or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.*
2. *Let E be an elliptic curve over $\mathbb{Q}(\sqrt{-3})$. Then $E(\mathbb{Q}(\sqrt{-3}))_{tors}$ is isomorphic to one of the groups from Mazur's theorem,*

Quadratic Cyclotomic fields

Filip Najman

Theorem (Najman, 2011)

1. *Let E be an elliptic curve over $\mathbb{Q}(i)$. Then $E(\mathbb{Q}(i))_{tors}$ is isomorphic to one of the groups from Mazur's theorem, or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.*
2. *Let E be an elliptic curve over $\mathbb{Q}(\sqrt{-3})$. Then $E(\mathbb{Q}(\sqrt{-3}))_{tors}$ is isomorphic to one of the groups from Mazur's theorem, or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.*

Question (Motivating question of the talk, v2)

Question (Motivating question of the talk, v2)

For K a quadratic field that is not $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, which of the 8 groups

$$\begin{array}{cc}
\mathbb{Z}/11\mathbb{Z} & \\
\mathbb{Z}/14\mathbb{Z} & \mathbb{Z}/13\mathbb{Z} \\
\mathbb{Z}/15\mathbb{Z} & \mathbb{Z}/16\mathbb{Z} \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} & \mathbb{Z}/18\mathbb{Z} \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} &
\end{array}$$

arise as a possible torsion group over K?

Question (Motivating question of the talk, v3)

For K a quadratic field that is not $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, which of the 8 modular curves

genus 1	*genus* 2
$X_1(11)$	
$X_1(14)$	$X_1(13)$
$X_1(15)$	$X_1(16)$
$X_1(2,10)$	$X_1(18)$
$X_1(2,12)$	

admit a noncuspidal K-rational point?

Elliptic cases


Sheldon Kamienny


Filip Najman

Elliptic cases

Theorem (Kamienny-Najman, 2012)

Let $K \neq \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-15})$ be a quadratic field. If any of the 5 genus 1 modular curves X from the motivating question admit a noncuspidal K-rational point, then $\mathrm{rk}(X(K))$ is positive.

Sheldon Kamienny

Filip Najman

Elliptic cases

Theorem (Kamienny-Najman, 2012)

Let $K \neq \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-15})$ be a quadratic field. If any of the 5 genus 1 modular curves X from the motivating question admit a noncuspidal K-rational point, then $\mathrm{rk}(X(K))$ is positive.

SLOGAN

To deal with the 5 elliptic modular curves, you 'just' need to compute their rank over K

Sheldon Kamienny

Filip Najman

Theorem

For $E/\mathbb{Q}$,

$$\mathrm{rk}(E(\mathbb{Q}(\sqrt{d}))) = \mathrm{rk}(E(\mathbb{Q})) + \mathrm{rk}(E_d(\mathbb{Q})).$$

Theorem

For $E/\mathbb{Q}$,

$$\mathrm{rk}(E(\mathbb{Q}(\sqrt{d}))) = \mathrm{rk}(E(\mathbb{Q})) + \mathrm{rk}(E_d(\mathbb{Q})).$$

SLOGAN

To deal with the 5 elliptic modular curves, you ‘just’ need to compute the $\mathbb{Q}$-rank of their twists!

Genus 2 cases

$$X_1(13) : y^2 = f_{13}(x) := x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$
$$X_1(16) : y^2 = f_{16}(x) := x(x^2 + 1)(x^2 + 2x - 1)$$
$$X_1(18) : y^2 = f_{18}(x) := x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

Genus 2 cases

$$X_1(13) : y^2 = f_{13}(x) := x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$
$$X_1(16) : y^2 = f_{16}(x) := x(x^2 + 1)(x^2 + 2x - 1)$$
$$X_1(18) : y^2 = f_{18}(x) := x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

Writing X as any of these curves,

Genus 2 cases

$$X_1(13) : y^2 = f_{13}(x) := x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$
$$X_1(16) : y^2 = f_{16}(x) := x(x^2 + 1)(x^2 + 2x - 1)$$
$$X_1(18) : y^2 = f_{18}(x) := x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

Writing X as any of these curves,

Theorem (Krumm, 2013)

David Krumm

Genus 2 cases

$$X_1(13) : y^2 = f_{13}(x) := x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$
$$X_1(16) : y^2 = f_{16}(x) := x(x^2 + 1)(x^2 + 2x - 1)$$
$$X_1(18) : y^2 = f_{18}(x) := x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

Writing X as any of these curves,

Theorem (Krumm, 2013)

If X admits a noncuspidal $\mathbb{Q}(\sqrt{d})$-point, then the x-coordinate of that point is in $\mathbb{Q}$

David Krumm

Genus 2 cases

$$X_1(13) : y^2 = f_{13}(x) := x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$
$$X_1(16) : y^2 = f_{16}(x) := x(x^2 + 1)(x^2 + 2x - 1)$$
$$X_1(18) : y^2 = f_{18}(x) := x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

Writing X as any of these curves,

Theorem (Krumm, 2013)

If X admits a noncuspidal $\mathbb{Q}(\sqrt{d})$-point, then the x-coordinate of that point is in $\mathbb{Q}$; i.e. it yields a $\mathbb{Q}$-point on the d-twist X^d.

David Krumm

More precisely,

More precisely,

Theorem (Krumm, 2013)

1. $Y_1(13)(\mathbb{Q}(\sqrt{d})) \neq \emptyset \iff X_1^d(13)(\mathbb{Q}) \neq \emptyset$
2. $Y_1(16)(\mathbb{Q}(\sqrt{d})) \neq \emptyset \iff X_1^d(16)(\mathbb{Q})$ *contains a point with nonzero* y *coordinate*
3. $Y_1(18)(\mathbb{Q}(\sqrt{d})) \neq \emptyset \iff X_1^d(18)(\mathbb{Q}) \neq \emptyset$

More precisely,

Theorem (Krumm, 2013)

1. $Y_1(13)(\mathbb{Q}(\sqrt{d})) \neq \emptyset \iff X_1^d(13)(\mathbb{Q}) \neq \emptyset$
2. $Y_1(16)(\mathbb{Q}(\sqrt{d})) \neq \emptyset \iff X_1^d(16)(\mathbb{Q})$ *contains a point with nonzero y coordinate*
3. $Y_1(18)(\mathbb{Q}(\sqrt{d})) \neq \emptyset \iff X_1^d(18)(\mathbb{Q}) \neq \emptyset$

SLOGAN

This reduces the problem to determining the existence of $\mathbb{Q}$-points on specific genus 2 curves over $\mathbb{Q}$ (or for $X_1(16)$, determining all $\mathbb{Q}$-points).

Using a variety of methods (which we introduce and build on later in the talk), Krumm *almost* dealt with the 13 and 18 cases for all $|d| < 1000$.

Using a variety of methods (which we introduce and build on later in the talk), Krumm *almost* dealt with the 13 and 18 cases for all $|d| < 1000$.

The Quadratic Torsion Challenge

Fix $B > 0$. For $|d| < B$, can you determine the torsion groups that occur over $\mathbb{Q}(\sqrt{d})$?

Using a variety of methods (which we introduce and build on later in the talk), Krumm *almost* dealt with the 13 and 18 cases for all $|d| < 1000$.

The Quadratic Torsion Challenge

Fix $B > 0$. For $|d| < B$, can you determine the torsion groups that occur over $\mathbb{Q}(\sqrt{d})$?

Definition

For $B > 0$ and $N \in \{13, 16, 18\}$, define

$$T_B(N) := \left\{ |d| < B \text{ squarefree } : \mathbb{Z}/N\mathbb{Z} \text{ is a torsion group over } \mathbb{Q}(\sqrt{d}) \right\}.$$

Using a variety of methods (which we introduce and build on later in the talk), Krumm *almost* dealt with the 13 and 18 cases for all $|d| < 1000$.

The Quadratic Torsion Challenge

Fix $B > 0$. For $|d| < B$, can you determine the torsion groups that occur over $\mathbb{Q}(\sqrt{d})$?

Definition

For $B > 0$ and $N \in \{13, 16, 18\}$, define

$$T_B(N) := \left\{ |d| < B \text{ squarefree } : \mathbb{Z}/N\mathbb{Z} \text{ is a torsion group over } \mathbb{Q}(\sqrt{d}) \right\}.$$

Theorem (Krumm, 2013)

$$\{17, 113, 193, 313, 481\} \subseteq T_{1000}(13) \subseteq \{17, 113, 193, 313, 481\} \cup \{257, 353, 601, 673\}$$

$$\{33, 337, 457\} \subseteq T_{1000}(18) \subseteq \{33, 337, 457\} \cup \{681\}.$$

Theorem (Trbović, 2018)

$$\{10, 15, 41, 51, 70, 93\} \subseteq T_{100}(16) \cap \mathbb{Z}_{\geq 1} \subseteq \{10, 15, 41, 51, 70, 93\} \cup \{26, 31, 47, 58, 62, 74, 78, 79, 82, 87, 94\}$$

Antonela Trbović

Statement of results

Theorem (B.-Derickx, 2023)

$$T_{10,000}(13) = \{17, 113, 193, 313, 481, 1153, 1417, 2257, 3769, 3961, 5449, 6217, 6641, 9881\}$$

$$T_{10,000}(18) = \{33, 337, 457, 1009, 1993, 2833, 7369, 8241, 9049\}$$

Theorem (B.-Derickx, 2023)

$$T_{800}(16) = \{-671, -455, -290, -119, -15, 10, 15, 41, 51, 70, 93, 105, 205, 217, 391, 546, 609, 679\}\,.$$

Corollary (B.-Derickx, 2023)

We solve the Quadratic Torsion Challenge for $B = 800$.

$X_1(13)$ and $X_1(18)$

Strategy

Basic idea

Strategy

Basic idea

1. Combine several necessary conditions for $X^d(\mathbb{Q})$ to be nonempty.

Strategy

Basic idea

1. Combine several necessary conditions for $X^d(\mathbb{Q})$ to be nonempty. This reduces the list of ds. For the remaining ds:

Strategy

Basic idea

1. Combine several necessary conditions for $X^d(\mathbb{Q})$ to be nonempty. This reduces the list of ds. For the remaining ds:
2. Search for points;

Strategy

Basic idea

1. Combine several necessary conditions for $X^d(\mathbb{Q})$ to be nonempty. This reduces the list of ds. For the remaining ds:
2. Search for points;
3. If none found, try using Mordell-Weil sieve to prove there are none.

Strategy

Basic idea

1. Combine several necessary conditions for $X^d(\mathbb{Q})$ to be nonempty. This reduces the list of ds. For the remaining ds:
2. Search for points;
3. If none found, try using Mordell-Weil sieve to prove there are none.

We're only going to show $X_1(13)$ because the two cases are basically identical.

ELS

Lemma

If $X_1^d(13)(\mathbb{Q}) \neq \emptyset$, then it is everywhere locally soluble.

Krumm's filter

Theorem (Krumm, 2013)

If $X_1^d(13)(\mathbb{Q}) \neq \emptyset$, *and* $d \neq -3$, *then*

1. $d > 0$;
2. $d \equiv 1 \pmod 8$.

Rank filter

Rank filter

First a preparatory lemma.

Rank filter

First a preparatory lemma.

Lemma

For every quadratic field K, we have

$$J_1(13)(K)_{tors} = J_1(13)(\mathbb{Q})_{tors} \cong \mathbb{Z}/19\mathbb{Z}.$$

Rank filter

First a preparatory lemma.

Lemma

For every quadratic field K, we have

$$J_1(13)(K)_{tors} = J_1(13)(\mathbb{Q})_{tors} \cong \mathbb{Z}/19\mathbb{Z}.$$

Proof.

For $p \geq 5, p \neq 13$, the torsion subgroup $J_1(13)(K)_{tors}$ injects into $J_1(13)(\mathbb{F}_{p^2})$.

Rank filter

First a preparatory lemma.

Lemma

For every quadratic field K, we have

$$J_1(13)(K)_{tors} = J_1(13)(\mathbb{Q})_{tors} \cong \mathbb{Z}/19\mathbb{Z}.$$

Proof.

For $p \geq 5, p \neq 13$, the torsion subgroup $J_1(13)(K)_{tors}$ injects into $J_1(13)(\mathbb{F}_{p^2})$. By computing this latter group for $p = 5$ and 7, one sees that it must be a subgroup of $\mathbb{Z}/19\mathbb{Z}$.

Rank filter

First a preparatory lemma.

Lemma

For every quadratic field K, we have

$$J_1(13)(K)_{tors} = J_1(13)(\mathbb{Q})_{tors} \cong \mathbb{Z}/19\mathbb{Z}.$$

Proof.

For $p \geq 5, p \neq 13$, the torsion subgroup $J_1(13)(K)_{tors}$ injects into $J_1(13)(\mathbb{F}_{p^2})$. By computing this latter group for $p = 5$ and 7, one sees that it must be a subgroup of $\mathbb{Z}/19\mathbb{Z}$. OTOH, the torsion over $\mathbb{Q}$ is $\mathbb{Z}/19\mathbb{Z}$. □

Proposition

Let $K = \mathbb{Q}(\sqrt{d})$. If $X_1(13)(K) \neq X_1(13)(\mathbb{Q})$, then $J_1(13)(K)$ and hence $J_1^d(13)(\mathbb{Q})$ has positive rank.

Proposition

Let $K = \mathbb{Q}(\sqrt{d})$. If $X_1(13)(K) \neq X_1(13)(\mathbb{Q})$, then $J_1(13)(K)$ and hence $J_1^d(13)(\mathbb{Q})$ has positive rank.

Proof.

If P is a K-point of $X_1(13)$ that is not a $\mathbb{Q}$-point,

Proposition

Let $K = \mathbb{Q}(\sqrt{d})$. If $X_1(13)(K) \neq X_1(13)(\mathbb{Q})$, then $J_1(13)(K)$ and hence $J_1^d(13)(\mathbb{Q})$ has positive rank.

Proof.

If P is a K-point of $X_1(13)$ that is not a $\mathbb{Q}$-point, then it embeds under the Abel-Jacobi map to a K-point of $J_1(13)$ that is not a $\mathbb{Q}$-point.

Proposition

Let $K = \mathbb{Q}(\sqrt{d})$. If $X_1(13)(K) \neq X_1(13)(\mathbb{Q})$, then $J_1(13)(K)$ and hence $J_1^d(13)(\mathbb{Q})$ has positive rank.

Proof.

If P is a K-point of $X_1(13)$ that is not a $\mathbb{Q}$-point, then it embeds under the Abel-Jacobi map to a K-point of $J_1(13)$ that is not a $\mathbb{Q}$-point. Therefore by the previous lemma it must be of infinite order.

Proposition

Let $K = \mathbb{Q}(\sqrt{d})$. If $X_1(13)(K) \neq X_1(13)(\mathbb{Q})$, then $J_1(13)(K)$ and hence $J_1^d(13)(\mathbb{Q})$ has positive rank.

Proof.

If P is a K-point of $X_1(13)$ that is not a $\mathbb{Q}$-point, then it embeds under the Abel-Jacobi map to a K-point of $J_1(13)$ that is not a $\mathbb{Q}$-point. Therefore by the previous lemma it must be of infinite order. The final part comes from $\text{rk}(J_1(K)) = \text{rk}(J_1(\mathbb{Q})) + \text{rk}(J_1^d(\mathbb{Q}))$. $\square$

Corollary

If $X_1^d(13)(\mathbb{Q}) \neq \emptyset$, then $J_1^d(13)$ has positive $\mathbb{Q}$-rank.

How to efficiently determine positive rank?

Determining whether the Jacobian of a modular curve has positive analytic rank or not can be done efficiently via a modular symbols computation involving the twisted winding element, a method that goes back to Johan Bosman's PhD thesis.

Johan Bosman

How to efficiently determine positive rank?

Determining whether the Jacobian of a modular curve has positive analytic rank or not can be done efficiently via a modular symbols computation involving the twisted winding element, a method that goes back to Johan Bosman's PhD thesis.

Johan Bosman

52 *CHAPTER 2. COMPUTATIONS WITH MODULAR FORMS*

The element $\sum_{v=0}^{l-1}\chi(-v)\{\infty,\frac{v}{\ell}\}$ of $\mathbb{M}_k(\Gamma_1(N))\otimes\mathbb{Z}[\chi]$ or of some other modular symbols space where it is well-defined is called a *twisted winding element* or, more precisely the *χ-twisted winding element*. Because of formula (2.7), we can calculate the pairings of newforms in $S_2(\Gamma_1(N))$ with twisted winding elements quite efficiently as well.

```
def is_rank_of_twist_zero(G, d):

    M = ModularSymbols(G)
    S = M.cuspidal_subspace()
    phi = S.rational_period_mapping()
    chi = kronecker_character(d)
    w = phi(M.twisted_winding_element(0, chi))
    return w != 0
```

Two cover descent

Let C/K be a nice curve of positive genus, with jacobian J.

Two cover descent

Let C/K be a nice curve of positive genus, with jacobian J.

Definition

An unramified cover of C is a nice curve D together with a finite étale morphism $D \to C$.

Two cover descent

Let C/K be a nice curve of positive genus, with jacobian J.

Definition

An unramified cover of C is a nice curve D together with a finite étale morphism $D \to C$.

If C has a K-rational point P, we can use it to define the Abel-Jacobi map

$$\begin{aligned} AJ_P : C &\hookrightarrow J \\ Q &\mapsto [(Q) - (P)] \end{aligned}$$

and hence view C as a subvariety of J.

Two cover descent

Let C/K be a nice curve of positive genus, with jacobian J.

Definition

An unramified cover of C is a nice curve D together with a finite étale morphism $D \to C$.

If C has a K-rational point P, we can use it to define the Abel-Jacobi map

$$\begin{aligned} AJ_P : C &\hookrightarrow J \\ Q &\mapsto [(Q) - (P)] \end{aligned}$$

and hence view C as a subvariety of J.
Fix $n \geq 1$. Define the map

$$\begin{aligned} \pi : J &\hookrightarrow J \\ Q &\mapsto nQ + P. \end{aligned}$$

Two cover descent

Let C/K be a nice curve of positive genus, with jacobian J.

Definition

An unramified cover of C is a nice curve D together with a finite étale morphism $D \to C$.

If C has a K-rational point P, we can use it to define the Abel-Jacobi map

$$\begin{aligned} AJ_P : C &\hookrightarrow J \\ Q &\mapsto [(Q) - (P)] \end{aligned}$$

and hence view C as a subvariety of J.
Fix $n \geq 1$. Define the map

$$\begin{aligned} \pi : J &\hookrightarrow J \\ Q &\mapsto nQ + P. \end{aligned}$$

The pullback $\pi^*(C)$ yields an unramified cover that has a rational point mapping to P.

Definition

An *n-cover* is any unramifed cover geometrically isomorphic to one of the above form. Equivalently, it is an unramified cover D/C over K such that

$$\mathrm{Aut}_{\overline{K}}(D/C) \cong J[n](\overline{K})$$

as $\mathrm{Gal}(\overline{K}/K)$-modules.

Definition

An *n-cover* is any unramifed cover geometrically isomorphic to one of the above form. Equivalently, it is an unramified cover D/C over K such that

$$\mathrm{Aut}_{\overline{K}}(D/C) \cong J[n](\overline{K})$$

as $\mathrm{Gal}(\overline{K}/K)$-modules.

Write $Cov^{(n)}(C/K)$ for the set of isomorphism classes of n-covers of C.

Definition

An *n-cover* is any unramifed cover geometrically isomorphic to one of the above form. Equivalently, it is an unramified cover D/C over K such that

$$\mathrm{Aut}_{\overline{K}}(D/C) \cong J[n](\overline{K})$$

as $\mathrm{Gal}(\overline{K}/K)$-modules.

Write $Cov^{(n)}(C/K)$ for the set of isomorphism classes of n-covers of C. Write $\mathrm{Sel}^{(n)}(C/K) \subseteq Cov^{(n)}(C/K)$ for the set of ELS n-covers. This is a finite set.

Definition

An *n-cover* is any unramifed cover geometrically isomorphic to one of the above form. Equivalently, it is an unramified cover D/C over K such that

$$\mathrm{Aut}_{\overline{K}}(D/C) \cong J[n](\overline{K})$$

as $\mathrm{Gal}(\overline{K}/K)$-modules.

Write $Cov^{(n)}(C/K)$ for the set of isomorphism classes of n-covers of C. Write $\mathrm{Sel}^{(n)}(C/K) \subseteq Cov^{(n)}(C/K)$ for the set of ELS n-covers. This is a finite set.
Since a curve with a rational point admits a globally soluble n-cover, and hence an ELS n-cover,

Definition

An *n-cover* is any unramifed cover geometrically isomorphic to one of the above form. Equivalently, it is an unramified cover D/C over K such that

$$\mathrm{Aut}_{\overline{K}}(D/C) \cong J[n](\overline{K})$$

as $\mathrm{Gal}(\overline{K}/K)$-modules.

Write $Cov^{(n)}(C/K)$ for the set of isomorphism classes of n-covers of C. Write $\mathrm{Sel}^{(n)}(C/K) \subseteq Cov^{(n)}(C/K)$ for the set of ELS n-covers. This is a finite set.
Since a curve with a rational point admits a globally soluble n-cover, and hence an ELS n-cover,

$$\mathrm{Sel}^{(n)}(C/K) = \emptyset \Rightarrow C(K) = \emptyset$$

We now set $n = 2$.

We now set $n = 2$. Bruin and Stoll define a quotient of $\mathrm{Sel}^{(2)}(C/K)$, called the fake 2-Selmer set $\mathrm{Sel}^{(2)}_{fake}(C/K)$ for which the above all still applies.

We now set $n = 2$. Bruin and Stoll define a quotient of $\mathrm{Sel}^{(2)}(C/K)$, called the fake 2-Selmer set $\mathrm{Sel}^{(2)}_{fake}(C/K)$ for which the above all still applies. This is good because $\mathrm{Sel}^{(2)}_{fake}(C/K)$ can be algorithmically and explicitly constructed.

Nils Bruin

Michael Stoll

This gives us a way to compute the fake Selmer-set explicitly.

define FakeSelmerSet(f):

$A := k[x]/(f(x))$
Let S be the set of primes of k described above.
if $2 \mid \deg(f)$:
    $G := A(2,S)/k(2,S)$
else :
    $G := A(2,S)$
$W := \{g \in G : N_{A/k}(g) \in f_n k^{*2}\}$. **if** $W = \emptyset$: **return** $\emptyset$
$T := S \cup$ "small" primes, as in Lemma 4.3
for $p \in T$:
    $A_p := A \otimes k_p$; $H'_p := A_p^*/A_p^{*2}$.
    $W'_p :=$ LocalImage$(f_p) \subset H'_p$ or, if $p \mid \infty$, use Section 5 to compute W'_p.
    if $2 \mid \deg(f)$:
        $H_p := H'_p/k_p^*$; $W_p :=$ image of W'_p in H_p
    else :
        $H_p := H'_p$; $W_p := W'_p$
    Determine $\rho_p : G \to H_p$.
    $W := \{w \in W : \rho(w) \in W_p\}$.
return W

```
> R<x> := PolynomialRing(Rationals());
> //y^2=f is isomorphic to  X_1(13)
> f := R![1, 2, 1, 2, 6, 4, 1];
> d := 7;
> C := HyperellipticCurve(d*f);
> TwoCoverDescent(C);
{}
```

Corollary

If $X_1^d(13)(\mathbb{Q}) \neq \emptyset$, then the fake 2-Selmer set is nonempty.

```
R<x> := PolynomialRing(Rationals());
//y^2=f is isomorphic to  X_1(13)
f := R![1, 2, 1, 2, 6, 4, 1];

B:= 10000
output := [];

for d in [-B..B] do
    if IsSquarefree(d) then
        if d gt 0 and d mod 8 eq 1 then  // Krumm filter
            if HasPointsEverywhereLocally(d*f,2) then  // ELS filter
                if IsRankOfTwistPositive(Gamma1(13),d) then // Rank filter
                    C := HyperellipticCurve(d*f);
                    if #TwoCoverDescent(C) gt 0 then  // Two cover descent filter
                        Append(~output, d);
                    end if;
                end if;
            end if;
        end if;
    end if;
end for;

output;
```

17, 113, 193, 313, 481, 673, 1153, 1417, 1609, 1921, 2089, 2161, 2257, 3769, 3961, 5449, 6217, 6641, 8473, 8641, 9689, 9881

Out of these values, we search for points;

Out of these values, we search for points; this then leaves the following list where it is likely that they don't have rational points:

$$673, 1609, 1921, 2089, 2161, 8473, 8641, 9689$$

Out of these values, we search for points; this then leaves the following list where it is likely that they don't have rational points:

$$673, 1609, 1921, 2089, 2161, 8473, 8641, 9689$$

These are dealt with via the Mordell-Weil sieve.

Mordell-Weil sieve

$$
\begin{tikzcd}
X(\mathbb{Q}) \arrow[r, hook, "\iota"] \arrow[d, "\alpha"] & J(\mathbb{Q}) \arrow[d, "\alpha"] \\
\prod_p X(\mathbb{Q}_p) \arrow[r, "\tilde{\iota}"] & \prod_p J(\mathbb{Q}_p)
\end{tikzcd}
$$

Mordell-Weil sieve

$$\begin{tikzcd} X(\mathbb{Q}) \arrow[r, hook, "\iota"] \arrow[d, "\alpha"] & J(\mathbb{Q}) \arrow[d, "\alpha"] \\ \prod_p X(\mathbb{Q}_p) \arrow[r, "\tilde{\iota}"] & \prod_p J(\mathbb{Q}_p) \end{tikzcd}$$

We assume we know a degree 1 divisor class on C (to define ι) , and generators of $J(\mathbb{Q})$.

Mordell-Weil sieve

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r, hook, "\iota"] \arrow[d, "\alpha"] & J(\mathbb{Q}) \arrow[d, "\alpha"] \\
\prod_p X(\mathbb{Q}_p) \arrow[r, "\tilde{\iota}"] & \prod_p J(\mathbb{Q}_p)
\end{tikzcd}$$

We assume we know a degree 1 divisor class on C (to define ι) , and generators of $J(\mathbb{Q})$.

Basic Idea

If the images of α and $\tilde{\iota}$ do not intersect, then $X(\mathbb{Q})$ is empty.

Mordell-Weil sieve

$$\begin{array}{ccc} X(\mathbb{Q}) & \xhookrightarrow{\iota} & J(\mathbb{Q}) \\ \downarrow \alpha & & \downarrow \alpha \\ \prod_p X(\mathbb{Q}_p) & \xrightarrow{\tilde{\iota}} & \prod_p J(\mathbb{Q}_p) \end{array}$$

We assume we know a degree 1 divisor class on C (to define ι) , and generators of $J(\mathbb{Q})$.

Basic Idea

If the images of α and $\tilde{\iota}$ do not intersect, then $X(\mathbb{Q})$ is empty.

These are infinite groups and sets, so the intersection can't be computed. Instead one works with a finite approximation.

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r, hook, "\iota"] \arrow[d, "\alpha"] & J(\mathbb{Q})/NJ(\mathbb{Q}) \arrow[d, "\alpha"] \\
\prod_{p\in S} X(\mathbb{Q}_p) \arrow[r, "\tilde{\iota}"] & \prod_{p\in S} J(\mathbb{Q}_p)/NJ(\mathbb{Q}_p)
\end{tikzcd}$$

$$\begin{tikzcd}
X(\mathbb{Q}) \arrow[r, hook, "\iota"] \arrow[d, "\alpha"] & J(\mathbb{Q})/NJ(\mathbb{Q}) \arrow[d, "\alpha"] \\
\prod_{p\in S} X(\mathbb{Q}_p) \arrow[r, "\tilde{\iota}"] & \prod_{p\in S} J(\mathbb{Q}_p)/NJ(\mathbb{Q}_p)
\end{tikzcd}$$

Here N is a positive integer, and S a finite set of primes. Now we can compute the intersection. Heuristically, if $X(\mathbb{Q}) = \emptyset$, then the intersection will be empty if S and N are large enough.

Theorem (B.-Derickx, 2023)

$$T_{10,000}(13) = \{17, 113, 193, 313, 481, 1153, 1417, \\ 2257, 3769, 3961, 5449, 6217, 6641, 9881\}$$

$$T_{10,000}(18) = \{33, 337, 457, 1009, 1993, 2833, 7369, 8241, 9049\}$$

$X_1(16)$

The strategy is different here because every twist of $X_1(16)$ has a (cuspidal) rational point.

The strategy is different here because every twist of $X_1(16)$ has a (cuspidal) rational point. So many of the filters from the previous section go out the window.

The strategy is different here because every twist of $X_1(16)$ has a (cuspidal) rational point. So many of the filters from the previous section go out the window.
As before, it's only the positive rank cases we need to worry about.

The strategy is different here because every twist of $X_1(16)$ has a (cuspidal) rational point. So many of the filters from the previous section go out the window.

As before, it's only the positive rank cases we need to worry about.

Proposition (B.-Derickx, 2023)

Let $K = \mathbb{Q}(\sqrt{d})$. If $\mathbb{Z}/16\mathbb{Z}$ arises as a possible torsion group over K, then $\mathrm{rk}(J_1^d(16)) > 0$.

Using the twisted winding element method from before, we compute the squarefree values of d with $|d| < 10{,}000$ for which $\mathrm{rk}(J_1^d(16)) > 0$; this yields 674 values.

Using the twisted winding element method from before, we compute the squarefree values of d with $|d| < 10{,}000$ for which $\mathrm{rk}(J_1^d(16)) > 0$; this yields 674 values.
We do a point search on these; 55 of them have extra points.

Using the twisted winding element method from before, we compute the squarefree values of d with $|d| < 10{,}000$ for which $\mathrm{rk}(J_1^d(16)) > 0$; this yields 674 values.
We do a point search on these; 55 of them have extra points.
How to deal with the remaining 619 values?

Elliptic Curve Chabauty

Theorem (Bruin-Stoll, souped-up version of Chevalley-Weil)

Every rational point on a hyperelliptic curve X lifts to a rational point on some $D \in$ `TwoCoverDescent(X)`*.*

Elliptic Curve Chabauty

Theorem (Bruin-Stoll, souped-up version of Chevalley-Weil)

Every rational point on a hyperelliptic curve X lifts to a rational point on some $D \in$ `TwoCoverDescent(X)`.

$$\begin{array}{c} D \\ \Big\downarrow \pi \\ X \\ \Big\downarrow x \\ \mathbb{P}^1 \end{array}$$

Elliptic Curve Chabauty

Theorem (Bruin-Stoll, souped-up version of Chevalley-Weil)

Every rational point on a hyperelliptic curve X lifts to a rational point on some $D \in$ `TwoCoverDescent(X)`*.*

So if, for each D, we can work out $\pi(D(\mathbb{Q}))$, then we're done.

$$\begin{array}{c} D \\ \downarrow{\scriptstyle \pi} \\ X \\ \downarrow{\scriptstyle x} \\ \mathbb{P}^1 \end{array}$$

Elliptic Curve Chabauty

Theorem (Bruin-Stoll, souped-up version of Chevalley-Weil)

Every rational point on a hyperelliptic curve X lifts to a rational point on some $D \in$ `TwoCoverDescent(X)`.

$$\begin{tikzcd} D \arrow[d, "\pi"] \\ X \arrow[d, "x"] \\ \mathbb{P}^1 \end{tikzcd}$$

So if, for each D, we can work out $\pi(D(\mathbb{Q}))$, then we're done.

PROBLEM: D has large genus, so computing $D(\mathbb{Q})$ is impossible ☹

Elliptic Curve Chabauty

Theorem (Bruin-Stoll, souped-up version of Chevalley-Weil)

Every rational point on a hyperelliptic curve X lifts to a rational point on some $D \in$ `TwoCoverDescent(X)`.

$$\begin{array}{c} D \\ \downarrow{\scriptstyle \pi} \\ X \\ \downarrow{\scriptstyle x} \\ \mathbb{P}^1 \end{array}$$

So if, for each D, we can work out $\pi(D(\mathbb{Q}))$, then we're done.

PROBLEM: D has large genus, so computing $D(\mathbb{Q})$ is impossible ☹

IDEA: Don't need to work with D directly; rather work with other quotients of D.

Elliptic Curve Chabauty

For simplicity assume $X : y^2 = f(x)$ with $\deg(f) = 5$.

Theorem (Bruin-Stoll, souped-up version of Chevalley-Weil)

Every rational point on a hyperelliptic curve X lifts to a rational point on some $D \in$ `TwoCoverDescent(X)`.

$$\begin{array}{c} D \\ \downarrow \pi \\ X \\ \downarrow x \\ \mathbb{P}^1 \end{array}$$

So if, for each D, we can work out $\pi(D(\mathbb{Q}))$, then we're done.

PROBLEM: D has large genus, so computing $D(\mathbb{Q})$ is impossible ☹

IDEA: Don't need to work with D directly; rather work with other quotients of D.

Elliptic Curve Chabauty

For simplicity assume $X : y^2 = f(x)$ with $\deg(f) = 5$.

Theorem (Bruin-Stoll, souped-up version of Chevalley-Weil)

Every rational point on a hyperelliptic curve X lifts to a rational point on some $D \in$ `TwoCoverDescent(X)`.

$$\begin{array}{c} D \\ \downarrow \pi \\ X \\ \downarrow x \\ \mathbb{P}^1 \end{array}$$

So if, for each D, we can work out $\pi(D(\mathbb{Q}))$, then we're done.

PROBLEM: D has large genus, so computing $D(\mathbb{Q})$ is impossible ☹

IDEA: Don't need to work with D directly; rather work with other quotients of D.

Can construct elliptic curve quotients by taking degree 3 factors g of f over a number field L:

$$E_D : \gamma_D y^2 = g(x)$$

So if, for each D, we can work out $\pi(D(\mathbb{Q}))$, then we're done.

PROBLEM: D has large genus, so computing $D(\mathbb{Q})$ is impossible ☹

IDEA: Don't need to work with D directly; rather work with other quotients of D.

Can construct elliptic curve quotients by taking degree 3 factors g of f over a number field L:

$$E_D : \gamma_D y^2 = g(x)$$

$$\begin{tikzcd}
& D \arrow[dl] \arrow[d, "\pi"] \\
E_D \arrow[dr, "x"] & X \arrow[d, "x"] \\
& \mathbb{P}^1
\end{tikzcd}$$

So if, for each D, we can work out $\pi(D(\mathbb{Q}))$, then we're done.

PROBLEM: D has large genus, so computing $D(\mathbb{Q})$ is impossible ☹

IDEA: Don't need to work with D directly; rather work with other quotients of D.

$$\begin{tikzcd}
 & D \arrow[dl] \arrow[d, "\pi"] \\
E_D \arrow[dr, "x"] & X \arrow[d, "x"] \\
 & \mathbb{P}^1
\end{tikzcd}$$

Can construct elliptic curve quotients by taking degree 3 factors g of f over a number field L:

$$E_D : \gamma_D y^2 = g(x)$$

FACT: If $\mathrm{rk}(E_D(L)) < [L : \mathbb{Q}]$, then $x(E_D(L)) \cap \mathbb{P}^1(\mathbb{Q})$ is finite and computable by an algorithm of Nils Bruin.

$$\begin{tikzcd} & D \arrow[dl] \arrow[d, "\pi"] \\ E_D \arrow[dr, "x"] & X \arrow[d, "x"] \\ & \mathbb{P}^1 \end{tikzcd}$$

So if, for each D, we can work out $\pi(D(\mathbb{Q}))$, then we're done.

PROBLEM: D has large genus, so computing $D(\mathbb{Q})$ is impossible ☹

IDEA: Don't need to work with D directly; rather work with other quotients of D.

Can construct elliptic curve quotients by taking degree 3 factors g of f over a number field L:

$$E_D : \gamma_D y^2 = g(x)$$

FACT: If $\mathrm{rk}(E_D(L)) < [L:\mathbb{Q}]$, then $x(E_D(L)) \cap \mathbb{P}^1(\mathbb{Q})$ is finite and computable by an algorithm of Nils Bruin.

SUMMARY: If, for every D, there is a degree 3 factor $g \in L[x]$ s.t. $E_D : \gamma_D y^2 = g(x)$ has $\mathrm{rk}(E_D(L)) < [L:\mathbb{Q}]$, then we're done.

$$\begin{tikzcd}
& D \arrow[dl] \arrow[d, "\pi"] \\
E_D \arrow[dr, "x"] & X \arrow[d, "x"] \\
& \mathbb{P}^1
\end{tikzcd}$$

So if, for each D, we can work out $\pi(D(\mathbb{Q}))$, then we're done.

PROBLEM: D has large genus, so computing $D(\mathbb{Q})$ is impossible ☹

IDEA: Don't need to work with D directly; rather work with other quotients of D.

Can construct elliptic curve quotients by taking degree 3 factors g of f over a number field L:

$$E_D : \gamma_D y^2 = g(x)$$

FACT: If $\mathrm{rk}(E_D(L)) < [L : \mathbb{Q}]$, then $x(E_D(L)) \cap \mathbb{P}^1(\mathbb{Q})$ is finite and computable by an algorithm of Nils Bruin.

SUMMARY: If, for every D, there is a degree 3 factor $g \in L[x]$ s.t. $E_D : \gamma_D y^2 = g(x)$ has $\mathrm{rk}(E_D(L)) < [L : \mathbb{Q}]$, then we're done.

For us, $f(x) = dx(x^2 + 1)(x^2 - 2x - 1)$, so L will always be quite small.

Running this on the 619 values of d, this successfully show that there are only the original two points on the twist 581 cases.

Running this on the 619 values of d, this successfully show that there are only the original two points on the twist 581 cases.

This includes some values where $\mathrm{rk}(J_1^d(\mathbb{Q})) = 4$ (e.g. $d = 679$).

Running this on the 619 values of d, this successfully show that there are only the original two points on the twist 581 cases.

This includes some values where $\mathrm{rk}(J_1^d(\mathbb{Q})) = 4$ (e.g. $d = 679$).

The remaining 38 values to be dealt with are:

Running this on the 619 values of d, this successfully show that there are only the original two points on the twist 581 cases.

This includes some values where $\mathrm{rk}(J_1^d(\mathbb{Q})) = 4$ (e.g. $d = 679$).

The remaining 38 values to be dealt with are:

$$\begin{aligned}
&-8259, -7973, -7615, -7161, -7006, -6711, -6503, -6095,\\
&-6031, -6005, -4911, -4847, -4773, -4674, -4371, -4191,\\
&-4074, -3503, -3199, -1810, -1749, -815, 969, 1186,\\
&3215, 3374, 3946, 4633, 5257, 5385, 7006, 7210,\\
&7733, 8459, 8479, 8569, 9709, 9961
\end{aligned}$$

Todo

- Deal with those values.

- Deal with those values.
- Could nonabelian Chabauty methods be used on these vals?

- Deal with those values.
- Could nonabelian Chabauty methods be used on these vals?
- What about cubic torsion?

- Deal with those values.
- Could nonabelian Chabauty methods be used on these vals?
- What about cubic torsion? i.e. for a fixed cubic field K, which of the 26 groups in the cubic torsion classification (due to Derickx-Etropolski, van Hoeij, Morrow, Zureick-Brown) arise as torsion subgroups for that K?