Torsion subgroups of elliptic curves over quadratic fields and a conjecture of Granville

Maarten Derickx [1] Barinder S. Banwait [2]

[1] University of Zagreb
[2] Boston University

ANTS XVI - MIT
2024-07-16

Slides at:
https://antsmath.org/ANTSXVI/slides/Derickx.pdf

Motivation I

Question

Let K be a number field and N be an integer, does there exist an elliptic curve E over K with a K-rational torsion point of order N?

Definition/Notation

- $Y_1(N)/\mathbb{Z}[1/N]$ *is the curve parametrizing tuples* (E, P) *of elliptic curve, with points of order* N.
- $X_1(N)/\mathbb{Z}[1/N]$ *is its projectivisation.*

Question

Does the curve $Y_1(N)$ *have a* K*-rational point?*

In this talk we will focus on the case where K is a quadratic field.

- $f(x) \in \mathbb{Z}[x]$ a squarefree polynomial of degree $n > 4$.
- d a squarefree integer.
- C_d the hyperelliptic curve given by $dy^2 = f(x)$.
- $g := \lceil n/2 \rceil - 1$ the genus of C_d.
- $N_D = \# \{|d| \leq D \mid C_d \text{ has a rational point with } y \neq 0, \infty\}$.

Conjecture (Granville)

There exists an explicitly computable constant κ_f such that

$$N_D \sim \kappa_f D^{1/(g+1)}.$$

Main Goal

Definition

Let N and B be positive integer, define

$$T_B(N) := \left\{ d \in \mathbb{Z} \mid d \text{ squarefree}, |d| \leq B \text{ and } Y_1(N)(\mathbb{Q}(\sqrt{d})) \neq \emptyset \right\}.$$

Goal: Determine all $T_B(N)$ for an as large as possible value of B.
This was studied for $d > 0$ and $B = 100$ by Trbović.

Results for all values of B

- $T_B(N) = \emptyset$ for $N > 18$ or $N = 17$. (Next slide)
- $T_B(N) = \{d \in \mathbb{Z} \mid d \text{ squarefree }, |d| \leq B\}$ for $N = 1, \ldots, 10, 12$.

What remains is to study $T_B(N)$ for $N = 11, 13, 14, 15, 16$ and 18.
$X_1(N)$ has genus 1 for $N = 11, 14, 15$. These cases are easy: computing ranks of twists of elliptic curves.
$X_1(N)$ has genus 2 for $N = 13, 16, 18$.

Uniform boundedness

Theorem (Merel, building on ideas of Mazur and Kamienny)

For every degree d there exist a finite set $M(d)$ such that $Y_1(N)$ has a point of degree d over $\mathbb{Q}$ if and only if $N \in M(d)$.

In other words:

Torsion orders of elliptic curves over degree d number fields are bounded, in terms of d alone!

The $M(d)$ for $d \leq 3$ are known:

- $M(1) = \{1, \ldots, 10, 12\}$ (Mazur)
- $M(2) = \{1, \ldots, 16, 18\}$ (Kenku, Momose), (Kamienny)
- $M(3) = \{1, \ldots, 16, 18, 20, 21\}$ (D., Etropolski, Hoeij, Morrow, Zureick-Brown)

Genus 2: Link with Granville

$$X_1^d(13) : dy^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$
$$X_1^d(16) : dy^2 = x(x^2 + 1)(x^2 + 2x - 1)$$
$$X_1^d(18) : dy^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

Theorem (Krumm)

Let $N = 13, 16$ *or* 18 *then*
$$Y_1(N)(\mathbb{Q}(\sqrt{d})) \neq \emptyset \iff Y_1^d(N)(\mathbb{Q}) \neq \emptyset.$$

This turns the study of $T_B(N)$ into a study of points on quadratic twists. In particular, Granville's conjecture predicts $\# T_B(N) \sim \kappa_f B^{1/3}$.

Genus 2: Known results

Theorem (Krumm)

- *If* $d \in T_B(13)$*, then* $d > 0$ *and* $d \equiv 1 \mod 8$*.*
- *If* $d \in T_B(18)$*, then* $d > 0$ *and* $d \equiv 1$ *or* $9 \mod 24$*.*

This result is proved by exhibiting local obstructions to $X_1^d(N)(\mathbb{Q}) \neq \emptyset$. $X_1^d(16)(\mathbb{Q}) \neq \emptyset$ for all values of d since it contains a rational cusp.

Theorem

- $T_{1000}(13) = \{33, 337, 457, \mathbf{681}?\}$ *(Krumm)*
- $T_{1000}(18) = \{17, 113, 193, \mathbf{257}?, 313, \mathbf{353}?, 481, \mathbf{601}?, \mathbf{673}?\}$ *(Krumm)*
- $T_{100}(16) \cap \mathbb{N} = \{10, 16, \mathbf{26}?, \mathbf{31}?, 41, \mathbf{47}?, 51, \mathbf{58}?, \mathbf{62}?, 70, \mathbf{74}?, \mathbf{78}?, \mathbf{79}?, \mathbf{82}?, \mathbf{87}?, 93, \mathbf{94}?\}$ *(Trbović)*

$T_B(16)$ is much more difficult due to rational cusps on all twists.

Genus 2: Techniques used

Techniques used by Krumm and Trbović:

- Local obstructions (Only for $N = 13, 18$)
- Two cover descent (Only for $N = 13, 18$)
- Point search
- Magma's **`RankBound`** and **`Chabauty0`** if **`RankBound`** is 0.

New techniques added to the mix:

- No need for **`Chabauty0`** anymore if rank = 0.
- Analytic ranks using twisted winding elements. Deals with 94%-98% of the cases $< 10,000$.
- Mordell-Weil sieve (Only for $N = 13, 18$)
- Two cover descent + Elliptic curve chabauty (Only for $N = 16$)

Results

Theorem (Banwait, D.)

$$T_{10,000}(13) = \{17, 113, 193, 313, 481, 1153, 1417, 2257, 3769, 3961, 5449, 6217, 6641, \mathbf{9689}?, 9881\}$$

$$T_{10,000}(18) = \{33, 337, 457, 1009, 1993, \mathbf{2841}?, 2833, 4729, 7369, 8241, 9049, \mathbf{9969}?\}$$

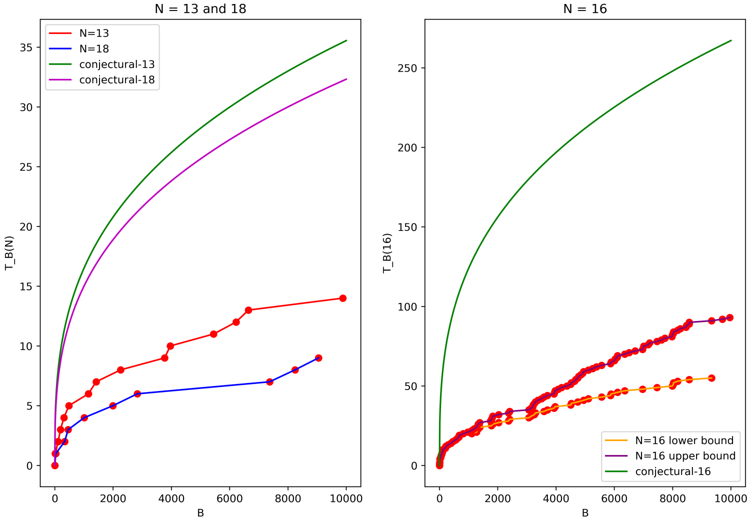
$$T_{1,000}(16) = \{-\mathbf{815}?, -671, -455, -290, -119, -15, 10, 15, 41, 51, 70, 93, 105, 205, 217, 391, 546, 609, 679, \mathbf{969}?\}$$

$$54 \leq \# T_{10,000}(16) \leq 92 = 54 + 38$$

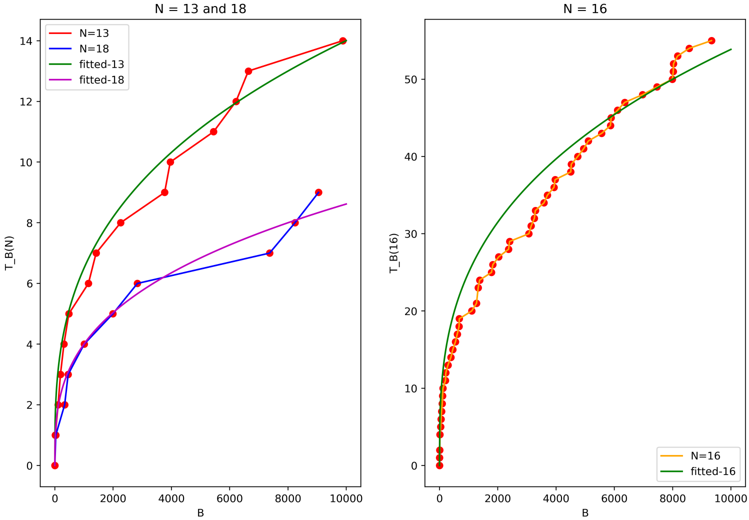
Unsolved cases:

- **13**, **18:** Magma couldn't find generators of $J_1^d(N)(\mathbb{Q})$ predicted to exist by BSD. These are needed for using the MW-Sieve.
- **16:** The elliptic curves for elliptic curve Chabauty either had to high rank or we failed to compute the rank.

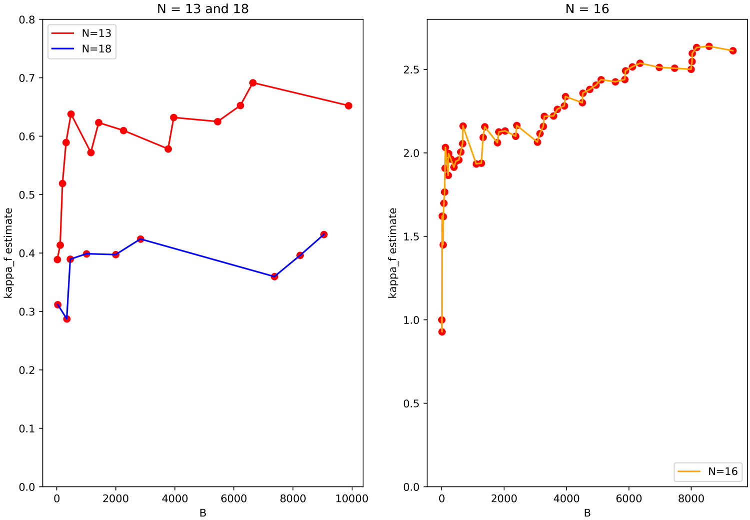
Conjectural vs actual growth



Actual growth with fitted constants



Approximated constant



abc-triples from points on twists

$a, b, c \in \mathbb{Z} \setminus \{0\}$ with $a + b = c$ and $gcd(a, b) = 1$ is an abc-triple if:

$$q(a, b, c) := \log(\max(|a|, |b|, |c|))/\log(\mathrm{rad}(abc)) > 1.$$

Conjecture (abc-conjecture)

Fix $\varepsilon > 0$, there are finitely many abc-triples with $q(a, b, c) \geq 1 + \varepsilon$.

Granville's hyperelliptic height bound (After Elkies).

Point of large height on C_d + Beyli map $\implies$ abc-triple.

abc-conjecture $\implies$ height bound of size $|d|^{1/(2g-2)+o(1)}$. □

$j/1728$ is a Beyli map on $X_1(16)$. The following abc-triple comes from a point P on $X_1^{4522}(16)$ with $j(P)/1728 = a/c$.

$$a = 2^{18} \cdot 3^{51} \cdot 5^4 \cdot 7 \cdot 11^{16} \cdot 17^2 \cdot 19^4 \cdot 601$$

$$b = 191^4 \cdot 353^2 \cdot 4289^2 \cdot 4993^2 \cdot 6143^2 \cdot 204751^2 \cdot 3945233^2$$

$$c = 4801^3 \cdot 31153^3 \cdot 116833^3 \cdot 9407089^3$$

$$q(a, b, c) \approx 1.06919289$$

The End

Thank you!

https://antsmath.org/ANTSXVI/slides/Derickx.pdf

Genus 2: Rank 0

Lemma (Banwait, D.)

Let $N = 13, 16, 18$ *and* d *a squarefree integer such that* $(N, d) \neq (16, -1), (16, 2), (18, -3)$ *then*

$$J_1(N)(\mathbb{Q}(\sqrt{d}))_{tors} = J_1(N)(\mathbb{Q})_{tors}.$$

$X_1^d(N)$ is the quadratic twist of $X_1(N)$ by d and $J_1^d(N)$ it's jacobian.

Corollary

If $(N, d) \neq (16, -1), (16, 2), (18, -3)$ *and* $J_1^d(N)$ *has rank 0 then*

$$Y_1(N)(\mathbb{Q}(\sqrt{d})) = \emptyset.$$

Using twisted winding elements in SageMath one can determine the d for which $J_1^d(N)$ has analytic and hence (by Kato) algebraic rank 0. This shows $Y_1(N)(\mathbb{Q}(\sqrt{d})) = \emptyset$ for all but 203, 675 resp. 249 values of d with $|d| \leq 10,000$ for $N = 13, 16$ resp 18. (out of 12166 cases)

Genus 2: Mordell-Weil sieve

If a curve X of genus 2 has an odd degree divisor then it has has divisor D of degree 1. In particular, we get a map $X \to J(X)$. If we can compute $J(X)(\mathbb{Q})$ then we can use the Mordell-Weil sieve:

$$\begin{tikzcd} X(\mathbb{Q}) \arrow[r] \arrow[d] & J(X)(\mathbb{Q}) \arrow[d] \\ \prod_{i=1}^{n} X(\mathbb{Z}/p_i^{e_i}\mathbb{Z}) \arrow[r] & \prod_{i=1}^{n} J(X)(\mathbb{Z}/p_i^{e_i}\mathbb{Z}) \end{tikzcd}$$

as implemented by Stoll to try and show $X(\mathbb{Q}) = \emptyset$.

Proposition (Banwait, D.)

Let $N = 13, 16$ and suppose that $X_1^d(N)(\mathbb{R}) \neq \emptyset$ and $X_1^d(N)(\mathbb{Q}_p) \neq \emptyset$ for all primes p, then $X_1(N)$ has an effective divisor of degree 3.

Proof.

There is an $f : X_1^d(N) \to C$ of degree 3 to a genus 0 curve. Since C has points everywhere locally $C \cong \mathbb{P}^1$ and we can take $D = f^*(\infty)$. □

Genus 2: Two cover descent

Let X be a genus 2 curve over $\mathbb{Q}$ with a rational point then we have $X \to J(X)$ and $[2] : J(X) \to J(X)$. Define $D := X \times_{J(X)} J(X)$.

$f : D \to X$ is etale of degree 16 and

$$\mathrm{Aut}\, D_{\overline{\mathbb{Q}}}/X_{\overline{\mathbb{Q}}} \cong J(X)(\overline{\mathbb{Q}})[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$$

Etale descent gives a finite set $S(X)$ of twists $f_\gamma : D_\gamma \to X$ such that

$$X(\mathbb{Q}) = \bigcup_{\gamma \in S(X)} f_\gamma(D_\gamma(\mathbb{Q})).$$

So instead of $X(\mathbb{Q})$ we can try to compute $\bigcup_{\gamma \in S(X)} f_\gamma(D_\gamma(\mathbb{Q}))$.
A variation of this was already used for $N = 13, 18$ by Krumm using the fact that $X_1^d(N)(\mathbb{Q}) = \emptyset$ if $S(X_1^d(N)) = \emptyset$.

This doesn't work for $N = 16$: $S(X_1^d(16)) \neq \emptyset$ since $X_1^d(16)(\mathbb{Q}) \neq \emptyset$.

Genus 2: Elliptic Curve Chabauty

Let $D := X \times_{J(X)} J(X)$ as before.
There are elliptic curves E_i over $\overline{\mathbb{Q}}$ such that

$$J(D)_{\overline{\mathbb{Q}}} \sim J(X)_{\overline{\mathbb{Q}}} \times \prod_{i=1}^{15} E_i$$

Suppose X is given by $y^2 = f(x)$ with f of degree 5 and leading coefficient c. Let $a_1, \ldots a_5$ be the roots of f then $D_{\overline{\mathbb{Q}}}$ is given by the 5 equations $y_i^2 = x - a_i$.
The map from $D_{\overline{\mathbb{Q}}}$ to $X_{\overline{\mathbb{Q}}}$ is given by $(y_1, \ldots, y_5, x) \mapsto (\sqrt{c} \prod y_i, x)$.
If g is a factor of degree 3 of f defined over a number field K, then there is an $a \in K$ and such that D_K maps to $E_{g,a} : z^2 = ag(x)$.
From the two cover descent we get an explicit $\varepsilon(\gamma) \in K$ such that $D_{\gamma,K} \to E_{g,\varepsilon(\gamma)}$. The points on $E_{g,\varepsilon(\gamma)}$ coming from $D_\gamma(\mathbb{Q})$ have $x \in \mathbb{Q}$.
If the rank of $E_{g,\varepsilon\gamma}(K)$ is smaller then deg K then elliptic curve chabauty can often compute $\{P \in E_{g,\varepsilon\gamma}(K) \mid x(P) \in \mathbb{Q}\}$.
From this one can easily compute $D_\gamma(\mathbb{Q})$.

The genus 1 cases

$X_1(N)$ has genus 1 for $N = 11, 14, 15$. We can use a rational cusp to view $X_1(N)$ as an elliptic curve.

Theorem (Kamienny-Najman)

If $N = 11, 14$ or 15, d squarefree such that $(N, d) \neq (14, -7), (15, -15)$ then every noncuspidal point on $X_1(N)(\mathbb{Q}(\sqrt{d}))$ is of infinite order.

Let $X_1^d(N)$ denote the quadratic twist of $X_1(N)$ by d.

Corollary

If $N, d \neq (14, -7), (15, -15)$ then $X_1(N)(\mathbb{Q}(\sqrt{d}))$ has a noncuspidal point if and only if $X_1^d(N)$ has positive rank.

The `Rank` function of Magma is good enough to determine $T_{5,000}(N)$ in these 3 cases.