Bounds on Torsion Groups From Geometric Isogeny Classes

Tyler Genao

Department of Mathematics
University of Georgia

(20-minute version)
arXiv: 2210.10177, 2112.11566.

- Throughout, we let $E_{/F}$ be an elliptic curve defined over a number field (unless otherwise stated!).
- The set $E(F)$ of F-rational points is an abelian group by the chord-and-tangent method.
- By the Mordell-Weil Theorem,

$$E(F) \cong \mathbb{Z}^{r(E,F)} \times E(F)[\mathrm{tors}]$$

  where $E(F)[\mathrm{tors}]$ is the **torsion subgroup of $E_{/F}$** and is a finite abelian group.
- **Broad goal:** Better understand $E(F)[\mathrm{tors}]$ when fixing an invariant of $E_{/F}$ (uniformity results).

Fixing the degree:

Elliptic curves over number fields satisfy a "strong uniform boundedness" in their torsion subgroup sizes.

Theorem (Merel, 1996).

For each $d \in \mathbb{Z}^+$, there exists a constant $B := B(d) \in \mathbb{Z}^+$ so that for all elliptic curves $E_{/F}$ where $[F : \mathbb{Q}] = d$ one has

$$\#E(F)[\text{tors}] \leq B := B(d).$$

- "Fix the number field degree, and get a uniform bound."
- Examples: for $E_{/F}$, one has:
  - $[F : \mathbb{Q}] = 1 \Rightarrow \#E(F)[\mathrm{tors}] \leq 16$;
  - $[F : \mathbb{Q}] = 2 \Rightarrow \#E(F)[\mathrm{tors}] \leq 24$;
  - $[F : \mathbb{Q}] = 3 \Rightarrow \#E(F)[\mathrm{tors}] \leq 28$.

Fixing the isogeny class:

- For two elliptic curves E, E' both defined over an algebraic extension $F/\mathbb{Q}$, an F-rational *isogeny* from E and E' is a nonconstant F-rational algebraic map $\phi\colon E \to E'$ which fixes basepoints.
- ϕ will induce a group homomorphism $\phi\colon E(F) \to E'(F)$.
- Example: with $E : y^2 = x^3 + x$, take

$$[-1] : (x, y) \mapsto (x, -y)$$

or

$$[2] : (x, y) \mapsto \left(\frac{(x^2 - 1)^2}{4(x^3 + x)}, \frac{y(x^6 + 5x^4 - 5x^2 - 1)}{8(x^3 + x)^2} \right).$$

- Fix an algebraic closure $\overline{\mathbb{Q}}$.
- The "$\overline{\mathbb{Q}}$-isogeny class of $E_{/F}$" is the collection of elliptic curves $E'_{/F'}$ which are $\overline{\mathbb{Q}}$-isogenous to E.
- As an adjective, *geometric* means $\overline{\mathbb{Q}}$-rational.
- Question: What can be said about torsion groups in a geometric isogeny class?

Theorem 1 (G., 2022).

Polynomial bounds: *Fix a $\overline{\mathbb{Q}}$-isogeny class $\mathcal{E}$. Then for each $\epsilon > 0$ there exists a constant $C_\epsilon := C_\epsilon(\mathcal{E})$ such that for all elliptic curves $E_{/F} \in \mathcal{E}$ one has*

$$\#E(F)[\text{tors}] \leq C_\epsilon \cdot [F : \mathbb{Q}]^{2+\epsilon}.$$

Theorem 2 (G., 2022).

Typical boundedness: *Fix a number field F_0. Then for each $\epsilon > 0$ there exists a constant $B_\epsilon := B_\epsilon(F_0)$ such that for all elliptic curves $E_{/F}$ $\overline{\mathbb{Q}}$-isogenous to some elliptic curve E' with $j(E') \in F_0$, one has*

$$\#E(F)[\text{tors}] \leq B_\epsilon$$

when $[F : \mathbb{Q}]$ does not lie in a certain subset of $\mathbb{Z}^+$ of upper density $\leq \epsilon$.

Polynomial Bounds on Torsion From Geometric Isogeny Classes

Folklore Conjecture (Clark, Cook and Stankewicz, 2013).

There exist constants $C, \alpha > 0$ such that for all elliptic curves $E_{/F}$, one has

$$\#E(F)[\mathrm{tors}] \leq C \cdot [F : \mathbb{Q}]^{\alpha}.$$

Support: for an elliptic curve $E_{/F}$ and $d := [F : \mathbb{Q}] > 1$,

1. (Hindry and Silverman, 1999) if $j(E)$ is integral then

$$\#E(F)[\mathrm{tors}] \leq 1977408 \cdot d \log d;$$

2. (Clark and Pollack, 2015) if E has *complex multiplication* (CM) then

$$\#E(F)[\mathrm{tors}] \leq C \cdot d \log \log d$$

for some effectively computable constant $C \in \mathbb{Z}^{+}$.

3. (Clark and Pollack, 2018) For each $\epsilon > 0$ there exists $C_\epsilon > 0$ such that for all elliptic curves $E_{/F}$ *base-changed from* $\mathbb{Q}$ one has

$$\#E(F)[\mathrm{tors}] \leq C_\epsilon \cdot d^{5/2+\epsilon}$$

where $d := [F : \mathbb{Q}]$.

More generally:

4. (Clark and Pollack, 2018) Fix a number field F_0. Assume that A. GRH is true, and that B. F_0 contains no Hilbert class fields of imaginary quadratic fields. Then for each $\epsilon > 0$ there exists $C_\epsilon > 0$ such that for all elliptic curves $E_{/F}$ *with* F_0*-rational* j*-invariant*, one has

$$\#E(F)[\mathrm{tors}] \leq C_\epsilon \cdot d^{5/2+\epsilon}$$

where $d := [F : \mathbb{Q}]$.

- A. and B. are the **LV Hypotheses.**

Theorem 1 (G., 2022).

Fix a number field F_0 and an elliptic curve E_{0/F_0}. Then for each $\epsilon > 0$ there exists $C_\epsilon := C_\epsilon(E_0, F_0) > 0$ such that for all elliptic curves $E_{/F}$ geometrically isogenous to E_{0/F_0} one has

$$\#E(F)[\text{tors}] \leq C_\epsilon \cdot d^{2+\epsilon}$$

where $d := [F : \mathbb{Q}]$.

Typically Bounding Torsion From $\mathcal{I}_{F_0}$

- Definition: a subset $S \subseteq \mathbb{Z}^+$ has *upper density*

$$\overline{\delta}(S) := \limsup_{x\to\infty} \frac{\#(S \cap [1,x])}{x}.$$

- Say that a family $\mathcal{F}$ of elliptic curves is **typically bounded in torsion** if for all $\epsilon > 0$ there exists $B := B(\epsilon) > 0$ so that the set

$$\{d \in \mathbb{Z}^+ : \max_{\substack{E_{/F}\in\mathcal{F}: \\ [F:\mathbb{Q}]=d}} \#E(F)[\mathrm{tors}] \geq B\} \subseteq \mathbb{Z}^+$$

has upper density $\leq \epsilon$.

- So for any $\epsilon > 0$, there is a bound on torsion subgroups which works over **any** degree, as long as one ignores a subset of degrees of arbitrarily small upper density.

1. $\mathcal{E}_{\mathrm{CM}} := \{\text{CM elliptic curves}\} \Rightarrow \mathcal{E}_{\mathrm{CM}}$ is typically bounded in torsion (Bourdon, Clark and Pollack, 2017).
2. $\mathcal{E} := \{\text{all elliptic curves}\} \Rightarrow \mathcal{E}$ is *not* typically bounded in torsion (Clark, Milosevic and Pollack, 2018).

P1: Given integers $\ell, n_0 \in \mathbb{Z}^+$ with ℓ prime, there exists $n := n(\mathcal{F}, \ell, n_0) \in \mathbb{Z}^+$ such that for all $E_{/F} \in \mathcal{F}$, if $E(F)[\ell^n] \setminus E(F)[\ell^{n-1}] \neq \emptyset$ then

$$\ell^{n_0} \mid [F : \mathbb{Q}].$$

P2: There exists $c := c(\mathcal{F}) \in \mathbb{Z}^+$ such that for all primes $\ell \in \mathbb{Z}^+$ and all $E_{/F} \in \mathcal{F}$, if $E(F)[\ell] \setminus \{O\} \neq \emptyset$ then

$$\ell - 1 \mid c[F : \mathbb{Q}].$$

Theorem (Theorem 3.2, Clark, Milosevic and Pollack, 2018).

If $\mathcal{F}$ satisfies **P1** *and* **P2,** *then $\mathcal{F}$ is typically bounded in torsion.*

- Let us define the family

$$\mathcal{I}_{F_0} := \{E_{/F} : E \text{ is } \overline{\mathbb{Q}}\text{-isogenous to some } E'_{/F_0}\}.$$

- "Elliptic curves $\overline{\mathbb{Q}}$-isogenous to at least one F_0-rational elliptic curve."

Theorem 2 (G., 2022).

For any number field F_0, the family $\mathcal{I}_{F_0}$ is typically bounded in torsion.

Continuing Work

Polynomial Bounds

Theorem 2 (G., 2022).

For each $\epsilon > 0$ and **fixed** *geometric isogeny class $\mathcal{E}$, there exists a constant $C_\epsilon := C_\epsilon(\mathcal{E})$ for which there are polynomial bounds of the form $C_\epsilon \cdot d^{1+\epsilon}$ on torsion subgroups from $\mathcal{E}$.*

Project A

- Can we produce **uniform** polynomial bounds on F_0-rational geometric isogeny classes (so C_ϵ can be made independent of $\mathcal{E}$)?

Conjecture.

For each number field F_0, there exists polynomial bounds on $\mathcal{I}_{F_0}$: for each $\epsilon > 0$ there are $B := B(F_0) > 0$ and $C_\epsilon := C_\epsilon(F_0) > 0$ such that for all $E_{/F} \in \mathcal{I}_{F_0}$ one has

$$\exp E(F)[\text{tors}] \leq C_\epsilon \cdot d^{B+\epsilon}.$$

- For $E_{/F} \in \mathcal{I}_{\mathbb{Q}}$ with $[F : \mathbb{Q}]$ odd, one has

$$\#E(F)[\text{tors}] \leq 720720\sqrt{35} \cdot [F : \mathbb{Q}]^{1/2}$$

(consequence of Bourdon and Najman, 2022).

Project B

Replace elliptic curves with abelian varieties:

Conjecture.

Fix a number field F_0 and an **abelian variety** A_{0/F_0} *of dimension* $g \in \{2, 6\} \cup \{\text{odd } \ n \in \mathbb{Z}^+\}$. *Then there exists polynomial bounds on the geometric isogeny class of* A_{0/F_0}.

- Would need analogous results on N-adic indices of isogenous abelian varieties, as well as an open image theorem for $\rho_{A_0,N}\colon G_{F_0} \to \mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$.
  - The latter exists for PPAV's A_{0/F_0} with $\mathrm{End}(A_0) = \mathbb{Z}$ and $\dim(A_0) \in \{2, 6\} \cup \{\text{odd } n \in \mathbb{Z}^+\}$ (Serre, 1986).

Project C

Recall

$$\mathcal{I}_{F_0} := \{E_{/F} : E \text{ is } \overline{\mathbb{Q}}\text{-isogenous to some } E' \text{ with } j(E') \in F_0\}.$$

Theorem 2 (G., 2022).

$\mathcal{I}_{F_0}$ *is* **typically bounded in torsion.**

- The study of $\mathcal{I}_{F_0}$ is originally motivated by a study of $\mathbb{Q}$-**curves.**
- Let us define the family of F_0-**curves**

$$\mathcal{Q}_{F_0} := \{E_{/F} : \forall \sigma \in G_{F_0},\ E \text{ is } \overline{\mathbb{Q}}\text{-isogenous to } E^{\sigma}{}_{/\sigma(F)}\}.$$

- "Geometrically isogenous to Galois conjugates".
- We have

$$\mathcal{I}_{F_0} \subseteq \mathcal{Q}_{F_0}.$$

Conjecture.

The family $\mathcal{Q}_{\mathbb{Q}}$ is typically bounded in torsion.

Thank you!