Growth of Torsion Groups of Elliptic Curves in Geometric Isogeny Classes

Tyler Genao

arXiv's: 2409.08214, 2112.11566

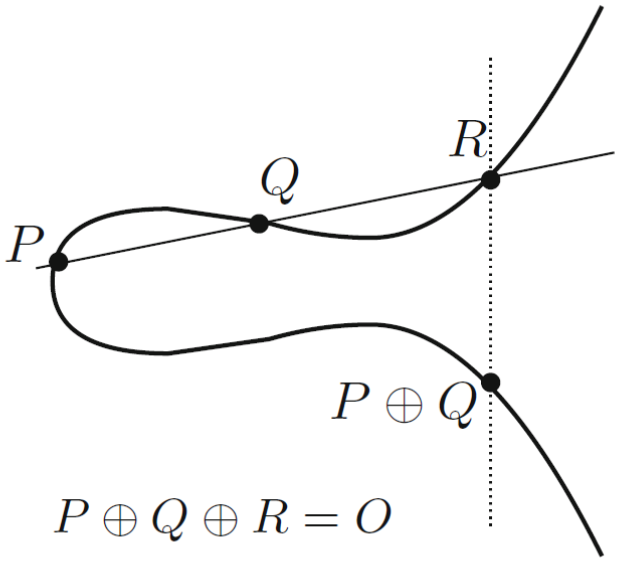
The Ohio State University

AMS Fall Eastern Virtual Sectional Meeting
October 26, 2025

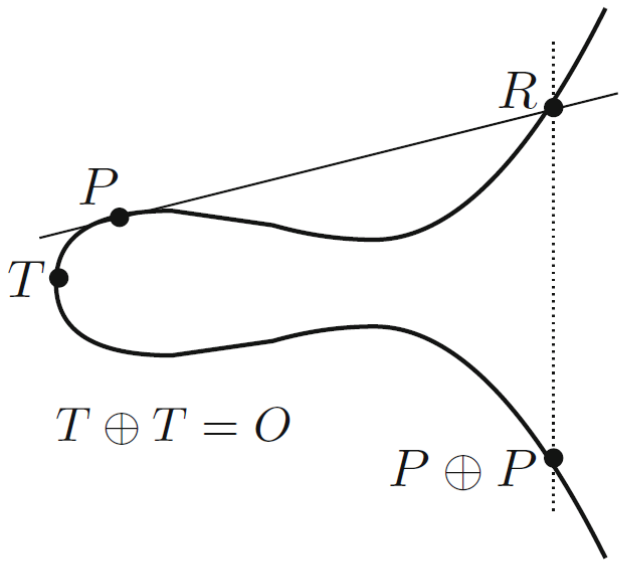
- For a field k, an *elliptic curve* E/k is a curve in k^2 defined by an equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

  where each $a_i \in k$, with a discriminant condition $\Delta \neq 0$.
- The most remarkable property of an elliptic curve is that the set $E(k)$ of k-rational points on E is an *abelian group:*



Addition of distinct points



Adding a point to itself

Figure 3.3: The composition law.

Figure: The chord and tangent method on an elliptic curve $E/\mathbb{R}$ in Weierstrass form. From Silverman's "The Arithmetic of Elliptic Curves."

- More can be said about the group structure of the *Mordell-Weil group* $E(k)$ when $k = F$ is a *number field* (finite degree extension of $\mathbb{Q}$).

Theorem (Mordell-Weil Theorem).

For a number field F and for any elliptic curve E/F, the group $E(F)$ is a **finitely generated** *abelian group: there exist points $P_1, P_2, \ldots, P_k \in E(F)$ such that for all $P \in E(F)$, one has*

$$P = n_1 P_1 \oplus n_2 P_2 \oplus \ldots \oplus n_k P_k$$

for some $n_1, n_2, \ldots, n_k \in \mathbb{Z}$.

- By the structure theorem for finitely generated abelian groups, this theorem implies that

$$E(F) \cong \mathbb{Z}^r \oplus E(F)[\text{tors}]$$

  for some integer $r \geq 0$ and some finite group $E(F)[\text{tors}]$.
- $E(F)[\text{tors}]$ is called the **torsion subgroup** of E over F. It is a finite abelian group.
- **What do we know about $E(F)$[tors] as E/F varies?**

- Here is a classic result on rational torsion groups due to Mazur.

Theorem (Mazur, 1977).

Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})[\text{tors}]$ is isomorphic to one of the following 15 groups:

$$\mathbb{Z}/N\mathbb{Z} \qquad N = 1, 2, \ldots, 10, 12,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} \qquad N = 1, 2, 3, 4.$$

- In this case, we have $\#E(\mathbb{Q})[\text{tors}] \leq 16$.

- There have been extensions to quadratic and cubic number fields, too:

Theorem (Kenku-Momose, 1988; Kamienny, 1992).

Let K be a quadratic number field and let E/K be an elliptic curve. Then $E(K)$[tors] is isomorphic to one of the following 26 groups:

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} && N = 1, 2, \ldots, 16, 18, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} && N = 1, 2, \ldots, 6, \\ &\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z} && N = 1, 2, \\ &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

- $\therefore \#E(K)[\text{tors}] \leq 24$ when $K/\mathbb{Q}$ is quadratic.

Theorem (Derickx, Etropolski, van Hoeij, Morrow, Zureick-Brown, 2021).

Let F be a cubic number field and let E/F be an elliptic curve. Then $E(F)$[tors] is isomorphic to one of the following 26 groups:

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} && 1, 2, \ldots, 16, 18, 20, 21, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} && N = 1, 2, \ldots, 7. \end{aligned}$$

- $\therefore \#E(F)[\text{tors}] \leq 28$ when $F/\mathbb{Q}$ is cubic.

- In general, $E(F)[\text{tors}]$ can be arbitrarily large when $[F : \mathbb{Q}]$ is arbitrarily large.
- However, when $[F : \mathbb{Q}]$ is bounded, so are torsion group 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

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

- Therefore, there is a "strong uniform boundedness" in torsion groups of elliptic curves over number fields.

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

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

- Explicitly, Merel gave a bound on $p \mid \#E(F)[\text{tors}]$ in terms of $d > 1$ (1996):

$$p \mid \#E(F)[\text{tors}] \Rightarrow p \leq d^{3d^2}.$$

- Parent later improved this (1999):

$$p^k \mid \#E(F)[\text{tors}] \Rightarrow p^k \leq 129(5^d - 1)(3d)^6.$$

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

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

- Can we sharpen the bounds B?
- Sharper bounds are currently not known, but we *can* do better once restricting to **special families** of elliptic curves.
- We will start with considering the family of elliptic curves with **complex multiplication** (or **CM** for short), which we denote by $\mathcal{F}_{\mathrm{CM}}$.
- CM elliptic curves have *endomorphism rings* are strictly larger than $\mathbb{Z}$.

Theorem (Clark and Pollack, 2015).

There exists an absolute, effectively computable constant $c \in \mathbb{Z}^+$ *such that for all number fields* $F/\mathbb{Q}$ *with* $d := [F : \mathbb{Q}] \geq 3$ *and for all CM elliptic curves* E/F*, one has*

$$\#E(F)[\text{tors}] \leq c \cdot d \log\log d.^*$$

**Here,* log *stands for* ln.

- Thus, for all $\epsilon > 0$, one has for CM elliptic curves E/F that

$$\#E(F)[\text{tors}] \ll_\epsilon d^{1+\epsilon}.$$

This is an example of a **polynomial bound.**

- Torsion groups of CM elliptic curves also exhibit "Merel-like" behavior in another way:

Theorem (Bourdon, Clark and Pollack, 2017).

For each $\epsilon > 0$, there exists a constant $B_\epsilon > 0$ such that the set

$$\{d \in \mathbb{Z}^+ : \exists F/\mathbb{Q} \text{ with } [F:\mathbb{Q}] = d \text{ and CM } E/F \text{ with } \#E(F)[\text{tors}] > B_\epsilon\}$$

has upper density $\leq \epsilon$.

- In particular, for each $0 < \epsilon < 1$, there is a bound B_ϵ which bounds torsion groups of CM elliptic curves, over a subset of degrees in $\mathbb{Z}^+$ of upper density $\geq 1 - \epsilon$.
- We say here that torsion groups of CM elliptic curves are **typically bounded.**

- Thus, our two types of torsion bounds on $\mathcal{F}_{\mathrm{CM}}$ are:
  1. Polynomial bounds;
  2. Typical bounds.
- By the above results, torsion groups of non-CM elliptic curves are more mysterious.
- One place to start studying non-CM torsion is in the family $\mathcal{F}_{\mathbb{Q}}$ of elliptic curves E/F with $\mathbb{Q}$-rational j-invariant:

$$\mathcal{F}_{\mathbb{Q}} := \{E/F : j(E) \in \mathbb{Q}\}.$$

Theorem (Clark and Pollack, 2018).

For all $\epsilon > 0$, there exists a constant $c_\epsilon > 0$ such that for all elliptic curves E/F with $j(E) \in \mathbb{Q}$, one has

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

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

Theorem (Clark, Milosevic and Pollack, 2018).

For each $\epsilon > 0$, there exists a constant $B_\epsilon > 0$ such that the set

$$\{d \in \mathbb{Z}^+ : \exists F/\mathbb{Q} \text{ with } [F : \mathbb{Q}] = d \text{ and CM } E/F \text{ with } \#E(F)[\text{tors}] > B_\epsilon\}$$

has upper density $\leq \epsilon$.

- Thus, like $\mathcal{F}_{\mathrm{CM}}$, the family $\mathcal{F}_{\mathbb{Q}}$ is both **polynomially bounded** and **typically bounded** in torsion.

- Torsion in $\mathcal{F}_{\mathbb{Q}}$ behaves well since it is intimately connected to torsion of *rational* elliptic curves, as well as their *Galois representations*, which are relatively well-understood.
- Our next family is a generalization of $\mathcal{F}_{\mathbb{Q}}$.
- For elliptic curves E, E' defined over $\overline{\mathbb{Q}}$, an isogeny $\phi\colon E \to E'$ defined over $\overline{\mathbb{Q}}$ is called a **geometric isogeny.**
- "Being geometrically isogenous" is an equivalence relation. An equivalence class here is called a **geometric isogeny class.**
- Unlike a rational isogeny class, a geometric isogeny class is *infinite.*

- Let us define

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

- $\mathcal{I}_{\mathbb{Q}}$ is the union over all *rational* geometric isogeny classes (those which contain at least one rational elliptic curve).
- We have $\mathcal{F}_{\mathbb{Q}} \subsetneq \mathcal{I}_{\mathbb{Q}}$; in fact, $\mathcal{I}_{\mathbb{Q}}$ contains elliptic curves with j-invariants of arbitrarily large degree over $\mathbb{Q}$.

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

Here is some context for the family $\mathcal{I}_{\mathbb{Q}}$.

- Torsion groups of (non-CM) elliptic curves $E/F \in \mathcal{I}_{\mathbb{Q}}$ behave very similarly to elliptic curves over $\mathbb{Q}$:
- By work of Cremona and Najman, if $[F : \mathbb{Q}]$ is a prime ≥ 11, then $E(F)[\text{tors}]$ is one of the 15 abelian groups from Mazur's torsion theorem over $\mathbb{Q}$.

$$\mathcal{F}_{\mathbb{Q}} := \{E/F : j(E) \in \mathbb{Q}\}.$$

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

The family $\mathcal{I}_{\mathbb{Q}}$ is a special subfamily of $\mathbb{Q}$-*curves:*

$$\mathcal{F}_{\mathbb{Q}} \subsetneq \mathcal{I}_{\mathbb{Q}} \subsetneq \mathcal{Q}_{\mathbb{Q}},$$

where

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

is the family of $\mathbb{Q}$-**curves.** We also have $\mathcal{Q}_{\mathbb{Q}} \supsetneq \mathcal{F}_{\mathrm{CM}}$.

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

- $\mathbb{Q}$-curves appear when studying solutions to Fermat-type equations. They are in analogy to *Frey curves*, which are curves over $\mathbb{Q}$ induced from (hypothetical) rational solutions to the Fermat equation $x^n + y^n = z^n$ where $n \geq 3$; these are crucial in the proof of Fermat's Last Theorem.
- These curves also have applications in cryptography. For example, they can be used to speed up computations for explicit isogenies between two isogenous supersingular elliptic curves defined over a finite field.
- The elliptic curves in $\mathcal{I}_{\mathbb{Q}}$ are called *rational* $\mathbb{Q}$-curves.

Here are our new results on $\mathcal{I}_{\mathbb{Q}}$:

Theorem 1 (Bourdon, G., 2025).

Torsion from $\mathcal{I}_{\mathbb{Q}}$ is **polynomially bounded.** *More precisely, for each $\epsilon > 0$, there exists $c_\epsilon > 0$ such that for any elliptic curve $E/F \in \mathcal{I}_{\mathbb{Q}}$, one has*

$$\#E(F)[\mathrm{tors}] \leq c_\epsilon \cdot d^{3+\epsilon}$$

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

- Towards this result, we prove new lower bounds on degrees of fields of definition of points on *modular curves:*

- Let $X_1(n)$ denote the *modular curve* which is a moduli space for elliptic curves $E/\overline{\mathbb{Q}}$ with a point $P \in E(\overline{\mathbb{Q}})$ of order n. Points on $X_1(n)$ have the form $x = [E, P] \in X_1(n)$.

Theorem 2 (Bourdon, G., 2025).

Suppose $n \in \mathbb{Z}^+$ is divisible only by primes $\ell > 37$. Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Then for any $x = [E, P] \in X_1(n)$, one has

$$\deg(x) \geq \frac{1}{24^k} \cdot \frac{1}{2} \cdot n^2 \cdot \prod_{\ell \mid n} \left(1 - \frac{1}{\ell^2}\right)$$

where k is the number of exceptional primes of $E/\mathbb{Q}$. This is what $\deg(X_1(n) \to X(1))$ is.

I have also shown that $\mathcal{I}_{\mathbb{Q}}$ is **typically bounded** in torsion.

Theorem 3 (G., 2023).

For each $\epsilon > 0$, there exists a constant $B_\epsilon > 0$ such that the set

$$\{d \in \mathbb{Z}^+ : \exists F/\mathbb{Q} \text{ with } [F:\mathbb{Q}] = d, E/F \in \mathcal{I}_{\mathbb{Q}} \text{ and } \#E(F)[\text{tors}] > B_\epsilon\}$$

has upper density $\leq \epsilon$.

- Towards this, I prove new results on ℓ-adic valuations for degrees of fields of definition of cyclic isogenies.

I am currently extending this work in two ways:

1. Polynomial bounds on torsion from geometric isogeny classes of higher-dimensional abelian varieties.
   - Unlike studying $\mathcal{I}_{\mathbb{Q}}$, I am doing this "one $\overline{\mathbb{Q}}$-isogeny class at a time."
   - Polynomial bounds are closely controlled by the endomorphism algebra of the abelian variety.
2. Polynomial *and* typical bounds on torsion of $\mathbb{Q}$-curves in $\mathcal{Q}_{\mathbb{Q}} \smallsetminus \mathcal{I}_{\mathbb{Q}}$.
   - A place to start is to understand *central* $\mathbb{Q}$-curves $E/\mathbb{Q}(j(E))$. By work of Sairaiji and Yamauchi, we know that $\#E(\mathbb{Q}(j(E)))[\text{tors}]$ only has 3 types of prime divisors, one of which is related to 2-cocyles of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which are induced from isogenies between E and its Galois conjugates.

Thank you!

References (in order of appearance):

- B. Mazur, *Modular curves and the Eisenstein ideal,* Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186.
- M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 109 (1988), 125–149.
- S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. 109 (1992), 221–229.
- S. Kamienny, *Torsion points on elliptic curves over fields of higher degree*, Internat. Math. Res. Notices (1992), 129–133.
- M. Derickx, A. Etropolski, M. van Hoeij, J. Morrow and D. Zureick-Brown, *Sporadic cubic torsion*, Algebra Number Theory 15 (2021), 1837–1864.
- L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), 437–449.
- P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. 506 (1999), 85–116.
- P.L. Clark and P. Pollack, *The truth about torsion in the CM case*, C. R. Math. Acad. Sci. Paris 353 (2015), no. 8, 683–688.
- A. Bourdon, P.L. Clark and P. Pollack, *Anatomy of torsion in the CM case*, Math. Z. 285 (2017), no. 795–820.
- P.L. Clark and P. Pollack, *Pursuing polynomial bounds on torsion*, Israel J. Math 227 (2018), 889–909.
- P.L. Clark, M. Milosevic and P. Pollack, *Typically bounding torsion*, J. Number Theory 192 (2018), 150–167.
- J. Cremona and F. Najman, $\mathbb{Q}$*-curves over odd degree number fields,* Res. Number Theory 7 (2021), Paper No. 62, 30.
- F. Sairaiji and T. Yamauchi, *On rational torsion points of central* $\mathbb{Q}$*-curves*, J. Théor. Nombres Bordeaux 20 (2008), 465–483.