Research Statement

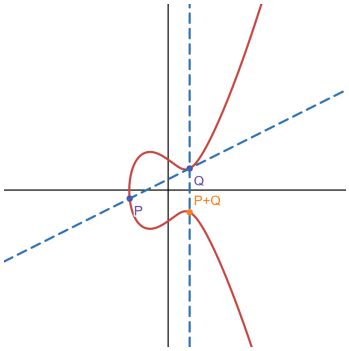
Tyler Genao

My research program is in understanding uniformity in torsion groups of elliptic curves, extending celebrated results of Mazur and Serre on torsion and Galois representations, respectively. I do this through direct computations with elliptic curve Galois representations, as well as through studying the geometry of modular curves. A big part of my work focuses on understanding torsion and representations under base change and "under isogeny."

Brief summary of work. A central part of my research is on understanding the size and behavior of torsion groups of elliptic curves over number fields whose degrees can be arbitrarily large. For example, I have proven **polynomial bounds** exist on torsion from *any fixed* geometric isogeny class of elliptic curves [Gen24b], as well as uniform polynomial bounds over *all rational* geometric isogeny classes [BG]. I've also proven the existence of **typical bounds** on torsion from the family of elliptic curves geometrically isogenous to an elliptic curve with rational j-invariant [Gen22, Gen23]. To understand **torsion growth upon base change,** I have established uniformity results for the degrees of fields of definition of torsion points [Gen24a], as well as fields of definition of isogenies [Gen], also proving results which establish possible evidence for Serre's Uniformity Question over number fields larger than $\mathbb{Q}$. I have also worked on torsion groups and Galois representations in other contexts [CGPS22, AG, GMR, FGMR].

1. Introduction

Given a field k, an **elliptic curve E over k,** written E/k, is a smooth, projective algebraic curve of genus one with a k-rational point. Elliptic curves are often given by an equation $y^2 = x^3 + Ax + B$, where $A, B \in k$. The most important property of an elliptic curve E/k is that the set $E(k)$ of its k-rational points is an *abelian group,* with a remarkably succinct group structure given by a "chord and tangent method" for adding any two points in $E(k)$ (pictured on the right). While inherently interesting, elliptic curves also enjoy a broad scope of applications, from providing a useful group structure for modern information encryption, to helping solve centuries-old problems on rational solutions to Diophantine equations.



When k is a number field (i.e., a finite extension of $\mathbb{Q}$), the Mordell-Weil theorem says that the group $E(k)$ is a *finitely generated* abelian group. In particular, the **torsion subgroup** $E(k)[\text{tors}]$, which is the subgroup of k-rational points with finite order, is a *finite abelian group.*

Here is a natural question that much of my work focuses on:

Question 1. *What do we know about the* size *of* $E(k)[\text{tors}]$*, as* E/k *varies?*

In a landmark paper, Mazur [Maz77a] showed that for any elliptic curve $E/\mathbb{Q}$, its torsion subgroup $E(\mathbb{Q})[\text{tors}]$ is one of 15 finite abelian groups up to isomorphism; this is often referred to as **Mazur's Theorem.** As a consequence of this theorem, any elliptic curve $E/\mathbb{Q}$ satisfies $\#E(\mathbb{Q})[\text{tors}] \leq \mathbf{16}$. Following this, work of Kamienny, Kenku and Momose [KM88, Kam92a, Kam92b] showed that for any elliptic curve E/k defined over a *quadratic* number field k, the torsion subgroup $E(k)[\text{tors}]$ is isomorphic to one of 26 finite abelian groups, and $\#E(k)[\text{tors}] \leq \mathbf{24}$. Almost 30 years later, Derickx et. al. [DEvH$^+$21] gave a classification of torsion subgroups over *cubic* fields: there are 26 possibilities for $E(k)[\text{tors}]$ when $[k : \mathbb{Q}] = 3$, and one has $\#E(k)[\text{tors}] \leq \mathbf{28}$.

The classification of torsion subgroups over number fields of fixed degree $d \geq 4$ is incomplete; it is an active area of research which involves deep results on the geometry of *modular curves,* which serve as a type of moduli space for elliptic curves with level structure. Nevertheless, Merel [Mer96] proved a remarkable result in the 1990's showing that torsion bounds always exist *in fixed degree d;* this is referred to as **Merel's Theorem.** More precisely, for each integer $d > 0$, there exists a constant $B := B(d)$ which depends only on d, such that for all elliptic curves E/k where $[k : \mathbb{Q}] = d$, one has $\#E(k)[\text{tors}] \leq B(d)$. Merel's work provided explicit bounds on primes $p \mid \#E(k)[\text{tors}]$ in terms of d, which Parent [Par99] later improved by showing that if $p^n \mid \#E(k)[\text{tors}]$ then $p^n \leq 129(5^d-1)(3d)^6$.

By Merel's Theorem, one can define an arithmetic function $B\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ where each $B(d)$ is a choice of torsion bound over degree d number fields. By Parent's work [Par99], one can construct an explicit function B whose growth is more than exponential in d. The growth of torsion groups of elliptic curves can then be understood through studying the asymptotic behavior of an appropriate choice of B. With this in mind, there is a natural question closely related to Question 1:

Question 2. *Which choice of bound function $B\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ is close to the* truth *of torsion growth?*

Finally, in contrast to Questions 1 and 2, one can ask whether there are uniform conditions one can impose on number field extensions ℓ/k to guarantee that elliptic curves have no torsion growth upon *base change* from k to ℓ (i.e., where we view E/k as defined over ℓ instead of k).

Question 3. *Given a number field extension ℓ/k, are there conditions on $[\ell : k]$ that guarantee the base change of any elliptic curve E/k to E/ℓ satisfies $E(\ell)[\text{tors}] = E(k)[\text{tors}]$?*

Each of the following three sections will introduce my work towards addressing Questions 1, 2 and 3:

- §2, Polynomial bounds on torsion;
- §3, typical boundedness of torsion;
- §4, torsion upon base change.

Much of my results apply to torsion subgroups from families of elliptic curves over number fields that are related to rational elliptic curves, via isogeny or base change. In this way, they can be considered generalizations of Mazur's theorem, where now the base field degree is allowed to vary. The upshot to studying these families is that one can leverage what is known about Galois representations of $\mathbb{Q}$-rational elliptic curves, to say something about torsion groups from these families. Similar families have also been recently studied by several others: see [BN, BRW, CMP18, CP18, CN21, GJN20], to name a few papers.

2. Polynomial bounds on torsion from geometric isogeny classes [Gen24b, BG].

This section concerns my work on Question 2 for families[1] of elliptic curves closed under geometric isogeny, following Merel's Theorem [Mer96]. One already has a sharp answer to Question 2 for the family of elliptic curves with *complex multiplication* (CM): by work of Clark and Pollack [CP15], there exists an absolute, effectively computable constant $c := c_{\text{CM}} \in \mathbb{Z}^+$ such that for all number fields k with degree $d \geq 3$ and for all CM elliptic curves E/k, one has

$$\#E(k)[\text{tors}] \leq c \cdot d \ln(\ln(d)).$$

[1]A *family* of elliptic curves is any collection $\mathcal{F}$ of pairs (k, E) where k is a number field and E is an elliptic curve defined over k.

In contrast to the above, the non-CM case (i.e., "without complex multiplication") is more mysterious. There are a number of conjectures and questions that appear in the literature which concern the truth of B for all elliptic curves, one of which involves bounds which are **polynomial** in the degree.

Conjecture. *There exist absolute constants $b, c > 0$ such that for any number field k of degree d and for any elliptic curve E/k, one has $\#E(k)[\text{tors}] \leq c \cdot d^b$.*

That such a bound might exist was first suggested in a question of Flexor and Oesterlé [FO90] for elliptic curves with everywhere good reduction, and the result was later established in this case by Hindry and Silverman [HS99]. More recent work of Clark and Pollack [CP18] implies there exist polynomial bounds on torsion from the family $\mathcal{F}_{\mathbb{Q}}$ of elliptic curves with $\mathbb{Q}$-*rational rational j-invariants* (i.e., elliptic curves with at least one $\mathbb{Q}$-rational model). Their results imply that for any $\epsilon > 0$ there exists a constant $c_\epsilon > 0$, *which depends only on ϵ,* such that for all degree d number fields k and for all elliptic curves $E/k \in \mathcal{F}_{\mathbb{Q}}$ one has $\#E(k)[\text{tors}] \leq c_\epsilon \cdot d^{5/2+\epsilon}$.

Inspired by the work of Flexor and Oesterlé, as well as Clark and Pollack, I have proven polynomial bounds on torsion from two families of elliptic curves, one of which generalizes $\mathcal{F}_{\mathbb{Q}}$. Recall that for two elliptic curves E_1 and E_2 defined over an algebraic extension $k/\mathbb{Q}$, a **k-rational isogeny** from E_1 to E_2, written as $\phi\colon E_1 \to E_2$, is a surjective k-rational morphism of curves that is also a group homomorphism $E_1(k) \to E_2(k)$. For two elliptic curves E_1/k_1 and E_2/k_2, a **geometric isogeny** from E_1 to E_2 is a $\overline{\mathbb{Q}}$-rational isogeny $\phi\colon E_1/\overline{\mathbb{Q}} \to E_2/\overline{\mathbb{Q}}$ (where $\overline{\mathbb{Q}}$ denotes an algebraic closure of $\overline{\mathbb{Q}}$). The collection of elliptic curves geometrically isogenous to E is called the **geometric isogeny class** of E.

My first theorem showed that polynomial bounds exist on torsion from any fixed geometric isogeny class of elliptic curves.

Theorem 1. [Gen24b] *Fix a number field k_0 and an elliptic curve E_0/k_0. Then for each $\epsilon > 0$ there exists a constant $c_\epsilon := c_\epsilon(E_0, k_0) > 0$ such that for any elliptic curve E/k geometrically isogenous to E_0/k_0, one has*

$$\#E(k)[\text{tors}] \leq c_\epsilon \cdot d^{1+\epsilon}$$

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

It is worth noting that the exponent $1 + \epsilon$ in Theorem 1 is **optimal** when one considers the family of all elliptic curves over all number fields: that is, the 1 cannot be replaced with a smaller number. A crucial step in Theorem 1 involves relating the *adelic Galois representations* of isogenous non-CM elliptic curves. Recall that for an elliptic curve E/k, its adelic Galois representation is the homomorphism

$$\rho_E\colon G_k \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

associated with the action of the absolute Galois group $G_k := \mathrm{Gal}(\overline{\mathbb{Q}}/k)$ on the full torsion subgroup $E[\text{tors}] := E(\overline{\mathbb{Q}})[\text{tors}]$; note that $E[\text{tors}]$ is a free rank two $\widehat{\mathbb{Z}}$-module, where $\widehat{\mathbb{Z}}$ is the ring of profinite integers. When E is a non-CM elliptic curve, celebrated work of Serre [Ser72] showed that the image $\rho_E(G_k)$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, which is equivalent to having finite index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$; this result is often called "Serres' open image theorem." I have proven the following result, which relates the adelic Galois representations of two isogenous elliptic curves; it serves as a crucial step in the proof of Theorem 1. This generalizes work of Greenberg [Gre12].

Theorem 2. [Gen24b] *Let E/k and E'/k be k-rationally isogenous non-CM elliptic curves. Then one has*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_k)] = [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E'}(G_k)].$$

Following this paper, in collaboration with Bourdon I have also proven a uniform version of polynomial bounds on torsion from a superfamily of $\mathcal{F}_{\mathbb{Q}}$. For a fixed number field k_0, let us define the family

$$\mathcal{I}_{k_0} := \{\text{elliptic curves } E/k : \exists E'/k_0 \text{ for which } E \text{ is geometrically isogenous to } E'\}.$$

The family $\mathcal{I}_{k_0}$ is essentially the union over all k_0-*rational* geometric isogeny classes, i.e., geometric isogeny classes which contain least one elliptic curve defined over k_0. It is clear that $\mathcal{F}_{k_0} \subseteq \mathcal{I}_{k_0}$. In fact, this is a strict containment since $\mathcal{I}_{k_0}$ contains elliptic curves whose j-invariants have arbitrarily large degree over $\mathbb{Q}$. The following theorem is a generalization of Clark and Pollack's result [CP18] for polynomial bounds on torsion from $\mathcal{F}_{\mathbb{Q}}$. This also generalizes my previous Theorem 1 to a larger family in the case of $\mathbb{Q}$-rational geometric isogeny classes.

Theorem 3. [BG] *Torsion from $\mathcal{I}_{\mathbb{Q}}$ is polynomially bounded. More precisely, for each $\epsilon > 0$ there exists a constant $c_\epsilon > 0$ such that for any elliptic curve $E/k \in \mathcal{I}_{\mathbb{Q}}$, one has*

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

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

The proof of this result involves a close analysis of fields of definition of prime-power order torsion points on $\mathbb{Q}$-rational elliptic curves. For primes $p > 37$, we know that the mod-p image of Galois is either surjective or equal to the normalizer of the non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, by [FL]. In the latter case, we can provide novel lower bounds on the degree of the field of definition via an analysis of ramification indices, and from this we obtain a nearly optimal power bound.

Following my work above, there is a more general problem I am working on. Recall that an **abelian variety over k,** denoted by A/k, is a smooth connected projective algebraic group variety defined over k. Abelian varieties are higher-dimensional analogs of elliptic curves; when k is a number field, their torsion groups $A(k)[\text{tors}]$ are also finite abelian groups by the Mordell-Weil theorem.

Problem 1. *For a fixed abelian variety A_0/k_0, show there exist polynomial bounds on torsion groups of abelian varieties A/k which are geometrically isogenous to A_0/k_0.*

When E/k is an elliptic curve, its endomorphism algebra $\mathrm{End}^0(E) := \mathrm{End}_{\overline{\mathbb{Q}}}(E) \otimes \mathbb{Q}$ is either $\mathbb{Q}$ or an imaginary quadratic field. In the latter case, E has CM, and polynomial bounds are already known [CP15]; and when E is non-CM, my Theorem 1 solves this problem. However, when one replaces E/k by an abelian variety A/k, "non-CM" and "CM" are two ends of a spectrum of possible structures for the $\mathbb{Q}$-algebra $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}$, which complicates an analysis of the torsion group $A(k)[\text{tors}]$.

I am tackling Problem 1 by proving an appropriate generalization of Theorem 2 on adelic indices. It is crucial to the proof of Theorem 2 that when E is a non-CM elliptic curve, the adelic Galois representation $\rho_E \colon G_k \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ has open image in its codomain $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. However, for an abelian variety A/k of dimension $g > 1$, the adelic representation $\rho_A \colon G_k \to \mathrm{GL}_{2g}(\widehat{\mathbb{Z}})$ will *never* have open image – equivalently, the index $[\mathrm{GL}_{2g}(\widehat{\mathbb{Z}}) : \rho_A(G_k)]$ is infinite. Despite this, the image $\rho_A(G_k)$ *will* be open in a particular reductive lie group which depends only on $\mathrm{End}^0(A)$.

To this end, I will prove an appropriate generalization of Theorem 2 for abelian varieties with fixed endomorphism algebra X where suitable "open image theorems" are known for $\rho_A(G_k)$ relative to X, and then generalize the proof of Theorem 1 appropriately. The varieties studied will include, for example, simple abelian varieties for which $\mathrm{End}^0(A) = \mathbb{Q}$ ("trivial endomorphism ring"; here, the adelic image $\rho_A(G_k)$ is open in the general symplectic group $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ when e.g. g is $2, 6$ or

odd, due to Serre [Sti17]), and for which $\mathrm{End}^0(A)$ is a totally real field of degree g ("real GL_2-type"; here, an open image theorem was proven by Ribet [Rib76]). I will prove various analogs of Theorem 2 relative to the endomorphism algebras considered, which can then be applied to produce polynomial bounds on torsion from geometric isogeny classes by mimicking the central ideas of the proof of Theorem 1.

3. Typically bounding torsion from geometric isogeny classes [Gen22, Gen23]

This section concerns my work on Question 1 for the families $\mathcal{F}_{k_0}$ and $\mathcal{I}_{k_0}$, for all number fields k_0; in particular, I have shown these families are *typically bounded in torsion.* Let us recall that any subset $S \subseteq \mathbb{Z}^+$ has a well-defined upper density

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

Then given a family $\mathcal{F}$ of elliptic curves defined over number fields, we say that $\mathcal{F}$ is **typically bounded in torsion** if for all $\epsilon > 0$ there exists a constant $B_\epsilon > 0$ such that the set of "bad degrees"

$$\{d \in \mathbb{Z}^+ : \exists E/k \in \mathcal{F} \text{ so that } [k : \mathbb{Q}] = d \text{ and } \#E(k)[\mathrm{tors}] \geq B_\epsilon\}$$

has upper density at most ϵ. Informally stated, $\mathcal{F}$ is typically bounded in torsion if torsion groups of elliptic curves from $\mathcal{F}$ are **absolutely bounded** after excluding the curves $E/k \in \mathcal{F}$ whose number field degrees $[k : \mathbb{Q}]$ lie in an arbitrarily small subset of $\mathbb{Z}^+$. Unlike polynomial bounds, "typical bounds" on torsion groups do not grow, even as the degrees $[k : \mathbb{Q}]$ get arbitrarily large. In this sense, typical bounds, when they exist, are a generalization of the bounds from Merel's Theorem.

Typical boundedness in torsion was first observed in the family of CM elliptic curves, by Bourdon, Clark and Pollack [BCP17]. Soon after this, Clark, Milosevic and Pollack showed [CMP18] that for a number field k_0, the family $\mathcal{F}_{k_0}$ of elliptic curves with **k_0-rational j-invariant** is typically bounded in torsion if one assumes the LV-hypotheses for k_0. Here is what we mean by the **LV-hypotheses for k_0:**

1. assume that the Generalized Riemann Hypothesis (GRH) is true;
2. assume that k_0 has *no rationally defined CM,* i.e., that k_0 contains no Hilbert class fields of imaginary quadratic fields.

Under these hypotheses, Larson and Vaintrob [LV14] have shown that for sufficiently large primes $p \in \mathbb{Z}^+$ there do not exist elliptic curves with a k_0-rational p-isogeny (kernel has size p).

When k_0 satisfies the LV-hypotheses, Clark, Milosevic and Pollack [CMP18] have shown that $\mathcal{F}_{k_0}$ is typically bounded in torsion. My first result on typical boundedness made this theorem **unconditional** of the LV-hypotheses.

Theorem 4. [Gen22] *For each number field k_0, the family $\mathcal{F}_{k_0}$ is typically bounded in torsion.*

A key idea in proving Theorem 4 is to analyze the *isogeny character* of an elliptic curve defined over k_0, and relate it to that of a CM elliptic curve. This builds on work of Larson and Vaintrob [LV14], and utilizes the fact that more precise results are known about torsion groups and Galois representations of CM elliptic curves relative to the non-CM case. An **isogeny character** of an elliptic curve E/k is a group representation arising from the action of the absolute Galois group G_k on a finite cyclic subgroup of $E[\mathrm{tors}]$; this can be thought of as a one-dimensional analog of the

usual mod-n Galois representation $\rho_{E,n}\colon G_k \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, which describes the action of G_k on the group $E[n]$ of points with order dividing n.

In a sequel paper, I generalized Theorem 4 to **all k_0-rational geometric isogeny classes.** Recall from §2 that $\mathcal{I}_{k_0}$ is the family of elliptic curves which are geometrically isogenous to at least one k_0-rational elliptic curve.

Theorem 5. [Gen23] *For each number field k_0, the family $\mathcal{I}_{k_0}$ is typically bounded in torsion.*

Following my work on typical boundedness for $\mathcal{F}_{k_0}$ and $\mathcal{I}_{k_0}$, there is a natural extension to a larger family of curves, namely that of *k_0-curves.* Given an automorphism $\sigma \in G_{k_0}$, for each elliptic curve E/k one has a "conjugated" elliptic curve $E^\sigma/\sigma(k)$ by applying σ to the coefficients of E. Let us define the family of **k_0-curves** as

$$\mathcal{Q}_{k_0} := \{\text{elliptic curves } E/k : \forall \sigma \in G_{k_0},\ E \text{ is geometrically isogenous to } E^\sigma\}.$$

We have the strict inclusions

$$\mathcal{F}_{k_0} \subsetneq \mathcal{I}_{k_0} \subsetneq \mathcal{Q}_{k_0}.$$

When $k_0 = \mathbb{Q}$, the family $\mathcal{Q}_{\mathbb{Q}}$ is the family of **$\mathbb{Q}$-curves.** These curves have extensive use in solving Fermat-type equations via the "modular method" [Ell04, BEN10, AS16].

Given that $\mathcal{F}_{\mathbb{Q}}$ and $\mathcal{I}_{\mathbb{Q}}$ are typically bounded in torsion, there is a natural problem following Theorems 4 and 5.

Problem 2. *Show that the family $\mathcal{Q}_{\mathbb{Q}}$ is typically bounded in torsion.*

A positive answer to this problem may be suggested in part by the fact that Galois representations of $\mathbb{Q}$-curves enjoy several uniformity results. For example, there is a strong uniform bound on degrees of cyclic isogenies of $\mathbb{Q}$-curves over odd degree number fields, due to Cremona and Najman [CN21]. Additionally, Le Fourn [LF16] has shown that over any fixed imaginary quadratic field K, one has for any non-CM $\mathbb{Q}$-curve $E/k \in \mathcal{Q}_{\mathbb{Q}} \smallsetminus \mathcal{I}_{\mathbb{Q}}$ and for all sufficiently large primes $p \in \mathbb{Z}^+$ that E has surjective mod-p Galois representation. Given these facts, one might also expect qualitative uniformity results on degrees of p-primary torsion points on non-CM $\mathbb{Q}$-curves, from which one may be able to apply the techniques of [Gen22, Gen23] to show that $\mathcal{Q}_{\mathbb{Q}}$ is typically bounded in torsion.

4. Torsion upon base change [Gen24a, Gen]

Given an elliptic curve E/k, it is interesting to ask what is known about the field extensions of k over which E obtains new torsion points. For example, by current progress towards Serre's Uniformity Question [FL], one knows that for any non-CM elliptic curve $E/\mathbb{Q}$ and for any prime $p > 37$, the image of the mod-p Galois representation $\rho_{E,p}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ either surjects onto $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, or equals the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Consequently, the action of $G_{\mathbb{Q}}$ on $E[p]$ is transitive, and so nontrivial torsion points $P \in E[p]$ have maximal degree: $[\mathbb{Q}(P) : \mathbb{Q}] = p^2 - 1$. In particular, over any *odd* degree number field $k/\mathbb{Q}$, there exist no elliptic curves $E/\mathbb{Q}$ with points of order p defined over k.

One can generalize this observation to account for all possible torsion growth in the following way. With our current computational and theoretical understanding of mod-p Galois representations of elliptic curves, we can show that for any elliptic curve $E/\mathbb{Q}$ and for any torsion point $P \in E[\mathrm{tors}]$, if $P \notin E(\mathbb{Q})$ then $[\mathbb{Q}(P) : \mathbb{Q}]$ is a multiple of $2, 3, 5$ or 7. Consequently:

Theorem. [GJN20] *Let k be a number field whose degree $[k:\mathbb{Q}]$ is coprime to $2\cdot 3\cdot 5\cdot 7 = 210$. Then for any elliptic curve $E/\mathbb{Q}$, one has no torsion growth upon base change to k, i.e.,*

$$E(k)[\text{tors}] = E(\mathbb{Q})[\text{tors}].$$

An analogous result where we replace $\mathbb{Q}$ with a larger number field k would require a better understanding of the behavior of elliptic curve Galois representations over k, and in general, much less is known about uniformity beyond $\mathbb{Q}$. However, I have proven such a generalization for all number fields k which satisfy the *LV-hypotheses* defined in §3. More precisely:

Theorem 6. [Gen24a] *Let k be a number field with no rationally defined CM. Then assuming GRH, there exists an effectively computable integer $B := B(k) \in \mathbb{Z}^+$ such that for any number field ℓ/k whose degree $[\ell:k]$ is coprime to B, one has for all elliptic curves E/k that*

$$E(\ell)[\text{tors}] = E(k)[\text{tors}].$$

Towards proving Theorem 6, I have given new evidence towards Serre's Uniformity Question over number fields. In particular, I have shown that for sufficiently large primes $p \in \mathbb{Z}^+$ with respect to k, if the mod-p Galois representation $\rho_{E,p}\colon G_k \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is *not* surjective, then the image $\rho_{E,p}(G_k)$ lands in the normalizer of a Cartan group in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and is "relatively uniformly large." More precisely:

Theorem 7. [Gen24a] *Let k be a number field with no rationally defined CM. Then assuming GRH, there exists a constant $c := c(k) \in \mathbb{Z}^+$ such that for all primes $p > c$, one has the following: for an elliptic curve E/k, if the mod-p image $G := \rho_{E,p}(G_k)$ does not equal $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, then it is contained in the normalizer of a Cartan group in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ up to conjugacy.*

Let $C_s(p)$ and $C_{ns}(p)$ denote split and nonsplit Cartan groups in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, respectively, and $N_s(p)$ and $N_{ns}(p)$ their normalizers. Then one of the following holds:

1. *If $G \subseteq N_s(p)$ then $C_s(p)^e \subseteq G$ for some $e \in \{1,2,3,4,6\}$, and G contains the subgroup of scalar matrices. Furthermore, the index of G in $N_s(p)$ satisfies*
$$[N_s(p) : G] \mid \gcd(p-1, e).$$
2. *If $G \subseteq N_{ns}(p)$ then either $G = N_{ns}(p)$ or G is an explicit index 3 subgroup of $N_{ns}(p)$. If $p \equiv 1 \pmod 3$ then $G = N_{ns}(p)$.*

In parallel to understanding torsion points, it is of interest to understand rationality of isogenies of elliptic curves. For a non-CM elliptic curve E/k, there is essentially a correspondence between k-rational isogenies from E, and cyclic subgroups $C \subseteq E[\text{tors}]$ which are stable under the action of G_k. With existing computational and theoretical results on Galois representations over $\mathbb{Q}$, one can prove the following.

Theorem. *For any number field $k/\mathbb{Q}$ whose degree $[k:\mathbb{Q}]$ is coprime to $2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 37 = 18888870$ and for any non-CM elliptic curve $E/\mathbb{Q}$, if E has a k-rational cyclic isogeny ϕ, then ϕ must be $\mathbb{Q}$-rational.*

Leveraging work on Galois representations over number fields (such as Theorem 7), I have also generalized this result from $\mathbb{Q}$ to those k which satisfy the LV-hypotheses. This also generalizes Theorem 6.

Theorem 8. [Gen] *Let k be a number field with no rationally defined CM. Then assuming GRH, there exists an effectively computable integer $C := C(k) \in \mathbb{Z}^+$ such that for any number field ℓ/k whose degree $[\ell:k]$ is coprime to C and for any non-CM elliptic curve E/k, if E has a ℓ-rational cyclic isogeny ϕ, then ϕ must be k-rational.*

Theorems 6, 7 and 8 can be viewed as progress towards *Mazur's Program B,* alongside work of Merel [Mer96] and Larson and Vaintrob [LV14]. This program, established in 1977 by Mazur [Maz77b], aims to classify the image of adelic Galois representations of elliptic curves over number fields.

Both Theorems 6 and 8 impose the LV-hypotheses on the fixed number field k in order to utilize Theorem 7, and show that $\rho_{E,p}(G_k)$ is relatively uniformly large when p is sufficiently large. The upshot is that in the analysis of $\rho_{E,p}(G_k)$, one can exclude the case where $\rho_{E,p}(G_k)$ is *Borel,* i.e., is contained in the subgroup $B_0(p)$ of upper triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ (up to conjugacy); this is precisely the case where E has a k-rational p-isogeny.

There is a natural follow-up problem to make these results **unconditional of the LV-hypotheses** in the case of non-CM elliptic curves. This requires us to better understand fields of definition of torsion points and isogenies in the case where a non-CM elliptic curve E/k has a k-rational p-isogeny.

Problem 3. *Let k be any number field, and assume that E/k is a non-CM elliptic curve with a k-rational p-isogeny, where p is large. What can be said about the index $[B_0(p) : \rho_{E,p}(G_k)]$ (and more generally, $\rho_{E,p}(G_k)$)?*

I gave one answer to Problem 3 in [Gen]: I showed that under GRH, for any number field k and for all sufficiently large primes p, if E/k has a k-rational p-isogeny then (up to conjugacy) the index

$$[B_0(p) : \rho_{E,p}(G_k)] \mid 864 \cdot [k : \mathbb{Q}].$$

However, unlike the index bounds in Theorem 7, this one is too large to prove Theorem 6 unconditionally. I would like to sharpen these bounds to generalize Theorem 6, and include them in a version of Theorem 7 that would serve as unconditional progress towards Serre's Uniformity Question/Mazur's Program B over a general number field k. I can reduce this analysis to studying the characters of the semisimplification of $\rho_{E,p}(G_k)$ over the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$, and then possibly refine the techniques I used in [Gen22] à la Larson and Vaintrob [LV14] to impose uniform bounds on the indices of these characters, which would provide a bound on the size of $[B_0(p) : \rho_{E,p}(G_k)]$.

References

[AG] Sam Allen and Tyler Genao, *Uniform bounds on small division fields of elliptic curves*, draft available at `https://tylergenao.wordpress.com/wp-content/uploads/2025/08/allen_genao_uniformboundsonsmalldivisionfields_aug25_2025.pdf`.

[AS16] Samuele Anni and Samir Siksek, *Modular elliptic curves over real abelian fields and the generalized Fermat equation $x^{2\ell} + y^{2m} = z^p$*, Algebra Number Theory **10** (2016), no. 6, 1147–1172. MR 3544293

[BCP17] Abbey Bourdon, Pete L. Clark, and Paul Pollack, *Anatomy of torsion in the CM case*, Math. Z. **285** (2017), no. 3-4, 795–820. MR 3623731

[BEN10] Michael A. Bennett, Jordan S. Ellenberg, and Nathan C. Ng, *The Diophantine equation $A^4 + 2^\delta B^2 = C^n$*, Int. J. Number Theory **6** (2010), no. 2, 311–338. MR 2646760

[BG] Abbey Bourdon and Tyler Genao, *Uniform polynomial bounds on torsion from rational geometric isogeny classes*, preprint available at https://arxiv.org/abs/2409.08214.

[BN] Abbey Bourdon and Filip Najman, *Sporadic points of odd degree on $X_1(N)$ coming from $\mathbb{Q}$-curves*, preprint available at `https://arxiv.org/abs/2107.10909`.

[BRW] Abbey Bourdon, Nina Ryalls, and Lori D. Watson, *Minimal torsion curves in geometric isogeny classes*, preprint available at `https://arxiv.org/abs/2407.14322`.

[CGPS22] Pete L. Clark, Tyler Genao, Paul Pollack, and Frederick Saia, *The least degree of a CM point on a modular curve*, J. Lond. Math. Soc. (2) **105** (2022), no. 2, 825–883. MR 4400938

[CMP18] Pete L. Clark, Marko Milosevic, and Paul Pollack, *Typically bounding torsion*, J. Number Theory **192** (2018), 150–167. MR 3841549

[CN21] J. E. Cremona and Filip Najman, *$\mathbb{Q}$-curves over odd degree number fields*, Res. Number Theory **7** (2021), no. 4, Paper No. 62, 30. MR 4314224

[CP15] Pete L. Clark and Paul Pollack, *The truth about torsion in the CM case*, C. R. Math. Acad. Sci. Paris **353** (2015), no. 8, 683–688. MR 3367634

[CP18] ———, *Pursuing polynomial bounds on torsion*, Israel J. Math. **227** (2018), no. 2, 889–909. MR 3846346

[DEvH+21] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown, *Sporadic cubic torsion*, Algebra Number Theory **15** (2021), no. 7, 1837–1864. MR 4333666

[Ell04] Jordan S. Ellenberg, *Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$*, Amer. J. Math. **126** (2004), no. 4, 763–787. MR 2075481

[FGMR] Kate Finnerty, Tyler Genao, Jacob Mayle, and Rakvi, *The possible adelic indices for elliptic curves admitting a rational cyclic isogeny*, draft available upon request.

[FL] Lorenzo Furio and Davide Lombardo, *Serre's uniformity question and proper subgroups of $c_{ns}^+(p)$*, preprint available at `https://arxiv.org/abs/2305.17780`.

[FO90] M. Flexor and J. Oesterlé, *Sur les points de torsion des courbes elliptiques*, no. 183, 1990, Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988), pp. 25–36. MR 1065153

[Gen] T. Genao, *New isogenies of elliptic curves over number fields*, accepted to Int. J. Number Theory. Preprint available at `https://www.worldscientific.com/doi/10.1142/S1793042125501143`.

[Gen22] Tyler Genao, *Typically bounding torsion on elliptic curves with rational j-invariant*, J. Number Theory **238** (2022), 823–841. MR 4430120

[Gen23] ———, *Typically bounding torsion on elliptic curves isogenous to rational j-invariant*, Proc. Amer. Math. Soc. **151** (2023), no. 5, 1907–1914. MR 4556187

[Gen24a] ———, *Growth of torsion groups of elliptic curves upon base change from number fields*, Ramanujan J. **63** (2024), no. 2, 409–429. MR 4694514

[Gen24b] ———, *Polynomial bounds on torsion from a fixed geometric isogeny class of elliptic curves*, J. Théor. Nombres Bordeaux **36** (2024), no. 2, 661–670. MR 4830946

[GJN20] Enrique González-Jiménez and Filip Najman, *Growth of torsion groups of elliptic curves upon base change*, Math. Comp. **89** (2020), no. 323, 1457–1485. MR 4063324

[GMR] Tyler Genao, Jacob Mayle, and Jeremy Rouse, *A uniform bound on the smallest surjective prime of an elliptic curve*, preprint available at `https://arxiv.org/abs/2501.02345`.

[Gre12] Ralph Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny*, Amer. J. Math. **134** (2012), no. 5, 1167–1196. MR 2975233

[HS99] Marc Hindry and Joseph Silverman, *Sur le nombre de points de torsion rationnels sur une courbe elliptique*, C. R. Acad. Sci. Paris Sér. I Math. **329** (1999), no. 2, 97–100. MR 1710502

[Kam92a] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229. MR 1172689

[Kam92b] ———, *Torsion points on elliptic curves over fields of higher degree*, Internat. Math. Res. Notices (1992), no. 6, 129–133. MR 1167117

[KM88] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. MR 931956

[LF16] Samuel Le Fourn, *Surjectivity of Galois representations associated with quadratic $\mathbb{Q}$-curves*, Math. Ann. **365** (2016), no. 1-2, 173–214. MR 3498908

[LV14] Eric Larson and Dmitry Vaintrob, *Determinants of subquotients of Galois representations associated with abelian varieties*, J. Inst. Math. Jussieu **13** (2014), no. 3, 517–559, With an appendix by Brian Conrad. MR 3211798

[Maz77a] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978), With an appendix by Mazur and M. Rapoport. MR 488287

[Maz77b] ———, *Rational points on modular curves*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Lecture Notes in Math., Vol. 601, Springer, Berlin-New York, 1977, pp. 107–148. MR 450283

[Mer96] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449. MR 1369424

[Par99] Pierre Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85–116. MR 1665681

[Rib76] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804. MR 457455

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[Sti17] Thomas Jan Stieltjes, *œuvres complètes. II/Collected papers. II*, Springer Collected Works in Mathematics, Springer, Berlin, 2017, Edited by Gerrit van Dijk, Reprinted from the 1993 edition [MR1272017]. MR 3643001