JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Tyler GENAO

Polynomial Bounds on Torsion From a Fixed Geometric Isogeny Class of Elliptic Curves

Tome 36, nº 2 (2024), p. 661-670.
https://doi.org/10.5802/jtnb.1292

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **36** (2024), 661–670

Polynomial Bounds on Torsion From a Fixed Geometric Isogeny Class of Elliptic Curves

par Tyler GENAO

Résumé. Nous montrons qu'il existe des bornes polynomiales pour la torsion des courbes elliptiques qui proviennent d'une classe d'isogénie géométrique fixe. Plus précisément, si E_0 est une courbe elliptique définie sur un corps de nombres F_0, alors pour chaque $\epsilon > 0$ il existe des constantes $c_\epsilon := c_\epsilon(E_0, F_0)$ et $C_\epsilon := C_\epsilon(E_0, F_0) > 0$ telles que pour toute courbe elliptique $E_{/F}$ géométriquement isogène à E_0, si $E(F)$ a un point d'ordre N alors

$$N \leq c_\epsilon \cdot [F : \mathbb{Q}]^{1/2+\epsilon},$$

et on a aussi

$$\#E(F)[\text{tors}] \leq C_\epsilon \cdot [F : \mathbb{Q}]^{1+\epsilon}.$$

Abstract. We show there exist polynomial bounds on torsion of elliptic curves which come from a fixed geometric isogeny class. More precisely, for an elliptic curve E_0 defined over a number field F_0, for each $\epsilon > 0$ there exist constants $c_\epsilon := c_\epsilon(E_0, F_0), C_\epsilon := C_\epsilon(E_0, F_0) > 0$ such that for any elliptic curve $E_{/F}$ geometrically isogenous to E_0, if $E(F)$ has a point of order N then

$$N \leq c_\epsilon \cdot [F : \mathbb{Q}]^{1/2+\epsilon},$$

and one also has

$$\#E(F)[\text{tors}] \leq C_\epsilon \cdot [F : \mathbb{Q}]^{1+\epsilon}.$$

1. Introduction

For an elliptic curve E defined over a number field F, the Mordell–Weil theorem states that the abelian group $E(F)$ of F-rational points on E is finitely generated. One consequence of this is that its torsion subgroup $E(F)[\text{tors}]$ is finite. In fact, a celebrated result of Merel [17, Corollaire] showed that the size $\#E(F)[\text{tors}]$ is uniformly bounded in the degree of F; more precisely, for each integer $d \in \mathbb{Z}^+$ there exists a bound $B(d)$ on torsion subgroup sizes $\#E(F)[\text{tors}]$ over all elliptic curves $E_{/F}$ where $[F : \mathbb{Q}] = d$.

Manuscrit reçu le 1er janvier 2023, révisé le 17 juillet 2023, accepté le 15 septembre 2023.
2020 *Mathematics Subject Classification.* 11G05.
Mots-clefs. Elliptic curve, Galois representation, isogeny, torsion subgroup.
This material is based upon work supported by the National Science Foundation Graduate Research Fellowship under Grant No. 1842396. Partial support was also provided by the Research and Training Group grant DMS-1344994 funded by the National Science Foundation.

Sharp values of $B(d)$ are only known for $d \leq 3$, via a complete classification of torsion groups of elliptic curves [7, 12, 13, 14, 16]. However, Merel [17] gave an explicit upper bound on prime power divisors of $\#E(F)[\text{tors}]$ in terms of d, which was later strengthened by Parent [19, Corollaire 1.8]: if $p^n \mid \#E(F)[\text{tors}]$ then $p^n \leq 129(5^d-1)(3d)^6$. This gives bounds $B(d)$ which are larger than exponential in the degree d.

It is a folklore conjecture that there exist polynomial bounds on torsion groups of elliptic curves over number fields. More precisely:

Conjecture 1 ([3])**.** There exist constants $C, \alpha > 0$ such that for all elliptic curves $E_{/F}$ one has $\#E(F)[\text{tors}] \leq C \cdot [F : \mathbb{Q}]^{\alpha}$.

Parent's bounds above [19] are more than an exponential factor away from this conjecture. However, several results in the literature support this conjecture once we restrict certain parameters of our elliptic curves. For example, for any elliptic curve $E_{/F}$ with integral j-invariant, Hindry and Silverman have shown that $\#E(F)[\text{tors}] \leq 1977408 \cdot d \log(d)$ when $d := [F : \mathbb{Q}] > 1$ [11, Théorème 1]. In a stricter case, if E has complex multiplication (CM) then Clark and Pollack have shown that $\#E(F)[\text{tors}] \leq C \cdot d \log\log d$ when $d > 2$, where $C \in \mathbb{Z}^+$ is some absolute, effectively computable constant [5, Theorem 1].

There are also polynomial bounds for elliptic curves with rational j-invariant: Clark and Pollack have shown that for each $\epsilon > 0$ there exists a constant $C_\epsilon > 0$ such that for any elliptic curve $E_{/F}$ whose j-invariant $j(E) \in \mathbb{Q}$, one has that the exponent[1] $\exp E(F)[\text{tors}] \leq C_\epsilon \cdot [F : \mathbb{Q}]^{3/2+\epsilon}$, and thus $\#E(F)[\text{tors}] \leq C_\epsilon \cdot [F : \mathbb{Q}]^{5/2+\epsilon}$ [6, Theorem 1.3]. An identical result holds when one assumes the Generalized Riemann Hypothesis (GRH) and replaces $\mathbb{Q}$ with a number field F_0 which contains no Hilbert class field of any imaginary quadratic field [6, Theorem 1.6].

The principal result of this paper constructs polynomial bounds on orders of torsion points (and thus torsion groups) of non-CM elliptic curves $E_{/F}$ within a fixed geometric isogeny class. Recall that an *isogeny* between elliptic curves E and E' is a nonconstant algebraic map $\phi\colon E \to E'$ which preserves basepoints. We say that ϕ is F-rational if E, E' and ϕ are defined over F. As an adjective, "geometric" will mean $\overline{\mathbb{Q}}$-rational, where $\overline{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$.

Theorem 1.1. *Fix a number field F_0 and a non-CM elliptic curve E_{0/F_0}. Then for each $\epsilon > 0$ there exist constants $c_\epsilon := c_\epsilon(E_0, F_0), C_\epsilon := C_\epsilon(E_0, F_0) > 0$ such that for any elliptic curve $E_{/F}$ geometrically isogenous*

[1]Given a finite group $(G, +)$, its *exponent* $\exp G$ is the least integer $n \in \mathbb{Z}^+$ such that $nG = 0$. When G is abelian, its exponent is equal to the largest possible order of an element in G.

to E_{0/F_0}*, one has both*

$$\exp E(F)[\text{tors}] \leq c_\epsilon \cdot [F : \mathbb{Q}]^{1/2+\epsilon}$$

and

$$\#E(F)[\text{tors}] \leq C_\epsilon \cdot [F : \mathbb{Q}]^{1+\epsilon}.$$

Remark 1.2. In Theorem 1.1, The power "$1/2+\epsilon$" in the exponent bound $c_\epsilon \cdot [F : \mathbb{Q}]^{1/2+\epsilon}$ is optimal "up to ϵ", since for any elliptic curve $E_{/F}$, any integer $N \in \mathbb{Z}^+$ and any torsion point $R \in E[N]$, one always has $[F(R) : F] \leq N^2$.

Remark 1.3. We must assume in Theorem 1.1 that our elliptic curves are non-CM to have the *torsion group exponent* bound $c_\epsilon \cdot [F : \mathbb{Q}]^{1/2+\epsilon}$ hold. Indeed, one can show using e.g. [1, Corollary 1.8] that for any imaginary quadratic field K, the geometric isogeny class of elliptic curves with CM field K contains infinitely many elliptic curves $E_{/F}$ with $[F : \mathbb{Q}]$ arbitrarily large and $\exp E(F)[\text{tors}] > [F : \mathbb{Q}]$. Despite this, as noted earlier there is an asymptotically sharp bound on the size of *full torsion groups* of CM elliptic curves: one always has $\#E(F)[\text{tors}] \leq C \cdot [F : \mathbb{Q}] \log\log[F : \mathbb{Q}]$ when $[F : \mathbb{Q}] > 2$ for some absolute, effectively computable constant $C \in \mathbb{Z}^+$ [5, Theorem 1].

With Remark 1.3 in mind, we will assume for the rest of this paper that our elliptic curves have no geometric CM. A key step for us in polynomially bounding torsion from a non-CM geometric isogeny class $\mathcal{E}$ will be to relate the adelic indices of two rationally isogenous non-CM elliptic curves (this is Corollary 2.3).

In contrast to [6, Theorem 1.3], the collection of elliptic curves in Theorem 1.1 will contain curves whose j-invariants j' have arbitrarily large degrees $[\mathbb{Q}(j') : \mathbb{Q}]$. However, both Theorem 1.1 and [6, Theorem 1.3] are part of a natural uniformity conjecture on torsion groups that is motivated by our current understanding of Galois representations of rational elliptic curves.

Conjecture 2. There exist constants $C, \alpha > 0$ such that for all elliptic curves $E_{/F}$ geometrically isogenous to some elliptic curve defined over $\mathbb{Q}$, one has $\#E(F)[tors] \leq C \cdot [F : \mathbb{Q}]^\alpha$.

This is a special case of Conjecture 1. There is recent work which suggests its tractability: a result of Bourdon and Najman [2, Proposition 4.1] can be used to show that when $[F : \mathbb{Q}]$ is odd and $E_{/F}$ is $\overline{\mathbb{Q}}$-isogenous to a rational elliptic curve, one has $\exp E(F) \leq 720720\sqrt{35} \cdot [F : \mathbb{Q}]^{1/2}$, and thus $\#E(F)[\text{tors}] \leq 1441440\sqrt{35} \cdot [F : \mathbb{Q}]^{1/2}$. On the other hand, if one assumes a uniformity conjecture of Zywina on indices of adelic Galois representations of non-CM elliptic curves over $\mathbb{Q}$ [21, Conjecture 1.3], then Conjecture 2

follows "up to ϵ" with the same bounds as in Theorem 1.1; the principal difference is that the constants in Theorem 1.1 will change and depend only on ϵ.

Acknowledgments. The author thanks Pete L. Clark for his comments on an earlier draft of this paper, and the suggestion that Greenberg's proof of [9, Proposition 2.1.1] might be adjustable to give a stronger result, which is now Proposition 2.2. The author also thanks the referee for their insightful comments, particularly on improving the degree bounds in Theorem 1.1. Finally, the author thanks Jacob Mayle for his comment that the original version of Corollary 2.3, which was an equality of n-adic indices, implied an equivalence of adelic indices; this simplifies some of the presentation of this paper.

2. Results on Galois Representations of Non-CM Elliptic Curves

2.1. Some profinite group theory. In this section, we will show that a result of Greenberg on ℓ-adic Galois representations [9, Proposition 2.1.1] has a proof which applies to n-adic representations for composite $n \in \mathbb{Z}^+$, after some modifications. We will then use this composite version to prove that rationally isogenous non-CM elliptic curves have adelic Galois representations with equal indices in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, a fact we will use in our proof of Theorem 1.1; this is recorded as Corollary 2.3.

Before we prove this adelic index result, we will prove a few general facts about subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. For each integer $n \in \mathbb{Z}^+$, we will denote by $\pi_n \colon \mathrm{GL}_2(\widehat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ the mod-n reduction map, and by $\pi_{n^\infty} \colon \mathrm{GL}_2(\widehat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}_n)$ the n-adic reduction map.

By profinite group theory, for any subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ one has that G is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ iff G has finite index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, iff G contains an open neighborhood $U(M) := \ker \pi_M$ for some $M \in \mathbb{Z}^+$. When G is open, we will call the least such M for which $U(M) \subseteq G$ the *level of* G.

Lemma 2.1. *Let G be a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.*

(a) *One has for all $n \in \mathbb{Z}^+$ that $U(n) \subseteq G$ iff $G = \pi_n^{-1}(\pi_n(G))$.*

(b) *If $U(n) \subseteq G$ then*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G] = [\mathrm{GL}_2(\mathbb{Z}_n) : \pi_{n^\infty}(G)] = [\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \pi_n(G)].$$

(c) *Suppose that G is open, and let $G' \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be another open subgroup. If for all $n \in \mathbb{Z}^+$ one has*

$$[\mathrm{GL}_2(\mathbb{Z}_n) : \pi_{n^\infty}(G)] = [\mathrm{GL}_2(\mathbb{Z}_n) : \pi_{n^\infty}(G')]$$

then one has the equality

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G] = [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G'].$$

Proof. For part (a), suppose first that $U(n) \subseteq G$. To check that $G = \pi_n^{-1}(\pi_n(G))$, we note that the containment $\subseteq$ is clear. For the reverse containment, observe that if $x \in \pi_n^{-1}(\pi_n(G))$ then $\pi_n(x) \in \pi_n(G)$, and so $\pi_n(x) = \pi_n(g)$ for some $g \in G$; in particular, $xg^{-1} \in \ker \pi_n \subseteq G$, whence we have $x \in G$. For the converse, assume that $\pi_n^{-1}(\pi_n(G)) = G$. Then we have $U(n) = \pi_n^{-1}(\{I\}) \subseteq G$, where $I \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is the identity matrix.

Part (b) follows from the general fact that if $f\colon G_0 \to K$ is a group homomorphism and $G \subseteq G_0$ is a subgroup containing the kernel $\ker f$, then a set of coset representatives $\{f(g_i)\}_i$ for $f(G)$ in $f(G_0)$ lifts to a set of coset representatives $\{g_i\}_i$ for G in G_0. In particular, when $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is a subgroup with $U(n) \subseteq G$, one has that $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G] = [\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \pi_n(G)]$. It also follows that $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G] = [\mathrm{GL}_2(\mathbb{Z}_n) : \pi_{n^\infty}(G)]$, via the containment $\ker \pi_{n^\infty} \subseteq G$ (the map π_n factors through π_{n^∞}).

For part (c), let us set $N := \mathrm{lcm}(M, M')$ where M and M' are the levels of G and G' respectively. Since $U(N) \subseteq U(M) \subseteq G$ and $U(N) \subseteq U(M') \subseteq G'$, by part b. we have both

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G] = [\mathrm{GL}_2(\mathbb{Z}_N) : \pi_{N^\infty}(G)]$$

and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G'] = [\mathrm{GL}_2(\mathbb{Z}_N) : \pi_{N^\infty}(G')].$$

Thus, our hypothesis implies that $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G] = [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G']$. □

2.2. A composite version of a result of Greenberg. Our next goal is to prove a composite version of [9, Proposition 2.1.1]. Given an integer $n \in \mathbb{Z}^+$, let us recall that the *ring of n-adic integers* is

$$\mathbb{Z}_n := \varprojlim_{\ell | n, k \geq 1} \mathbb{Z}/\ell^k\mathbb{Z} \cong \prod_{\ell | n} \mathbb{Z}_\ell.$$

Following this, the *ring of n-adic numbers* is

$$\mathbb{Q}_n := \prod_{\ell | n} \mathbb{Q}_\ell.$$

For a free $\mathbb{Q}_n$-module V of finite rank, we call the $\mathbb{Z}_n$-span of any basis of V a *$\mathbb{Z}_n$-lattice.*

Proposition 2.2. *Fix a positive integer n. Let V be a free finite rank $\mathbb{Q}_n$-module. Suppose that G is a compact open subgroup of $\mathrm{Aut}_{\mathbb{Q}_n}(V)$. If T and T' are two G-invariant $\mathbb{Z}_n$-lattices in V, then*

$$[\mathrm{Aut}_{\mathbb{Z}_n}(T) : G] = [\mathrm{Aut}_{\mathbb{Z}_n}(T') : G].$$

Proof. Suppose that V is free of rank d over $\mathbb{Q}_n$. Fixing a basis for V, one has an isomorphism $\mathrm{Aut}_{\mathbb{Q}_n}(V) \cong \mathrm{GL}_d(\mathbb{Q}_n) \cong \prod_{\ell | n} \mathrm{GL}_d(\mathbb{Q}_\ell)$.

For each prime $\ell \in \mathbb{Z}^+$, the group $\mathrm{GL}_d(\mathbb{Q}_\ell)$ is a locally compact topological group, and thus has a left Haar measure. In fact, since $\mathrm{GL}_d(\mathbb{Q}_\ell)$

is a reductive ℓ-adic group it is also *unimodular*: every left Haar measure is also a right Haar measure [8, Theorem 5.1]. It follows then that the finite product $\prod_{\ell|n} \mathrm{GL}_d(\mathbb{Q}_\ell) \cong \mathrm{GL}_d(\mathbb{Q}_n)$ is also unimodular for composite $n \in \mathbb{Z}^+$.

Fix a Haar measure μ on $\mathrm{GL}_d(\mathbb{Q}_n)$; since G is compact open in $\mathrm{GL}_d(\mathbb{Q}_n)$, we have $\mu(G) > 0$, so we may assume that $\mu(G) = 1$. Given a $\mathbb{Z}_n$-lattice T in V, we can identify $\mathrm{Aut}_{\mathbb{Z}_n}(T) \cong \mathrm{GL}_d(\mathbb{Z}_n)$ once we choose a $\mathbb{Z}_n$-basis for T. For any $\sigma \in \mathrm{Aut}_{\mathbb{Q}_n}(V)$ one has that $\sigma(T)$ is a $\mathbb{Z}_n$-lattice; this gives us an action of $\mathrm{Aut}_{\mathbb{Q}_n}(V)$ on the set of $\mathbb{Z}_n$-lattices in V. This action is clearly transitive, and the stabilizer of any $\mathbb{Z}_n$-lattice T is $\mathrm{Aut}_{\mathbb{Z}_n}(T)$. Additionally, $\mathrm{Aut}_{\mathbb{Z}_n}(T)$ is a compact open subgroup of $\mathrm{Aut}_{\mathbb{Q}_n}(V)$, and G is contained in $\mathrm{Aut}_{\mathbb{Z}_n}(T)$ and has finite index. Since $\mathrm{Aut}_{\mathbb{Z}_n}(T)$ is a finite disjoint union of left cosets of G, and since $\mu(G) = 1$ and μ is left invariant, it follows that

$$\mu(\mathrm{Aut}_{\mathbb{Z}_n}(T)) = [\mathrm{Aut}_{\mathbb{Z}_n}(T) : G]. \tag{2.1}$$

Let T and T' be G-invariant $\mathbb{Z}_n$-lattices of V. Since $\mathrm{Aut}_{\mathbb{Q}_n}(V)$ acts transitively on $\mathbb{Z}_n$-lattices, there exists $\sigma \in \mathrm{Aut}_{\mathbb{Q}_n}(V)$ with $\sigma(T) = T'$. It follows then that $\mathrm{Aut}_{\mathbb{Z}_n}(T') = \sigma \,\mathrm{Aut}_{\mathbb{Z}_n}(T)\sigma^{-1}$. As μ is both left and right invariant, we conclude that $\mu(\mathrm{Aut}_{\mathbb{Z}_n}(T')) = \mu(\mathrm{Aut}_{\mathbb{Z}_n}(T))$, which by (2.1) implies our result. □

2.3. Galois representations of elliptic curves. Given an elliptic curve E over a number field F, for each integer $n \in \mathbb{Z}^+$ the absolute Galois group $G_F := \mathrm{Gal}(\overline{F}/F)$ acts on the n-torsion subgroup $E[n]$ of E. This action is described by the *mod-n Galois representation of E,* denoted by

$$\rho_{E,n} \colon G_F \longrightarrow \mathrm{Aut}(E[n]).$$

Since $E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank two, choosing a basis $\{P, Q\}$ for $E[n]$ gives an isomorphism $\mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$; we will often work with a basis implicitly, suppressing dependence on one.

The action of G_F on each torsion subgroup $E[n]$ for all $n \in \mathbb{Z}^+$ induces an action on their inverse limit $T(E) := \varprojlim E[n]$, called the *adelic Tate module of* $E_{/F}$. Since each $E[n]$ is a free rank two $\mathbb{Z}/n\mathbb{Z}$-module, it follows that $T(E)$ is free of rank two over the profinite integers $\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}$. The action of G_F on $T(E)$ is called the *adelic Galois representation of* $E_{/F}$, denoted by

$$\rho_E \colon G_F \longrightarrow \mathrm{Aut}_{\widehat{\mathbb{Z}}}(T(E)).$$

This also describes the action of G_F on the full torsion subgroup $E[\mathrm{tors}]$. Choosing a basis for $T(E)$ gives an isomorphism $\mathrm{Aut}_{\widehat{\mathbb{Z}}}(T(E)) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$. Assume hereafter that our elliptic curves are non-CM; then it follows by [20, Théorème 2] that the image $\rho_E(G_F)$ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. We say that the *adelic level of* $E_{/F}$ is the level of $\rho_E(G_F)$ as a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. By abuse of notation, we will often suppress its dependence on E and F.

Given an integer $n \in \mathbb{Z}^+$, let us define the *n-adic Tate module of $E_{/F}$* as $T_n(E) := \varprojlim_{k \geq 1} E[n^k]$. We have that $T_n(E)$ is a free rank two $\mathbb{Z}_n$-module. The *n-adic representation of $E_{/F}$* is the action of G_F on $T_n(E)$, denoted by

$$\rho_{E,n^\infty} \colon G_F \longrightarrow \mathrm{Aut}_{\mathbb{Z}_n}(T_n(E)).$$

This also describes the action of G_F on the n-primary torsion subgroup $E[n^\infty] := \bigcup_{k \geq 1} E[n^k] = \sum_{\ell | n} E[\ell^\infty]$. Since $\rho_{E,n^\infty}(G_F)$ is a projection of $\rho_E(G_F)$, it is open in $\mathrm{GL}_2(\mathbb{Z}_n)$.

The action of G_F on $T_n(E)$ extends naturally to an action on the rational n-adic Tate module $V_n(E) := T_n(E) \otimes_{\mathbb{Z}_n} \mathbb{Q}_n$. We can realize $\rho_{E,n^\infty}(G_F)$ as finite-index subgroup of $\mathrm{Aut}_{\mathbb{Z}_n}(T_n(E))$, the latter of which is a compact open subgroup of $\mathrm{Aut}_{\mathbb{Q}_n}(V_n(E))$.

Suppose two elliptic curves $E_{/F}$ and $E'_{/F}$ are F-isogenous; let us write this isogeny as $\phi \colon E \to E'$. Choose an integer $n \in \mathbb{Z}^+$; then this isogeny induces a $\mathbb{Z}_n[G_F]$-module homomorphism $\phi \colon T_n(E) \to T_n(E')$. In fact, we have a short exact sequence of $\mathbb{Z}_n[G_F]$-modules,

$$0 \longrightarrow T_n(E) \xrightarrow{\phi} T_n(E') \longrightarrow C \longrightarrow 0,$$

for some finite module C. Tensoring this sequence to $\mathbb{Q}_n$ shows that the rational Tate modules $V_n(E)$ and $V_n(E')$ are isomorphic G_F-modules, and so $T_n(E)$ and $T_n(E')$ may be realized as G_F-stable $\mathbb{Z}_n$-lattices in $V_n(E)$. By Proposition 2.2, this implies that

$$[\mathrm{GL}_2(\mathbb{Z}_n) : \rho_{E,n^\infty}(G_F)] = [\mathrm{GL}_2(\mathbb{Z}_n) : \rho_{E',n^\infty}(G_F)].$$

Since $n \in \mathbb{Z}^+$ was arbitrary, we have proven the following key result after applying Lemma 2.1.

Corollary 2.3. *Let $E_{/F}$ and $E'_{/F}$ be F-isogenous non-CM elliptic curves. Then one has*

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

Let us note one more fact about Galois representations of elliptic curves with a rational torsion point. For each integer $n \geq 2$, we define a distinguished subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$,

$$B_1(n) := \left\{ \begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \right\}.$$

When an elliptic curve $E_{/F}$ has an F-rational order n torsion point, it follows that the image $\rho_{E,n}(G_F)$ is contained in $B_1(n)$ up to conjugacy. This implies the index divisibility

$$[\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : B_1(n)] \mid [\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \rho_{E,n}(G_F)].$$

The former index can be written more explicitly. Let us recall Euler's phi function $\varphi \colon \mathbb{Z}^+ \to \mathbb{Z}^+$ and the Dedekind psi function $\psi \colon \mathbb{Z}^+ \to \mathbb{Z}^+$, both

arithmetic multiplicative functions defined on prime powers via $\varphi(\ell^k) = \ell^{k-1}(\ell-1)$ and $\psi(\ell^k) = \ell^{k-1}(\ell+1)$ respectively.

Lemma 2.4. *For $n \geq 2$ one has*

$$[\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : B_1(n)] = \varphi(n)\psi(n).$$

Proof. See e.g. [4, Section 7.2]. □

3. Polynomial Bounds on Torsion

We are ready to prove the main result of this paper.

Proof of Theorem 1.1. To recapitulate Theorem 1.1, we will show that for any fixed non-CM elliptic curve E_{0/F_0}, for all $\epsilon > 0$ there exist constants $c_\epsilon := c_\epsilon(E_0, F_0), C_\epsilon := C_\epsilon(E_0, F_0) > 0$ such that for all elliptic curves $E_{/F}$ geometrically isogenous to E_0, one has both

$$\exp E(F)[\mathrm{tors}] \leq c_\epsilon \cdot [F : \mathbb{Q}]^{1/2+\epsilon}$$

and

$$\#E(F)[\mathrm{tors}] \leq C_\epsilon \cdot [F : \mathbb{Q}]^{1+\epsilon}.$$

First, observe that the desired bound on $\#E(F)[\mathrm{tors}]$ will follow from the desired bound on the exponent $\exp E(F)[\mathrm{tors}]$, via the divisibility

$$\#E(F)[\mathrm{tors}] \mid (\exp E(F)[\mathrm{tors}])^2$$

(one can take $C_\epsilon := c_{\epsilon/2}^2$). To this end, our proof will focus on bounding $\exp E(F)[\mathrm{tors}]$.

Let us write $n := \exp E(F)[\mathrm{tors}]$. Then up to conjugacy we have $\rho_{E,n}(G_F) \subseteq B_1(n)$, so by Lemma 2.4 we get

$$\varphi(n)\psi(n) \mid [\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \rho_{E,n}(G_F)]. \tag{3.1}$$

By [15, Lemma 3.1] there exists a(n at worst) quadratic extension L/FF_0 for which E and E_0 are L-isogenous. Thus, Corollary 2.3 implies that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_L)] = [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E_0}(G_L)]. \tag{3.2}$$

Since the extension $F_0(E_0[\mathrm{tors}])/F_0$ is normal, so is the extension $L(E_0[\mathrm{tors}])/L$, and we have

$$\mathrm{Gal}(L(E_0[\mathrm{tors}])/L) \cong \mathrm{Gal}(F_0(E_0[\mathrm{tors}])/L \cap F_0(E_0[\mathrm{tors}]))$$

(this general fact is e.g. [18, Proposition 7.15]). Since $\rho_{E_0}(G_L) \cong \mathrm{Gal}(L(E_0[\mathrm{tors}])/L)$, we see that $\rho_{E_0}(G_L)$ is a subgroup of $\rho_{E_0}(G_{F_0})$ of index $[L \cap F_0(E_0[\mathrm{tors}]) : F_0]$. Thus, we deduce that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E_0}(G_L)] \mid [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E_0}(G_{F_0})] \cdot [L : F_0]. \tag{3.3}$$

Finally, since $[FF_0 : \mathbb{Q}] = [FF_0 : F] \cdot [F : \mathbb{Q}] \mid [F_0 : \mathbb{Q}]! \cdot [F : \mathbb{Q}]$ and $[L : F_0] \mid 2[FF_0 : F_0]$, we find that

$$[L : F_0] \mid 2([F_0 : \mathbb{Q}] - 1)! \cdot [F : \mathbb{Q}].$$

Combining this fact with (3.1), (3.2) and (3.3), we conclude that

$$\varphi(n)\psi(n) \mid 2I([F_0 : \mathbb{Q}] - 1)! \cdot [F : \mathbb{Q}], \tag{3.4}$$

where $I := [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_{E_0}(G_{F_0})]$ is the adelic index of our fixed elliptic curve E_{0/F_0}.

One can check directly that $\psi(n) > n$ for any $n > 1$. Fixing an $\epsilon \in (0, 1)$, by [10, Theorem 327] there exists a constant $b_\epsilon > 0$ such that for all $n \in \mathbb{Z}^+$ one has

$$\varphi(n) > b_\epsilon \cdot n^{1-\epsilon}.$$

Thus, from (3.4) we deduce that

$$n^{2-\epsilon} < 2Ib_\epsilon^{-1}([F_0 : \mathbb{Q}] - 1)! \cdot [F : \mathbb{Q}].$$

Since $n := \exp E(F)[\mathrm{tors}]$, we conclude that

$$\exp E(F)[\mathrm{tors}] < c_\epsilon \cdot [F : \mathbb{Q}]^{1/2+\epsilon}$$

where $c_\epsilon := c_\epsilon(E_0, F_0) := (2Ib_\epsilon^{-1}([F_0 : \mathbb{Q}] - 1)!)^{1/(2-\epsilon)}$, which is the desired upper bound on the exponent of $E(F)[\mathrm{tors}]$. □

References

[1] A. Bourdon & P. L. Clark, "Torsion points and Galois representations on CM elliptic curves", *Pac. J. Math.* **305** (2020), no. 1, p. 43-88.

[2] A. Bourdon & F. Najman, "Sporadic points of odd degree on $X_1(N)$ coming from $\mathbb{Q}$-curves", 2021, `https://arxiv.org/abs/2107.10909`.

[3] P. L. Clark, B. Cook & J. Stankewicz, "Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)", *Int. J. Number Theory* **9** (2013), no. 2, p. 447-479.

[4] P. L. Clark, T. Genao, P. Pollack & F. Saia, "The least degree of a CM point on a modular curve", *J. Lond. Math. Soc.* **105** (2022), no. 2, p. 825-883.

[5] P. L. Clark & P. Pollack, "The truth about torsion in the CM case", *C. R. Math. Acad. Sci. Paris* **353** (2015), no. 8, p. 683-688.

[6] ———, "Pursuing polynomial bounds on torsion", *Isr. J. Math.* **227** (2018), no. 2, p. 889-909.

[7] M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow & D. Zureick-Brown, "Sporadic cubic torsion", *Algebra Number Theory* **15** (2021), no. 7, p. 1837-1864.

[8] H. Glöckner, "Haar measure on linear groups over local skew fields", *J. Lie Theory* **6** (1996), no. 2, p. 165-177.

[9] R. Greenberg, "The image of Galois representations attached to elliptic curves with an isogeny", *Am. J. Math.* **134** (2012), no. 5, p. 1167-1196.

[10] G. H. Hardy & E. M. Wright, *An introduction to the theory of numbers*, 6th ed., Oxford University Press, 2008.

[11] M. Hindry & J. Silverman, "Sur le nombre de points de torsion rationnels sur une courbe elliptique", *C. R. Acad. Sci. Paris* **329** (1999), no. 2, p. 97-100.

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

[13] ———, "Torsion points on elliptic curves over fields of higher degree", *Int. Math. Res. Not.* **1992** (1992), no. 6, p. 129-133.

[14] M. A. Kenku & F. Momose, "Torsion points on elliptic curves defined over quadratic fields", *Nagoya Math. J.* **109** (1988), p. 125-149.

[15] S. Le Fourn & F. Najman, "Torsion of $\mathbb{Q}$-curves over quadratic fields", *Math. Res. Lett.* **27** (2020), no. 1, p. 209-225.

[16] B. Mazur, "Modular curves and the Eisenstein ideal", *Publ. Math., Inst. Hautes Étud. Sci.* **47** (1977), p. 33-186.
[17] L. Merel, "Bornes pour la torsion des courbes elliptiques sur les corps de nombres", *Invent. Math.* **124** (1996), no. 1-3, p. 437-449.
[18] J. S. Milne, "Fields and Galois theory", v5.10, course notes, `https://www.jmilne.org/math/CourseNotes/FT.pdf`.
[19] P. Parent, "Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres", *J. Reine Angew. Math.* **506** (1999), p. 85-116.
[20] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1972), p. 259-331.
[21] D. Zywina, "Explicit open images for elliptic curves over $\mathbb{Q}$", 2022, `https://arxiv.org/abs/2206.14959`.

Tyler Genao
Department of Mathematics
The Ohio State University
231 W. 18th Ave., Columbus, OH 43210, USA
E-mail: `genao.5@osu.edu`
URL: `https://tylergenao.com`