Typical and Polynomial Bounds on Torsion of Elliptic Curves, and Torsion Upon Base Change

by

Tyler Genao

(Under the Direction of Pete L. Clark)

Abstract

This thesis studies uniformity results for torsion growth of elliptic curves over number fields in two contexts: asymptotically in the degree, where the elliptic curves vary in fixed geometric isogeny classes; and with regards to prime factors of the degree, where the base field is fixed.

Index words: [Elliptic curves, torsion groups, Galois representations, isogeny, complex multiplication]

Typical and Polynomial Bounds on Torsion of Elliptic Curves, and Torsion Upon Base Change

by

Tyler Genao

B.Sc., Florida Atlantic University, 2017

A Dissertation Submitted to the Graduate Faculty of the
University of Georgia in Partial Fulfillment of the Requirements for the Degree.

Doctor of Philosophy

Athens, Georgia

2023

Typical and Polynomial Bounds on Torsion of Elliptic Curves, and Torsion Upon Base Change

by

Tyler Genao

Major Professor: Pete L. Clark

Committee: Daniel Litt
Dino J. Lorenzini
Paul Pollack

Electronic Version Approved:

Ron Walcott
Dean of the Graduate School
The University of Georgia
May 2023

Acknowledgments

I am immeasurably grateful for every person in my life, as they've all shaped me into who I am today. First, I am thankful for my thesis advisor, Pete Clark, for his continual advice and support throughout my graduate studies. His thoughtful comments have helped my research program and dissertation come to fruition, and continue to inspire me. I am grateful for Daniel Litt, Dino Lorenzini and Paul Pollack for serving on my committee, as well as for teaching engaging and interesting courses in number theory, each of which has stimulated my research in one way or another. I am also grateful for my friends in the math department who made it a pleasure to come to work each week, as well as the friends I've made through conferences and workshops.

Second, I am grateful for Jeremy Rouse for giving me my first mathematical research experience as an undergraduate. My time spent working on his summer REU project helped me decide to pursue a PhD in mathematics.

Finally, I am deeply grateful for my family, whose consistent encouragement, love and support has helped me accomplish everything I've set out to do.

Contents

Chapter 1

Introduction

This thesis studies uniformity results for torsion growth of elliptic curves over number fields in two contexts: asymptotically in the degree, where the elliptic curves vary in fixed geometric isogeny classes; and with regards to prime factors of the degree, where the base field is fixed. These results are from recent papers [Gen1, Gen2, Gen3, Gen4].

Let $E_{/F}$ denote an elliptic curve E defined over a field F, i.e., a smooth, connected, projective algebraic curve of genus one with a distinguished F-rational point. Then the set $E(F)$ of F-rational points on E is is an abelian group, via a chord and tangent process. When F is a number field, the Mordell-Weil Theorem implies that the torsion group $E(F)[\text{tors}]$ is finite.

Within the last century, it has been of great interest to understand torsion groups of elliptic curves *uniformly*. For example, for a field extension $F/\mathbb{Q}$ with degree $[F : \mathbb{Q}] \leq 3$, classification results have completely determined what the group $E(F)[\text{tors}]$ can be for any elliptic curve $E_{/F}$ [Maz77, KM88, Kam92a, Kam92b, DEvH+21]; moreover, these papers show there are finitely many possibilities for $E(F)[\text{tors}]$ over such degrees.

In this direction, a celebrated result of Merel [Mer96] showed that the size $\#E(F)[\text{tors}]$ is always uniformly bounded in the degree:

Theorem 1. [Mer96] *For each integer $d > 0$ there exists a constant $B(d) \in \mathbb{Z}^+$ such that for all number fields $F/\mathbb{Q}$ with $[F : \mathbb{Q}] = d$ and for all elliptic curves $E_{/F}$ one has*

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

In this thesis, we present uniformity results on the size of torsion groups of elliptic curves over number fields whose degrees can be arbitrarily large. Each result employs a close study of degrees of fields of definition of torsion points on elliptic curves. The collections of elliptic curves that we study can be contextualized in terms of $\mathbb{Q}$-curves.

By a *family* of elliptic curves, we mean any collection of elliptic curves defined over number fields. The families that we study in [Gen1, Gen2, Gen3, Gen4] are defined as follows. Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and a number field $F_0 \subseteq \overline{\mathbb{Q}}$. Let us define four families

$$\mathcal{B}_{F_0} := \{\text{Elliptic curves } E_{/F} \text{ base-changed from } F_0\}, \tag{1.1}$$

$$\mathcal{E}_{F_0} := \{\text{Elliptic curves } E_{/F} \text{ with } F_0\text{-rational } j\text{-invariant}\}, \tag{1.2}$$

$$\mathcal{I}_{F_0} := \{\text{Elliptic curves } E_{/F} \text{ which are } \overline{\mathbb{Q}}\text{-isogenous to some } E' \text{ with } j(E') \in F_0\} \tag{1.3}$$

and

$$\mathcal{Q}_{F_0} := \{\text{Elliptic curves } E_{/F} : \forall \sigma \in \text{Gal}(\overline{\mathbb{Q}}/F_0),\ E \text{ is } \overline{\mathbb{Q}}\text{-isogenous to } E^\sigma\}. \tag{1.4}$$

We have the following containments:

$$\mathcal{B}_{F_0} \subset \mathcal{E}_{F_0} \subset \mathcal{I}_{F_0} \subset \mathcal{Q}_{F_0}.$$

Notice that when $F_0 = \mathbb{Q}$, the family $\mathcal{Q}_{\mathbb{Q}}$ is the family of $\mathbb{Q}$-curves.

Elliptic curves $E_{/F}$ from each family above can be defined over number fields F with arbitrarily large degree $[F : \mathbb{Q}]$, and in particular $\#E(F)[\text{tors}]$ can be arbitrarily large. However, in this thesis we will show that $E(F)[\text{tors}]$ is "well-behaved" once we impose certain restrictions on the degrees $[F : \mathbb{Q}]$.

This thesis is organized as follows. Chapter 2 gives some background on elliptic curve torsion points, Galois representations and isogenies that will be used throughout the thesis. Chapters 3, 4 and 5 concern asymptotic results on the growth of torsion groups from $\mathcal{E}_{F_0}$ and $\mathcal{I}_{F_0}$, namely *typical boundedness* and *polynomial bounds.* Chapter 6 will study torsion growth of elliptic curves in $\mathcal{B}_{F_0}$.

1.1.1 Typical boundedness

Recall that any subset $S \subseteq \mathbb{Z}^+$ has a well-defined *upper (asymptotic) density*

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

Given a family $\mathcal{F}$ of elliptic curves closed under rational isomorphism (i.e., given an elliptic curve $E_{/F} \in \mathcal{F}$ and another curve $E'_{/F}$ with $E' \cong_F E'$, one has $E'_{/F} \in \mathcal{F}$; this includes our four families above), we say that $\mathcal{F}$ is *typically bounded in torsion* if for all $\epsilon > 0$ there is a constant $B_\epsilon > 0$ such that the set of "bad degrees"

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

has upper density at most ϵ. Informally stated, $\mathcal{F}$ is typically bounded in torsion if the torsion groups of elliptic curves in $\mathcal{F}$ are absolutely bounded away from a subset of elliptic curves $E_{/F} \in \mathcal{F}$ whose degrees $[F : \mathbb{Q}]$ lie in an arbitrarily thin subset of $\mathbb{Z}^+$.

Typical boundedness has been previously studied by Clark, Milosevic and Pollack [CMP18]; in particular, they show that if one assumes the Generalized Riemann Hypothesis (GRH), as well as the technical assumption that F_0 has no "rationally defined CM", then the family $\mathcal{E}_{F_0}$ is typically bounded in torsion. In Chapter 3 we will prove this result for $\mathcal{E}_{F_0}$ *unconditionally on* F_0.

Theorem (Theorem 4)**.** *For any number field F_0, torsion is typically bounded on $\mathcal{E}_{F_0}$.*

In Chapter 4, we extend this result to $\mathcal{I}_{F_0}$.

Theorem (Theorem 12)**.** *For any number field F_0, torsion is typically bounded on $\mathcal{I}_{F_0}$.*

The family $\mathcal{I}_{F_0}$ is significantly larger than $\mathcal{E}_{F_0}$, as we now explain. Given an algebraic number $j \in \overline{\mathbb{Q}}$ and any elliptic curve E with j-invariant $j(E) = j$, the $\overline{\mathbb{Q}}$-rational isogeny class of E contains j-invariants j' of arbitrarily large degree $[\mathbb{Q}(j') : \mathbb{Q}]$. In the case where E has complex multiplication (henceforth abbreviated as CM) this follows from class field theory: given a CM elliptic curve E whose geometric endomorphism ring is (isomorphic to) an imaginary quadratic order $\mathcal{O}$, its j-invariant has degree $[\mathbb{Q}(j(E)) : \mathbb{Q}] = \#\mathrm{Pic}(\mathcal{O})$, where $\mathrm{Pic}(\mathcal{O})$ is the class group of $\mathcal{O}$. By a classic result of Heilbronn [Hei34], as the discriminant $\Delta(\mathcal{O}) \to -\infty$ the class number $\#\mathrm{Pic}(\mathcal{O}) \to \infty$. Since any two CM elliptic curves will be geometrically isogenous if their geometric endomorphism rings have isomorphic fraction fields, one concludes that the isogeny class of any CM elliptic curve will have j-invariants of arbitrarily large degree. On the other hand, given any non-CM elliptic curve E defined over a number field F_0, Serre's open image theorem [Ser72, Théorème 2] tells us that for $\ell \gg_{E,F_0} 0$ one has that the mod-ℓ Galois representation of E is surjective. It follows then that for any order ℓ subgroup $C_\ell \subseteq E$, the field of definition of C_ℓ over F_0 has degree $\ell + 1$. By [Cla, Proposition 3.2] the field of definition equals $F_0(j_\ell)$ where j_ℓ is the j-invariant of the quotient elliptic curve E/C_ℓ. Thus the isogeny class of E contains j-invariants of degree $\ell + 1$ over F_0 for all primes $\ell \gg_{E,F_0} 0$.

1.1.2 Polynomial bounds

We say that a family $\mathcal{F}$ is *polynomially bounded in torsion* if there exist constants $c(\mathcal{F}), B(\mathcal{F}) > 0$ such that for all elliptic curves $E_{/F} \in \mathcal{F}$ one has

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

Polynomial bounds are tied in with Theorem 1. In this theorem, Merel gave an explicit upper bound on prime power divisors of $\#E(F)[\mathrm{tors}]$ in terms of d, which was later strengthened by Parent [Par99, Corollaire 1.8]: if $p^n \mid \#E(F)[\mathrm{tors}]$ then $p^n \leq 129(5^d - 1)(3d)^6$. This gives *explicit* bounds $B(d)$ which are larger than exponential in the degree d. It is a folklore

conjecture that there exists polynomial bounds on torsion groups of elliptic curves over number fields. More precisely:

Conjecture 2. *There exist constants $c, B > 0$ such that for all elliptic curves $E_{/F}$ one has $\#E(F)[\text{tors}] \leq c \cdot [F : \mathbb{Q}]^B$.*

Parent's bounds [Par99] 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 $d := [F : \mathbb{Q}] > 1$ [HS99, 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 [CP15, Theorem 1].

There are also polynomial bounds for elliptic curves in the family $\mathcal{E}_{\mathbb{Q}}$: 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]

$$\exp E(F)[\text{tors}] \leq C_\epsilon \cdot [F : \mathbb{Q}]^{3/2+\epsilon},$$

as well as

$$\#E(F)[\text{tors}] \leq C_\epsilon \cdot [F : \mathbb{Q}]^{5/2+\epsilon}$$

[CP18, 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 has no rationally defined CM [CP18, Theorem 1.6].

Our result on polynomial bounds is for any fixed geometric isogeny class of elliptic curves. In contrast to the family $\mathcal{E}_{\mathbb{Q}}$ for [CP18, Theorem 1.3], a geometric isogeny class will contain elliptic curves whose j-invariants have arbitrarily large degree.

Theorem (Theorem 21)**.** *Fix a number field F_0 and an elliptic curve E_{0/F_0}. Then for each $\epsilon > 0$ there exists a constant $C_\epsilon := C_\epsilon(E_0, F_0) > 0$ such that for any elliptic curve $E_{/F}$*

[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, the exponent is equal to the largest possible order of an element in G.

geometrically isogenous to E_{0/F_0} one has both

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

and

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

1.1.3 Base change

In Chapter 6 we study the growth of torsion groups in the family $\mathcal{B}_{F_0}$. Previously, González-Jiménez and Najman have shown that for all elliptic curves $E_{/F} \in \mathcal{B}_{\mathbb{Q}}$, if $[F : \mathbb{Q}]$ is coprime to 210 then one has $E(F)[\text{tors}] = E(\mathbb{Q})[\text{tors}]$ [GJN20, Theorem 7.2.i]. The main result of Chapter 6 is a generalization of this.

Theorem (Theorem 28)**.** *Assume that GRH is true, and let F_0 be a number field with no rationally defined CM. Then there exists an effectively computable constant $B := B(F_0) \in \mathbb{Z}^+$ for which the following holds: for any finite extension L/F_0 whose degree $[L : F_0]$ is coprime to B, one has for all elliptic curves E defined over F_0 that*

$$E(L)[\text{tors}] = E(F_0)[\text{tors}].$$

We also show that this result fails when F_0 has rationally defined CM, due to the existence of F_0-rational isogenies of arbitrarily large prime degrees satisfying certain congruence conditions.

Theorem (Theorem 30)**.** *Let F_0 be a number field with rationally defined CM. Then for all integers $B \in \mathbb{Z}^+$ there exists a finite extension L/F_0 whose degree $[L : F_0]$ is coprime to B, and a CM elliptic curve $E_{/F_0}$ for which*

$$E(L)[\text{tors}] \neq E(F_0)[\text{tors}].$$

Finally, towards proving Theorem 28, we prove a result on relative uniform divisibility of the index of a mod-ℓ Galois representation of an elliptic curve over F_0. Each of the subgroups below are defined in Chapter 2.

Theorem (Theorem 29)**.** *Assume that GRH is true, and let F_0 be a number field with no rationally defined CM. Then for all primes $\ell \gg_{F_0} 0$, one has for any elliptic curve $E_{/F_0}$ that its mod-ℓ Galois representation $G := \rho_{E,\ell}(G_{F_0})$ is either surjective, or is contained in $N_s(\ell)$ or $N_{ns}(\ell)$ up to conjugacy.*

1. *If $G \subseteq N_s(\ell)$ then $\mathcal{D}^e \subseteq G$ for some $e \in \{1, 2, 3, 4, 6\}$, and if $\ell \neq 37, 73$ then the center $Z(\ell) \subseteq G$, and in fact*
$$[N_s(\ell) : G] \mid \gcd(\ell - 1, e).$$

2. *If $G \subseteq N_{ns}(\ell)$ then $C_{ns}(\ell)^e \subseteq G$ for some $e \in \{1, 2, 3, 4, 6\}$, and in fact*
$$[N_{ns}(\ell) : G] \mid 6.$$

   a. *If $\ell \equiv 1 \pmod 3$, then G equals $N_{ns}(\ell)$ or $C_{ns}(\ell)$, with $G = N_{ns}(\ell)$ if F_0 has a real embedding.*

   b. *If $\ell \equiv 2 \pmod 3$, then G equals $N_{ns}(\ell)$, $C_{ns}(\ell)$, $G(\ell)$ or $C_{ns}(\ell)^3$, with $G = N_{ns}(\ell)$ or $G(\ell)$ if F_0 has a real embedding.*

Chapter 2

Background

Throughout this thesis, we are interested in understanding the rationality of torsion points on elliptic curves over number fields. To this end, we also seek to understand the Galois representations associated to such elliptic curves, and their connections to fields of definition of torsion points.

2.1.1 Galois representations of elliptic curves

Let us recall the *ring of profinite integers*, which is the inverse limit

$$\hat{\mathbb{Z}} := \varprojlim_{n \in \mathbb{Z}^+} \mathbb{Z}/n\mathbb{Z}.$$

For each integer $N \in \mathbb{Z}^+$, we also have the *ring of N-adic integers*

$$\mathbb{Z}_N := \varprojlim_{k \in \mathbb{Z}^+} \mathbb{Z}/N^k\mathbb{Z}.$$

Then one has an isomorphism

$$\hat{\mathbb{Z}} \cong \prod_{\text{prime } \ell \in \mathbb{Z}^+} \mathbb{Z}_\ell.$$

Let us also define the *ring of N-adic numbers* as $\mathbb{Q}_N := \mathbb{Z}_N \otimes \mathbb{Q} \cong \prod_{\ell | N} \mathbb{Q}_\ell$.

For the rest of this thesis, fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Let $F/\mathbb{Q}$ be an algebraic extension, regarded as a subextension of $\overline{\mathbb{Q}}$. We will write $G_F := \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ for the *absolute Galois group of* F. Let us consider an elliptic curve E defined over F, written $E_{/F}$. Since E is defined over F, the Galois group G_F acts on $E(\overline{\mathbb{Q}})$. For each integer $N \in \mathbb{Z}^+$, we write $E[N] := E(\overline{\mathbb{Q}})[N]$ for the N-torsion subgroup of E. Since addition of points in $E(\overline{\mathbb{Q}})$ is F-rational, it follows that $E[N]$ is stable under the action of G_F. The corresponding group homomorphism

$$\rho_{E,N} \colon G_F \to \mathrm{Aut}_{\mathbb{Z}/N\mathbb{Z}}(E[N])$$

is called the *mod-N Galois representation of* E. Since $E[N]$ is a free rank two $\mathbb{Z}/N\mathbb{Z}$-module [Sil09, Corollary 6.4], it follows that fixing a basis for $E[N]$ gives an isomorphism $\mathrm{Aut}_{\mathbb{Z}/N\mathbb{Z}}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$; thus, the image $\rho_{E,N}(G_F)$ may be realized as a subgroup of matrices in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

For each integer $N \in \mathbb{Z}^+$, let us define the *N-adic Tate module* as the inverse limit $T_N(E) := \varprojlim_{k \geq 1} E[N^k]$. It follows that $T_N(E)$ is a free rank two $\mathbb{Z}_N$-module. The action of G_F on N-power torsion induces an action on $T_N(E)$, and we are afforded the *N-adic Galois representation of E,* denoted

$$\rho_{E,N^\infty} \colon G_F \to \mathrm{Aut}_{\mathbb{Z}_N}(T_N(E)).$$

When fixing a basis for $T_N(E)$, one can identify $\mathrm{Aut}_{\mathbb{Z}_N}(T_N(E)) \cong \mathrm{GL}_2(\mathbb{Z}_N)$.

Finally, we have the *adelic Tate module* $T(E) := \varprojlim_{n \geq 1} E[n]$, which is a free rank two $\hat{\mathbb{Z}}$-module. The action of G_F on $E[\mathrm{tors}]$ induces an action on $T(E)$, and we have the *adelic Galois representation of E,* denoted

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

When fixing a basis for $T(E)$, we have an isomorphism $\mathrm{Aut}_{\hat{\mathbb{Z}}}(T(E)) \cong \mathrm{GL}_2(\hat{\mathbb{Z}})$.

The adelic Galois representation packages together all information of rationality of torsion points on E. When E has no *complex multiplication* (see Section 2.1.5) the image $\rho_E(G_F)$ of

its adelic Galois representation is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ [Ser72, Théorème 2]. Equivalently, its image contains an open neighborhood of the identity matrix I, say $\ker(\pi_M \colon \mathrm{GL}_2(\hat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z}))$ for some $M \in \mathbb{Z}^+$, where π_M denotes the natural projection map mod M. We will call the least such M the *adelic level of* $E_{/F}$. Since $\rho_E(G_F)$ is open, it follows for each integer $N \in \mathbb{Z}^+$ that the N-adic image $\rho_{E,N^\infty}(G_F)$ is also open in $\mathrm{GL}_2(\mathbb{Z}_N)$; the least integer $k \in \mathbb{Z}^+$ for which $\rho_{E,N^\infty}(G_F)$ contains $\ker(\pi_{N^k} \colon \mathrm{GL}_2(\mathbb{Z}_N) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/N^k\mathbb{Z}))$ is called the *N-adic level of* E (or simply the level of $\rho_{E,N^\infty}(G_F)$).

In each of the following chapters, we will study the image $\rho_{E,\ell}(G_F)$ for large primes ℓ, utilizing the fact that it lands inside certain maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ (see Theorem 3). In Chapters 4 and 5 we also study the N-adic image $\rho_{E,N^\infty}(G_F)$.

2.1.2 Degrees of torsion points

Given an elliptic curve $E_{/F}$, one can recontextualize degrees of torsion points of E in terms of the sizes of orbits under the action of G_F. To be precise, fix an integer $N \in \mathbb{Z}^+$, and fix a basis $\{P, Q\}$ of $E[N]$ for which the image $G := \rho_{E,N}(G_F) := \rho_{E,N,P,Q}(G_F)$ is realized as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Identifying P and Q with unit basis vectors e_1, e_2 over $\mathbb{Z}/N\mathbb{Z}$, the action of G_F on $E[N]$ is given by the action of G on the $\mathbb{Z}/N\mathbb{Z}$-module $V := (\mathbb{Z}/N\mathbb{Z})\langle e_1, e_2\rangle$, via left multiplication.

Given a torsion point $R \in E[N]$, its *field of definition over F,* denoted $F(R)$, is the minimal field extension of F over which R becomes rational. This field can be characterized as the fixed field of the stabilizer of R under the action of G_F on $E[N]$. When E is given via an explicit equation, $F(R)$ can be obtained by adjoining the coordinates of R to F. The *N-division field of $E_{/F}$,* written as $F(E[N])$, is the compositum of all fields $F(R)$ for which $R \in E[N]$. The N-division field is also characterized as the fixed field for the action of G_F on $E[N]$.

Given a torsion point $R \in E[N]$, let us write $\mathcal{O}_G(R)$ for the orbit of R under G. Then the Orbit-Stabilizer Theorem implies that $\#\mathcal{O}_G(R) = [F(R) : F]$. Thus the degree of an N-torsion point over F is the size of its orbit under the action of $\rho_{E,N}(G_F)$, a vantage point

we will exploit with the classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ when N is prime. It's worth noting that this size is invariant under a change of basis for $E[N]$.

2.1.3 Subgroups of $\mathbf{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

Let us review an important classification result for subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ as seen in [Ser72], essentially due to Dickson [Dic58].

Throughout the following, we let $\ell \geq 5$ be a prime; we will sometimes write $\mathbb{F}_\ell := \mathbb{Z}/\ell\mathbb{Z}$. We define the *split Cartan subgroup mod-ℓ* as the subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$,

$$C_s(\ell) := \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : a, d \in \mathbb{F}_\ell^\times \right\}.$$

Fix the least positive integer ϵ which generates $\mathbb{F}_\ell^\times$. Then we define the *non-split Cartan subgroup mod-ℓ* as the regular representation of $\mathbb{F}_\ell[\sqrt{\epsilon}]^\times$ acting on itself via multiplication with respect to the basis $\{1, \sqrt{\epsilon}\}$; this representation is

$$C_{ns}(\ell) = \left\{ \begin{bmatrix} a & b\epsilon \\ b & a \end{bmatrix} : (a, d) \neq (0, 0) \in \mathbb{F}_\ell \times \mathbb{F}_\ell \right\}.$$

Note that $C_{ns}(\ell) \cong \mathbb{F}_{\ell^2}^\times$. For these two Cartan subgroups, one has their normalizers

$$\begin{aligned} N_s(\ell) &= C_s(\ell) \cup \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} C_s(\ell) \\ &= \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}, \begin{bmatrix} 0 & d \\ a & 0 \end{bmatrix} : a, d \in \mathbb{F}_\ell^\times \right\} \end{aligned}$$

and

$$N_{ns}(\ell) = C_{ns}(\ell) \cup \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} C_{ns}(\ell)$$
$$= \left\{ \begin{bmatrix} a & b\epsilon \\ b & a \end{bmatrix}, \begin{bmatrix} a & b\epsilon \\ -b & -a \end{bmatrix} : (a,b) \neq (0,0) \in \mathbb{F}_\ell \times \mathbb{F}_\ell \right\}.$$

Clearly, both Cartan subgroups have index two in their respective normalizers.

Let us also define the *Borel subgroup mod-ℓ* as the subgroup of upper triangular matrices,

$$B(\ell) := \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, d \in \mathbb{F}_\ell^\times \right\}.$$

In his seminal paper on the adelic open image theorem for elliptic curves, Serre [Ser72] analyzed the various mod-ℓ Galois representations of a fixed elliptic curve E over a number field. To do this, he used the following classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ [Ser72, §2].

Theorem 3 (Classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$)**.** *Let $\ell \geq 5$ be a prime, and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*

1. *If $\ell \mid \#G$, then one of the following holds:*
   a. *G contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*
   b. *G is contained in $B(\ell)$, up to conjugacy.*
2. *If $\ell \nmid \#G$, then one of the following holds:*
   a. *G is contained in $N_s(\ell)$ or $N_{ns}(\ell)$, up to conjugacy.*
   b. *The image $\overline{G}$ of G in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) := \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})/\mathbb{F}_\ell^\times$ is isomorphic to one of the groups A_4, S_4 or A_5.*

In Chapter 6, we will also need two more subgroups. We will let $\mathcal{D}$ denote the semi-Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, and $G(\ell)$ the unique subgroup of $N_{ns}(\ell)$ with $G(\ell) \not\subseteq C_{ns}(\ell)$ and

$[C_{ns}(\ell) : G(\ell) \cap C_{ns}(\ell)] = 3$; these are defined as

$$\mathcal{D} := \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} : a \in \mathbb{F}_\ell^\times \right\}$$

and

$$G(\ell) := \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, C_{ns}(\ell)^3 \right\rangle.$$

2.1.4 Isogenies

Our definitions and terminology for isogenies follow Silverman [Sil09]. Given two elliptic curves E and E' defined over $\overline{\mathbb{Q}}$, an *isogeny* from E to E' is a nonconstant algebraic map $\phi\colon E \to E'$ which preserves basepoints. Such a morphism induces a group homomorphism $\phi\colon E(\overline{\mathbb{Q}}) \to E'(\overline{\mathbb{Q}})$ [Sil09, Theorem III.4.8]. The kernel of such an isogeny is a finite subgroup of $E[\text{tors}]$ [Sil09, Corollary III.4.9]. We say that ϕ is *cyclic* if its kernel is cyclic, and call ϕ a cyclic N-isogeny, where $N := \#\ker\phi$.

For an algebraic extension $F/\mathbb{Q}$, we say that an isogeny $\phi\colon E \to E'$ is *F-rational* if E, E' and ϕ are defined over F. Observe that "Being F-rationally isogenous" is an equivalence relation. When $F = \overline{\mathbb{Q}}$, we say that ϕ is a *geometric isogeny.* For a fixed elliptic curve E, its *geometric isogeny class* is its equivalence class under "being geometrically isogenous."

Given an F-rational isogeny $\phi\colon E \to E'$, we let $\phi^\vee\colon E' \to E$ denote its *dual isogeny* [Sil09, Chapter III.6]. The dual isogeny has the same degree and field of definition as ϕ, and when ϕ is cyclic, so is $\phi^\vee$.

When a cyclic N-isogeny $\phi\colon E \to E'$ is F-rational, its kernel $C_N := \ker\phi$ is stable under the action of G_F. In particular, we are afforded a group homomorphism

$$r\colon G_F \to \mathrm{Aut}(C_N)$$

called the *isogeny character of ϕ.* Fixing a generator for C_N gives an isomorphism $\mathrm{Aut}(C_N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$.

2.1.5 Complex multiplication

Given an algebraic extension $F/\mathbb{Q}$ and an elliptic curve $E_{/F}$, the *F-rational endomorphism ring of E,* denoted $\mathrm{End}_F(E)$, is the ring of F-rational isogenies from E to itself. It is a standard fact that $\mathrm{End}_F(E)$ is isomorphic either to $\mathbb{Z}$ or to an order $\mathcal{O}$ in an imaginary quadratic number field [Sil09, Corollary III.9.4]. In the latter case, we say that E has *F-rational complex multiplication by $\mathcal{O}$,* or F-rational $\mathcal{O}$-CM. Without qualifications, when we say that an elliptic curve $E_{/F}$ has CM, we mean that E has $\overline{\mathbb{Q}}$-rational $\mathcal{O}$-CM for some imaginary quadratic order $\mathcal{O}$.

In general, given an algebraic extension $F/\mathbb{Q}$, we say that F has *rationally defined CM* if there exists an elliptic curve defined over F with F-rational CM.

Chapter 3

Typically Bounding Torsion on $\mathcal{E}_{F_0}$

3.1 Introduction

3.1.1 Bounds on torsion groups

Recall that Merel's Theorem (Theorem 1) says that there exists a uniform bound on torsion groups of elliptic curves over number fields of a fixed degree. A natural follow-up question is what the sharpest bound can be over a fixed degree. Let us define a function which records such values:

$$T(d) := \max_{E_{/F},[F:\mathbb{Q}]=d} \#E(F)[\text{tors}].$$

Only a few values of $T(d)$ are currently known. Via a complete classification of torsion subgroups over degree $d \leq 3$ number fields, one has $T(1) = 16$ [Maz77], $T(2) = 24$ [KM88, Kam92a, Kam92b] and $T(3) = 28$ [DEvH+21]. In general, a lower bound of the form $C \cdot \sqrt{d} \leq T(d)$ is also known [CMP18]. Finally, we have explicit upper bounds on $T(d)$ which are greater than exponential in d [Par99].

Let us also define the CM-analogue of $T(d)$,

$$T_{\text{CM}}(d) := \max_{\text{CM } E_{/F},[F:\mathbb{Q}]=d} \#E(F)[\text{tors}].$$

This arithmetic function records the largest size over all CM elliptic curve torsion subgroups over all degree d number fields. One clearly has $T_{\mathrm{CM}}(d) \leq T(d) < \infty$.

Via a complete classification of CM torsion subgroups over number fields of a fixed degree, many values of $T_{\mathrm{CM}}(d)$ are known. For example, for a CM elliptic curve $E_{/F}$ where $[F : \mathbb{Q}] \leq 13$, $E(F)[\mathrm{tors}]$ is recorded in [CCRS14]. For all primes $\ell > 5$ one has $T_{\mathrm{CM}}(\ell) = 6$ [BCS17, Theorem 1.4]. For each $n \in \mathbb{Z}^+$ one has for sufficiently large primes $\ell \gg_n 0$ that $T_{\mathrm{CM}}(\ell^n) = 6$ [BCP17, Theorem 1.4]. In fact, for any odd $d \in \mathbb{Z}^+$ $T_{\mathrm{CM}}(d)$ is also known [BP17, Theorem 1.1].

Bourdon, Clark and Pollack [BCP17] also treat $T_{\mathrm{CM}}(d)$ as an arithmetic function and study its behavior as $d \to \infty$. As noted above, $T_{\mathrm{CM}}(d) = 6$ for infinitely many $d \in \mathbb{Z}^+$. In general, one has the lower bound $T_{\mathrm{CM}}(d) \geq 6$ for all $d \in \mathbb{Z}^+$ due to Olson [Ols76], whence the "lower order" of $T_{\mathrm{CM}}(d)$ is

$$\liminf_{d\to\infty} T_{\mathrm{CM}}(d) = 6.$$

Similarly, Clark and Pollack have shown the "upper order" result ([CP17, Theorem 1.1])

$$\limsup_{d\to\infty} \frac{T_{\mathrm{CM}}(d)}{d \log\log d} = \frac{e^\gamma \pi}{\sqrt{3}}.$$

Bourdon, Clark and Pollack [BCP17] also study the *typical order* of $T_{\mathrm{CM}}(d)$, e.g., its statistical behavior away from certain sets of arbitrarily small upper density. Recall that the *upper (asymptotic) density* of a subset $S \subseteq \mathbb{Z}^+$ is

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

They prove the following typical order result on $T_{\mathrm{CM}}(d)$.

Theorem. [BCP17, Theorem 1.1.(i)] *For all $\epsilon > 0$ there exists $B_\epsilon \in \mathbb{Z}^+$ so that*

$$\bar{\delta}(\{d \in \mathbb{Z}^+ : T_{\mathrm{CM}}(d) \geq B_\epsilon\}) \leq \epsilon.$$

The above theorem says that for any $\epsilon > 0$ we choose, by removing some subset $S \subseteq \mathbb{Z}^+$ of upper density $\leq \epsilon$, there exists a uniform bound B_ϵ on all CM torsion subgroups over all degree $d \notin S$ number fields; writing this out,

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

for any CM elliptic curve $E_{/F}$ where F is a number field whose degree $[F : \mathbb{Q}] \notin S$. In light of this, we say that the family of CM elliptic curves over number fields is *typically bounded in torsion.*

Compare this result to the following, which shows that torsion is decidedly not typically bounded on the family of all elliptic curves over all number fields, which we denote by $\mathcal{A}(1)$.

Theorem. [CMP18, Theorem 1.7] *For all $B \in \mathbb{Z}^+$ the set*

$$\{d \in \mathbb{Z}^+ : T(d) \geq B\}$$

is cofinite in $\mathbb{Z}^+$, whence its upper density is equal to 1.

3.1.2 Typically bounding torsion for other families

Despite the failure of $\mathcal{A}(1)$ to be typically bounded in torsion, we saw that the proper subfamily $\mathcal{A}_{\text{CM}}(1)$ of CM elliptic curves over number fields is. We will see there are also other familiar subfamilies of $\mathcal{A}(1)$ which are typically bounded in torsion.

Let $\mathcal{F} = \{E_{i/F_i}\}_{i \in I}$ be a family of elliptic curves E_i defined over number fields F_i. From here on out, we assume that any such $\mathcal{F}$ is "closed under rational isomorphism", e.g., if $E_{1/F} \in \mathcal{F}$ and $E_{2/F}$ is an elliptic curve with $E_2 \cong_F E_1$, then $E_{2/F} \in \mathcal{F}$. We say that $\mathcal{F}$ is *typically bounded in torsion* if the torsion subgroups $E(F)[\text{tors}]$ of elliptic curves $E_{/F} \in \mathcal{F}$ can be made uniformly bounded after removing those elements whose number field degrees all lie in a certain subset of $\mathbb{Z}^+$ of arbitrarily small upper density. Formally stated, $\mathcal{F}$ is

typically bounded in torsion if for all $\epsilon > 0$ there is a constant $B_\epsilon > 0$ so that the set

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

has upper density at most ϵ.

For a family $\mathcal{F}$ of elliptic curves, one can define an $\mathcal{F}$-analogue of $T(d)$,

$$T_{\mathcal{F}}(d) := \max_{E_{/F} \in \mathcal{F}, [F:\mathbb{Q}]=d} \#E(F)[\text{tors}].$$

Observe that $T_{\mathcal{F}}(d) \leq T(d) < \infty$. By our notation, $T_{\text{CM}}(d) = T_{\mathcal{A}_{\text{CM}}(1)}(d)$. It is clear that $\mathcal{F}$ is typically bounded in torsion iff for all $\epsilon > 0$ there exists a constant $B_\epsilon > 0$ so that

$$\overline{\delta}(\{d \in \mathbb{Z}^+ : T_{\mathcal{F}}(d) \geq B_\epsilon\}) \leq \epsilon.$$

Compare this to [BCP17, Theorem 1.1.(i)] above.

One important family of elliptic curves is $\mathcal{B}_{\mathbb{Q}}$, which are those base-changed from $\mathbb{Q}$ (see also (1.1)). For example, Lozano-Robledo shows that for all elliptic curves $E_{/F} \in \mathcal{B}_{\mathbb{Q}}$ and all primes $\ell \geq 11$ with $\ell \neq 13, 37$, if $\ell \mid \#E(F)[\text{tors}]$ then $\ell \leq 2[F : \mathbb{Q}] + 1$ [LR13, Theorem 1.3]. On the other hand, González-Jiménez and Najman show that for elliptic curves $E_{/F} \in \mathcal{B}_{\mathbb{Q}}$, one has $E(F)[\text{tors}] = E(\mathbb{Q})[\text{tors}]$ when $2, 3, 5, 7 \nmid [F : \mathbb{Q}]$ [GJN20, Theorem 7.2.i]; as an aside, this latter result is generalized in Chapter 6.

A (subtly) larger family is $\mathcal{E}_{\mathbb{Q}}$, that of elliptic curves $E_{/F}$ with $\mathbb{Q}$-rational j-invariant. For example, the elliptic curve $E : y^2 = x^3 + ix$ is clearly defined over $\mathbb{Q}(i)$, but its j-invariant $j(E) = 1728$. For an elliptic curve $E_{/F} \in \mathcal{E}_{\mathbb{Q}}$, Propp [Pro18] provides (conditional) bounds on prime divisors of $E(F)[\text{tors}]$ when $[F : \mathbb{Q}]$ is fixed. Clark and Pollack [CP18] also show that for each $\epsilon > 0$ there is a constant $C(\epsilon) > 0$ such that for all $E_{/F} \in \mathcal{E}_{\mathbb{Q}}$, one has polynomial bounds $\#E(F)[\text{tors}] \leq C(\epsilon)[F : \mathbb{Q}]^{\frac{5}{2}+\epsilon}$.

For this section, we study the more general family $\mathcal{E}_{F_0}$ (see also (1.2)). Clark, Milosevic and Pollack study the subfamily $\mathcal{E}'_{F_0}$ of elliptic curves $E_{/L} \in \mathcal{E}_{F_0}$ with $L \supseteq F_0$ [CMP18]. They show that torsion is typically bounded in $\mathcal{E}'_{F_0}$, provided F_0 contains no Hilbert class fields of

imaginary quadratic fields and that GRH is true [CMP18, Theorem 1.8]. By a brief twisting argument, their proof also shows that $\mathcal{E}_{F_0}$ is typically bounded in torsion when one imposes these conditions on F_0.

Our main result is a generalization of [CMP18, Theorem 1.8]: we prove it for $\mathcal{E}_{F_0}$ unconditionally.

Theorem 4. *For any number field F_0, torsion is typically bounded on the family $\mathcal{E}_{F_0}$.*

3.1.3 Strategy of the proof

Our proof of Theorem 4 will be broken down into several steps, following [CMP18]. To begin with, let us recall from [CMP18] properties **P1** and **P2** which apply to certain families $\mathcal{F}$ of elliptic curves. For an elliptic curve $E_{/F}$ and an integer $N \in \mathbb{Z}^+$, we will use $E(F)[N]^*$ to denote the set of F-rational torsion points on E of exact order N.

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 $E(F)[\ell^n]^* \neq \emptyset$ 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 $E(F)[\ell]^* \neq \emptyset$ then

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

Remark 1. For a family $\mathcal{F}$, if for some constants $c, \ell_0 \in \mathbb{Z}^+$ we show that for all $E_{/F} \in \mathcal{F}$ and for all primes $\ell \geq \ell_0$ with $E(F)[\ell]^* \neq \emptyset$ one has $\ell - 1 \mid c[F : \mathbb{Q}]$, then it follows that $\mathcal{F}$ satisfies **P2** with the constant $c(\mathcal{F}) := c \cdot \prod_{\ell \leq \ell_0}(\ell - 1)$. In particular, to prove that $\mathcal{F}$ satisfies **P2,** we only need to show that $\ell - 1 \mid c[F : \mathbb{Q}]$ holds for sufficiently large primes ℓ with respect to $\mathcal{F}$.

The utility of property **P1** and **P2** is in the following theorem (which was partially referred to in Chapter 3).

Theorem 5. [CP18, Theorem 3.2] *If a family $\mathcal{F}$ satisfies **P1** and **P2**, then $\mathcal{F}$ is typically bounded in torsion.*

Note that by Remark 1, for property **P2** to hold for a family $\mathcal{F}$, it only needs to hold for sufficiently large primes with respect to $\mathcal{F}$. Property **P1** is based off the fact that over number fields of a fixed degree, degrees of ℓ-primary torsion points on elliptic curves uniformly tend to infinity as the torsion point orders get larger. Property **P2** is related to a theorem of Erdős and Wagstaff [EW80, Theorem 2]. For more context, see the proof of [CMP18, Theorem 3.2].

For an integer $d \in \mathbb{Z}^+$ let us consider the family $\mathcal{E}_d$ of elliptic curves over number fields with degree d j-invariant,

$$\mathcal{E}_d := \{E_{/F} : [F : \mathbb{Q}] < \infty, [\mathbb{Q}(j(E)) : \mathbb{Q}] = d\}.$$

By [CMP18, Theorems 3.2.b and 3.5] any subfamily of a finite union of $\mathcal{E}_d$ will be typically bounded in torsion if and only if the subfamily satisfies **P2**. In particular, from the containment

$$\mathcal{E}_{F_0} \subseteq \bigcup_{d=1}^{[F_0:\mathbb{Q}]} \mathcal{E}_d,$$

to prove Theorem 4 it suffices to show that $\mathcal{E}_{F_0}$ satisfies condition **P2**.

Following the proof of [CMP18, Theorem 4.3], to show that **P2** holds for $\mathcal{E}_{F_0}$ it suffices to construct a constant $c := c(F_0) \in \mathbb{Z}^+$ such that for any prime $\ell \gg_{F_0} 0$ and any elliptic curve $E_{/F_0}$ with an F_0-rational ℓ-isogeny, one has for all nontrivial $R \in E[\ell]$ that

$$\ell - 1 \mid c \cdot [F_0(R) : \mathbb{Q}]. \tag{3.1}$$

Since E has an F_0-rational ℓ-isogeny, the image G of its mod-ℓ Galois representation is conjugate to a subgroup of upper triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. We will use this fact to compare the orbits of this representation acting on the standard unit vectors, to the orbits of its semisimplification.

First, a careful analysis of the description of our isogeny character from case 1 of Theorem 7 (see the following section) will allow us to relate the semisimplification of G to the mod-ℓ

Galois representation of some CM elliptic curve $E'_{/F_0}$ with F_0-rational CM. By an orbit-divisibility argument, we will show that (3.1) holds when we replace E with E', and conclude that such a divisibility holds for E with constant $c := 864$. Following this, we will show that the same constant also works when in case 2 of Theorem 7.

It is worth noting that Lozano-Robledo [LR18] uses a similar analysis of Theorem 7 to deduce, under certain hypotheses, degree-linear bounds on the order of any rational prime power torsion point. In fact, [LR18, Theorem 1.9] proves (3.1) in the form of an inequality. However, divisibility allows us to apply [CMP18, Theorem 3.2] and conclude that torsion is typically bounded on $\mathcal{E}_{F_0}$.

3.1.4 An additional result

In our proof of Theorem 4, the constant $c := 864$ for which (3.1) holds is independent of the choice of base field F_0. We will use this to improve [CMP18, Theorem 1.10].

For a fixed integer $d_0 \in \mathbb{Z}^+$, we denote by $\mathbf{SI}(d_0)$ the *strong isogeny conjecture in degree* d_0, which asserts that there exists a prime $\ell_0 := \ell_0(d_0) \in \mathbb{Z}^+$ so that for all primes $\ell > \ell_0$ there do not exist non-CM elliptic curves $E_{/F}$ with an F-rational ℓ-isogeny when $[F : \mathbb{Q}] = d_0$. The strong isogeny conjecture $\mathbf{SI}(d_0)$ would follow from a stronger conjecture of Serre which has been used to prove other results, see for example [BELOV19, Theorem 1.6].

Let us denote by $\mathbf{LV}(d_0)$ the hypothesis that the set S_F of primes from Theorem 7 (see the next section) depends only on d_0 for all number fields F of degree d_0. One may check that $\mathbf{LV}(d_0)$ is a weaker hypothesis than $\mathbf{SI}(d_0)$.

Theorem 6. *Fix an integer $d_0 \in \mathbb{Z}^+$. If $\mathbf{LV}(d_0)$ holds, then the family*

$$\mathcal{E}_{d_0} := \{E_{/F} : [F : \mathbb{Q}] < \infty, [\mathbb{Q}(j(E)) : \mathbb{Q}] = d_0\}$$

is typically bounded in torsion.

The proof of Theorem 6 is similar to the proof of [CMP18, Theorem 1.8], which boils down to the proof of [CMP18, Theorem 4.3]. By [CMP18, Theorem 3.5], to show that $\mathcal{E}_{d_0}$ is

typically bounded in torsion it suffices to show it satisfies condition **P2**. In turn, this reduces to showing that for any prime $\ell \gg_{d_0} 0$ one has a constant $c := c(d_0) \in \mathbb{Z}^+$ such that for any non-CM elliptic curve $E_{/\mathbb{Q}(j(E))}$ with a $\mathbb{Q}(j(E))$-rational ℓ-isogeny, the divisibility

$$\ell - 1 \mid c \cdot [\mathbb{Q}(j(E))(R) : \mathbb{Q}]$$

holds for all nontrivial $R \in E[\ell]$. In [CMP18], the authors cite $\mathbf{SI}(d_0)$ to exclude this case. But if one assumes $\mathbf{LV}(d_0)$ instead, then our proof of Theorem 4 applies here and we may take $c := 864$.

3.2 Isogeny Characters à la Larson and Vaintrob

Given a group homomorphism $f\colon G \to H$, we sometimes write $\operatorname{im} f$ for its image $f(G)$. We will also sometimes write $\mathbb{F}_\ell := \mathbb{Z}/\ell\mathbb{Z}$.

A crucial component of the proof of Theorem 4 is an analysis of the description of our isogeny character from a result of Larson and Vaintrob [LV14].

Theorem 7. [LV14, Theorem 1] *Let F_0 be a number field. Then there is a finite set of primes $S_{F_0} \subseteq \mathbb{Z}^+$ such that for all primes $\ell \notin S_{F_0}$, if $E_{/F_0}$ is an elliptic curve with an F_0-rational ℓ-isogeny, then for the corresponding isogeny character $r\colon G_{F_0} \to \mathbb{F}_\ell^\times$ one of the following holds:*

1. There exists a CM elliptic curve E' defined over F_0 such that its CM field $K := \operatorname{End}(E') \otimes \mathbb{Q}$ is contained in F_0. Furthermore, there exists a character $\psi'\colon G_F \to \overline{\mathbb{F}_\ell}^\times$ for which we have both similarity

$$(\rho_{E',\ell} \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}_\ell})(G_{F_0}) \sim \operatorname{im} \begin{bmatrix} \psi' & * \\ 0 & \chi_\ell \psi'^{-1} \end{bmatrix}$$

and equality

$$r^{12} = \psi'^{12}.$$

2. GRH fails for $F_0(\sqrt{-\ell})$, and we have

$$r^{12} = \chi_\ell^6.$$

As per the theory of complex multiplication, the ring class field of an order $\mathcal{O}$ in an imaginary quadratic field K will equal $K(j(E'))$ for any $\mathcal{O}$-CM elliptic curve E', and all such fields will contain the Hilbert class field of K. In particular, for F_0 not to contain Hilbert class fields of imaginary quadratic fields is equivalent to there being no CM elliptic curve E' defined over F_0 for which $\mathrm{End}(E') \otimes \mathbb{Q} \subseteq F_0$. For such a field F_0, if one also assumes that GRH is true then Theorem 7 tells us that for $\ell \gg_{F_0} 0$ there are no F_0-rational ℓ-isogenies on any elliptic curve. It is this observation, coupled with the fact that if $\mathcal{F}$ satisfies condition **P2** then one can exclude finitely many primes $\ell \in \mathbb{Z}^+$ and still have condition **P2** hold for $\mathcal{F}$, which shows us that $\mathcal{E}_{F_0}$ satisfies condition **P2** – this is outlined in [CMP18, Theorem 4.3.b]. In particular, torsion is typically bounded on $\mathcal{E}_{F_0}$, conditionally.

To prove Theorem 4 we will not assume that GRH is true nor that F_0 does not contain the Hilbert class field of any imaginary quadratic field. Instead, we will leverage the extra information from Theorem 7 on our possible isogeny characters to construct a constant c for which (3.1) holds for all $\ell \gg_{F_0} 0$ and all $E_{/F_0}$ with an F_0-rational ℓ-isogeny.

3.3 Orbits Under the Galois Representation

In our study of the mod-ℓ Galois representations of an elliptic curve $E_{/F}$, it will help to understand the orbits of the $\mathbb{F}_\ell[G_F]$-module $E[\ell]$ under various subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

3.3.1 The semisimplification of an upper triangular subgroup of $\mathbf{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

Fix a prime ℓ, and suppose $G \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is a subgroup of upper triangular matrices. Let us consider its *semisimplification*

$$G^{\mathrm{ss}} := \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \exists b \in \mathbb{F}_\ell \ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in G \right\}.$$

The group $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ acts on the $\mathbb{F}_\ell$-vector space V spanned by the column vectors $e_1 := \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $e_2 := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ via multiplication on the left. Consequently, its subgroups G and G^{ss} also act on V via left multiplication.

Ultimately, we will compare divisibility of the sizes of such orbits from the action of $\mathrm{Gal}(F(E[\ell])/F)$ on $E[\ell]^\bullet := E[\ell] \smallsetminus \{O\}$. The following lemma is an important step towards such a comparison.

Lemma 8. *Let $\ell \in \mathbb{Z}^+$ be prime, and let G be an upper triangular subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Then $G^{\mathrm{ss}} \subseteq G$ or G is diagonalizable.*

Proof. We will break the proof into three cases. In the first two cases, we will show containment $G^{\mathrm{ss}} \subseteq G$.

Case 1: G contains a non-diagonal matrix with repeated eigenvalues. Such a matrix is of the form $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$ with $b \neq 0$. For such a matrix γ, its power $\gamma^{\ell-1}$ equals

$$\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \in G \tag{3.2}$$

where $\lambda := (\ell-1)ba^{\ell-2} \neq 0$. It follows that G contains the transvection

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \gamma^A \in G,$$

where $A \in \mathbb{Z}$ is taken so that $A \equiv \lambda^{-1} \pmod{\ell}$. We conclude that for each $n \in \mathbb{Z}$ we have

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \in G.$$

It follows that $G^{\mathrm{ss}} \subseteq G$. Indeed, for any element $\delta := \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in G$ we check that

$$\delta \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & an+b \\ 0 & d \end{bmatrix},$$

so taking $n \in \mathbb{Z}$ such that $n \equiv -ba^{-1} \pmod{\ell}$ shows that $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \in G$.

Case 2: G is not commutative. Then choosing any $\gamma_1, \gamma_2 \in G$ with nontrivial commutator, their commutator $\gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}$ must be of the form $\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}$ for some $\lambda \in \mathbb{F}_\ell^\times$. Then the steps following (3.2) show that $G^{\mathrm{ss}} \subseteq G$.

Case 3: Neither case 1 nor case 2 holds. Then G is commutative, and its non-diagonal matrices have distinct $\mathbb{F}_\ell$-rational eigenvalues. In particular, each non-diagonal matrix is diagonalizable over $\mathbb{F}_\ell$, and since all matrices in G commute we deduce that there is a simultaneous diagonalization for these matrices over $\mathbb{F}_\ell$.[1] The conclusion is that G is conjugate to a subgroup of diagonal matrices. □

[1] For a proof of this fact, see e.g. [Con].

3.3.2 Orbits in the diagonal case

In our describing the orbits of the action of $\mathrm{Gal}(F(E[\ell])/F)$ on $E[\ell]^\bullet$, we will relate them to the orbits of $E[\ell]^\bullet$ under its semisimplification, the latter of which is contained in the subgroup $C_s(\ell)$ of diagonal matrices.

Let $G' \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ be a subgroup of diagonal matrices. Associated to this group are the two characters which describe the diagonal entries of matrices in G',

$$\chi_1 \colon G' \to \mathbb{F}_\ell^\times, \quad \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \mapsto a$$

and

$$\chi_2 \colon G' \to \mathbb{F}_\ell^\times, \quad \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \mapsto d.$$

We will study the orbits of elements v in $V^\bullet := \mathbb{F}_\ell\langle e_1, e_2\rangle \smallsetminus \{0\}$ under G'; we will use $\mathcal{O}_{G'}(v)$ to denote G'-orbits.

The following lemma describes the orbits under a diagonal subgroup.

Lemma 9. *Let $G' \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ be a subgroup of diagonal matrices, with diagonal characters χ_1 and χ_2. Then the number of orbits of the form $\mathcal{O}_{G'}(ae_1)$ (resp. $\mathcal{O}_{G'}(de_2)$) with $a \in \mathbb{F}_\ell^\times$ (resp. $d \in \mathbb{F}_\ell^\times$) is equal to the index $[\mathbb{F}_\ell^\times : \mathrm{im}\chi_1]$ (resp. $[\mathbb{F}_\ell^\times : \mathrm{im}\chi_2]$), and each such orbit is of size $\#\mathrm{im}\chi_1$ (resp. $\#\mathrm{im}\chi_2$). Orbits of the form $\mathcal{O}_{G'}(ae_1 + de_2)$ with $a, d \in \mathbb{F}_\ell^\times$ are in bijection with the orbit $\mathcal{O}_{G'}(e_1 + e_2)$, and the number of such orbits is $(\ell-1)^2/\#\mathcal{O}_{G'}(e_1+e_2)$.*

Proof. First, we claim that there are $I_1 := [\mathbb{F}_\ell^\times : \mathrm{im}\,\chi_1]$ distinct orbits of the form $\mathcal{O}_{G'}(ae_1)$ where $a \in \mathbb{F}_\ell^\times$. To see this, let us check that the map

$$\mathbb{F}_\ell^\times/\mathrm{im}\,\chi_1 \to \{\text{Orbits } \mathcal{O}_{G'}(ae_1) : a \in \mathbb{F}_\ell^\times\}, \ \overline{a} \mapsto \mathcal{O}_{G'}(ae_1)$$

is a well-defined bijection:

1. Well-defined: if $a = \chi_1(\gamma)b$ then $\gamma = \begin{bmatrix} ab^{-1} & 0 \\ 0 & d \end{bmatrix}$ for some $d \in \mathbb{F}_\ell^\times$, and thus

$$\mathcal{O}_{G'}(be_1) = \mathcal{O}_{G'}(\gamma be_1) = \mathcal{O}_{G'}(ae_1).$$

2. Injective: suppose that $\mathcal{O}_{G'}(ae_1) = \mathcal{O}_{G'}(be_1)$. Then for some $\gamma \in G'$ we have $ab^{-1}e_1 = \gamma e_1$, whence we have $\chi_1(\gamma) = ab^{-1}$, i.e., $a \cdot \operatorname{im}\chi_1 \equiv b \cdot \operatorname{im}\chi_1$ in $\mathbb{F}_\ell^\times/\operatorname{im}\chi_1$.

3. Surjective: obvious.

We conclude that e_1 contributes I_1 distinct orbits of the form $\mathcal{O}_{G'}(ae_1)$ with $a \in \mathbb{F}_\ell^\times$, each of size $\#\operatorname{im}\chi_1$. An identical argument shows that e_2 contributes $I_2 := [\mathbb{F}_\ell^\times : \operatorname{im}\chi_2]$ distinct orbits of the form $\mathcal{O}_{G'}(de_2)$ where $d \in \mathbb{F}_\ell^\times$, each of size $\#\operatorname{im}\chi_2$. The remaining orbits are of the form $\mathcal{O}_{G'}(ae_1+de_2)$ where $ad \neq 0$. A similar argument shows that $\#\mathcal{O}_{G'}(ae_1+de_2) = \#\mathcal{O}_{G'}(e_1+e_2)$ when $ad \neq 0$.

The orbits above partition $V^\bullet := \mathbb{F}_\ell\langle e_1, e_2\rangle \smallsetminus \{0\}$. If we let X denote the number of distinct orbits of the form $\mathcal{O}_{G'}(ae_1 + de_2)$ with $ad \neq 0$, then we deduce that

$$I_1\#\operatorname{im}\chi_1 + I_2\#\operatorname{im}\chi_2 + X\#\mathcal{O}_{G'}(e_1 + e_2) = \ell^2 - 1.$$

In particular, since $I_1\#\operatorname{im}\chi_1 = I_2\#\operatorname{im}\chi_2 = \ell - 1$ we conclude that

$$X\#\mathcal{O}_{G'}(e_1 + e_2) = (\ell - 1)^2. \qquad \square$$

3.3.3 Uniform orbit divisibility

Suppose that a group G acts on a finite set X. For an element $x \in X$ let us use $\mathcal{O}_G(x)$ to denote its orbit. Let us say that an integer $M \in \mathbb{Z}^+$ *uniformly divides* G-orbits if there exists an integer $c \in \mathbb{Z}^+$ such that for all $x \in X$ one has

$$M \mid c \cdot \#\mathcal{O}_G(x).$$

Clearly, any integer $M > 0$ will uniformly divide G-orbits if we take $c := M$. The relevance of uniform divisibility comes from the following lemma, which will allow us to prove (3.1) when we replace the image G of our mod-ℓ Galois representation with a particular subgroup, and then "carry over" this constant c to the divisibility (3.1) for E. As will be shown in the proof of (3.1), such a constant will not depend on $M := \ell - 1$, nor on E.

Lemma 10. *Let G be a group which acts on a finite set X on the left, and let $H \subseteq G$ be a finite index subgroup.*

1. *If for an integer $M > 0$ there is a constant $c \in \mathbb{Z}^+$ such that for all $x \in X$ we have $M \mid c \cdot \#\mathcal{O}_H(x)$, then we also have for all $x \in X$ the divisibility $M \mid c \cdot \#\mathcal{O}_G(x)$.*

2. *If for an integer $M > 0$ there is a constant $C \in \mathbb{Z}^+$ such that for all $x \in X$ we have $M \mid C \cdot \#\mathcal{O}_G(x)$, then we also have for all $x \in X$ the divisibility $M \mid C \cdot [G : H] \cdot \#\mathcal{O}_H(x)$.*

Proof. Let us write the left coset representatives of H as $g_1^{-1}, \ldots, g_{[G:H]}^{-1}$. Then one has

$$\mathcal{O}_G(x) = \bigsqcup_{i=1}^{[G:H]} \mathcal{O}_H(g_i x).$$

It follows that for all $x \in X$ one has

$$\#\mathcal{O}_G(x) = \sum_{i=1}^{[G:H]} \#\mathcal{O}_H(g_i x),$$

from which the first part follows. The second part follows from the fact that for each $x \in X$ one has $\#\mathcal{O}_G(x) \mid [G : H] \cdot \#\mathcal{O}_H(x)$. □

3.3.4 Action on ℓ-torsion

Let F be a number field and $E_{/F}$ an elliptic curve. Throughout this paper we are considering for various primes $\ell \in \mathbb{Z}^+$ the mod-ℓ Galois representation of the absolute Galois group G_F acting on the $\mathbb{F}_\ell$-module $E[\ell]$. At each level ℓ, our action induces a faithful action $\rho_{E,\ell} \colon \mathrm{Gal}(F(E[\ell])/F) \hookrightarrow \mathrm{Aut}(E[\ell])$. We will often work with a basis $\{P, Q\}$ of $E[\ell]$ in

mind, in which case the image $G := \rho_{E,\ell,P,Q}(\mathrm{Gal}(F(E[\ell])/F))$ of our Galois representation is identified with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

3.4 Part One of the Proof: Allowing Rationally Defined CM

To recapitulate our goals: we will prove Theorem 4, which is an unconditional form of [CMP18, Theorem 1.8]. This means we will allow our number field F to contain Hilbert class fields of imaginary quadratic fields, and we will not assume that GRH is true. Following the proof of [CMP18, Theorem 4.3], we will show the following: for all primes $\ell \gg_{F_0} 0$ and all non-CM elliptic curves $E_{/F_0}$ whose mod-ℓ Galois representation image $G := \rho_{E,\ell}(G_{F_0})$ is contained in a Borel subgroup – i.e., G is conjugate to a subgroup of upper triangular matrices – one has that all G-orbits are uniformly divisible by $\ell - 1$ with an absolute constant, i.e., there exists $c \in \mathbb{Z}^+$ such that for all ℓ-torsion $R \in E[\ell]^\bullet$, one has that Equation (3.1) holds,

$$\ell - 1 \mid c \cdot [F_0(R) : \mathbb{Q}].$$

For this section, let us assume that GRH is true. This will land us in case 1 of Theorem 7, where our isogeny character agrees with a CM "mod-ℓ associated character" up to twelfth powers.

3.4.1 Reducing to the split prime case

As per Remark 1, we can exclude any finite amount of primes from our consideration. We will show why this lets us assume that $\ell \gg_{F_0} 0$ is split in the orders which come from Theorem 7.

For any $\mathcal{O}$-CM elliptic curve E' defined over F_0 where $K := \mathcal{O} \otimes \mathbb{Q} \subseteq F_0$, we have that the ring class field $K(\mathcal{O}) = K(j(E')) \subseteq F_0$. Since F_0 may contain only finitely many such ring class fields,[2] we need only to consider finitely many imaginary quadratic orders $\mathcal{O}$ and

[2]This is an application of Heilbronn's classic result on imaginary quadratic class numbers [Hei34] towards showing that the class number of an imaginary quadratic order $\mathcal{O}$ tends to infinity as its discriminant $\Delta(\mathcal{O}) \to -\infty$.

(up to isomorphism) finitely many $\mathcal{O}$-CM $E'_{/F_0}$. In particular, for the rest of the section let us assume that ℓ is unramified in any imaginary quadratic order $\mathcal{O}$ with $[K(\mathcal{O}) : \mathbb{Q}] \leq [F : \mathbb{Q}]$. It will follow that our CM associated character ψ' in Theorem 7 will give us a diagonalization of the image of our CM Galois representation over $\overline{\mathbb{F}_\ell}$.

Suppose that $E_{/F_0}$ is an elliptic curve whose mod-ℓ Galois representation image is contained in a Borel subgroup, i.e., suppose that E has an F_0-rational ℓ-isogeny. Let $r\colon G_{F_0} \to \mathbb{F}_\ell^\times$ denote its isogeny character. Assuming $\ell \gg_{F_0} 0$ as above and $\ell \notin S_F$ where S_{F_0} is as in Theorem 7, there exists an elliptic curve $E'_{/F_0}$ with CM by an imaginary quadratic order $\mathcal{O}$ whose CM field $K := \mathcal{O} \otimes \mathbb{Q} \subseteq F_0$, and there exists a character $\psi'\colon G_{F_0} \to \overline{\mathbb{F}_\ell}^\times$ for which both

$$(\rho_{E',\ell} \otimes \overline{\mathbb{F}_\ell})(G_{F_0}) \sim \text{im} \begin{bmatrix} \psi' & 0 \\ 0 & \chi_\ell \psi'^{-1} \end{bmatrix} \tag{3.3}$$

and

$$r^{12} = \psi'^{12}. \tag{3.4}$$

We note that Equation (3.4) implies

$$\gcd(12, \#\psi'(G_{F_0})) \cdot \#r(G_{F_0}) = \gcd(12, \#r(G_{F_0})) \cdot \#\psi'(G_{F_0}). \tag{3.5}$$

We may assume that ℓ is odd. Suppose that ℓ is inert in $\mathcal{O}$. In this case, up to conjugation the image $\rho_{E',\ell}(G_{F_0})$ of the CM Galois representation lands in the non-split Cartan subgroup $C_{ns}(\ell)$ of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, see Section 2.1.3. For $\ell > 2$, one has an isomorphism $\mathbb{F}_\ell(\sqrt{\epsilon})^\times \cong C_{ns}(\ell)$ by sending each element $a + b\sqrt{\epsilon} \in \mathbb{F}_\ell(\sqrt{\epsilon})^\times$ to its regular matrix representation $\begin{bmatrix} a & b\epsilon \\ b & a \end{bmatrix}$. The eigenvalues of such matrices are $a \pm b\sqrt{\epsilon}$, and since the Galois group $\mathrm{Gal}(\mathbb{F}_\ell(\sqrt{\epsilon})/\mathbb{F}_\ell)$ is generated by the Frobenius automorphism $\alpha \mapsto \alpha^\ell$, these eigenvalues are Galois conjugates. This implies that ψ' and $\chi_\ell \psi'^{-1}$ are Galois conjugates. Therefore, Equation (3.3) shows that

$$\#\rho_{E',\ell}(G_{F_0}) = \#\psi'(G_{F_0}).$$

Since $\#r(G_{F_0}) \mid (\ell-1)$, comparing this to (3.5) shows that

$$\#\rho_{E',\ell}(G_{F_0}) \mid 12(\ell-1). \tag{3.6}$$

On the other hand, $\mathcal{O}$-CM theory with ℓ inert tells us that for any torsion point $P' \in E'[\ell]^\bullet$ one has

$$(\ell^2-1) \mid \#\mathcal{O}^\times \cdot [F_0 : K(\mathcal{O})] \cdot [F_0(P') : F_0]$$

where $\mathcal{O}^\times$ denotes the unit group of $\mathcal{O}$, see [BC20, Theorem 7.2]. In particular, from

$$[F_0(P') : F_0] \mid [F_0(E'[\ell]) : F_0] = \#\rho_{E',\ell}(G_{F_0})$$

we find that

$$(\ell^2-1) \mid \#\mathcal{O}^\times \cdot [F_0 : K(\mathcal{O})] \cdot \#\rho_{E',\ell}(G_{F_0}).$$

Comparing this with (3.6), we conclude that $\ell+1 \mid 72[F_0 : K(\mathcal{O})]$, which bounds ℓ that come from the case where an elliptic curve has an F_0-rational ℓ-isogeny for ℓ inert in an imaginary quadratic order in F_0.

Henceforth, we assume that ℓ splits in any order $\mathcal{O}$ we are considering. This implies that the CM image $\rho_{E',\ell}(G_{F_0})$ lands in the split Cartan subgroup $C_s(\ell)$ of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ up to conjugacy, and so $\rho_{E',\ell}(G_{F_0})$ is diagonalizable over $\mathbb{F}_\ell$. In particular, our character ψ' must be the isogeny character of an F_0-rational ℓ-isogeny $\langle P' \rangle$ of E'.

3.4.2 Showing that $\mathcal{E}_{F_0}$ satisfies P2, conditional on GRH

As per Lemma 4, by conjugating if necessary we may assume that with respect to a basis $\{P, Q\}$ of $E[\ell]$, G is both upper triangular and contains its semisimplification G^{ss}. Without loss of generality, let us suppose that $\langle P \rangle$ is an F_0-rational ℓ-isogeny whose isogeny character is $r \colon G_{F_0} \to \mathbb{F}_\ell^\times$. Then we have

$$G := \rho_{E,\ell,P,Q}(G_{F_0}) = \mathrm{im} \begin{bmatrix} r & * \\ 0 & \chi_\ell r^{-1} \end{bmatrix}$$

where $*\colon G_{F_0} \to \mathbb{F}_\ell^\times$ is not necessarily a character. Let us assume that $\ell \gg_{F_0} 0$ as in the previous subsection and $\ell \notin S_{F_0}$. Then Theorem 7 applies: we have an $\mathcal{O}$-CM elliptic curve $E'_{/F_0}$ with an F_0-rational ℓ-isogeny $\langle P' \rangle$, say with isogeny character $\psi'\colon G_{F_0} \to \mathbb{F}_\ell^\times$, and there is a complementary basis element Q' to P' so that the image of the mod-ℓ Galois representation of E' is diagonal with respect to the basis $\{P', Q'\}$. Let us write

$$G' := \rho_{E',\ell,P',Q'}(G_{F_0}) = \mathrm{im} \begin{bmatrix} \psi' & 0 \\ 0 & \chi_\ell \psi'^{-1} \end{bmatrix}.$$

We have written our actions here as left multiplication on the two-dimensional $\mathbb{F}_\ell$-vector space $V := \mathbb{F}_\ell\langle e_1, e_2 \rangle$ with e_i the unit column vectors. So for each $v = ae_1 + de_2 \in V$, under G one has that v corresponds to $R_v := aP + dQ \in E[\ell]$, and under G' one has that v corresponds to $R'_v := aP' + dQ' \in E'[\ell]$.

Since both $G^{\mathrm{ss}} \subseteq G$ and $r^{12} = \psi'^{12}$, we have the inclusions

$$C_s(\ell) \supseteq G' \supseteq G'^{12} \subseteq G^{\mathrm{ss}} \subseteq G.$$

Suppose we have a constant $C \in \mathbb{Z}^+$ so that uniform $C_s(\ell)$-orbit divisibility by $\ell - 1$ holds with C: i.e., for all $v \in V^\bullet$

$$\ell - 1 \mid C \cdot \#\mathcal{O}_{C_s(\ell)}(v).$$

Then by Lemma 10, the containment $C_s(\ell) \supseteq G'$ implies that for all $v \in V^\bullet$

$$\ell - 1 \mid C \cdot [C_s(\ell) : G'] \cdot \#\mathcal{O}_{G'}(v).$$

With uniform divisibility of G'-orbits via the constant $C \cdot [C_s(\ell) : G']$, we apply Lemma 10 to the containment $G' \supseteq G'^{12}$ and find that for all $v \in V^\bullet$

$$\ell - 1 \mid C \cdot [C_s(\ell) : G'] \cdot [G' : G'^{12}] \cdot \#\mathcal{O}_{G'^{12}}(v).$$

A final application of Lemma 10 towards the containment $G'^{12} \subseteq G$ implies that for all $v \in V^\bullet$ one has

$$\ell - 1 \mid C \cdot [C_s(\ell) : G'] \cdot [G' : G'^{12}] \cdot \#\mathcal{O}_G(v),$$

i.e., for all $R \in E[\ell]^\bullet$

$$\ell - 1 \mid C \cdot [C_s(\ell) : G'] \cdot [G' : G'^{12}] \cdot [F_0(R) : F_0].$$

Since $[G' : G'^{12}] \mid (12)^2$, this simplifies to

$$\ell - 1 \mid 144C \cdot [C_s(\ell) : G'] \cdot [F_0(R) : F_0]. \tag{3.7}$$

With (3.7) in mind, we will conclude that (3.1) holds with an absolute constant by showing that uniform $C_s(\ell)$-orbit divisibility by $\ell - 1$ holds with an absolute constant, and that the index $[C_s(\ell) : G']$ is bounded in terms of $[F_0 : \mathbb{Q}]$.

First, we claim that uniform $C_s(\ell)$-orbit divisibility by $\ell - 1$ holds with constant $C := 1$ – i.e., all $C_s(\ell)$-orbit sizes are divisible by $\ell - 1$. By Lemma 9, there are exactly three orbits of $C_s(\ell)$ under its action on $V^\bullet$: they are $\mathcal{O}_{C_s(\ell)}(e_1), \mathcal{O}_{C_s(\ell)}(e_2)$ and $\mathcal{O}_{C_s(\ell)}(e_1 + e_2)$, and each are of size $\ell - 1, \ell - 1$ and $(\ell - 1)^2$, respectively. This proves our first claim.

Next, we will show that the index $[C_s(\ell) : G']$ is bounded in terms of $[F_0 : \mathbb{Q}]$. In general, for an $\mathcal{O}$-CM elliptic curve $E'_{/F_0}$ with F_0-rational CM – i.e., $\mathcal{O} \otimes \mathbb{Q} \subseteq F_0$ – one has for any $N \in \mathbb{Z}^+$ that the image of its mod-N Galois representation will land inside the mod-N Cartan subgroup $C_N(\mathcal{O}) := (\mathcal{O}/N\mathcal{O})^\times$. In fact, the indices of *all* mod-N Galois representation images of E' are uniformly bounded in terms which involve F_0.

Theorem 11. [BC20, Corollary 1.5] *Let K be an imaginary quadratic field. Then the index of the image of the mod-N Galois representation of any $\mathcal{O}$-CM elliptic curve $E'_{/F}$ with $\mathcal{O} \otimes \mathbb{Q} = K \subseteq F$ satisfies*

$$[C_N(\mathcal{O}) : \rho_{E',N}(G_F)] \mid \#\mathcal{O}^\times [F : K(j(E'))].$$

Since ℓ splits in $\mathcal{O}$, the mod-ℓ Cartan subgroup is split, i.e., $C_N(\mathcal{O}) = C_s(\ell)$. Then by Theorem 11, we have that the index of the image of our CM mod-ℓ Galois representation G' satisfies

$$[C_s(\ell) : G'] \mid 6[F_0 : \mathbb{Q}].$$

Combining this with (3.7) shows that for all $R \in E[\ell]^\bullet$ one has

$$\ell - 1 \mid 864[F_0 : \mathbb{Q}] \cdot [F_0(R) : F_0].$$

We conclude that (3.1) holds for E with constant $c := 864$.

3.5 Part Two of the Proof: Removing GRH

Let $E_{/F_0}$ be an elliptic curve with an F_0-rational ℓ-isogeny for $\ell \gg_{F_0} 0$. We will show that (3.1) holds with constant $c := 864$ without assuming that GRH is true. In doing so, there is an additional case which may appear from Theorem 7 that will be dealt with in this section.

Let $\langle P \rangle$ be an F_0-rational ℓ-isogeny of E; let us write its isogeny character as $r \colon G_{F_0} \to \mathbb{F}_\ell^\times$. Suppose we are in case 2 of Theorem 7, so that

$$r^{12} = \chi_\ell^6 \tag{3.8}$$

where $\chi_\ell \colon G_{F_0} \to \mathbb{F}_\ell^\times$ is the mod-ℓ cyclotomic character.

As per Lemma 8, let us choose a basis $\{P, Q\}$ of $E[\ell]$ for which $G := \rho_{E,\ell,P,Q}(G_{F_0})$ is upper triangular and $G^{\mathrm{ss}} \subseteq G$. Then we have

$$G = \mathrm{im} \begin{bmatrix} r & * \\ 0 & \chi_\ell r^{-1} \end{bmatrix}$$

and thus

$$G^{\mathrm{ss}} = \mathrm{im} \begin{bmatrix} r & 0 \\ 0 & \chi_\ell r^{-1} \end{bmatrix}.$$

By Equation (3.8) we have $(\chi_\ell r^{-1})^6 = r^6$, whence we deduce that

$$(G^{\mathrm{ss}})^6 = \mathrm{im} \begin{bmatrix} r^6 & 0 \\ 0 & r^6 \end{bmatrix}$$

is a subgroup of scalars. As per the inclusions $(G^{\mathrm{ss}})^6 \subseteq G^{\mathrm{ss}} \subseteq G$, to show that (3.1) holds it suffices by Lemma 10 to show that $\ell - 1$ uniformly divides $(G^{\mathrm{ss}})^6$-orbits with constant $864[F_0 : \mathbb{Q}]$. In fact, we will show that for all $v \in \mathbb{F}_\ell \langle e_1, e_2 \rangle^\bullet$ one has

$$\ell - 1 \mid 36[F_0 : \mathbb{Q}] \cdot \#\mathcal{O}_{(G^{\mathrm{ss}})^6}(v).$$

By Lemma 9 the sizes of orbits of the form $\mathcal{O}_{(G^{\mathrm{ss}})^6}(ae_1)$ and $\mathcal{O}_{(G^{\mathrm{ss}})^6}(de_2)$ with $ad \neq 0$ are $\#r^6(G_F)$, and the rest of the orbits $\mathcal{O}_{(G^{\mathrm{ss}})^6}(ae_1 + de_2)$ with $ad \neq 0$ share the same size as the orbit $\mathcal{O}_{(G^{\mathrm{ss}})^6}(e_1 + e_2)$. Since the action under G^{ss} is scalar, it is clear that $\#\mathcal{O}_{(G^{\mathrm{ss}})^6}(e_1 + e_2) = \#r^6(G_{F_0})$. Therefore, to prove (3.1) with constant $c := 864$ it suffices to show that

$$\ell - 1 \mid 864[F_0 : \mathbb{Q}] \cdot \#r^6(G_{F_0}). \tag{3.9}$$

Since $r(G_{F_0})$ is cyclic, we observe that

$$\#r^{12}(G_{F_0}) = \frac{\#r(G_{F_0})}{\gcd(12, \#r(G_{F_0}))}.$$

Since $\chi_\ell(G_{F_0})$ is also cyclic, the image of its sixth power has size

$$\#\chi_\ell^6(G_{F_0}) = \frac{\ell - 1}{\gcd(6, \ell - 1)}.$$

Since $\chi_\ell^6 = r^{12}$, we compare these sizes and find that

$$\#\chi_\ell(G_{F_0}) \cdot \gcd(12, \#r(G_{F_0})) = \gcd(6, \#\chi_\ell(G_{F_0})) \cdot \#r(G_{F_0}),$$

whence we have

$$\#\chi_\ell(G_{F_0}) \mid 6 \cdot \#r(G_{F_0}).$$

Since we also have

$$\#r(G_{F_0}) = \#r^6(G_{F_0}) \cdot \gcd(6, \#r(G_{F_0}))$$

it follows that

$$\#\chi_\ell(G_{F_0}) \mid 36 \cdot \#r^6(G_{F_0}).$$

Finally, since $\chi_\ell \colon G_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ is surjective, we have $[\mathbb{F}_\ell^\times : \chi_\ell(G_{F_0})] \mid [F_0 : \mathbb{Q}]$, and so we conclude that

$$\ell - 1 \mid 36[F_0 : \mathbb{Q}] \cdot \#r^6(G_{F_0}).$$

This proves (3.9), which concludes our proof of Theorem 4.

Chapter 4

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

4.1 Introduction

The results in this chapter are a direct extension of those from Chapter 3. In particular, the following theorem extends Theorem 4.

Theorem 12. *For each number field F_0, the family $\mathcal{I}_{F_0}$ is typically bounded in torsion.*

As noted in the introduction, the study of torsion subgroups from $\mathcal{I}_{F_0}$ fits into a larger program of studying Galois representations of F_0-curves. Recall that for the family $\mathcal{Q}_{F_0}$ of F_0-curves (see also (1.4)), one has $\mathcal{I}_{F_0} \subset \mathcal{Q}_{F_0}$. If $F_0 = \mathbb{Q}$, then $\mathcal{Q}_{F_0} = \mathcal{Q}_{\mathbb{Q}}$ is the well-studied family of $\mathbb{Q}$-curves. By results of [Rib92, KW09a, KW09b], an elliptic curve is a $\mathbb{Q}$-curve iff it is a modular elliptic curve, i.e., is a quotient of the Jacobian $J_1(N)$ of the modular curve $X_1(N)$ for some $N \in \mathbb{Z}^+$. Furthermore, for any non-CM $\mathbb{Q}$-curve $E_{/F}$, if $[F : \mathbb{Q}]$ is odd then E is isogenous over F to an elliptic curve with $\mathbb{Q}$-rational j-invariant [CN21, Theorem 2.7]. Additionally, this forces the prime divisors of $\#E(F)[\text{tors}]$ to lie in the set $\{2, 3, 5, 7, 11, 13\}$, and in fact $\#E(F)[\text{tors}] \leq 1441440\sqrt{35} \cdot \sqrt{[F : \mathbb{Q}]}$ – these are consequences of recent work of Bourdon and Najman [BN, Proposition 4.1]. These results on torsion subgroups from $\mathcal{I}_{\mathbb{Q}}$ are part of the motivation for studying the family $\mathcal{I}_{F_0}$ in this paper.

It is very interesting to ask whether $\mathcal{Q}_{\mathbb{Q}}$ is typically bounded in torsion. Proving this using properties **P1** and **P2** (defined in Chapter 3) requires at least knowledge of degrees of torsion points on *central* $\mathbb{Q}$-curves (these are defined in e.g. [CN21]). Alternatively, a certain uniform boundedness conjecture for rational non-cuspidal non-CM points on the full Atkin-Lehner quotient modular curves $X^*(N)$, as described by Elkies [Elk04, Section 3] (see also Ellenberg [Ell04, Conjecture 3]), would imply that $\mathcal{Q}_{\mathbb{Q}}$ is typically bounded in torsion. But a proof of this boundedness conjecture currently seems out of reach.

4.1.1 An additional result

Similar to [Gen1, Theorem 2] we have an additional result under an extra hypothesis. For each integer $d_0 \in \mathbb{Z}^+$, let us define the family

$$\mathcal{I}_{d_0} := \{E_{/F} : E \text{ is geometrically isogenous to some } E' \text{ with } [\mathbb{Q}(j(E')) : \mathbb{Q}] = d_0\}.$$

Theorem 7 says that for any number field F_0 and for all primes $\ell \gg_{F_0} 0$, if an elliptic curve defined over F_0 has an F_0-rational isogeny of degree ℓ, then the twelfth power of its isogeny character is either the twelfth power of an isogeny character from a CM elliptic curve, or the sixth power of the mod-ℓ cyclotomic character. In [LV14, Theorem 7.9] Larson and Vaintrob give an upper bound on the implied constant $\ell \gg_{F_0} 0$ from Theorem 7, which depends on F_0. For $d_0 \in \mathbb{Z}^+$, recall from Chapter 3 that $\mathbf{LV}(d_0)$ denotes the hypothesis that this implied constant $\ell \gg_{F_0} 0$ can be chosen to be the same between any degree d_0 number field F_0. Then our proof of Theorem 12 also proves the following.

Theorem 13. *For any integer $d_0 \in \mathbb{Z}^+$, if $\mathbf{LV}(d_0)$ is true then the family $\mathcal{I}_{d_0}$ is typically bounded in torsion.*

4.1.2 Notations and conventions

We will follow the notation and conventions set forth in Chapter 2. Given an elliptic curve $E_{/F}$, for any integer $N \in \mathbb{Z}^+$ we will use $E(F)[N]^*$ to denote the set of F-rational points on

E of exact order N. Additionally, for a prime $\ell \in \mathbb{Z}^+$ we will use $v_\ell \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ to denote the usual ℓ-adic valuation.

4.2 Strong Uniform ℓ-Adic Divisibilities for Fields of Definition of Cyclic ℓ-Primary Isogenies

Before we prove that $\mathcal{I}_{F_0}$ and $\mathcal{I}_{d_0}$ are typically bounded in torsion, let us develop some necessary theory for fields of definition of cyclic isogenies.

The following result is due to Cremona and Najman [CN21].

Proposition 14. [CN21, Proposition 3.7] *If $E_{/F}$ is a non-CM elliptic curve defined over a number field and $\ell \in \mathbb{Z}^+$ is a prime for which the ℓ-adic representation $\rho_{E,\ell^\infty}(G_F)$ has level N, then for all $n > N$ and for any cyclic subgroup $C \subseteq E(\overline{\mathbb{Q}})$ of order ℓ^n one has*

$$[F(C) : F(\ell C)] = \ell.$$

The following proposition is a generalization of Proposition 14, which we will prove in this section and apply in the next.

Proposition 15. *Fix an integer $d_0 \in \mathbb{Z}^+$ and a prime $\ell \in \mathbb{Z}^+$. Then there exists an integer $A(d_0, \ell) \in \mathbb{Z}^+$ for which the following holds: for all integers $n \in \mathbb{Z}^+$ with $n \geq A(d_0, \ell)$, and for all non-CM elliptic curves $E_{/F}$ where $[F : \mathbb{Q}] = d_0$, one has for any cyclic subgroup $C \subseteq E(\overline{\mathbb{Q}})$ of order ℓ^n the equality*

$$[F(C) : F(\ell^{n-A(d_0,\ell)}C)] = \ell^{n-A(d_0,\ell)}.$$

In particular, one has the divisibility

$$\ell^{n-A(d_0,\ell)} \mid [F(C) : F].$$

Our strengthening uses the following uniformity result on levels of ℓ-adic representations of non-CM elliptic curves, first proven by Arai [Ara08, Theorem 1.2] and later strengthened by Clark and Pollack [CP18, Theorem 2.3.a].

Theorem 16. [CP18, Theorem 2.3.a] *Fix an integer $d_0 \in \mathbb{Z}^+$. Then for each prime $\ell \in \mathbb{Z}^+$ there exists an integer $A(d_0, \ell) \in \mathbb{Z}^+$ such that for all number fields F with $[F : \mathbb{Q}] = d_0$ and for all non-CM elliptic curves $E_{/F}$, the ℓ-adic representation $\rho_{E,\ell^\infty}(G_F)$ has level at most $A(d_0, \ell)$.*

Proof of Proposition 15. Suppose that $E_{/F}$ is a non-CM elliptic curve with $[F : \mathbb{Q}] = d_0$, and suppose that $\ell \in \mathbb{Z}^+$ is a prime for which $\rho_{E,\ell^\infty}(G_F)$ has level N; then by Theorem 16 we have $N \leq A(d_0, \ell)$.

Fix $n > N$ and a cyclic subgroup $C \subseteq E(\overline{\mathbb{Q}})$ of order ℓ^n. Then Proposition 14 implies that for each $0 \leq k < n - N$, the cyclic ℓ^{n-k}-isogeny $\ell^k C \subseteq E(\overline{\mathbb{Q}})$ is such that

$$[F(\ell^k C) : F(\ell^{k+1} C)] = \ell.$$

Since $N \leq A(d_0, \ell)$, from the tower of degree ℓ extensions

$$F(C) \supsetneq F(\ell C) \supsetneq \ldots \supsetneq F(\ell^{n-N-1} C) \supsetneq F(\ell^{n-N} C)$$

our results immediately follow. □

4.3 Typically Bounding Torsion on $\mathcal{I}_{F_0}$ and $\mathcal{I}_{d_0}$

Recall that by Theorem 5, a family $\mathcal{F}$ of elliptic curves which satisfies properties **P1** and **P2** will be typically bounded in torsion. In this section, we will show that both $\mathcal{I}_{F_0}$ and $\mathcal{I}_{d_0}$ satisfy **P1**, and that $\mathcal{I}_{F_0}$ satisfies **P2** but $\mathcal{I}_{d_0}$ only does conditionally. Let us note that a finite union of families which are typically bounded in torsion will also be typically bounded in torsion. Therefore, since the family of CM elliptic curves is typically bounded in torsion [BCP17, Theorem 1.1.i], we will assume hereafter that all of our elliptic curves are non-CM.

4.3.1 $\mathcal{I}_{F_0}$ and $\mathcal{I}_{d_0}$ satisfy P1

Proposition 17. *For each $d_0 \in \mathbb{Z}^+$, the family $\mathcal{I}_{d_0}$ satisfies **P1.***

Proof. Fix an integer $n_0 \in \mathbb{Z}^+$ and a prime $\ell \in \mathbb{Z}^+$. Let us take $A := A(d_0, \ell)$ to be the "strong uniform ℓ-adic Arai level" from Theorem 16. Let us set $n := 2(A + n_0 + v_\ell(d_0!)) + 1$; we will show that **P1** holds for $\mathcal{I}_{d_0}$ with this integer n.

Let $E_{/F}$ be a non-CM elliptic curve isogenous to an elliptic curve with degree d_0 j-invariant, denoted j'. Taking a quadratic twist if necessary, by [Cla, Proposition 3.2] we have that E is L-rationally isogenous to an elliptic curve E' defined over $\mathbb{Q}(j')$ with $j(E') = j'$, where $L/F(j')$ is at most a quadratic extension. Let us write this L-rational isogeny as $\phi : E \to E'$; we may assume that ϕ is cyclic.

Let us assume that $E(F)[\ell^n]^* \neq \emptyset$; choose any point $P \in E(F)[\ell^n]^*$. Let us set $k := v_\ell(|\phi(P)|)$, so that the order $|\phi(P)| = \ell^k$ where $k \geq \max\{n - v_\ell(\deg \phi), 0\}$. Then $\phi(P)$ generates an L-rational cyclic ℓ^k-subgroup $C' \subseteq E'(\overline{\mathbb{Q}})$. We consider two cases.

1. If $n - v_\ell(\deg \phi) \geq A + n_0 + v_\ell(d_0!) + 1$: then necessarily $n - v_\ell(\deg \phi) \geq 0$. We get that $k \geq A + n_0 + v_\ell(d_0!) + 1$, so by applying Proposition 15 to the L-rational cyclic ℓ^k-subgroup C', we have

$$\ell^{n_0 + v_\ell(d_0!) + 1} \mid [\mathbb{Q}(j')(C') : \mathbb{Q}(j')] \mid [L : \mathbb{Q}(j')] \mid 2(d_0)![F : \mathbb{Q}].$$

2. If $n - v_\ell(\deg \phi) < A + n_0 + v_\ell(d_0!) + 1$: then $v_\ell(\deg \phi) > n - 1 - (A + n_0 + v_\ell(d_0!)) = A + n_0 + v_\ell(d_0!)$. The subgroup $C'' := (\deg \phi / \ell^{v_\ell(\deg \phi)}) \cdot \ker \phi^\vee$ is an L-rational cyclic $\ell^{v_\ell(\deg \phi)}$-subgroup of E', so because $v_\ell(\deg \phi) \geq A + n_0 + v_\ell(d_0!) + 1$, Proposition 15 implies that

$$\ell^{n_0 + v_\ell(d_0!) + 1} \mid [\mathbb{Q}(j')(C'') : \mathbb{Q}(j')] \mid [L : \mathbb{Q}(j')] \mid 2(d_0)![F : \mathbb{Q}].$$

We thus find in both cases that $\ell^{n_0} \mid [F : \mathbb{Q}]$, whence we conclude that $\mathcal{I}_{d_0}$ satisfies **P1.** □

Corollary 18. *For each number field F_0, the family $\mathcal{I}_{F_0}$ satisfies **P1.***

Proof. Since $\mathcal{I}_{d_0}$ satisfies **P1** for all $d_0 \in \mathbb{Z}^+$ by Proposition 17, from the containment

$$\mathcal{I}_{F_0} \subseteq \bigcup_{1 \leq d \leq [F_0:\mathbb{Q}]} \mathcal{I}_d$$

it immediately follows that $\mathcal{I}_{F_0}$ also satisfies **P1**, since this property is closed under finite unions of families. □

4.3.2 $\mathcal{I}_{F_0}$ satisfies P2, as does $\mathcal{I}_{d_0}$ conditionally

Throughout the following, we let d_0 denote the degree of F_0.

Proposition 19. *For each number field F_0, the family $\mathcal{I}_{F_0}$ satisfies **P2.***

Proof. We must construct a constant $c := c(\mathcal{I}_{F_0}) \in \mathbb{Z}^+$ such that for any non-CM elliptic curve $E_{/F}$ isogenous to an elliptic curve with F_0-rational j-invariant, if $\ell \in \mathbb{Z}^+$ is a prime such that $E(F)[\ell]^* \neq \emptyset$, then one has

$$\ell - 1 \mid c[F : \mathbb{Q}]. \tag{4.1}$$

Before doing this, we will explain the constant $c(\mathcal{E}_{F_0})$ that we get in Theorem 4, since it is closely related to the constant $c(\mathcal{I}_{F_0})$ we will construct. As shown in the proof that the family

$$\mathcal{E}_{F_0} := \{E_{/F} : j(E) \in F_0\}$$

conditionally satisfies **P2** [CMP18, Theorem 4.3], for any non-CM elliptic curve $E_{/F_0}$ and for any prime $\ell \in \mathbb{Z}^+$, at least one of the following holds: one has $\ell - 1 \mid 2[F_0(R) : \mathbb{Q}]$ for all $R \in E[\ell]^*$, or else $\ell \leq 15d_0 + 1$ or E has an F_0-rational ℓ-isogeny; these correspond to Case 1-3, Case 4 and Case 5 of the proof of [CMP18, Theorem 4.3], respectively. For Case 1-3 the authors can take $c := 2$ in (4.1), and by Remark 1 they can exclude Case 4. For Case 5, their hypotheses imply that ℓ is contained in a *finite* set of primes S_{F_0} from [LV14, Theorem 1], which they then exclude by Remark 1. Then Theorem 4 makes Case 5 unconditional: if $\ell \notin S_{F_0}$, as well as $\ell > 72d_0 - 1$ and ℓ is unramified in any imaginary quadratic order

whose whose ring class field has degree at most d_0, then one has $\ell - 1 \mid 864[F_0(R) : \mathbb{Q}]$ for all $R \in E[\ell]^*$. By Remark 1, this proves that $\mathcal{E}_{F_0}$ satisfies **P2** – an arbitrary non-CM $E_{/F} \in \mathcal{E}_{F_0}$, while not necessarily defined over F_0, will be isomorphic to an elliptic curve $E'_{/F_0}$ over a quadratic extension of F. Note that working up to quadratic twist implies one must take $c(\mathcal{E}_{F_0}) := 2 \cdot 864 = 1728$ for $\ell \gg_{F_0} 0$.

For the rest of this proof, let us take $\ell \gg_{F_0} 0$ to mean that $\ell \notin S_{F_0}$, $\ell > 72d_0 - 1$ and that ℓ is unramified in all imaginary quadratic orders $\mathcal{O}$ whose ring class field $K(\mathcal{O})$ satisfies $[K(\mathcal{O}) : \mathbb{Q}] \leq d_0$. Then as noted above, we have for all non-CM elliptic curves $E_{/F} \in \mathcal{E}_{F_0}$ and for all primes $\ell \gg_{F_0} 0$ that $\ell - 1 \mid 1728[F : \mathbb{Q}]$ whenever $E(F)[\ell]^* \neq \emptyset$.

Let $E_{/F} \in \mathcal{I}_{F_0}$ be a non-CM elliptic curve. Then by assumption, E is isogenous to an elliptic curve with F_0-rational j-invariant, denoted j'. Arguing as in the last subsection, by [Cla, Proposition 3.2] there exists both an elliptic curve E' defined over $\mathbb{Q}(j')$ with $j(E') = j'$ and an L-rational isogeny $\phi : E \to E'$, where $L/F(j')$ is at most a quadratic extension.

Fix a prime $\ell \gg_{F_0} 0$, and suppose that $E(F)[\ell]^* \neq \emptyset$. Then by [BN, Corollary 4.3] there exists an extension M/L of degree dividing ℓ for which $E'(M)[\ell]^* \neq \emptyset$. Since $E'_{/M} \in \mathcal{E}_{F_0}$, by our previous discussion on $c(\mathcal{E}_{F_0})$ it follows that

$$\ell - 1 \mid 1728[M : \mathbb{Q}].$$

We check that

$$[M : \mathbb{Q}] \mid 2\ell[F(j') : \mathbb{Q}] = 2\ell[F(j') : F] \cdot [F : \mathbb{Q}] \mid 2\ell(d_0)! \cdot [F : \mathbb{Q}].$$

Since $\gcd(\ell - 1, \ell) = 1$, we deduce that

$$\ell - 1 \mid 3456(d_0)! \cdot [F : \mathbb{Q}].$$

Thus the constant $c := 3456(d_0)!$ is such that (4.1) holds for all non-CM elliptic curves $E_{/F} \in \mathcal{I}_{F_0}$ when $\ell \gg_{F_0} 0$. We conclude by Remark 1 that $\mathcal{I}_{F_0}$ satisfies **P2.** □

For our final result, recall that $\mathbf{LV}(d_0)$ is the assumption that the set S_{F_0} from [LV14, Theorem 1] can be chosen to be the same between any degree d_0 number field F_0.

Corollary 20. *For any integer $d_0 \in \mathbb{Z}^+$, if $\mathbf{LV}(d_0)$ is true then the family $\mathcal{I}_{d_0}$ satisfies **P2.***

Proof. Our proof of Proposition 19 showed that for any number field F_0, for sufficiently large primes $\ell \gg_{F_0} 0$ and for all non-CM $E_{/F} \in \mathcal{I}_{F_0}$, if $E(F)[\ell]^* \neq \emptyset$ then

$$\ell - 1 \mid 3456(d_0)! \cdot [F : \mathbb{Q}] \tag{4.2}$$

where $d_0 := [F_0 : \mathbb{Q}]$. Our implied constant $\ell \gg_{F_0} 0$ was such that $\ell \notin S_{F_0}$, $\ell > 72d_0 - 1$ and ℓ is unramified in any imaginary quadratic order whose whose ring class field has degree at most d_0. Since we are assuming that $\mathbf{LV}(d_0)$ is true, this implied constant $\ell \gg_{F_0} 0$ can be chosen to be the same between any number field of degree d_0; let us write this as $\ell \gg_{d_0} 0$. In particular, for any non-CM $E_{/F} \in \mathcal{I}_{d_0}$, fixing a degree d_0 j-invariant j' which is isogenous to E, we have $E_{/F} \in \mathcal{I}_{F_0}$ where $F_0 := \mathbb{Q}(j')$, and so our proof of Proposition 19 shows that (4.2) holds when $\ell \gg_{d_0} 0$ and $E(F)[\ell]^* \neq \emptyset$. Since $E_{/F} \in \mathcal{I}_{d_0}$ was arbitrary and the implied constant $\ell \gg_{d_0} 0$ depends only on d_0, we conclude by Remark 1 that $\mathcal{I}_{d_0}$ satisfies **P2.** □

Chapter 5

Polynomial Bounds on Torsion From Geometric Isogeny Classes

5.1 Introduction

The principal result of this chapter constructs polynomial bounds on orders of torsion points (and thus torsion groups) of elliptic curves within a fixed geometric isogeny class.

Theorem 21. *Fix a number field F_0 and an elliptic curve E_{0/F_0}. Then for each $\epsilon > 0$ there exists a constant $C_\epsilon := C_\epsilon(E_0, F_0) > 0$ such that for any elliptic curve $E_{/F}$ geometrically isogenous to E_{0/F_0}, one has both*

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

and

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

The family of CM elliptic curves is polynomially bounded in its torsion subgroups – in fact, stronger bounds are known for CM curves [CP15, Theorem 1]. Thus, we will assume for

the rest of this paper that our elliptic curves have no CM. A key step for us in polynomially bounding torsion from a non-CM geometric isogeny class $\mathcal{E}$ will be to polynomially bound the orders of torsion points that are supported away from the adelic level of E_{0/F_0}.

In contrast to [CP18, Theorem 1.3], the collection of elliptic curves in Theorem 21 will contain curves whose j-invariants j' have arbitrarily large degrees $[\mathbb{Q}(j') : \mathbb{Q}]$. However, both Theorem 21 and [CP18, 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 22. *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 $\#E(F)[\text{tors}] \leq C \cdot [F : \mathbb{Q}]^{\alpha}$.*

This is a special case of Conjecture 2. There is recent work which suggests its tractability: as noted earlier, work of Bourdon and Najman [BN, Proposition 4.1] shows that when $[F : \mathbb{Q}]$ is odd and $E_{/F}$ is $\overline{\mathbb{Q}}$-isogenous to a rational elliptic curve, one has $\exp E(F) \leq 720720\sqrt{35} \cdot [F : \mathbb{Q}]^{\frac{1}{2}}$, and thus $\#E(F)[\text{tors}] \leq 1441440\sqrt{35} \cdot [F : \mathbb{Q}]^{\frac{1}{2}}$.

5.2 Results on Galois Representations of Elliptic Curves

5.2.1 A composite version of a result of Greenberg

In this section, we will show that a result of Greenberg on ℓ-adic Galois representations [Gre12, Proposition 2.1.1] has a proof which applies to n-adic representations for composite $n \in \mathbb{Z}^+$ after some modifications. We will use this composite version to show that rationally isogenous non-CM elliptic curves have n-adic Galois representations whose images in $\mathrm{GL}_2(\mathbb{Z}_n)$ share equal indices, which will be applied in our proof of Theorem 21. For notation, refer to Chapter 2.

Proposition 23. *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 [Glö96, 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

$$\mu(\mathrm{Aut}_{\mathbb{Z}_n}(T)) = [\mathrm{Aut}_{\mathbb{Z}_n}(T) : G]. \tag{5.1}$$

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 (5.1) implies our result. □

5.2.2 Rational Galois representations of elliptic curves

Given an elliptic curve E over a number field F, one has an associated adelic Galois representation $\rho_E \colon G_F \to \mathrm{Aut}_{\hat{\mathbb{Z}}}(E[\mathrm{tors}]) \cong \mathrm{GL}_2(\hat{\mathbb{Z}})$ (see Chapter 2). Assume hereafter that our elliptic curves are non-CM.

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-rationally isogenous; let us write this (cyclic, without loss of generality) isogeny as $\phi\colon E \to E'$. 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,

$$0 \to T_N(E') \xrightarrow{\phi} T_N(E) \to C \to 0,$$

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 23, this implies that

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

We record this important fact as a corollary, along with an additional consequence.

Corollary 24. *Let $E_{/F}$ and $E'_{/F}$ be F-rationally isogenous non-CM elliptic curves. Then for each integer $N \in \mathbb{Z}^+$ one has*

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

In particular, one has

$$[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \rho_{E,N}(G_F)] \mid [\mathrm{GL}_2(\mathbb{Z}_N) : \rho_{E',N^\infty}(G_F)].$$

Proof. For the latter divisibility, we note that the mod-N projection map $\pi_N\colon \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ factors through the N-adic projection map $\pi_{N^\infty}\colon \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_N)$. □

By abuse of notation, we will often suppress its dependence on E and F.

Proposition 25. *Let $E_{/F}$ be a non-CM elliptic curve with adelic level M. Then for each integer $N \in \mathbb{Z}^+$ coprime to M, one has that $\rho_{E,N^\infty}(G_F)$ is surjective.*

Proof. Let $x \in \mathrm{GL}_2(\mathbb{Z}_N)$ be an arbitrary element; we will show that x lies in $\rho_{E,N^\infty}(G_F)$. Since the reduction map $\mathrm{GL}_2(\mathbb{Z}_N \times \mathbb{Z}/M\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}_N) \times \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ is an isomorphism, there exists a (unique) element $x_0 \in \mathrm{GL}_2(\mathbb{Z}_N \times \mathbb{Z}/M\mathbb{Z})$ with $x_0 \equiv x \pmod{\mathbb{Z}_N}$ and $x_0 \equiv I \pmod{M}$. Lift x_0 to an element $X \in \mathrm{GL}_2(\hat{\mathbb{Z}})$. Since $X \equiv I \pmod{M}$, we have $X \in \ker(\pi_M \colon \mathrm{GL}_2(\hat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})) \subseteq \rho_E(G_F)$, and so $\pi_{N^\infty}(X) = x \in \pi_{n^\infty}(\rho_E(G_F)) = \rho_{E,N^\infty}(G_F)$. We thus conclude that $\mathrm{GL}_2(\mathbb{Z}_N) = \rho_{E,N^\infty}(G_F)$. □

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 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 26. *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. [CGPS22, §7.2]. □

5.3 Polynomial Bounds on Torsion

5.3.1 Polynomial bounds over a finite support

Before we prove Theorem 21, let us prove one more fact. The following theorem is an "isogenous" variant of [CP18, Theorem 2.8]. It will be used to polynomially bound a uniformly supported factor of the exponent of our torsion groups.

Theorem 27. *Fix integers $d_0, N > 0$. Then there exists a constant $C := C(d_0, N) > 0$ such that for any non-CM elliptic curve $E_{/F}$ geometrically isogenous to an elliptic curve whose j-invariant j_0 has degree $[\mathbb{Q}(j_0) : \mathbb{Q}] = d_0$, one has*

$$\exp E(F)[N^\infty] \leq C \cdot [F : \mathbb{Q}]^{1/2}.$$

Proof. By [LFN20, Lemma 3.1] there exists an elliptic curve E_0 defined over $F_0 := \mathbb{Q}(j_0)$ whose j-invariant $j(E_0) = j_0$, for which E and E_0 are L-rationally isogenous, where L/FF_0 is at most quadratic. As a consequence of e.g. Corollary 24, one has for all primes $\ell \in \mathbb{Z}^+$ that

$$[\mathrm{GL}_2(\mathbb{Z}_\ell) : \rho_{E,\ell^\infty}(G_L)] = [\mathrm{GL}_2(\mathbb{Z}_\ell) : \rho_{E_0,\ell^\infty}(G_L)]. \tag{5.2}$$

Fix any prime $\ell \in \mathbb{Z}^+$ for which both $\ell \mid N$ and $\ell \mid \exp E(F)[\mathrm{tors}]$; let us write $\ell^k \parallel \exp E(F)[\mathrm{tors}]$. It follows that $\rho_{E,\ell^k}(G_F) \subseteq B_1(\ell^k)$ once fixing an appropriate basis, and so $\rho_{E,\ell^\infty}(G_F) \subseteq \pi_{\ell^k}^{-1}(B(\ell^k))$ where $\pi_{\ell^k} \colon \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ is the mod-ℓ^k reduction map. Since $[\mathrm{GL}_2(\mathbb{Z}_\ell) : \pi_{\ell^k}^{-1}(B(\ell^k))] = [\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z}) : B_1(\ell^k)] = \ell^{2(k-1)}(\ell^2 - 1)$ (Lemma 26), we have that $\ell^{2(k-1)}(\ell^2 - 1) \mid [\mathrm{GL}_2(\mathbb{Z}_\ell) : \rho_{E,\ell^\infty}(G_F)]$. Additionally, as the fixed field of the ℓ-adic representation $\rho_{E_0,\ell^\infty} \colon G_{F_0} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is $F_0(E_0[\ell^\infty])$, we also find that

$$[\mathrm{GL}_2(\mathbb{Z}_\ell) : \rho_{E_0,\ell^\infty}(G_L)] = [\mathrm{GL}_2(\mathbb{Z}_\ell) : \rho_{E_0,\ell^\infty}(G_{F_0})] \cdot [L \cap F_0(E_0[\ell^\infty]) : F_0].$$

Combining these facts with (5.2), we deduce that

$$\ell^{2(k-1)}(\ell^2 - 1) \mid [\mathrm{GL}_2(\mathbb{Z}_\ell) : \rho_{E_0,\ell^\infty}(G_{F_0})] \cdot [L : F_0].$$

By the Strong Uniform ℓ-adic Arai Theorem (see Theorem 16), there exists a constant $a(d_0, \ell) \in \mathbb{Z}^+$ *which depends only on* d_0 *and* ℓ for which the ℓ-adic valuation $v_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \rho_{E_0,\ell^\infty}(G_{F_0})]) \leq a(d_0, \ell)$. It follows that

$$\ell^{\max\{0,2(k-1)-a(d_0,\ell)\}} \mid [L : F_0] \mid 2(d_0 - 1)! \cdot [F : \mathbb{Q}]. \tag{5.3}$$

Compiling the divisibilities from (5.3) across all $\ell \mid n$, we conclude that

$$\exp E(F)[n^\infty]^2 \mid 2 \prod_{\ell \mid N} \ell^{2+a(d_0,\ell)} \cdot (d_0 - 1)! \cdot [F : \mathbb{Q}].$$

The result then follows by taking $C := \sqrt{2 \prod_{\ell \mid N} \ell^{2+a(d_0,\ell)} \cdot (d_0 - 1)!}$. □

5.3.2 Proof of the main theorem

Proof of Theorem 21. Let us factorize the exponent of $E(F)[\mathrm{tors}]$ as

$$\exp E(F)[\mathrm{tors}] = \prod_{\ell \mid M} \exp E(F)[\ell^\infty] \cdot \prod_{\ell \nmid M} \exp E(F)[\ell^\infty],$$

where $M := M(E_0, F_0)$ is the adelic level of E_{0/F_0}. For our first term, Theorem 27 shows that

$$\prod_{\ell \mid M} \exp E(F)[\ell^\infty] \leq c_1 \cdot [F : \mathbb{Q}]^{1/2} \tag{5.4}$$

for some $c_1 := c_1(E_0, F_0) \in \mathbb{Z}^+$. For the remainder of this proof, we will deal with bounding the second term $\prod_{\ell \nmid M} \exp E(F)[\ell^\infty]$. More precisely, we will show that it is bounded above by $c_2(d_0, \epsilon) \cdot [F : \mathbb{Q}]^{1/2+\epsilon}$ for some constant $c_2(d_0, \epsilon) > 0$.

Let us write $N := \prod_{\ell \nmid M} \exp E(F)[\ell^\infty]$. Since $E(F)$ has a torsion point of order N, up to conjugacy we have $\rho_{E,n}(G_F) \subseteq B_1(N)$, and so by Lemma 26 we get

$$\varphi(N)\psi(N) \mid [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \rho_{E,N}(G_F)]. \tag{5.5}$$

By [LFN20, Lemma 3.1] there exists a quadratic extension L/FF_0 for which E and E_0 are L-rationally isogenous. Write this L-rational isogeny as $\phi\colon E \to E_0$; we may assume that ϕ is cyclic. Since E_0 is defined over $F_0 \subseteq L$, we find that

$$[\mathrm{GL}_2(\mathbb{Z}_N) : \rho_{E_0,N^\infty}(G_L)] = [\mathrm{GL}_2(\mathbb{Z}_N) : \rho_{E_0,N^\infty}(G_{F_0})] \cdot [L \cap F_0(E_0[N^\infty]) : F_0].$$

Furthermore, as N is coprime to M, Proposition 25 shows us that $[\mathrm{GL}_2(\mathbb{Z}_N) : \rho_{E_0,N^\infty}(G_{F_0})] = 1$. Combining these two facts, we check using Corollary 24 that

$$\begin{aligned}[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : \rho_{E,N}(G_L)] \mid [\mathrm{GL}_2(\mathbb{Z}_N) : \rho_{E_0,N^\infty}(G_{F_0})] \cdot [L \cap F_0(E_0[N^\infty]) : F_0] \\ = 1 \cdot [L \cap F_0(E_0[N^\infty]) : F_0] \\ \mid [L : F_0] \\ \mid 2(d_0 - 1)! \cdot [F : \mathbb{Q}].\end{aligned}$$

Combining this with (5.5) gives us the divisibility

$$\varphi(N)\psi(N) \mid 2(d_0 - 1)! \cdot [F : \mathbb{Q}]. \tag{5.6}$$

One can check directly that $\psi(N) > N$ for any $N > 1$. Fixing an $\epsilon \in (0, 1)$, by [HW08, Theorem 327] there exists a constant $c'_\epsilon > 0$ such that for all $N \geq 1$ one has

$$\varphi(N) > c'_\epsilon \cdot N^{1-\epsilon}.$$

Thus, from (5.6) we deduce that

$$N^{2-\epsilon} < c_\epsilon \cdot [F : \mathbb{Q}]$$

for some $c_\epsilon := c_\epsilon(d_0) > 0$, i.e.,

$$N \leq c_\epsilon^{1/(2-\epsilon)} \cdot [F : \mathbb{Q}]^{1/(2-\epsilon)}.$$

By definition of N, this is an upper bound on $\prod_{\ell \nmid M} \exp E(F)[\ell^\infty]$. We combine this with (5.4) to conclude that

$$\exp E(F)[\text{tors}] \leq C_{\epsilon,1} \cdot [F : \mathbb{Q}]^{1+\epsilon} \tag{5.7}$$

for some $C_{\epsilon,1} := C_{\epsilon,1}(E_0, F_0) > 0$.

Next we will give our polynomial bound on $\#E(F)[\text{tors}]$, following [CP18, §3.3]. Writing $N := \exp E(F)[\text{tors}]$, we have $E(F)[\text{tors}] \cong \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for some $d \mid N$ where $d > 0$. Since E has full d-torsion over F, we find that F contains a primitive d'th root of unity [Sil09, Corollary 8.1.1], and so $\varphi(d) \mid [F : \mathbb{Q}]$. By [HW08, Theorems 327 and 328], this implies that $d \leq C'_\epsilon \cdot [F : \mathbb{Q}]^{1+\epsilon}$ for some $C'_\epsilon > 0$. Since $\#E(F)[\text{tors}] = dN$, we combine this with (5.7) and conclude that

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

for some $C_{\epsilon,2} := C_{\epsilon,2}(E_0, F_0) > 0$. □

Chapter 6

Torsion in $\mathcal{B}_{F_0}$ Upon Base Change

6.1 Introduction

Fix a number field F_0, and let $E_{/F_0}$ be an elliptic curve defined over F_0. By the Mordell-Weil Theorem, the set $E(F_0)$ of F_0-rational points on E is a finitely generated abelian group; consequently, the F_0-rational torsion subgroup $E(F_0)[\text{tors}]$ is finite. For any extension L/F_0, one has the inclusion of subgroups $E(F_0) \subseteq E(L)$. A natural question to ask is how much the torsion subgroup $E(F_0)[\text{tors}]$ grows once base-changed to L.

When the base field is $F_0 := \mathbb{Q}$, there are several results which establish constraints on torsion growth uniformly in the degree $[L : \mathbb{Q}]$. For example, when $[L : \mathbb{Q}] < \infty$, Lozano-Robledo gave a linear bound on the prime divisors of $\#E(L)[\text{tors}]$ in terms of $[L : \mathbb{Q}]$ [LR13, Theorem 1.3]. He did this in part by determining lower bounds on the degrees of fields of definition of torsion points on E of prime order ℓ, via analyzing the image of the mod-ℓ Galois representation of E as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ à la Serre [Ser72] (see also Theorem 3).

Continuing this idea of studying Galois representations of elliptic curves to better understand their torsion points, González-Jiménez and Najman [GJN20] have determined restrictions on the degrees of number fields over which torsion can grow for rational elliptic curves under base change. One of their results is as follows.

Theorem. [GJN20, Theorem 7.2.i] *For all finite extensions $L/\mathbb{Q}$ whose degree is coprime to $2 \cdot 3 \cdot 5 \cdot 7$, one has for all elliptic curves E defined over $\mathbb{Q}$ that*

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

In this chapter, we prove a number field analogue of [GJN20, Theorem 7.2.i] wherein our base field can be larger than $\mathbb{Q}$. The proof of our theorem is split into Propositions 31 and 33.

Theorem 28. *Assume that GRH is true, and let F_0 be a number field with no rationally defined CM. Then there exists an effectively computable constant $B := B(F_0) \in \mathbb{Z}^+$ for which the following holds: for any finite extension L/F_0 whose degree $[L : F_0]$ is coprime to B, one has for all elliptic curves E defined over F_0 that*

$$E(L)[\text{tors}] = E(F_0)[\text{tors}].$$

As we will see, the proof of Theorem 28 reduces to determining a finite set A_{F_0} of prime numbers such that for any elliptic curve $E_{/F_0}$ and for any prime order torsion point $R \in E$, the degree $[F_0(R) : F_0]$ of the field of definition of R equals 1 or is divisible by some prime in A_{F_0}; in fact, we will show that $[F_0(R) : F_0]$ is always even when $\ell \gg_{F_0} 0$.

For our analysis of torsion point degrees, we will prove Theorem 29, a result on relative uniform bounds for mod-ℓ Galois representations of elliptic curves over fields larger than $\mathbb{Q}$. The proof will utilize Serre's work on the image of inertia under mod-ℓ Galois representations [Ser72] (see also Theorems 3 and 38).

In the following, we will let S_{F_0} denote the finite set of primes from [LV14, Theorem 1], see Remark 2.

Theorem 29. *Assume that GRH is true, and let F_0 be a number field with no rationally defined CM. Then for all primes $\ell \gg_{F_0} 0$, one has for any elliptic curve $E_{/F_0}$ that its mod-ℓ Galois representation $G := \rho_{E,\ell}(G_{F_0})$ is either surjective, or is contained in $N_s(\ell)$ or $N_{ns}(\ell)$ up to conjugacy.*

1. *If $G \subseteq N_s(\ell)$ then $\mathcal{D}^e \subseteq G$ for some $e \in \{1,2,3,4,6\}$, and if $\ell \neq 37, 73$ then the center $Z(\ell) \subseteq G$, and in fact*

$$[N_s(\ell) : G] \mid \gcd(\ell - 1, e).$$

2. *If $G \subseteq N_{ns}(\ell)$ then $C_{ns}(\ell)^e \subseteq G$ for some $e \in \{1,2,3,4,6\}$, and in fact*

$$[N_{ns}(\ell) : G] \mid 6.$$

   a. *If $\ell \equiv 1 \pmod 3$, then G equals $N_{ns}(\ell)$ or $C_{ns}(\ell)$, with $G = N_{ns}(\ell)$ if F_0 has a real embedding.*

   b. *If $\ell \equiv 2 \pmod 3$, then G equals $N_{ns}(\ell)$, $C_{ns}(\ell)$, $G(\ell)$ or $C_{ns}(\ell)^3$, with $G = N_{ns}(\ell)$ or $G(\ell)$ if F_0 has a real embedding.*

Remark 2. As we will see in our proof of Theorem 29, by $\ell \gg_{F_0} 0$ we can take $\ell \geq \max\{29, 15[F_0 : \mathbb{Q}] + 2\}$, ℓ unramified in F_0 and $\ell \notin S_{F_0}$, where S_{F_0} is from [LV14, Theorem 1].

Let us briefly explain S_{F_0} and the two assumptions from Theorems 28 and 29: that GRH is true and F_0 has no rationally defined CM. Under these assumptions, Theorem 7 shows there exists a finite set of primes S_{F_0} such that the prime degree of any F_0-rational isogeny of an elliptic curve lies in S_{F_0}. As noted previously, there also exists an effectively computable upper bound on the primes from S_{F_0} [LV14, Theorem 7.9].

Remark 3. One has additional information about the mod-ℓ Galois representation of an elliptic curve over $\mathbb{Q}$: for any prime $\ell > 1.4 \times 10^7$ and any elliptic curve $E_{/\mathbb{Q}}$, one has that $\rho_{E,\ell}(G_{\mathbb{Q}})$ equals either $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or $N_{ns}(\ell)$ up to conjugacy [LFL21, Theorem 1.2].

It is natural to ask whether the "rationally defined CM" hypothesis on F_0 is necessary. Indeed it is, as is shown by the following theorem – we will prove this in Section 6.5.

Theorem 30. *Let F_0 be a number field with rationally defined CM. Then for all integers $B \in \mathbb{Z}^+$ there exists a finite extension L/F_0 whose degree $[L : F_0]$ is coprime to B, and a*

CM elliptic curve $E_{/F_0}$ for which

$$E(L)[\text{tors}] \neq E(F_0)[\text{tors}].$$

6.2 Towards the Proof of Theorem 28

6.2.1 Definition of A_{F_0} and B_{F_0}

To prove Theorem 28, we need to keep track of prime divisors of torsion point degrees of elliptic curves over F_0. Once and for all, fix an algebraic closure $\overline{\mathbb{Q}}$; let $F_0/\mathbb{Q}$ be an algebraic extension. Let us call a subset $A_{F_0} \subseteq \mathbb{Z}^+$ of prime numbers F_0-*admissible* if for all elliptic curves $E_{/F_0}$ and all prime order torsion points $R \in E(\overline{\mathbb{Q}})$, one has that either $[F_0(R) : F_0] = 1$ or there exists $p \in A_{F_0}$ so that $p \mid [F_0(R) : F_0]$. For example, [GJN20, Theorem 5.8] shows that $A_{\mathbb{Q}} := \{2, 3, 5, 7\}$ is $\mathbb{Q}$-admissible. As we will see in the proof of Proposition 31, if A_{F_0} is any F_0-admissible set and $[L : F_0]$ is coprime to all primes $p \in A_{F_0}$, then for all elliptic curves $E_{/F_0}$ one has $E(L)[\ell] = E(F_0)[\ell]$ for all primes $\ell \in \mathbb{Z}^+$.

Next, let us define R_{F_0} as the set of prime divisors of F_0-rational torsion subgroups of elliptic curves,

$$R_{F_0} := \{p \in \mathbb{Z}^+ : \exists E_{/F_0} \text{ with } p \mid \#E(F_0)[\text{tors}]\}.$$

Equivalently, R_{F_0} is the set of all primes that are the order of some F_0-rational torsion point on an elliptic curve. If F_0 is a number field, then one has that $\#R_{F_0}$ is finite and bounded uniformly in the degree $[F_0 : \mathbb{Q}]$ – this is a consequence of Merel's strong uniform boundedness theorem [Mer96, Corollaire].

Following R_{F_0}, we define the set B_{F_0} as follows,

$$B_{F_0} := \bigcup_{p \in R_{F_0}} \{p\} \cup \{\text{prime divisors of } p - 1\}.$$

Obviously $R_{F_0} \subseteq B_{F_0}$, and if $\#R_{F_0} < \infty$ then $\#B_{F_0} < \infty$. When $F_0 = \mathbb{Q}$, Mazur's torsion theorem [Maz76] shows that $R_{\mathbb{Q}} = B_{\mathbb{Q}} = \{2, 3, 5, 7\}$. As we will see in the proof of Proposition

31, B_{F_0} controls which primary torsion point orders can appear upon finite degree base change for any elliptic curve $E_{/F_0}$.

With F_0-admissible sets and B_{F_0} defined, we are able to prove the first key step in the proof of Theorem 28.

Proposition 31. *Let $F_0/\mathbb{Q}$ be an algebraic extension and A_{F_0} an F_0-admissible set. Let L/F_0 be any finite extension for which all primes $p \in A_{F_0} \cup B_{F_0}$ do not divide $[L : F_0]$. Then for all elliptic curves $E_{/F_0}$ one has that*

$$E(L)[\text{tors}] = E(F_0)[\text{tors}].$$

Before we prove Proposition 31, let us record an important lemma which controls the degrees of finite extensions over which one attains new prime power torsion.

Lemma 32. [GJN20, Proposition 4.6] *Let $F_0/\mathbb{Q}$ be an algebraic extension, $E_{/F_0}$ an elliptic curve and $R \in E_{/F_0}$ a torsion point of prime order $\ell^n > \ell$. Then $[F_0(R) : F_0(\ell R)]$ divides ℓ^2 or $\ell(\ell - 1)$.*

Proof of Proposition 31. It suffices to show that for all primes $\ell \in \mathbb{Z}^+$ one has

$$E(L)[\ell^\infty] = E(F_0)[\ell^\infty],$$

which is equivalent to showing that for each prime $\ell \in \mathbb{Z}^+$ and for all integers $n > 0$ one has

$$E(L)[\ell^n] = E(F_0)[\ell^n].$$

We proceed via induction on n. The case $n = 1$ follows from the assumption that $[L : F_0]$ is coprime to all primes $p \in A_{F_0}$. Suppose then that both $n > 1$ and the result is true for $k < n$. Let $R \in E(L)[\ell^n]$ be a point of exact order ℓ^n. Then the inductive hypothesis implies that $\ell^{n-1}R$ is an F_0-rational point of order ℓ, whence $\ell \in R_{F_0}$. The inductive hypothesis also implies $F_0(\ell R) = F_0$, so by Lemma 32 we have

$$[F_0(R) : F_0] \mid \ell^2(\ell - 1).$$

By this divisibility, any prime divisor $p \mid [F_0(R) : F_0]$ divides $\ell(\ell - 1)$, which from $\ell \in R_{F_0}$ implies $p \in B_{F_0}$ – which would be impossible since $[F_0(R) : F_0] \mid [L : F_0]$ and $[L : F_0]$ is coprime to all primes in B_{F_0}. This forces $[F_0(R) : F_0] = 1$, which shows that $R \in E(F_0)[\ell^n]$. We conclude by induction that $E(L)[\ell^\infty] = E(F_0)[\ell^\infty]$. □

As noted earlier, the existence of the constant $B := B(F_0) \in \mathbb{Z}^+$ in Theorem 28 depends on the existence of a *finite* F_0-admissible set A_{F_0}. When assuming GRH, the following proposition gives us a class of number fields for which this happens.

Proposition 33. *Assume that GRH is true. Then for any number field F_0 which has no rationally defined CM, one can make a finite choice of F_0-admissible set A_{F_0}.*

Theorem 28 is an immediate consequence of combining Propositions 31 and 33. Sans including Section 6.5, the rest of our paper is devoted to proving Theorem 29 and then using it to prove Proposition 33. Our proofs will involve an analysis of the mod-ℓ Galois representation of an arbitrary elliptic curve defined over F_0. As noted earlier, the assumption that both GRH is true and that F_0 has no rationally defined CM will rule out the case where an elliptic curve $E_{/F_0}$ has an F_0-rational isogeny of uniformly large prime degree.

6.2.2 Orbits under the normalizer of a Cartan subgroup

Let $V := \{e_1, e_2\}$ be the two-dimensional $\mathbb{F}_\ell$-vector space spanned by the unit vectors $e_1 := \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $e_2 := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Then one has an action of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ on V via left multiplication. For a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and a vector $v \in V^\bullet := V \smallsetminus \{0\}$, we will use $\mathcal{O}_G(v)$ to denote the orbit of v under G. We will also use $\langle v \rangle$ to denote the subspace spanned by v.

In our applications, $V := E[\ell]$ is the ℓ-torsion subgroup of an elliptic curve. As noted earlier, by the Orbit-Stabilizer Theorem one has for any point $R \in E[\ell]$ that the size of its orbit $\mathcal{O}_{\rho_{E,\ell}(G_{F_0})}(R)$ is equal to its degree $[F_0(R) : F_0]$. In this subsection, we will see how we can exploit this to determine factors of the degree via the classification in Theorem 3.

The following proposition describes the orbits of $V^\bullet$ under the action of $N_s(\ell)$.

Proposition 34. *$V^\bullet$ has two $N_s(\ell)$-orbits: they are $\mathcal{O}_{N_s(\ell)}(e_1) = \mathcal{O}_{N_s(\ell)}(e_2)$ and $\mathcal{O}_{N_s(\ell)}(e_1 + e_2)$, which are of size $2(\ell-1)$ and $(\ell-1)^2$, respectively.*

Proof. Since both $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \cdot e_1 = ae_1$ and $\begin{bmatrix} 0 & d \\ a & 0 \end{bmatrix} \cdot e_1 = ae_2$, we find that $\mathcal{O}_{N_s(\ell)}(e_1) = \mathcal{O}_{N_s(\ell)}(e_2) = \{xe_1 + ye_2 : \text{either } x = 0 \text{ or } y = 0\} = \langle e_1 \rangle \cup \langle e_2 \rangle \smallsetminus \{0\}$. On the other hand, $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \cdot (e_1 + e_2) = \begin{bmatrix} 0 & a \\ d & 0 \end{bmatrix} \cdot (e_1 + e_2) = ae_1 + de_2$, and so $\mathcal{O}_{N_s(\ell)}(e_1 + e_2) = \{xe_1 + ye_2 : xy \neq 0\} = V^\bullet \smallsetminus (\langle e_1 \rangle \cup \langle e_2 \rangle)$. □

The following proposition describes the orbits of $V^\bullet$ under $C_{ns}(\ell)$, and thus $N_{ns}(\ell)$.

Proposition 35. *The group $C_{ns}(\ell)$ acts transitively on $V^\bullet$. In particular, for each $v \in V^\bullet$ we have $\#\mathcal{O}_{N_{ns}(\ell)}(v) = \#\mathcal{O}_{C_{ns}(\ell)}(v) = \ell^2 - 1$.*

Proof. For any $v := xe_1 + ye_2 \in V^\bullet$, one sees that the matrix $\begin{bmatrix} x & y\epsilon \\ y & x \end{bmatrix} \in C_{ns}(\ell)$ takes e_1 to v. □

Recall the following basic fact about orbit divisibility for subgroups.

Lemma 36. *Let a finite group G act on a set X. Then for any subgroup $H \subseteq G$, one has for all $x \in X$ that*

$$\#\mathcal{O}_G(x) \mid [G : H] \cdot \#\mathcal{O}_H(x).$$

Remark 4. Suppose we have an elliptic curve $E_{/F_0}$ for which $G := \rho_{E,\ell,P,Q}(G_{F_0})$ is contained in a subgroup $N(\ell) \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Then by Lemma 36, for each $R \in E[\ell]^\bullet$ one has

$$\#\mathcal{O}_{N(\ell)}(R) \mid [N(\ell) : G] \cdot [F_0(R) : F_0]. \tag{6.1}$$

By Propositions 34 and 35, this can give us divisibility information about the degree $[F_0(R) : F_0]$. For example, Proposition 35 implies that if $N(\ell) = N_{ns}(\ell)$ then

$$\ell^2 - 1 \mid [N_{ns}(\ell) : G] \cdot [F_0(R) : F_0].$$

When $N(\ell) = N_s(\ell)$, using Proposition 34 one has for nonzero $R \in \langle P \rangle \cup \langle Q \rangle$ that

$$2(\ell - 1) \mid [N_s(\ell) : G] \cdot [F_0(R) : F_0],$$

and when $R \notin \langle P \rangle \cup \langle Q \rangle$ one has instead that

$$(\ell - 1)^2 \mid [N_s(\ell) : G] \cdot [F_0(R) : F_0].$$

To prove Proposition 33, we will use this remark to show that when ℓ is sufficiently large with respect to F_0, one has for all nontrivial $R \in E[\ell]$ that $[F_0(R) : F_0]$ is even.

6.3 The Image of Inertia

In this section, we will describe the image of inertia under our mod-ℓ Galois representation when $\ell \gg_{F_0} 0$. This will be towards proving Theorem 29.

6.3.1 The image lies in the normalizer of a Cartan subgroup

In the following subsection, we will show that under sufficient assumptions, for an elliptic curve $E_{/F_0}$ and a prime $\ell \in \mathbb{Z}^+$, the image $\rho_{E,\ell}(G_{F_0})$ either equals $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or is contained in the normalizer of a Cartan subgroup.

Proposition 37. *Assume that GRH is true, and fix a number field F_0 without rationally defined CM. Then for all primes $\ell > 15[F_0 : \mathbb{Q}] + 1$ unramified in F_0 with $\ell \notin S_{F_0}$ (see Remark 2), for any elliptic curve $E_{/F_0}$ the image $\rho_{E,\ell}(G_{F_0})$ of its mod-ℓ Galois representation is either equal to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or contained in $N_s(\ell)$ or $N_{ns}(\ell)$ up to conjugacy.*

Proof. Let $G := \rho_{E,\ell}(G_{F_0})$. By Theorem 3, either G contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, is contained in $B(\ell)$, $N_s(\ell)$ or $N_{ns}(\ell)$ up to conjugacy, or has a projective image $\overline{G} := G/\mathbb{F}_\ell^\times \subseteq \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ isomorphic to either A_4, S_4 or A_5.

Since ℓ is unramified in F_0, it follows that the mod-ℓ cyclotomic character $\chi_\ell\colon G_{F_0} \to \mathbb{F}_\ell^\times$ is surjective. Since both $\chi_\ell(G_{F_0}) = \det(G)$ and $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) := \ker(\det\colon \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \to \mathbb{F}_\ell^\times)$, it follows that G contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ iff $G = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Henceforth, let us assume that $G \neq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. If $\overline{G}$ is isomorphic to either A_4, S_4 or A_5, then Etropolski has shown that $\ell \leq 15[F_0 : \mathbb{Q}] + 1$ [Etr, Proposition 2.6]. The case where G is contained in $B(\ell)$ up to conjugacy is equivalent to E having an F_0-rational ℓ-isogeny, which cannot happen since $\ell \notin S_{F_0}$ [LV14, Theorem 1]. We thus conclude that G is contained in the normalizer of a Cartan subgroup up to conjugacy. □

6.3.2 The shape of the inertia subgroup

Let F_0 be a number field and $E_{/F_0}$ an elliptic curve. Following [Ser72], depending on the reduction type of E at a prime $\mathfrak{L} \subseteq E$ lying above $\ell \geq 5$, we will see that the image $\rho_{E,\ell}(I_\mathfrak{L})$ of the inertia group $I_\mathfrak{L} \subseteq G_{F_0}$ contains a uniformly large subgroup.

Let us regard E as lying over the local field $K := (F_0)_\mathfrak{L}$, the $\mathfrak{L}$-adic completion of F_0 at $\mathfrak{L}$. Then there exists a finite extension L/K for which E has semistable reduction [Sil09, §VII.5]. Assume L is such an extension of minimal degree. If $E_{/L}$ has bad multiplicative reduction, then $[L : K] \leq 2$ by the theory of Tate curves [Sil09, §C.14]. If $E_{/L}$ has good reduction, then the ramification index $e(L/K) \in \{1, 2, 3, 4, 6\}$ – a more precise version of this is given in e.g. [LR18, Theorem 6.1].

The following result is essentially due to Serre [Ser72], with a slight generalization to account for elliptic curves defined over a finite extension of $\mathbb{Q}_\ell$. Fix a prime $\ell \in \mathbb{Z}^+$ and an algebraic closure $\overline{\mathbb{Q}_\ell}$ of $\mathbb{Q}_\ell$. Given a local field $K/\mathbb{Q}_\ell$, we let K^{nr} denote the maximal unramified extension of K, and $I_K := \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/K^{\mathrm{nr}})$ the inertia group of K. We also let K_t/K^{nr} denote the maximal tamely ramified extension of K, and $I_{K,\ell} := \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/K_t)$ the wild inertia group; $I_{K,\ell}$ is a pro-ℓ-group. Additionally, the tame inertia group is defined as $I_{K,t} := \mathrm{Gal}(K_t/K^{\mathrm{nr}}) \cong I_K/I_{K,\ell}$, and is a pro-cyclic group.

The following theorem describes the image of inertia based on the reduction type of $E_{/L}$, with a few extra conditions to simplify the result.

Theorem 38. *Let $\ell \geq 5$ be a prime and $K/\mathbb{Q}_\ell$ a finite unramified extension. Let $E_{/K}$ be an elliptic curve, and L/K a minimal extension such that $E_{/L}$ is semistable. Then the absolute ramification index $e := e(L/\mathbb{Q}_\ell) = e(L/K) \in \{1, 2, 3, 4, 6\}$. Assuming that $\ell \nmid \#\rho_{E,\ell}(I_L)$, one also has the following subgroup of $\rho_{E,\ell}(I_L)$, based on the reduction type of $E_{/L}$:*

- *Good ordinary reduction: then $\rho_{E,\ell}(I_L)$ contains $\mathcal{D}^e$ up to conjugacy.*
- *Good supersingular reduction: then $\rho_{E,\ell}(I_L) = C_{ns}(\ell)^e$ up to conjugacy.*
- *Bad multiplicative reduction: same as good ordinary.*

Remark 5. Assume that GRH is true, and let $E_{/F_0}$ be an elliptic curve over a number field F_0 with no rationally defined CM. If ℓ is sufficiently large, then by Proposition 37 we must have $\ell \nmid \#\rho_{E,\ell}(G_{F_0})$ when $\rho_{E,\ell}(G_{F_0})$ isn't surjective. In such a case, the conditions $e((F_0)_{\mathfrak{L}}/\mathbb{Q}_\ell) = 1$ and $\ell \nmid \#\rho_{E,\ell}(I_L)$ of Theorem 38 are automatically satisfied for any prime $\mathfrak{L} \subseteq F_0$ above ℓ and appropriate choice of extension $L/(F_0)_{\mathfrak{L}}$.

Remark 6. The theorem above is a very mild generalization of [LR13, Theorem 3.1] in the case $\ell \nmid \#\rho_{E,\ell}(I_L)$ where our elliptic curve is defined over $(F_0)_{\mathfrak{L}}$ instead of $\mathbb{Q}_\ell$. In fact, [LR13, Theorem 3.1] is a generalization of several results of [Ser72], where Lozano-Robledo does not assume that $e(L/\mathbb{Q}_\ell) = 1$ – this is to allow his elliptic curves $E_{/\mathbb{Q}}$ to have additive reduction. Since Theorem 28 is a uniformity result independent of reduction type, we must also allow $E_{/F_0}$ to have additive reduction.

Proof of Theorem 38. If $E_{/L}$ has bad reduction, then $e(L/K) \mid 2$ follows from the theory of Tate curves. If $E_{/L}$ has good reduction, then one has $e(L/K) \in \{1, 2, 3, 4, 6\}$ by e.g. [LR18, Theorem 6.1]. We are thus left to determine the image of inertia. Since $I_{L,\ell}$ is a pro-ℓ-group and $\ell \nmid \#\rho_{E,\ell}(I_L)$, it follows that the action factors through tame inertia $I_{L,t}$; In particular, the results from [Ser72] for the image $\rho_{E,\ell}(I_{L,t})$ will also apply to $\rho_{E,\ell}(I_L)$.

Suppose that $E_{/L}$ has good ordinary or bad multiplicative reduction. Then by [Ser72, Propositions 11 and 13], $I_{L,t}$ acts on the semisimplification of $E[\ell]$ via the trivial charac-

ter and $\theta_{\ell-1}^e$, where $\theta_{\ell-1}\colon I_{L,t} \to \mathbb{F}_\ell^\times$ is a surjective character.[1] The kernel of the reduction map $E[\ell] \to \widetilde{E}[\ell]$ is an L-rational ℓ-subgroup, and so one can identify $\rho_{E,\ell}(G_L) \subseteq B(\ell)$. With this identification, one has $\rho_{E,\ell}(I_L) \subseteq \left\{ \begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix} \right\}$. Thus, its semisimplification $\mathrm{im}\left(\begin{bmatrix} \theta_{\ell-1}^e & 0 \\ 0 & 1 \end{bmatrix} \right) = \mathcal{D}^e$ is a subgroup of $\rho_{E,\ell}(I_L)$ by e.g. [Gen1, Lemma 4].

Suppose then that $E_{/L}$ has good supersingular reduction. Following the proof of [LR13, Theorem 3.1], since $\ell \nmid \#\rho_{E,\ell}(I_L)$ one has that $I_{L,t}$ acts on $E[\ell]$ via a character $\theta_{\ell^2-1}^e$, where $\theta_{\ell^2-1}\colon I_{L,t} \to \mathbb{F}_{\ell^2}^\times$ is surjective [Ser72, Proposition 10]. Therefore, $\rho_{E,\ell}(I_L)$ is a cyclic subgroup of $\mathbb{F}_{\ell^2}^\times$ with index $\gcd(\ell^2-1, e)$, and so is isomorphic to the e'th power of $C_{ns}(\ell)$. □

Next, we will mildly generalize part of [LR13, Theorem 3.2]. For a diagonal matrix $\gamma := \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \in C_s(\ell)$, we let γ_f denote its "flip" $\begin{bmatrix} d & 0 \\ 0 & a \end{bmatrix}$. For a subgroup $H \subseteq C_s(\ell)$, we let $H_f := \{\gamma_f : \gamma \in H\}$.

Proposition 39. *With assumptions as in Theorem 38, assume further that $\ell \geq 17$ with $\ell \neq 23$. Let us set $H := \rho_{E,\ell}(I_L)$.*

- *If $H \subseteq N_s(\ell)$, then $\mathcal{D}^e \subseteq H$ or $\mathcal{D}_f^e \subseteq H$.*
- *If $H \subseteq N_{ns}(\ell)$, then $H = C_{ns}(\ell)^e$.*

Proof. First, let us assume that $H \subseteq N_s(\ell)$. Then by Theorem 38, $\mathcal{D}^e$ is contained in H up to conjugacy – otherwise we'd have $C_{ns}(\ell)^e = H$ up to conjugacy, which is impossible since $\ell+1 \nmid 48$. Thus, for some $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ we have $M\mathcal{D}^eM^{-1} \subseteq H \subseteq N_s(\ell)$. Since $\mathcal{D}^e$ is cyclic and $\#\mathcal{D}^e > 2$, it must have an element of order at least 3, and so one can show through calculations that either $a = d = 0$ or $b = c = 0$, whence we have $M\mathcal{D}^eM^{-1} = \mathcal{D}^e \subseteq H$ or $M\mathcal{D}^eM^{-1} = \mathcal{D}_f^e \subseteq H$.

[1] For $\ell \nmid d$ and a uniformizer x of L^{nr}, one has a character θ_d via the natural isomorphism $\theta_d\colon \mathrm{Gal}(L^{\mathrm{nr}}(\sqrt[d]{x})/L^{\mathrm{nr}}) \xrightarrow{\sim} \mu_d \subseteq \overline{L}$, where μ_d is the group of d'th roots of unity. Such characters parametrize the continuous $\overline{\mathbb{F}_\ell}$-valued characters of $I_{L,t}$ [Ser72, Proposition 5].

Next, let us assume that $H \subseteq N_{ns}(\ell)$. We claim that $\mathcal{D}^e$ is not contained in $N_{ns}(\ell)$ up to conjugacy. To see this, we note that elements of $\mathcal{D}^e$ have eigenvalues a and 1 where $a \in \mathbb{F}_\ell^\times$, whereas elements of $N_{ns}(\ell)$ have Galois-conjugate eigenvalues of the form $a \pm b\sqrt{\epsilon}$ or $\pm\sqrt{a^2 - b^2\epsilon}$ where $(a, b) \in \mathbb{F}_\ell^2 \smallsetminus \{(0, 0)\}$. As noted in the previous paragraph, $\mathcal{D}^e$ has an element of order at least 3, which then must have eigenvalues 1 and $a \in \mathbb{F}_\ell^\times \smallsetminus \{\pm 1\}$; in particular, such an element does not have an eigenvalue pair of the form $a \pm b\sqrt{\epsilon}$ or $\pm\sqrt{a^2 - b^2\epsilon}$. We thus deduce by Theorem 38 that H equals $C_{ns}(\ell)^e$ *up to conjugacy.*

We are left to show that $H = C_{ns}(\ell)^e$, not just up to conjugacy. We claim that $H \subseteq C_{ns}(\ell)$; observe that if this were true, then both H and $C_{ns}(\ell)^e$ are subgroups of the cyclic group $C_{ns}(\ell)$ with equal sizes, whence they must be equal. Both by cyclicity of H and $\#H = \#C_{ns}(\ell)^e$, there exists an element in H of order at least $(\ell^2 - 1)/6$. Since elements of $N_{ns}(\ell) \smallsetminus C_{ns}(\ell)$ have order dividing $2(\ell - 1)$, we deduce that H must be generated by an element of $C_{ns}(\ell)$, whence we conclude that $H = C_{ns}(\ell)^e$. □

Before we prove Theorem 29, let us record the following simple yet useful fact about non-diagonal subgroups of $N_s(\ell)$.

Lemma 40. *Let G be a subgroup of $N_s(\ell)$ that is not contained in $C_s(\ell)$. Then for all $\gamma \in G \cap C_s(\ell)$, one has $\gamma_f \in G$.*

Proof. For any matrix $M \in N_s(\ell) \smallsetminus C_s(\ell)$, one checks that $M \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} M^{-1} = \begin{bmatrix} d & 0 \\ 0 & a \end{bmatrix}$. □

6.4 The Proofs of Theorems 28 and 29

We will first prove Theorem 29. After doing so, we will also prove Proposition 33 in the following subsection, thereby proving Theorem 28.

6.4.1 The proof of Theorem 29

Proof of Theorem 29. Fix a prime $\ell \geq \max\{29, 15[F_0 : \mathbb{Q}] + 2\}$ unramified in F_0 where $\ell \notin S_{F_0}$. Fix an elliptic curve $E_{/F_0}$, and assume that $\rho_{E,\ell}(G_{F_0})$ is not equal to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Then by Proposition 37, we may fix a basis $\{P, Q\}$ of $E[\ell]$ such that $G := \rho_{E,\ell,P,Q}(G_{F_0})$ is contained in $N_s(\ell)$ or $N_{ns}(\ell)$.

Fix a prime $\mathfrak{L} \subseteq F_0$ over ℓ, and set $K := (F_0)_{\mathfrak{L}}$. Taking an extension L/K of minimal degree for which $E_{/L}$ is semistable, we know by Theorem 38 that $e := e(L/K) = e(L/\mathbb{Q}_\ell) \in \{1, 2, 3, 4, 6\}$.

Suppose first that $G \subseteq N_s(\ell)$; assume that $\ell \neq 37, 73$. Since $\ell \notin S_{F_0}$, we must have $G \not\subseteq C_s(\ell)$. By Proposition 39 we have $\mathcal{D}^e \subseteq \rho_{E,\ell}(I_L)$, without loss of generality. We claim that $\rho_{E,\ell}(I_K) \subseteq C_s(\ell)$: for the sake of contradiction, suppose this isn't true. Then since $\rho_{E,\ell}(I_K)$ is cyclic, it must be generated by an element M in $N_s(\ell) \smallsetminus C_s(\ell)$; such an element has order dividing $2(\ell-1)$. By Lemma 40, we have both containments $\mathcal{D}^e \subseteq \rho_{E,\ell}(I_K)$ and $\mathcal{D}_f^e \subseteq \rho_{E,\ell}(I_K)$. Since $\mathcal{D}^e$ and $\mathcal{D}_f^e$ commute with each other, it follows that their product $\mathcal{D}^e\mathcal{D}_f^e = C_s(\ell)^e$ is a subgroup of $\rho_{E,\ell}(I_K)$. We thus have that $\#C_s(\ell)^e = (\ell-1)^2/\gcd(\ell-1, e)^2$ divides $\#\rho_{E,\ell}(I_K)$, which is impossible since $\#\rho_{E,\ell}(I_K) \mid 2(\ell-1)$. We deduce that $\rho_{E,\ell}(I_K) \subseteq C_s(\ell)$.

The following work will construct a subgroup of G with size $2(\ell-1)^2/\gcd(\ell-1, e)$, which will prove the main index result for the case $G \subseteq N_s(\ell)$. First, we note that $\det \rho_{E,\ell}(I_K) = \chi_\ell(I_K)$, which surjects onto $\mathbb{F}_\ell^\times$ since $K/\mathbb{Q}_\ell$ is unramified. Additionally, for any matrix $\gamma \in C_s(\ell)$ one has $\gamma\gamma_f = \det(\gamma)I$. Therefore, since $\rho_{E,\ell}(I_K) \subseteq G \cap C_s(\ell)$ and $G \not\subseteq C_s(\ell)$, Lemma 40 implies that $Z(\ell) \subseteq G$.

Since $\mathcal{D}^e$ is a subgroup of G, it follows that $\mathcal{D}^e\mathcal{D}_f^e = C_s(\ell)^e$ is also a subgroup, and has size $(\ell-1)^2/\gcd(\ell-1, e)^2$. In fact, since $C_s(\ell)^e \cap Z(\ell) = Z(\ell)^e$ with size $(\ell-1)/\gcd(\ell-1, e)$, we find that $Z(\ell)C_s(\ell)^e$ is a subgroup of G with size

$$\#Z(\ell)C_s(\ell)^e = \#Z(\ell) \cdot \#C_s(\ell)^e \cdot \frac{1}{\#C_s(\ell)^e \cap Z(\ell)} = \frac{(\ell-1)^2}{\gcd(\ell-1, e)}.$$

Next, we fix an element $N \in G \smallsetminus C_s(\ell)$; writing $N = \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix}$, one has $N^2 = bcI = -\det(N)I \in Z(\ell)$. As shown in the proof of Lemma 40, one has for all $\gamma \in C_s(\ell)$ that $N\gamma N^{-1} = \gamma_f$, whence we have $N(Z(\ell)C_s(\ell)^e)N^{-1} = Z(\ell)C_s(\ell)^e$. In particular, $\langle N \rangle Z(\ell)C_s(\ell)^e$

is a subgroup of G, whose size is $2|-\det(N)| \cdot \frac{(\ell-1)^2}{\gcd(\ell-1,e)} \cdot \frac{1}{\#\langle N\rangle \cap Z(\ell)C_s(\ell)^e}$. One checks that $\langle N\rangle \cap Z(\ell)C_s(\ell)^e = \langle -\det(N)I\rangle$, from which we deduce that

$$\#\langle N\rangle Z(\ell)C_s(\ell)^e = \frac{2(\ell-1)^2}{\gcd(\ell-1,e)}.$$

From the containments $\langle N\rangle Z(\ell)C_s(\ell)^e \subseteq G \subseteq N_s(\ell)$, we compare indices and conclude that

$$[N_s(\ell) : G] \mid \gcd(\ell-1, e).$$

Suppose next that $G \subseteq N_{ns}(\ell)$. This argument will follow a proof of Le Fourn and Lemos [LFL21, Proposition 1.4], which itself follows an unpublished note of Zywina [Zyw, Proposition 1.13]. By Proposition 39 we have $C_{ns}(\ell)^e = \rho_{E,\ell}(I_L)$; the final paragraph of that proof can also be used to show that $\rho_{E,\ell}(I_K) \subseteq C_{ns}(\ell)$.

Since $\rho_{E,\ell}(I_L)$ has index $\gcd(\ell^2-1, e)$ in $C_{ns}(\ell)$, the index of $\rho_{E,\ell}(I_K)$ in $C_{ns}(\ell)$ divides $\gcd(\ell^2-1, e)$. Since $K/\mathbb{Q}_\ell$ is unramified, it follows that $\det(\rho_{E,\ell}(I_K)) = \mathbb{F}_\ell^\times$. This forces the index $[C_{ns}(\ell) : \rho_{E,\ell}(I_K)]$ to be odd, since otherwise $\rho_{E,\ell}(I_K)$ is a subgroup of the square elements of $C_{ns}(\ell)$, which contradicts surjectivity of the determinant of $\rho_{E,\ell}(I_K)$. We conclude that $[C_{ns}(\ell) : \rho_{E,\ell}(I_K)] \mid 3$.

Let us set $C(G) := G \cap C_{ns}(\ell)$. By the containment $\rho_{E,\ell}(I_K) \subseteq C(G)$, one has $[C_{ns}(\ell) : C(G)] \mid 3$; in particular, $C(G) = C_{ns}(\ell)$ or $C_{ns}(\ell)^3$. Since $\det\colon \rho_{E,\ell}(I_K) \to \mathbb{F}_\ell^\times$ is surjective and $\rho_{E,\ell}(I_K)$ is contained in $C(G)$, we have that $\det C(G) = \mathbb{F}_\ell^\times$.

We break our analysis into two cases:

1. $\ell \equiv 1 \pmod 3$. It follows that $C(G) = C_{ns}(\ell)$, since otherwise $\det C_{ns}(\ell)^3 = \mathbb{F}_\ell^\times$, which is impossible since $\#(\mathbb{F}_\ell^\times)^3 < \ell - 1$. In particular, we have $C_{ns}(\ell) \subseteq G$, and so $G = C_{ns}(\ell)$ or $N_{ns}(\ell)$.

2. $\ell \equiv 2 \pmod 3$. If $C(G) = C_{ns}(\ell)$, then $G = C_{ns}(\ell)$ or $N_{ns}(\ell)$. Suppose then that $C(G) = C_{ns}(\ell)^3$. One checks that $\overline{N_{ns}(\ell)} := N_{ns}(\ell)/C_{ns}(\ell)^3$ is isomorphic to the dihedral group D_3 of order 6, and the quotient group $\overline{G} := G/C_{ns}(\ell)^3$ has index

$I := [\overline{N_{ns}(\ell)} : \overline{G}] \mid 6$; note that $I = [N_{ns}(\ell) : G]$. Keeping in mind that $C(G) = G \cap C_{ns}(\ell) = C_{ns}(\ell)^3$, we have several cases for the index:

a. $I = 1$: then $G = N_{ns}(\ell)$, which is impossible since $G \cap C_{ns}(\ell) = C_{ns}(\ell)^3$.

b. $I = 2$: then $[N_{ns}(\ell) : G] = 2$. Thus we have

$$6 = [N_{ns}(\ell) : C_{ns}(\ell)^3] = 2[G : G \cap C_{ns}(\ell)],$$

and so $[G : G \cap C_{ns}(\ell)] = 3$. This is impossible since $[G : G \cap C_{ns}(\ell)] \leq [N_{ns}(\ell) : C_{ns}(\ell)] = 2$.

c. $I = 3$: then the even order element $\gamma := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ must lie in G (recall that $N_{ns}(\ell) = \langle \gamma, C_{ns}(\ell) \rangle$). Therefore, since the subgroup $G(\ell) := \langle \gamma, C_{ns}(\ell)^3 \rangle$ of G has the property that $[N_{ns}(\ell) : G(\ell)] = [N_{ns}(\ell) : G]$, we deduce that $G = G(\ell)$.

d. $I = 6$: then $[N_{ns}(\ell) : C_{ns}(\ell)^3] = [N_{ns}(\ell) : G]$, and so $G = C_{ns}(\ell)^3$.

We conclude that when $\ell \equiv 2 \pmod 3$ one has that G equals either $N_{ns}(\ell)$, $C_{ns}(\ell)$, $G(\ell)$ or $C_{ns}(\ell)^3$, which are of index $1, 2, 3$ and 6 in $N_{ns}(\ell)$, respectively.

Finally, we conclude our proof by noting that if F_0 has a real embedding, then it must have an element of trace 0 and determinant -1, from which we get $G \not\subseteq C_{ns}(\ell)$. □

6.4.2 The proof of Proposition 33

Recall that a set of primes A_{F_0} is F_0-admissible if for any elliptic curve $E_{/F_0}$, any prime $\ell \in \mathbb{Z}^+$ and any point $R \in E[\ell]$, if $R \notin E(F_0)$ then there exists a prime $p \in A_{F_0}$ for which

$$p \mid \#\mathcal{O}_{\rho_{E,\ell}(G_{F_0})}(R) = [F_0(R) : F_0].$$

Assume that GRH is true, and that F_0 has no rationally defined CM. We will now prove Proposition 33, which is that one can pick a finite choice of A_{F_0}.

Proof of Proposition 33. Fix an elliptic curve $E_{/F_0}$; below, for each prime $\ell \in \mathbb{Z}^+$ we will write $G := \rho_{E,\ell}(G_{F_0})$. First, we observe that we may exclude any finite amount of primes ℓ from our analysis. This is because for any point $R \in E[\ell]^\bullet$, the size of its orbit $\mathcal{O}_G(R)$ equals the index of the stabilizer of R in G, and this index divides $\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) = \ell(\ell-1)^2(\ell+1)$. To this end, let us start by adding to $A_{F_0} := \emptyset$ the set of prime divisors of $\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, where we range over ℓ ramified in F_0, $\ell < \max\{29, 15[F_0 : \mathbb{Q}] + 2\}$, $\ell = 37, 73$ and $\ell \in S_{F_0}$.

Fix a prime $\ell \notin A_{F_0}$. We will show that every order ℓ point of E has even degree over F_0, which will show that A_{F_0} is F_0-admissible. If $G = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then G acts transitively on $E[\ell]^\bullet$ and thus the degree of any point in $E[\ell]^\bullet$ over F_0 is $\ell^2 - 1$, which is a multiple of 8. To this end, let us assume that $G \neq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$; then Proposition 37 implies that G lies in the normalizer of a Cartan subgroup up to conjugacy. Let us fix a basis $\{P, Q\}$ of $E[\ell]$ for which $G := \rho_{E,\ell,P,Q}(G_{F_0})$ is contained in $N_s(\ell)$ or $N_{ns}(\ell)$.

Suppose G is contained in $N_s(\ell)$. Since $\ell \notin S_{F_0}$, we must have $G \subseteq N_s(\ell) \smallsetminus C_s(\ell)$. Fix a point $R \in E[\ell]^\bullet$ which is not F_0-rational, and set $H := \rho_{E,\ell,P,Q}(G_{F_0(R)})$. Then we have

$$[G : H] = [F_0(R) : F_0].$$

Since H acts trivially on the subgroup $\langle R \rangle$, [LR13, Lemma 6.6] applies and we land in one of the following 3 cases:

i. H is contained in $\mathcal{D}$;

ii. H is contained in $\mathcal{D}_f$;

iii. H equals $\left\{ I, \begin{bmatrix} 0 & b \\ b^{-1} & 0 \end{bmatrix} \right\}$ for some $b \in \mathbb{F}_\ell^\times$.

By Theorem 29 we have that $Z(\ell) \subseteq G$. Thus, since $Z(\ell) \cap H = 1$ in all three cases, we find that $Z(\ell)H$ is a subgroup of G of size $(\ell-1)\#H$, and so $\ell - 1 \mid [G : H]$, i.e., $\ell - 1 \mid [F_0(R) : F_0]$, whence we find that $[F_0(R) : F_0]$ is even.

Suppose G is contained in $N_{ns}(\ell)$. Then combining Equation (6.1) with Theorem 29, we have for all points $R \in E[\ell]^\bullet$ that

$$\ell^2 - 1 \mid 6 \cdot [F_0(R) : F_0].$$

Since $\ell^2 \equiv 1 \pmod 8$, we deduce that $4 \mid [F_0(R) : F_0]$. We thus conclude that our finite set A_{F_0} is F_0-admissible. □

6.5 The Case Where CM is Rationally Defined

We conclude this paper by proving Theorem 30, which says that the conclusion of Theorem 28 fails when we allow F_0 to have rationally defined CM. In particular, we will show in this situation that no F_0-admissible set A_{F_0} is finite. To construct the appropriate counterexamples, we will use a mild generalization of Dirichlet's theorem on primes in arithmetic progressions.

Lemma 41 (Primes in multiple arithmetic progressions)**.** *Let $M_1, \ldots, M_r$ be pairwise coprime positive integers. For each $1 \leq i \leq r$, fix an integer a_i coprime to M_i. Then there are infinitely many primes $\ell \in \mathbb{Z}^+$ such that for each $1 \leq i \leq r$ one has $\ell \equiv a_i \pmod{M_i}$.*

Proof. By the Chinese Remainder Theorem, there exists an integer $x \in \mathbb{Z}$ such that for each $1 \leq i \leq r$ we have

$$x = a_i + M_i k_i$$

for some $k_i \in \mathbb{Z}$. Since each $\gcd(a_i, M_i) = 1$, it follows that x is coprime to the product $M_1 M_2 \cdots M_r$.

Dirichlet's theorem on primes in arithmetic progressions tells us there are infinitely many primes in the congruency class $\{x + M_1 M_2 \cdots M_r k : k \in \mathbb{Z}\}$. Let $\ell \in \mathbb{Z}^+$ be any such prime; then we can write

$$\ell = x + M_1 M_2 \cdots M_r k$$

for some $k \in \mathbb{Z}$. Thus for each $1 \leq i \leq r$ one has

$$\ell = a_i + M_i(k_i + M_1 M_2 \cdots M_{i-1} M_{i+1} \cdots M_r k)$$

from which it follows that $\ell \equiv a_i \pmod{M_i}$. □

As we will see, our proof of Theorem 30 requires the existence of an arbitrarily large prime which both splits in at least one imaginary quadratic order in F_0 and satisfies certain coprimality conditions.

Lemma 42. *Let K be an imaginary quadratic field and $\mathcal{O} \subseteq K$ an order. Then for any integer $B > 0$ there are infinitely many primes ℓ which split in $\mathcal{O}$ and, depending on the fundamental discriminant Δ_K, will satisfy one of the following:*

1. *If $\Delta_K = -3$, then $\frac{\ell-1}{6}$ is coprime to B.*
2. *If $\Delta_K = -4$, then $\frac{\ell-1}{4}$ is coprime to B.*
3. *If $\Delta_K < -4$, then $\frac{\ell-1}{2}$ is coprime to B.*

Proof. Throughout this proof, we will assume that B is squarefree and $B > 2$. Let us write $K = \mathbb{Q}(\sqrt{-d})$ where $d \in \mathbb{Z}^+$ is squarefree. Given an integer $n \in \mathbb{Z}^+$, let us also write $\mathrm{odd}(n)$ for the odd part of n.

First, let us suppose that $d = -1$, i.e., $\mathcal{O} = \mathbb{Z}[fi]$ where $f := [\mathbb{Z}[i] : \mathcal{O}]$. Then by Lemma 41 there are infinitely many primes $\ell \in \mathbb{Z}^+$ with $\ell \nmid f$ for which $\ell \equiv -3 \pmod 8$ and $\ell \equiv -1 \pmod{\mathrm{odd}(B)}$. The first congruence shows that $\frac{\ell-1}{4}$ is odd, and since $\ell \equiv 1 \pmod 4$ we have that ℓ splits in $\mathcal{O}$. From the second congruence, we get that $\ell - 1 \equiv -2 \not\equiv 0 \pmod{\mathrm{odd}(B)}$, whence $\mathrm{odd}(B)$ is also coprime to $\frac{\ell-1}{4}$. We conclude that both the splitting and coprimality conditions hold.

Next we suppose that $d = -3$, i.e., $\mathcal{O} = \mathbb{Z}[f\zeta_3]$ where ζ_3 is a primitive cube root of unity and $f := [\mathbb{Z}[\zeta_3] : \mathcal{O}]$. Let us write $\mathrm{odd}(B) = 3^e B'$ where $\gcd(6, B') = 1$ and $0 \leq e \leq 1$. Then by Lemma 41 there are infinitely many primes $\ell \in \mathbb{Z}^+$ with $\ell \nmid f$ for which $\ell \equiv -5$

(mod 36) and $\ell \equiv -1 \pmod{B'}$. One similarly checks that $\frac{\ell-1}{6}$ is coprime to B, and since $\ell \equiv 1 \pmod 3$ it follows that ℓ splits in $\mathcal{O}$. Thus both desired conditions on ℓ hold.

In what follows, we suppose that $d \neq -1, -3$; we will check several cases for d. Recall that for any prime $\ell \in \mathbb{Z}^+$, ℓ splits in $\mathcal{O}$ iff both $\ell \nmid f$ and the Legendre symbol

$$\left(\frac{-d}{\ell}\right) = 1.$$

Let us write

$$d = -2^e \cdot \prod_{i=1}^{r} p_i \cdot \prod_{j=1}^{s} q_j,$$

where $0 \leq e \leq 1$ and the primes $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ (allowing $r = 0$ or $s = 0$). Then given a prime $\ell \in \mathbb{Z}^+$, the Legendre symbol factorizes as

$$\left(\frac{-d}{\ell}\right) = \left(\frac{-1}{\ell}\right) \cdot \left(\frac{2}{\ell}\right)^e \cdot \prod_{i=1}^{r} \left(\frac{p_i}{\ell}\right) \cdot \prod_{j=1}^{s} \left(\frac{q_j}{\ell}\right).$$

In particular, if $\ell \equiv -1 \pmod 4$ then quadratic reciprocity implies

$$\left(\frac{-d}{\ell}\right) = (-1)^{s+1} \cdot \left(\frac{2}{\ell}\right)^e \cdot \prod_{i=1}^{r} \left(\frac{\ell}{p_i}\right) \cdot \prod_{j=1}^{s} \left(\frac{\ell}{q_j}\right). \tag{6.2}$$

We divide our work into three cases:

1. $e = 1$: then there are infinitely many primes $\ell \in \mathbb{Z}^+$ with $\ell \nmid f$ such that $\ell \equiv 3 \pmod 8$ and $\ell \equiv -1 \pmod{\text{odd}(\text{lcm}(d, B))}$. The former condition implies $\left(\frac{2}{\ell}\right)^e = -1$, and the latter condition implies that each $\left(\frac{\ell}{p_i}\right) = 1$ and $\left(\frac{\ell}{q_j}\right) = -1$, whence we have by (6.2) that $\left(\frac{-d}{\ell}\right) = 1$. Furthermore, from $\ell \equiv -1 \pmod{\text{odd}(B)}$ and $\ell \equiv -1 \pmod 4$, we find that B is coprime to $\frac{\ell-1}{2}$.

2. $e = 0$ and $r \neq 0$: fix $1 \leq k \leq r$ with $p_k \equiv 1 \pmod 4$, and fix a nonsquare $\alpha \bmod p_k$. Then by Lemma 15, there are infinitely many primes $\ell \in \mathbb{Z}^+$ with $\ell \nmid f$ such that $\ell \equiv \alpha \pmod{p_k}$ and $\ell \equiv -1 \pmod{4 \cdot \frac{\text{odd}(\text{lcm}(d,B))}{p_k}}$. We check by (6.2) that $\left(\frac{-d}{\ell}\right) = 1$, and that B is coprime to $\frac{\ell-1}{2}$.

3. $e = 0$ and $r = 0$: then there exists $1 \leq k \leq s$ with $q_k \neq 3$, since otherwise we have $d = -3$. Fix such a k, and fix a square $\alpha \not\equiv 1 \pmod{q_k}$. Then by Lemma 41, there are infinitely many primes $\ell \in \mathbb{Z}^+$ with $\ell \nmid f$ such that $\ell \equiv \alpha \pmod{q_k}$ and $\ell \equiv -1 \pmod{4 \cdot \frac{\mathrm{odd}(\mathrm{lcm}(d,B))}{q_k}}$. Thus by (6.2) we have that both ℓ splits in $\mathcal{O}$ and B is coprime to $\frac{\ell-1}{2}$. □

Proof of Theorem 30. We will first prove the case where $F_0 := K_{\mathcal{O}}$ is a ring class field of an order $\mathcal{O}$ from an imaginary quadratic field K.

Fix an integer $B \in \mathbb{Z}^+$. First, let us assume that the fundamental discriminant $\Delta_K \neq -3, -4$. Then by Lemma 42, there exists a prime $\ell \geq 7$ for which both ℓ splits in $\mathcal{O}$ and $\frac{\ell-1}{2}$ is coprime to B. By [BC20, Corollary 1.8], there exists an $\mathcal{O}$-CM elliptic curve $E_{/K_{\mathcal{O}}}$ whose mod-ℓ Galois representation image $\rho_{E,\ell}(G_{K_{\mathcal{O}}})$ equals $C_s(\ell)$ with respect to some basis $\{P, Q\}$ of $E[\ell]$. It follows that the $G_{K_{\mathcal{O}}}$-stable subgroup $\langle P \rangle$ induces a $K_{\mathcal{O}}$-rational ℓ-isogeny of E, and since $\rho_{E,\ell}(G_{K_{\mathcal{O}}}) = C_s(\ell)$ the degree of P over $K_{\mathcal{O}}$ is

$$[K_{\mathcal{O}}(P) : K_{\mathcal{O}}] = \ell - 1.$$

Let $r \colon G_{K_{\mathcal{O}}} \to \mathbb{F}_\ell^\times$ denote the isogeny character of $\langle P \rangle$, i.e., the action of $G_{K_{\mathcal{O}}}$ on $\langle P \rangle$. Then we have

$$\#r(G_{K_{\mathcal{O}}}) = [K_{\mathcal{O}}(P) : K_{\mathcal{O}}] = \ell - 1.$$

Let us define a new character $\chi \colon G_{K_{\mathcal{O}}} \to \mathbb{F}_\ell^\times$ via

$$\chi(\sigma) := r(\sigma)^{\frac{\ell-1}{2}}.$$

Thus $\chi(\sigma) = 1$ if $r(\sigma)$ is a square mod ℓ, and is -1 otherwise. Let E' be the quadratic twist of E by χ; then E' is also defined over $K_{\mathcal{O}}$ and has CM by $\mathcal{O}$. Furthermore, P induces a point $P' \in E'[\ell]^\bullet$ that generates a $K_{\mathcal{O}}$-rational ℓ-isogeny, and whose isogeny character is $r' := \chi \cdot r$.

We claim that the order $\#r'(G_{K_{\mathcal{O}}}) = \frac{\ell-1}{2}$. To see this, we first note that for each $\sigma \in G_{K_{\mathcal{O}}}$, if the image $r(\sigma)$ has even order, then it must be a non-square modulo ℓ; this follows from $\ell \equiv 3 \pmod 4$. It follows that $r'(\sigma) = -r(\sigma)$ has odd order equal to $\frac{\ell-1}{\gcd(\ell-1, \frac{\ell-1}{2}+k)}$, where

we've written $\langle g \rangle = \mathbb{F}_\ell^\times$ and $r(\sigma) = g^k$. So taking a generator $g := r(\sigma)$ of $\mathbb{F}_\ell^\times$, it follows that $r'(\sigma)$ has order $\frac{\ell-1}{2}$, whence we deduce that $r'(G_{K_\mathcal{O}})$ is an index two subgroup of $\mathbb{F}_\ell^\times$.

By the above work, we conclude that

$$[K_\mathcal{O}(P') : K_\mathcal{O}] = \frac{\ell-1}{2},$$

whence the degree of P' over $K_\mathcal{O}$ is coprime to B. Since $\frac{\ell-1}{2} > 1$, we find that P' is not $K_\mathcal{O}$-rational. We conclude that

$$E'(L)[\ell] \supsetneq E'(K_\mathcal{O})[\ell]$$

where $L := K_\mathcal{O}(P')$. In particular, for a set $A_{K_\mathcal{O}}$ of primes to be $K_\mathcal{O}$-admissible, for any integer $B \in \mathbb{Z}^+$ it must contain a prime coprime to B, which forces $\#A_{K_\mathcal{O}} = \infty$.

Next, we suppose that $\Delta_K = -4$, and so $\mathcal{O} \subseteq \mathbb{Z}[i]$. By Lemma 42, we can choose a prime $\ell \geq 13$ which splits in $\mathcal{O}$ – by its proof, let us choose $\ell \equiv -3 \pmod 8$ – and for which $\frac{\ell-1}{4}$ is coprime to B. Again by [BC20, Corollary 1.8] there exists an $\mathcal{O}$-CM elliptic curve $E_{/K_\mathcal{O}}$ for which

$$\rho_{E,\ell}(G_{K_\mathcal{O}}) = C_s(\ell) \tag{6.3}$$

with respect to some basis $\{P, Q\}$ of $E[\ell]$.

By [BP17, Proposition 2.2] there exists a $\mathbb{Z}[i]$-CM elliptic curve $E''_{/K_\mathcal{O}}$ and a $K_\mathcal{O}$-rational cyclic f-isogeny $E \to E''$, where $f := [\mathbb{Z}[i] : \mathcal{O}]$. Since $\ell \nmid f$, this restricts to a $\mathbb{F}_\ell[G_{K_\mathcal{O}}]$-module isomorphism $E[\ell] \xrightarrow{\sim} E''[\ell]$, whence we have isomorphic mod-ℓ Galois representations, $\rho_{E,\ell}(G_{K_\mathcal{O}}) \cong \rho_{E'',\ell}(G_{K_\mathcal{O}})$.

So without loss of generality, let us assume that $\mathcal{O} = \mathbb{Z}[i]$. Then (6.3) tells us there is a $K_\mathcal{O}$-rational ℓ-isogeny $\langle P \rangle \subseteq E[\ell]$ for which $[K_\mathcal{O}(P) : K_\mathcal{O}] = \ell - 1$; write its isogeny character as $r \colon G_{K_\mathcal{O}} \to \mathbb{F}_\ell^\times$. Let us define the quartic character $\chi := r^{\frac{\ell-1}{4}} : G_{K_\mathcal{O}} \to \mathbb{F}_\ell^\times$. Then one obtains a quartic twist $E'_{/K_\mathcal{O}}$ of E via χ. Corresponding to $P \in E$, one has an ℓ-torsion point $P' \in E'$ whose isogeny character is $\chi \cdot r$. Since $\ell \equiv -3 \pmod 8$, we find that the image

$(\chi \cdot r)(G_{K_\mathcal{O}})$ is an index 4 subgroup of $\mathbb{F}_\ell^\times$, whence we have

$$[K_\mathcal{O}(P') : K_\mathcal{O}] = \frac{\ell - 1}{4}.$$

In particular, over the extension $K_\mathcal{O}(P')$ of $K_\mathcal{O}$, the elliptic curve E' obtains a new torsion point P' whose nontrivial degree $[K_\mathcal{O}(P') : K_\mathcal{O}] = \frac{\ell-1}{4}$ is coprime to B. We conclude that $\#A_{K_\mathcal{O}} = \infty$ for any $K_\mathcal{O}$-admissible set $A_{K_\mathcal{O}}$.

A similar analysis shows that when $K = \mathbb{Q}(\sqrt{-3})$ there exists a prime $\ell \geq 31$ with $\ell \equiv -5 \pmod{36}$, for which a sextic twist E' of a $\mathbb{Z}[\zeta_3]$-CM elliptic curve $E_{/K_\mathcal{O}}$ with $\rho_{E,\ell}(G_{K_\mathcal{O}}) = C_s(\ell)$ will have an ℓ-torsion point P' of degree $\frac{\ell-1}{6} > 1$ over $K_\mathcal{O}$, and for which $\frac{\ell-1}{6}$ is coprime to B. This concludes the proof in the case where the base field F_0 is a ring class field $K_\mathcal{O}$ of an imaginary quadratic order.

Finally, let us assume that F_0 contains a ring class field $K_\mathcal{O}$ of an imaginary quadratic field. Then our work above shows that for $B \in \mathbb{Z}^+$, there exists a prime $\ell \gg_{K_\mathcal{O},B} 0$, an $\mathcal{O}$-CM elliptic curve $E_{/K_\mathcal{O}}$ and a torsion point $P \in E[\ell]$ such that $E(K_\mathcal{O}(P))[\ell] \neq E(K_\mathcal{O})[\ell]$ and the degree $[K_\mathcal{O}(P) : K_\mathcal{O}]$ is coprime to B. Since ℓ is allowed to be arbitrarily large with respect to F_0, we may assume that $[F_0(P) : F_0] > 1$; for example, by Merel's Theorem we can take $\ell > \max\{7, [F_0 : \mathbb{Q}]^{3[F_0:\mathbb{Q}]^2}\}$ [Mer96, Théorème]. Furthermore, since $K_\mathcal{O}(P)/K_\mathcal{O}$ is Galois we find that $[F_0(P) : F_0] \mid [K_\mathcal{O}(P) : K_\mathcal{O}]$, and so it follows that the degree of P over F_0 is also coprime to B. We deduce that $E(F_0(P))[\ell] \neq E(F_0)[\ell]$, and so we conclude that any F_0-admissible set A_{F_0} must have $\#A_{F_0} = \infty$. $\square$

Bibliography

[Ara08] K. Arai, *On uniform lower bound of the Galois images associated to elliptic curves*, J. Théor. Nombres Bordeaux 20 (2008), 23–43.

[BC20] A. Bourdon and P.L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. 305 (2020), 43–88.

[BCP17] A. Bourdon, P.L. Clark and P. Pollack, *Anatomy of torsion in the CM case*, Math. Z. 285 (2017), no. 795–820.

[BCS17] A. Bourdon, P.L. Clark and J. Stankewicz, *Torsion points on CM elliptic curves over real number fields*, Trans. Amer. Math. Soc 369 (2017), 8457–8496.

[BELOV19] A. Bourdon, Ö. Ejder, Y. Liu, F. Odumodu and B. Viray, *On the level of modular curves that give rise to isolated j-invariants*, Adv. Math 357 (2019), 106824, 33.

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

[BP17] A. Bourdon and P. Pollack, *Torsion subgroups of CM elliptic curves over odd degree number fields*, Int. Math. Res. Not. IMRN 16 (2017), 4923–4961.

[Cla] P.L. Clark, *CM elliptic curves: volcanoes, reality and applications, Part I,* preprint, `https://arxiv.org/abs/2212.13316`.

[CCRS14] P.L. Clark, P. Corn, A. Rice and J. Stankewicz, *Computations on elliptic curves with complex multiplication*, LMS J. Computation and Mathematics 17 (2014), 509–535.

[CGPS22] P.L. Clark, T. Genao, P. Pollack and F. Saia, *The least degree of a CM point on a modular curve*, J. Lond. Math. Soc. (2) 105 (2022), no. 2, 825–883.

[CMP18] P.L. Clark, M. Milosevic and P. Pollack, *Typically bounding torsion,* J. Number Theory 192 (2018), 150–167.

[CP15] 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.

[CP17] P.L. Clark and P. Pollack, *The truth about torsion in the CM case, II*, Q. J. Math. 68 (2017), 1313–1333.

[CP18] P.L. Clark and P. Pollack, *Pursuing polynomial bounds on torsion*, Israel J. Math 227 (2018), 889–909

[Con] K. Conrad, *Simultaneous commutativity of operators,* `https://kconrad.math.uconn.edu/blurbs/linmultialg/simulcomm.pdf`.

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

[DEvH+21] M. Derickx, A. Etropolski, M. van Hoeij, J. Morrow and D. Zureick-Brown, *Sporadic cubic torsion*, Algebra Number Theory 15 (2021), 1837–1864.

[DS17] M. Derickx and A.V. Sutherland, *Torsion subgroups of elliptic curves over quintic and sextic number fields*, Proc. Amer. Math. Soc. 145 (2017), 4233–4245.

[Dic58] L.E. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover Publications, Inc., New York (1958).

[Elk04] N. Elkies, *On elliptic K-curves*, Modular curves and abelian varieties, Progr. Math. 224 (2004), 81–91.

[Ell04] J. Ellenberg, *$\mathbb{Q}$-curves and Galois representations*, Progr. Math. 224 (2004), 93–103.

[EW80] P. Erdős and S.S. Wagstaff Jr., *The fractional parts of the Bernoulli numbers*, Illinois J. Math. 24 (1980), 104–112.

[Etr] A. Etropolski, *A local-global principle for images of Galois representations,* preprint.

[Gen1] T. Genao, *Typically bounding torsion on elliptic curves with rational j-invariant,* J. Number Theory 238 (2022), 823–841.

[Gen2] T. Genao, *Typically bounding torsion on elliptic curves isogenous to rational j-invariant,* Proc. Amer. Math. Soc. 151 (2023), no. 5, 1907–1914.

[Gen3] T. Genao, *Polynomial bounds on torsion from a fixed geometric isogeny class*, preprint, `https://arxiv.org/abs/2210.10177`.

[Gen4] T. Genao, *Growth of torsion groups of elliptic curves upon base change from number fields*, preprint, `https://arxiv.org/abs/2210.16977`.

[Glö96] H. Glöckner, *Haar measure on linear groups over local skew fields*, J. Lie Theory 6 (1996), 165–177.

[GJN20] E. González-Jiménez and F. Najman, *Growth of torsion groups of elliptic curves upon base change*, Math. Comp. 89 (2020), 1457–1485.

[Gre12] R. Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny*, Amer. J. Math. 134 (2012), 1167–1196.

[HW08] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, 6th Ed., Oxford University Press, Oxford (2008).

[Hei34] H. Heilbronn, *On the Class Number in Imaginary Quadratic Fields.* Quart. J. Math. Oxford Ser. 25 (1934), 150–160.

[HS99] M. Hindry and J. 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.

[JKP06] D. Jeon, C.H. Kim and E. Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. 74 (2006), 1–12.

[Kam92a] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. 109 (1992), 221–229.

[Kam92b] S. Kamienny, *Torsion points on elliptic curves over fields of higher degree*, Internat. Math. Res. Notices (1992), 129–133.

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

[KW09a] C. Khare and J-P. W, *Serre's modularity conjecture. I*, Invent. Math. 178 (2009), 485–504.

[KW09b] C. Khare and J-P. W, *Serre's modularity conjecture. II*, Invent. Math. 178 (2009), 505–586.

[LV14] E. Larson and D. Vaintrob, *Determinants of subquotients of Galois representations associated with abelian varieties, with an appendix by Brian Conrad,* J. Inst. Math. Jussieu 13 (2014), 517–559.

[LFL21] S. Le Fourn and P. Lemos, *Residual Galois representations of elliptic curves with image contained in the normaliser of a nonsplit Cartan*, Algebra Number Theory 15 (2021), 747–771.

[LFN20] S. Le Fourn and F. Najman, *Torsion of $\mathbb{Q}$-curves over quadratic fields*, Math. Res. Lett. 27 (2020), 209–225.

[LR13] Á. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. 357 (2013), 279–305.

[LR18] Á. Lozano-Robledo, *Uniform boundedness in terms of ramification*, Res. Number Theory 4 (2018), Paper No. 6, 39.

[Maz76] B. Mazur, *Rational points on modular curves*, Modular functions of one variable, V, Lecture notes in Math., Vol. 601 (1977), 107–148.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal,* Inst. Hautes Études Sci. Publ. Math. No. 47 (1977).

[Mer96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), 437–449.

[Ols76] L.D. Olson, *Points of finite order on elliptic curves with complex multiplication*, Manuscripta Math. 14 (1974), 195–205.

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

[Pro18] O. Propp, *Cartan images and ℓ-torsion points of elliptic curves with rational j-invariant*, Res. Number Theory 4 (2018), Paper No. 12, 23.

[Rib92] K. Ribet, *Abelian varieties over $\mathbb{Q}$ and modular forms*, Algebra and topology 1992 (Taejŏn) (1992), 53–79.

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331.

[Ser98] J-P. Serre, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics (1998).

[Sil09] J. Silverman, *The arithmetic of elliptic curves*, 2nd Ed., Graduate Texts in Mathematics, vol. 106, Springer (2009).

[Zyw] D. Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over* $\mathbb{Q}$, preprint, `https://arxiv.org/abs/1508.07660`.