Torsion of Elliptic Curves

by

Marko Milosevic

(Under the Direction of Pete L. Clark)

Abstract

This dissertation describes two papers, one published and one in preparation, about the torsion subgroups of Elliptic Curves. The first chapter gives a brief introduction to elliptic curves and the history of research on torsion points of elliptic curves. The second chapter establishes a concept of *typical boundedness* for the torsion groups of a family of elliptic curves. The third chapter gives a partial classification for torsion groups of elliptic curves with complex multiplication defined over Abelian number fields.

Index words: Elliptic Curves, Torsion

Torsion of Elliptic Curves

by

Marko Milosevic

B.S. Mathematics and Computer Science, 2011

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

2018

Torsion of Elliptic Curves

by

Marko Milosevic

Major Professor:	Pete L. Clark
Committee:	Daniel Krashen
	Paul Pollack
	Robert Rumely

Electronic Version Approved:

Suzanne Barbour
Dean of the Graduate School
The University of Georgia
December 2018

Torsion of Elliptic Curves

Marko Milosevic

November 27, 2018

Acknowledgments

I must first acknowledge Pete Clark, Michael Chou, and Paul Pollack who were my coauthors on the works this dissertation is based on. In particular, I must thank Pete for his mentorship, wisdom and patience over my entire graduate career at the University of Georgia. My entire family has been a constant source of love and support throughout this entire experience.

Contents

Chapter 1

Introduction to Torsion of Elliptic Curves

This dissertation describes two sets of results on the torsion subgroups of elliptic curves. In the first part of chapter one we will cover some of the preliminaries on the theory of elliptic curves. In the second part, we will review some of the major results, both historical and recent, in the study of torsion points on elliptic curves.

1.1 Preliminaries on Elliptic Curves

Elliptic curves are smooth, projective curves of genus one with at least one rational point. Every such curve can be defined by a Weierstrass equation of the form

$$E: \ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^4 + a_6Z^3,$$

where if $a_1, a_2, a_3, a_4, a_6 \in K$ for some field K, we say that E is defined over K [Sil86, Section III.1]. If an elliptic curve is defined over some field, we denote it with E/K. Normally, the equation is given dehomogenized as

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

For fields K of characteristic not equal to two or three, the Weierstrass Equation can be further reduced to the equation

$$E: \ y^2 = x^3 + Ax + B.$$

We will only consider elliptic curves defined over such number fields. To each Weierstrass equation of an elliptic curve, we will associate two invariants called the *discriminant* Δ, and *j-invariant* J_E. To define them, we first define some auxiliary variables $b_2, b_4, b_6, b_8, c_4, c_6$ in terms of the coefficients a_1, a_2, a_3, a_4, a_6 of the Weierstrass equation defined above.

$$\begin{aligned}
b_2 &= a_1^2 + 4a_4 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= (b_2b_6 - b_4^2)/8 \\
c_4 &= b_2^3 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6
\end{aligned}$$

Now we can give the definition of the discriminant and j-invariant as

$$\begin{aligned}
\Delta &= \frac{c_4^3 - c_6^2}{1728} \\
J_E &= \frac{c_4^3}{\Delta}
\end{aligned}$$

In the case of char(K) $\neq 2, 3$, with the reduced Weierstrass equation $y^2 = x^3 + Ax + B$, then the discriminant and j-invariant can also be simplified to

$$\Delta = -16(4A^3 + 27B^2)$$
$$J_E = \frac{-1728(4A)^3}{\Delta}$$

The Weierstrass equation must have discriminant not equal to zero for it to be an elliptic curve. The j-invariant classifies the isomorphism classes of elliptic curves over the algebraic closure of the field K. While the study of elliptic curves can be traced back to certain classical Diophantine problems, the modern study of elliptic curves can be attributed to Poincaré. Poincaré proved that the rational points on an elliptic curve $E(\mathbb{Q})$ form an Abelian group [HP1901] by using the chord-and-tangent process: given two points on an elliptic curve, the line through them intersects the elliptic curve at a third rational point, or given a single point, the tangent line to that point intersects the elliptic curve at a second rational point. We define the addition of two points P, Q by finding this point of intersection of the line and the elliptic curve, and then reflecting it over the x-axis. We assign the identity to be the point at infinity, given by projective coordinates [0 : 1 : 0]. Additive inverses are given by reflecting the point across the x-axis.

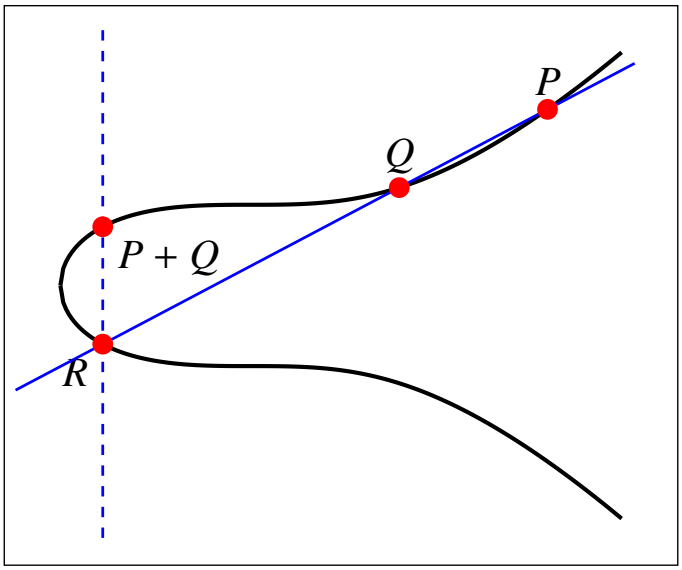


Figure 1.1: An example of the elliptic curve group law for the elliptic curve $y^2 = x^3 + 17$ where the points are $P = (4, 9)$, $Q = (2, 5)$, $R = (-2, -3)$, and $P + Q = (-2, 3)$

Morphisms of elliptic curves need not preserve the group law of elliptic curves; therefore, we need to define maps between elliptic curves that preserve the group structure of elliptic curves.

Definition 1.1. *Given two elliptic curves E_1, E_2, an isogeny of elliptic curves is a morphism that fixes the identity.*

$$\phi : E_1 \to E_2 \text{ with } \phi(O) = O.$$

We say that two elliptic curves E_1, E_2 are isogenous if there is a nonzero isogeny between E_1 and E_2. The degree of an nonzero isogeny is the size of its kernel i.e. $\deg(\phi) = |\phi^{-1}(O)|$.

Isogenies are indeed group homomorphisms on the rational points of elliptic curves [Sil86, Theorem III.4.8]. We define scalar multiplication of points as follows: given a point P on an elliptic curve and $n \in \mathbb{Z}^+$, then we write that $nP = \sum_{i=1}^{n} P$. Similarly, if $n \in \mathbb{Z}^-$, then $nP = \sum_{i=1}^{|n|} -P$, and if $n = 0$, then $nP = 0$. This gives us the following class of isogenies described below.

Definition 1.2. *Given an integer n, the multiplication-by-n isogeny is defined as follows*

$$[n] : E \to E$$

$$P \mapsto nP$$

This leads us to consider our object of study, the points of finite order of elliptic curves, which we call the *torsion points* of the elliptic curve.

Definition 1.3. *Let E be an elliptic curve and $n \in \mathbb{Z}^+$. The n-torsion subgroup of E is*

$$E[n] = \{P \in E : nP = O\}.$$

The torsion subgroup of E, E[tors] *is the set of all points of finite order, i.e. the union of all the n-torsion subgroups. The set of torsion points in some field K is denoted E*(*K*)[tors].

We will establish preliminary results here. Later, we will introduce more results in chapters II and III as needed.

Theorem 1.4. *For an elliptic curve E defined over a number field K*

$$E[n] \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

For a proof see [Sil86, Theorem 6.4]. To clarify $E[n] = \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$ over the algebraic closure $\mathbb{C}$. For the torsion points of $F \supset K$ is a subgroup of $E[N]$, in other words $E(F)[N] \subset E[N]$; however, determining precisely what the subgroup $E(K)[N]$ is for various number fields K, requires more consideration. This leads us to one of the most important classical theorems of Elliptic curves.

Theorem 1.5 (Mordell-Weil Theorem [Mor1922], [W1929])**.** *For a number field K and elliptic curve E*/*K, the set of rational points E*(*K*) *is finitely generated.*

This implies that $E(K) \cong \mathbb{Z}^r \oplus E(K)[\text{tors}]$, where $r \geq 0$ is called the rank of the elliptic curve and $E(K)[\text{tors}]$, the torsion subgroup, is finite.

An important auxiliary object of elliptic curves is the endomporphism ring $\text{End}(E)$, the set of isogenies that map E onto itself. Clearly, the set of multiplication-by-n isogenies are all endomorphisms, so we can conclude that $\mathbb{Z} \hookrightarrow \text{End}(E)$, i.e. there is an injective homomorphism. Indeed, somewhat surprisingly, for most elliptic curves defined over a number field, $\text{End}(E)$ is isomorphic to $\mathbb{Z}$.

Theorem 1.6. *For a number field F, the endomorphism ring for an elliptic curve E/F is either $\mathbb{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field K.*

For a proof of this see [Sil86, Corollary III.9.4]. We say that elliptic curves E/F such that $End(E) \cong \mathcal{O}$ have *complex multiplication*. Elliptic curves with complex multiplication are a special class of elliptic curves and often require separate consideration from elliptic curves without complex multiplication. The theory of elliptic curves with complex multiplication is deeply intertwined with class field theory. We omit here a more thorough treatment of elliptic curves with complex multiplication; however, we provide more information in chapter III.

1.2 Torsion of Elliptic Curves

Given a number field F and elliptic curve E/F, we have seen that $E(F)[\text{tors}]$ is a finite abelian group. The study of the torsion subgroups of elliptic groups aims to classify these torsion subgroups under various criteria. In this pursuit, some questions that have been asked are:

- Given a fixed number field F, what is the set of all torsion subgroups $E(F)[\text{tors}]$ for any E/F?
- Given a fixed degree d, what is the set of all torsion subgroups for elliptic curves E/F where F is any number field such that $[F : \mathbb{Q}] = d$?

- Given a fixed degree d, can we bound the size of the torsion subgroups $|E(F)[\text{tors}]|$ for all elliptic curves E/F where F is any number field of degree d?
- Given a family of elliptic curves $\mathcal{F}$, can we say what prime torsion exists, i.e. for what primes p does there exist a point of order p for some elliptic curve $E/F \in \mathcal{F}$?

For each of these questions, as we will see, we may need to separately consider elliptic curves with and without complex multiplication. In this section, we provide a survey of the research done on the torsion subgroups of elliptic curves.

The first major result of the classification of torsion subgroups is due to Mazur, who classified the torsion subgroups of elliptic curves defined over the rationals.

Theorem 1.7 ([M78])**.** *Let $E/\mathbb{Q}$ be an elliptic curve, then*

$$E(\mathbb{Q})[\text{tors}] \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & \text{for } 1 \leq N \leq 10, N = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} & \text{for } 1 \leq N \leq 4 \end{cases}$$

and each of these cases occur for some elliptic curve $E/\mathbb{Q}$.

Merel proved a uniform boundedness for the order of torsion subgroups as a function of the degree of the number field they are defined over.

Theorem 1.8 ([Me96])**.** *For every degree $d \in \mathbb{Z}^+$ there exists a bound $B(d) \in \mathbb{Z}^+$ such that for all elliptic curves E/F with $[F : Q] = d$, we have $|E(F)[\text{tors}]| \leq B(d)$.*

Merel's theorem unfortunately does not give us a better than exponential bound on the size of the torsion subgroup. Hindry-Silverman have proven such a better than exponential bound for elliptic curves with integral j-invariant, which includes the class of ellitpic curves with complex multiplication [HS99].

Theorem 1.9. *[HS99, Thm. 1] Let $d \geq 2$. Let K be a degree d number field, and let E/K be an elliptic curve over K with algebraic integral j-invariant: equivalently, E has potentially good reduction at all finite places of K. Then $\#E(K)[tors] \leq 1977408 d \log d$.*

Furthermore, there is a more recent result by Clark and Pollack that improves on this result.

Theorem 1.10 ([CP2015])**.** *There exists an absolute, effective constant C such that for all number fields F with $[F : \mathbb{Q}] \geq 3$ and all elliptic curves E/F with complex multiplication*

$$E(F)[\text{tors}] \leq Cd \log(\log(d)).$$

Indeed, we not only have a bound on the size of the torsion subgroup, but we also have a much stronger bound on the size of the largest prime power dividing the order of the torsion subgroup. Merel provided such a bound in his original work, but it was soon afterwards improved by Parent.

Theorem 1.11 ([P99])**.** *Let E/K be an elliptic curve over a number field K of degree d, and let E have a rational point of order p^n. Then*

$$p^n \leq \begin{cases} 129(3^d - 1)(3d)^6 & \text{if } p = 2 \\ 65(5^d - 1)(2d^6) & \text{if } p = 3 \\ 65(3^d - 1)(2d^6) & \text{if } p \geq 5. \end{cases}$$

In a series of papers from Kamienny, Kenku and Momose, the classification for quadratic number fields was completed about fifteen years after the rational case.

Theorem 1.12 (Kamienny-Kenku-Momose [KM88],[K92])**.** *Given a quadratic number field K*

and elliptic curve E/K, then

$$E(K)[\text{tors}] \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & \text{for } 1 \leq N \leq 16, N = 18 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} & \text{for } 1 \leq N \leq 6 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z} & \text{for } 1 \leq N \leq 2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

Each possible group is realized by some quadratic field K and elliptic curve E/K.

For cubic fields, a complete classification has not yet been published; however, there has been much recent progress. There are recent studies from Daniels, Lozano-Robledo, Najman, and Sutherland on the compositum of all cubic fields $\mathbb{Q}(3^\infty)$, that limits the possible torsion subgroups to just twenty in addition to providing the $\overline{\mathbb{Q}}$-isomorphism classes of the elliptic curves in each class [DLNS2018]. There are some classification results for elliptic curves defined over higher degree number fields; however, already for quartic and quintic fields there is much work left to be done.

For elliptic curves with complex multiplication, there have been many recent results. For instance, for number fields of degree $1 \leq d \leq 13$, all possible torsion subgroups of elliptic curves with complex multiplication have been found [CCRS2014]. In chapter II, we find that the size of the torsion subgroups of a large family of elliptic curves is *typically* bounded. In chapter III, we continue a classification for all elliptic curves defined over abelian number fields that was started by Clark in 2015 [C15].

Chapter 2

Typically Bounded Families of Elliptic Curves

2.1 Introduction

The work in this chapter is a product of currently unpublished collaboration with Pete L. Clark and Paul Pollack at the University of Georgia [CMP2017]. In this work we define a concept of *typical boundedness* of torsion on a family of abelian varieties; however, in this chapter I restrict my treatment to families of elliptic curves.

We define a family $\mathcal{F}$ of elliptic curves to be a set whose elements are pairs $E_{/F}$ of an elliptic curve E and the number field F it is defined over. A natural question in the study of torsion points of elliptic curves is whether the torsion subgroups of the elements of some family $\mathcal{F}$ are uniformly bounded. Similarly, we can ask when a family of elliptic curves has torsion that is *almost* bounded.

Definition 2.1. *For a subset of the positive integers $S \subset \mathbb{Z}^+$, we define the* upper density *and* lower

density *respectively as:*

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

Taking the set of torsion subgroups of some family of elliptic curves defined over various number fields F, we will prohibit a set of degrees $[F:\mathbb{Q}]$ of arbitrarily small density.

Definition 2.2. *A family of elliptic curves $\mathcal{F}$ is said to have typically bounded torsion if for all $\epsilon > 0$, there is $B_\epsilon \in \mathbb{Z}^+$ such that the set*

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

has upper density at most ϵ.

By the work of Bourdon, Clark, and Pollack [BCP17, Theorem 1.1a], we know that the family of elliptic curves with complex multiplication $\mathcal{E}_{cm}$ has typically bounded torsion over all number fields. Therefore, the next question would be whether the family of all elliptic curves has typically bounded torsion. The following result was communicated to us by Filip Najman from University of Zagreb.

Theorem 2.3. *[CMP2017, Theorem 1.7] Let $\mathcal{E}$ be the family of all elliptic curves over all number fields. For each $B \in \mathbb{Z}^+$, the set $\mathcal{S}(\mathcal{E}, B)$ contains all but finitely many positive integers.*

Thus, torsion is *not* typically bounded on the family of all elliptic curves over all number fields. Therefore, we must restrict our family of elliptic curves to find typically bounded torsion. Our main results produce such a family of elliptic curves with typically bounded torsion.

Theorem 2.4. *Let F_0 be a number field with $[F_0:\mathbb{Q}] \geq 3$ that does not contain the Hilbert class field of any imaginary quadratic field. Under the Generalized Riemann Hypothesis, torsion is*

typically bounded on the family $\mathcal{E}_{F_0}$ of all elliptic curves E defined over a number field $F \supset F_0$ such that $j(E) \in F_0$.

For our next result, we replace the Generalized Riemann Hypothesis with an alternative hypothesis. For $d_0 \in \mathbb{Z}^+$, we introduce a hypothesis $\mathrm{SI}(d_0)$ defined as follows:

$\mathrm{SI}(d_0)$: There is prime $\ell_0 = \ell_0(d_0)$ such that for all primes $\ell > \ell_0$, the modular curve $X_0(\ell)$ has no noncuspidal non-CM points of degree d_0.

When $d_0 = 1$, Mazur has shown that $\mathrm{SI}(1)$ holds with $\ell_0 = 37$ [M78]. It is conjectured that $\mathrm{SI}(d_0)$ holds for all $d_0 \in \mathbb{Z}^+$; however, it is currently unproven for all $d_0 \geq 2$.

Theorem 2.5. *Let $d_0 \in \mathbb{Z}^+$. If $\mathrm{SI}(d_0)$ holds, then torsion is typically bounded on the family $\mathcal{E}_{d_0}$ of all elliptic curves $E_{/F}$ defined over some number field F, and satisfying $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d_0$.*

2.2 Two Conditions for Typically Bounded Torsion

For a family of elliptic curves $\mathcal{F}$ of elliptic curves over number fields, consider the following two conditions:

(C1): For all primes p and all positive integers N, there exists an $n(p, N)$ such that for elliptic curves $E_{/F} \in \mathcal{F}$, if $E(F)$ has a point of order p^n, then $p^N \mid [F : \mathbb{Q}]$. In other words, the order of p^n torsion in E/F is bounded in terms of the power of p dividing $[F : \mathbb{Q}]$.

(C2): There exists a positive integer c such that for all prime numbers p and elliptic curves $E_{/F} \in \mathcal{F}$, if $E(F)$ has a point of order p, then

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

Where nonzero, rational y, x, $y|x$ if and only if $\frac{y}{x}$ is an integer. For any finite set of prime numbers $p_1, p_2, \ldots, p_n$, if we take c to be divisible by $\prod_{i=1}^{n}(p_i - 1)$, then we get that condition (C2) holds trivially. Therefore, we can exclude finitely many primes from our consideration. In other words, condition $(C2)$ holds if there is a positive integer c' and prime p_0 such that for all prime numbers $p \geq p_0$ and $E_{/F} \in \mathcal{F}$, if $E(F)$ has a point of order p, then $\frac{p-1}{c'} \mid [F : \mathbb{Q}]$.

These conditions are sufficient to determine if a family of elliptic curves has typically bounded torsion.

Theorem 2.6. *Let $\mathcal{F}$ be a family of elliptic curves over number fields that satisfies both conditions (C1) and (C2), then $\mathcal{F}$ has typically bounded torsion.*

Proof. The Erdös-Wagstaff Theorem [EW80, Theorem 2] states that for all $\epsilon > 0$, there exists a constant C_ϵ such that the set of positive integers that have a divisor of the form $\ell - 1 > C_\epsilon$ for a prime number ℓ has an *upper density* of at most ϵ. As a result, for any fixed $c \in \mathbb{Z}^+$ there exists a $C = C(c, \epsilon)$ such that the set of positive integers d for where there exists a prime $\ell > C$ such that

$\ell - 1 \mid cd$ has upper density at most ϵ.

By condition (C2), there exists a $c \in \mathbb{Z}^+$ such that for all $d \in \mathbb{Z}^+$, if F is a number field of degree d and $E_{/F} \in \mathcal{F}$ with $\ell \mid \#E(F)[\text{tors}]$, we have $\ell - 1 \mid cd$. Thus after removing a set of degrees d of upper density at most $\epsilon/2$, there exists an $L \in \mathbb{Z}^+$ such that if $\ell \mid \#E(F)[\text{tors}]$ for some $E_{/F} \in \mathcal{F}$ with $[F : \mathbb{Q}] = d$, then $\ell \leq L$. For each $\ell \leq L$ and $N \in \mathbb{Z}^+$, the set of d, which are divisible by ℓ^N, has a density of $\frac{1}{\ell^N}$. Therefore, if N is sufficiently large, then the set of positive integers d which is divisible by ℓ^N for some $\ell \leq L$ has density at most $\epsilon/2$. By condition $(C1)$, there is a positive integer n such that if $\ell \leq L$ and $E_{/F} \in \mathcal{F}$ has a point of order ℓ^{n+1} then $\ell^N \mid [F : \mathbb{Q}]$. This gives a set $\mathcal{D}_\epsilon \subset \mathbb{Z}^+$ of upper density at most ϵ such that if $E_{/F} \in \mathcal{F}$ and $[F : \mathbb{Q}] \notin \mathcal{D}_\epsilon$, then the order of any torsion point of $E(F)$ divides $P = \prod_{\ell \leq L} \ell^n$. Hence, if we choose that $B_\epsilon = 1 + \prod_{\ell \leq L} \ell^n$, we can see that the *exponent* of torsion is typically bounded in $\mathcal{F}$, in the sense that the set

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

has upper density at most ϵ. Therefore, since $\#E(F)[\text{tors}] \mid (\exp E(F)[\text{tors}])^2$, then we can conclude that $\mathcal{F}$ has typically bounded *torsion* as well. □

Now that we have established a criterion for typically bounded torsion, we shall show that our families of elliptic curves satisfy both conditions. By [Me96] the family $\mathcal{E}$ of all elliptic curves has the following property: For all $d \in \mathbb{Z}^+$, there is a $B(d) \in \mathbb{Z}^+$ such that for all number fields F of degree d, if $E_{/F} \in \mathcal{E}$ then $\#E(F)[\text{tors}] \leq B(d)$.

Theorem 2.7. *Let $\mathcal{F}$ be a family of elliptic curves over number fields that is closed under base extension, and let $\mathcal{F}_d$ be the subfamily of $\mathcal{F}$ consisting of all elliptic curves $E_{/F}$ such that there is a subfield $F_0 \subset F$ with $[F_0 : \mathbb{Q}] = d$ and an elliptic curve $(E_0)_{/F_0}$ such that $(E_0)_{/F} \cong E_{/F}$. Then, such a family $\mathcal{F}_d$ satisfies Condition (C1).*

Proof. Fix a prime number p and a positive integer N. If $E_{/F} \in \mathcal{F}_d$, then there is a subfield $F' \subset F$ with $[F' : \mathbb{Q}] = d$ such that E has a model over F'. Let $P \in E(F)$ have order p^n for some $n \geq N$.

Then $F'(P) \subset F'(E[p^n])$, so

$$[F'(P) : F'] \mid [F'(E[p^n]) : F'] \mid \#\,\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}).$$

Moreover, for a certain integer c with $\gcd(c, p) = 1$, depending only on p (and not on n), we can write

$$\#\,\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}) = cp^G$$

for some positive integer G. On the other hand, because $\mathcal{F}_d$ has the above property from Merel's theorem, when n is sufficiently large compared to N, then

$$[F'(P) : F'] \geq cp^N.$$

It follows that

$$p^N \mid [F'(P) : F'] \mid [F : \mathbb{Q}]. \quad \square$$

Theorem 2.8. *Let $d_0 \in \mathbb{Z}^+$. The family $\mathcal{E}_{d_0}$ of all elliptic curves $E_{/F}$ defined over number fields such that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d_0$ satisfies Condition (C1).*

Proof. Fix p a prime number, N a positive integer, and let $n \in \mathbb{Z}^+$ be such that for every elliptic curve $E_{/F}$ arising by base extension from a number field of degree d_0 such that $E(F)$ has a point of order p^n, we have $p^{N+2} \mid [F : \mathbb{Q}]$.

Let F be any number field, let $E_{/F}$ be an elliptic curve with $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d_0$, and suppose that $E(F)$ has a point of order p^n. Let $F_0 = \mathbb{Q}(j(E))$, let $(E_0)_{/F_0}$ be any elliptic curve. Then $F_0 \subset F$, and there is F'/F of degree dividing 12 such that $E_{/F'} \cong (E_0)_{/F'}$. Then $E_0(F') \cong E(F') \supset E(F)$ has a point of order p^n, so

$$p^{N+2} \mid [F' : \mathbb{Q}] = [F' : F][F : \mathbb{Q}] \mid 12[F : \mathbb{Q}],$$

and thus

$$\mathrm{ord}_p[F : \mathbb{Q}] \geq N.$$

Therefore, by using Theorem 2.7 with Merel's Theorem we get that the family of elliptic curves arising by base extension from a number field of degree d_0 satisfies condition (C1). □

2.3 Divisibility of Torsion Fields

Let E/F be an elliptic curve defined over a number field F and $E(F)[\mathrm{tors}]$ be the torsion subgroup. Let $R \in E[p]$ be a torsion point of exact order prime p and let $F(R) = F(x(R), y(R))$ be the field of definition of R. Álvaro Lozano-Robledo [LR13] has shown that, under certain conditions, for $\mathbb{Q}$-Rational elliptic curves

$$[\mathbb{Q}(R) : \mathbb{Q}] \geq \frac{p-1}{2}.$$

We generalize this inequality condition to a class of number fields F and to a divisibility for almost all primes.

We denote the Mod-p Galois representation of E/F

$$\rho_{E,p} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

Let G be image of the $\rho_{E,p}$ the Galois representation. Under the hypotheses of Theorems 2.4 and 2.5 condition (C1) always holds, and we must show that condition (C2) holds as well. We therefore reduce Theorem 2.4 and Theorem 2.5 to Theorem 2.9, below:

Theorem 2.9.

a) Let $d_0 \in \mathbb{Z}^+$ be such that $\mathrm{SI}(d_0)$ *holds. The family $\mathcal{E}_{d_0}$ of all elliptic curves defined over number fields such that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = d_0$ satisfies condition (C2).*

b) Let F_0 be a number field that does not contain the Hilbert class field of any imaginary

quadratic field. If $[F_0 : \mathbb{Q}] \geq 3$ *and we assume the Generalized Riemann Hypothesis (GRH), then the family* $\mathcal{E}_{F_0}$ *of all elliptic curves defined over a number field* $F \supset F_0$ *such that* $j(E) \in F_0$ *satisfies condition (C2).*

The proof of part a)

We begin our proof of 2.9. As previously stated, we know that in the case of complex multiplication we have typically bounded torsion [BCP17], so we may restrict ourselves to elliptic curves without complex multiplication. We will first prove part (a) of the theorem and then address part (b) at the end.

Let $d_0 \in \mathbb{Z}^+$ be such that SI(d_0) holds: that for all primes $\ell > \ell_0$, the modular curve $X_0(\ell)$ has no noncuspidal non-CM points of degree d_0. For $E_{/F} \in \mathcal{E}_{d_0}$, let $F_0 = \mathbb{Q}(j(E))$ and let $(E_0)_{/F_0}$ be an elliptic curve with $j(E_0) = j(E)$, so $F_0 \subset F$. Since E has no CM, there is a quadratic extension F'/F such that $E_{/F'} \cong (E_0)_{/F'}$. Since $[F' : \mathbb{Q}] = 2[F : \mathbb{Q}]$, if the family $\mathcal{G}_{d_0}$ of all elliptic curves $E_{/F}$ that arise by base extension from $(E_0)_{/\mathbb{Q}(j(E_0))}$ with $[\mathbb{Q}(j(E_0)) : \mathbb{Q}] = d_0$ satisfies condition (C2) for some $c \in \mathbb{Z}^+$, then the family $\mathcal{E}_{d_0}$ satisfies (C2) for $2c$. So we may work with $\mathcal{G}_{d_0}$.

Let F_0 be a number field of degree d_0, and let $(E_0)_{/F_0}$ be an elliptic curve with $\mathbb{Q}(j(E)) = F_0$. Let p be a prime number, let

$$\rho_p \colon \mathfrak{g}_{F_0} \to \mathrm{GL}(E_0[p])$$

be the mod p Galois representation attached to $(E_0)_{/F_0}$, let $G = \rho_p(\mathfrak{g}_{F_0})$ be its image, and let $\overline{G}$ be its projective image, i.e., the image of G under the homomorphism $\mathrm{GL}(E_0[p]) \to \mathrm{PGL}(E_0[p])$. The degrees of extensions F/F_0 such that $E_0(F)$ has a point of order p are the multiples of the sizes of the orbits of G on $E_0[p] \setminus \{0\}$. Thus it is sufficient to show that there is $c = c(d_0)$ such that for all $(E_0)_{/F_0}$ as above and for all nonzero $P \in E_0[p]$, we have

$$\frac{p-1}{c} \,\Big|\, [F_0(P) : \mathbb{Q}].$$

Recall that $\det \rho_p \colon \mathfrak{g}_{F_0} \to (\mathbb{Z}/p\mathbb{Z})^\times$ is the mod p cyclotomic character χ_p. Let

$$i(p) = [(\mathbb{Z}/p\mathbb{Z})^\times : \chi_p(\mathfrak{g}_{F_0})].$$

Then $i(p)$ depends on F_0 and not just d_0; however, since $\chi_p(\mathfrak{g}_\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$, we have $i(p) \mid d_0$. In particular, we have in all cases that

$$\frac{p-1}{d_0} \,\Big|\, \frac{p-1}{i(p)} \,\Big|\, \#G.$$

A choice of $\mathbb{F}_p$-basis e_1, e_2 for $E_0[p]$ induces an isomorphism $\mathrm{GL}(E_0[p]) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{F}_p)$, thus G may be viewed as a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, well-defined up to conjugacy.

By Serre's classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ [S72][Section 2], we know that there are five cases for image of the Galois representation G.

1. The subgroup G contains $\mathrm{SL}_p(E_0[p])$.
2. G is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(E_0[p])$.
3. G is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(E_0[p])$.
4. The projective image G in $\mathrm{PGL}_2(E_0[p])$, $\overline{G}$, is isomorphic to one of three exceptional subgroups A_4, S_4, or A_5.
5. G is contained in a Borel subgroup of $\mathrm{GL}_2(E_0[p])$.

Case 1

Suppose $G = \rho_p(\mathfrak{g}_{F_0})$ contains $\mathrm{SL}_2(E_0[p])$. Then

$$[\mathrm{GL}_2(E_0[p]) : G] \mid i(p) \mid d_0.$$

Since $\mathrm{GL}(E_0[p])$ acts transitively on $E_0[p] \setminus \{0\}$, the size of any orbit of G on $E_0[p] \setminus \{0\}$ is divisible by

$$\frac{\#(E_0[p] \setminus \{0\})}{d_0} = \frac{(p+1)(p-1)}{d_0}.$$

Thus $\frac{p-1}{d_0} \mid [F_0(P) : F_0]$, so $p - 1 \mid [F_0(P) : \mathbb{Q}]$: we may take $c = 1$.

Case 2

Definition 2.10. *The split Cartan subgroup of $GL_2(\mathbb{F}_p)$ is the subgroup*

$$C_{sp} = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| \, a, b \in \mathbb{F}_p^x \right\}$$

We can see that the normalizer of a split Cartan in $GL_2(\mathbb{F}_p)$ is

$$C_{sp}^+ = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{F}_p^x \right\}$$

If G is contained in a split Cartan, then it is contained in a Borel subgroup, namely the set of matrices $m \in \mathrm{GL}_2(E_0[p])$ that fix a single line L, which we leave for case 5. So suppose that G is contained in C_{sp}^+ but not contained in C_{sp}. Let $F \supset F_0$ be a number field such that $E_0(F)$ has a point P of order p. Then $\rho_p\big|_{\mathfrak{g}_F}$ has image contained in C_{sp}^+ and also fixes P and thus the one-dimensional subspace $L = \langle P \rangle$, so the following result applies with $H = \rho_p(\mathfrak{g}_F)$.

Lemma 2.11. *([LR13, Lemma 6.6]) Let H be a non-trivial subgroup of C_{sp}^+ that fixes each element in an one-dimensional $\mathbb{F}_p$-subspace V of $\mathbb{F}_p^2$. Then, there are three possible cases for H.*

(i) $H \leq \left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \middle| \, b \in \mathbb{F}_p^x \right\}$ *and* $V = \langle (1, 0) \rangle$.

(ii) $H \leq \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \middle| \, a \in \mathbb{F}_p^x \right\}$ *and* $V = \langle (0,1) \rangle$.

(iii) $H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & c \\ c^{-1} & 0 \end{pmatrix} \middle| \, \text{for some } c \text{ in } \mathbb{F}_p^x \right\}$ *and* $V = \langle (c,1) \rangle$.

Proof. The diagonal matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ has eigenvectors (1,0), (0,1) with eigenvalues a,b respectively. The anti-diagonal matrix $\begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}$ has characteristic polynomial $\lambda^2 - cd$. Thus $\lambda_1 = -\lambda_2$. Knowing that one of the eigenvalues must be 1, the other must be -1, and thus $d = c^{-1}$. □

Proposition 2.12. *Let E/F be an elliptic curve with a torsion point $R \in E[p]$ of exact order prime p, where F is any number field. Suppose that there is an $\mathbb{F}_p$-basis of $E[p]$ such that G is a subgroup of C_{sp}^+, but $G \not\leq C_{sp}$. Let $F(R)$ be minimal field of definition for the point R. For all primes,*

$$\frac{p-1}{2} \Big| \, [F(R) : F].$$

Proof. First suppose that we are in case **(iii)** of our above Lemma 2.11, then $|H| = 2$. By case 1, we have that $(p-1) \Big| \, |G|$. Thus, we can deduce that

$$\frac{p-1}{2} \Big| \, \frac{|G|}{|H|} = [F(R) : F].$$

Now, suppose that we are in case **(i)** (case **(ii)** is identical). We can consider

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \middle| \, b \in J \leq \mathbb{F}_p^x \right\},$$

where J is a subgroup of $\mathbb{F}_p^x$. We can see that $|H| = |J|$. Let g be a generator of the multiplicative

group $\mathbb{F}_p^x$ with order $\frac{p-1}{i(p)}$, and $M_g \in G \subseteq C_{\text{sp}}^+$ such that $\det(M_g) = g$. We have two sub-cases, either $M_g = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, or $M_g = \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}$.

If M_g is a diagonal matrix, then we have that $\det(M_g) = ab$. Thus, we have that $ab = g$. Since, $G \nsubseteq C_{\text{sp}}$, there exists an anti-diagonal matrix in G. Thus,

$$\begin{pmatrix} 0 & d^{-1} \\ c^{-1} & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix} \in G$$

Then we can see that

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} = \begin{pmatrix} g & 0 \\ 0 & g \end{pmatrix} \in G$$

By taking power of this diagonal matrix, we get that $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in G$ for all $a \in \mathbb{F}_p^x$. We can construct a subgroup $\tilde{J}$ of G that contains $H \cong J$ as follows

$$J \leq \tilde{J} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \middle| \, \forall a \in \mathbb{F}_p^x, b \in J \right\} \leq G$$

Thus since $|\tilde{J}| = (p-1)|J|$, we can conclude that $(p-1)|\frac{|G|}{|H|} = [F(R) : F]$. Now suppose that M_g is the anti-diagonal matrix. We get that $\det(M_g) = -cd$, so $cd = -g$. We get that

$$M_g^2 = \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}^2 = \begin{pmatrix} cd & 0 \\ 0 & cd \end{pmatrix} = \begin{pmatrix} -g & 0 \\ 0 & -g \end{pmatrix} \in G$$

Once again, we have two cases. Suppose that $p \equiv 1 (\text{mod } 4)$, in which case $-g$ is a generator for $\mathbb{F}_p^x$, in which case we can replicate our previous argument to get that $(p-1)|[F(R) : F]$. Now suppose that $p \equiv 3 (\text{mod } 4)$, i.e. $-g$ is not a generator of $\mathbb{F}_p^x$. In this case since $-g$ has order $(p-1)/2$, by

taking powers of M_g^2, we can generate the group of diagonal matrices

$$\left\{ \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \middle| \, t \in (\mathbb{F}_p^x)^2 \right\}$$

We can construct a subgroup $\tilde{J}$ of G that contains $H \cong J$ as follows

$$J \leq \tilde{J} = \left\{ \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \middle| \, \forall t \in (\mathbb{F}_p^x)^2, b \in J \right\} \leq G.$$

Since $|\tilde{J}| = \frac{p-1}{2} \cdot |J|$, we can conclude that $\frac{p-1}{2} |\frac{|G|}{|H|} = [F(R) : F]$. □

Case 3

Definition 2.13. *Let $p \geq 3$ prime. The non-split Cartan Subgroup of $GL_2(\mathbb{F}_p)$ is*

$$C_{ns} = \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} \middle| \, (a, b) \in (\mathbb{F}_p)^2 / \{(0, 0)\} \right\}$$

where ϵ is fixed quadratic non-residue $\mathbb{F}_p$.

The normalizer of a non-split Cartan Subgroup in $GL_2(\mathbb{F}_p)$ is

$$C_{ns}^+ = \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}, \begin{pmatrix} c & \epsilon d \\ -d & -c \end{pmatrix} \middle| \, (a, b), (c, d) \in (\mathbb{F}_p)^2 / \{(0, 0)\} \right\}$$

Lemma 2.14. *([LR13, Lemma 7.4]) Let H be a non-trivial subgroup of C_{ns}^+ that fixes each element*

in an one-dimensional $\mathbb{F}_p$-subspace V of $\mathbb{F}_p^2$. Then,

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} c & \epsilon d \\ -d & -c \end{pmatrix} \right\}$$

for some $c, d \in \mathbb{F}_p$ with $c^2 - \epsilon d^2 = 1$, where ϵ is a fixed quadratic non-residue of $\mathbb{F}_p$.

Proof. We need to consider matrices of both forms in C_{ns}^+. A matrix of the form $\begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} \in C_{\text{ns}}^+$ has eigenvalues $a \pm b\sqrt{\epsilon} \in \overline{\mathbb{F}_p}$. For this matrix to fix a non-trivial vector of $\mathbb{F}_p^2$, $a = 1$ and $b = 0$, i.e. identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

A matrix of the form $\begin{pmatrix} c & \epsilon d \\ -d & -c \end{pmatrix}$ has a eigenvalues $\pm\lambda$ of the form $\lambda^2 = c^2 - \epsilon d^2$. One of the eigenvalues being 1 means that $c^2 - \epsilon d^2 = 1$. The corresponding eigenvectors to such a matrix are multiples of $(-\epsilon d, c - 1)$ if $c \neq 1$, else it is a multiple of $(1, 0)$ with $c = 1$ and $d = 0$. Suppose you have two matrices

$$\begin{pmatrix} c & \epsilon d \\ -d & -c \end{pmatrix} \text{ and } \begin{pmatrix} c' & \epsilon d' \\ -d' & -c' \end{pmatrix}$$

with the same eigenvector and eigenvalue 1. This is true if and only if $(-\epsilon d, c - 1)$ is in the kernel of

$$\begin{pmatrix} c & \epsilon d \\ -d & -c \end{pmatrix} - \begin{pmatrix} c' & \epsilon d' \\ -d' & -c' \end{pmatrix} = \begin{pmatrix} c - c' & \epsilon d - d' \\ -d + d' & -c + c' \end{pmatrix}$$

Thus, the determinant of the above matrix must be 0, i.e. $-(c - c')^2 + \epsilon(d - d')^2 = 0$. Since ϵ is a quadratic non-residue, then in fact $c = c'$, $d = d'$. Thus, any such matrices are equivalent in $\mathrm{GL}_2(\mathbb{F}_p)$, so such a matrix is unique. □

Therefore for a nonzero $P \in E_0[P]$, we have

$$\frac{p-1}{2i(p)} \mid \frac{p-1}{2d_0} \mid [G : H] = [F_0(P) : F_0],$$

so $\frac{p-1}{2} \mid [F_0(P) : \mathbb{Q}]$ and we may take $c = 2$.

Case 4

We have the following result from Etropolski to address the case (4) of the exceptional subgroups.

Proposition 2.15 ([Et16, Prop. 2.6])**.** *Let $E_{/K_0}$ be an elliptic curve defined over a number field K_0 of degree d_0. For a prime number p, let $\overline{G}$ be the projective image of the mod p Galois representation.*

a) If $\overline{G} \cong A_4$, then $p \leq 9d_0 + 1$.

b) If $\overline{G} \cong S_4$, then $p \leq 12d_0 + 1$.

c) If $\overline{G} \cong A_5$, then $p \leq 15d_0 + 1$.

So this case can occur only if $p \leq 15d_0 + 1$; therefore we can omit these primes.

Case 5

The subgroup G is contained in a Borel subgroup if and only if E admits an F_0-rational p-isogeny. By our assumption SI(d_0) is exactly that the set of primes p, for which a non-CM elliptic curve defined over a number field of degree d_0 is finite. Therefore, by the above remark we can omit these primes.

This completes the proof of part (a) of 2.9.

The proof of part b)

The hypothesis SI(d_0) was only used in Case 5, so only Case 5 needs to be revised under the hypotheses of part b): suppose that F_0 does not contain the Hilbert class field of any imaginary quadratic field. This precisely prohibits having an elliptic curve $E_{/F_0}$ for which the CM is F_0-rationally defined. Then the following result of Larson-Vaintrob gives Case 5 under (GRH).

Lemma 2.16. *[LV14, Corollary 2] Under GRH, the degrees of the prime degree isogenies of elliptic curves over F are bounded uniformly if and only if F does not contain the Hilbert class field of an imaginary quadratic field K (i.e. if and only if there are no elliptic curves with CM defined over K).*

Finally, suppose moreover that $[F_0 : \mathbb{Q}] = 2$. Then the hypothesis on F_0 becomes that F_0 is not itself an imaginary quadratic field of class number 1. Under this hypothesis, Momose showed [Mo95] that the set of primes p such that an elliptic curve $E_{/F_0}$ admits an F-rational p-isogeny is finite. This completes the proof of Case 5 and thus the proof of Theorem 2.9(b).

Chapter 3

Torsion of CM-Elliptic Curves over Abelian Number Fields

This chapter is joint work still in progress with Pete Clark and Michael Chou. Clark [C15] showed that exists a uniform bound on the size of the torsion subgroup of a CM-elliptic curve defined over $\mathbb{Q}^{ab}$ i.e, there exists a $T \in \mathbb{Z}^+$ such that for every CM elliptic curve $E/\mathbb{Q}^{ab}$, $\#E(\mathbb{Q}^{ab})[\text{tors}] \leq T$. Furthermore, under the Generalized Riemann Hypothesis, Voight classified the 101 possible discriminants of Hilbert class fields of imaginary quadratic fields that are abelian over $\mathbb{Q}$ [Vo07], which due to the fundamental connection between class fields and CM-elliptic curves, we will use to restrict the possible torsion of CM-elliptic curves over abelian number fields. We partially classify the torsion groups of such CM elliptic curves defined over $\mathbb{Q}^{ab}$.

3.1 Preliminaries

Let $E/\mathbb{Q}^{ab}$ be an elliptic curve with CM-field K, $\mathcal{O}_K$ be the maximal order of K, and $K^{\mathfrak{I}}$ be the ray class field for the ideal $\mathfrak{I}$ of $\mathcal{O}_K$. The $\mathfrak{I}$-torsion kernel is denoted as $E[\mathfrak{I}]$. To continue, we need to mention the following fundamental theorem of complex multiplication.

Theorem 3.1. *[Sil94][Theorem 5.] Let $E_{/\mathbb{C}}$ be an $\mathcal{O}_K$-CM elliptic curve, and let $W : E \to \mathbb{P}^1$ be a Weber function, and let $\mathfrak{I} \subset \mathcal{O}_K$ be a nonzero ideal. Then, we have an equality between the field given by adjoining the values of the Weber-function on the J-torsion kernel $\mathfrak{I}$ and the ray class fields associated to $\mathfrak{I}$:*

$$K(j(E), W(E[\mathfrak{I}])) = K^{\mathfrak{I}}$$

Given a torsion point P of E, define $\langle\langle P\rangle\rangle$ to be the $\mathcal{O}_K$ submodule generated by P which is a subset of $E(\mathbb{C})$. Next let us consider the following theorem.

Theorem 3.2. *[BC16][Theorem 2.6] Let $E/\mathbb{C}$ be an $\mathcal{O}_K$-CM elliptic curve, and let $M \subset E(\mathbb{C})$ be a finite $\mathcal{O}_K$-submodule. Then $M = E[ann\ M] \cong_{\mathcal{O}} \mathcal{O}/ann\ M$, and thus $\#M = |ann\ M|$.*

By the above theorem, we can say that $\langle\langle P\rangle\rangle = E[\text{ann } \langle\langle P\rangle\rangle]$. Thus, for the Weber function field for a torsion point $K(j(E), W(\langle\langle P\rangle\rangle))$ over which all torsion is rational for maximal orders $\mathcal{O}_K$, we will get a class-field theoretic containment. Whether or not these corresponding ray class fields are abelian over $\mathbb{Q}$, will determine whether the torsion subgroup is abelian.

3.2 Initial Bounds

Let $m \in \mathbb{Z}^+$ be a conductor of an order $\mathcal{O}$ in an imaginary quadratic field K, with maximal order $\mathcal{O}_K$ and discriminant Δ. Then, $h(\Delta)$ is the class number of an order $\mathcal{O}$ with discriminant Δ. By [Cox, Cor 7.28], we know that

$$h(m^2\Delta) = \frac{h(\Delta)m}{\left[\mathcal{O}_K^* : \mathcal{O}^*\right]} \prod_{p|m} \left(1 - \left(\frac{\Delta}{p}\right)\frac{1}{p}\right).$$

It follows that

$$\begin{aligned} h(m^2\Delta) &\geq \frac{h(\Delta)m}{\left[\mathcal{O}_K^* : \mathcal{O}^*\right]} \prod_{p|m} \left(1 - \frac{1}{p}\right) \\ &= \frac{h(\Delta)}{\frac{w_K}{2}} \varphi(m), \end{aligned}$$

where w_K denotes the number of units in $\mathcal{O}_K$ and φ is the Euler-totient function.

Now, applying this as in [C15], we obtain a bound on the degree $[K^{(m)}F^{\mathrm{cyc}} : F^{\mathrm{cyc}}]$ where F is $K(j(\mathcal{O}_K))$. Recall that we are considering only abelian number fields, and so $F^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{cyc}}$.

$$\begin{aligned}[K^{(m)}\mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q}^{\mathrm{cyc}}] &\geq [K(m)\mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q}^{\mathrm{cyc}}] \\ &= \frac{[K(m) : \mathbb{Q}]}{[K(m) \cap \mathbb{Q}^{\mathrm{cyc}} : \mathbb{Q}]}\end{aligned}$$

To bound the numerator we have that

$$\begin{aligned}[K(m) : \mathbb{Q}] &\geq 2h(m^2\Delta) \\ &\geq 4\frac{h(\Delta)}{w_K}\varphi(m).\end{aligned}$$

We define the Picard group of the order $\mathcal{O}$ as $\mathrm{Pic} \cong \mathrm{Aut}(K(j(\mathbb{C}/\mathcal{O})/K)$. To bound the denominator, we recall that the maximal abelian subextension of $K(m)/\mathbb{Q}$ has degree equal to the order of the abelianization of $\mathrm{Pic}\,\mathcal{O}_m \rtimes \mathbb{Z}/2\mathbb{Z}$, i.e., to $2\#(\mathrm{Pic}\,\mathcal{O}_m)[2]$ [C15]. Now, we have various lower bounds on $\#(\mathrm{Pic}\,\mathcal{O}_m[2])$ depending on congruence conditions on $D = m^2\Delta$ from [Cox, Prop 3.11].

Let r denote the number of odd primes dividing D. If $D \equiv 1 \bmod 4$, then $\#(\mathrm{Pic}\,\mathcal{O}_m[2]) = 2^{r-1}$. If $D \equiv 0 \bmod 4$, we have that $D = -4n$ for some $n > 0$, and we obtain the following table of values of $\#(\mathrm{Pic}\,\mathcal{O}_m[2])$:

n	$\#(\operatorname{Pic} \mathcal{O}_m[2])$
$n \equiv 3 \bmod 4$	2^{r-1}
$n \equiv 1, 2 \bmod 4$	2^r
$n \equiv 4 \bmod 8$	2^r
$n \equiv 0 \bmod 8$	2^{r+1}

Therefore,

$$[K(m) \cap \mathbb{Q}^{\text{cyc}} : \mathbb{Q}] = 2\#(\operatorname{Pic} \mathcal{O}_m[2]) \leq \begin{cases} 2(2^{r-1}) = 2^r & \text{if } m^2\Delta \equiv 1 \bmod 4 \\ 2(2^{r+1}) = 2^{r+2} & \text{if } m^2\Delta \equiv 0 \bmod 4. \end{cases}$$

Putting these estimates together, we get

$$[K^{(m)}\mathbb{Q}^{\text{cyc}} : \mathbb{Q}^{\text{cyc}}] \geq [K(m)\mathbb{Q}^{\text{cyc}} : \mathbb{Q}^{\text{cyc}}] = \frac{[K(m) : \mathbb{Q}]}{[K(m) \cap \mathbb{Q}^{\text{cyc}} : \mathbb{Q}]} \geq \begin{cases} \frac{h(\Delta)\varphi(m)}{2^{r-2}w_K} & \text{if } m^2\Delta \equiv 1 \bmod 4 \\ \frac{h(\Delta)\varphi(m)}{2^r w_K} & \text{if } m^2\Delta \equiv 0 \bmod 4. \end{cases}$$

3.3 Specialized Bounds

We now consider the above inequality for the case of composite m divisible only by ramified or inert primes in K. As we will see later in Section 3.4, for split primes $p \neq 2$, the fields $K^{(p)}$ are never abelian over $\mathbb{Q}$, and so we can ignore split primes in our considerations. This allows us to obtain finer bounds on m so that $K^{(m)}$ is abelian, in particular, it allows us to remove the dependence on $\varphi(m)$ in our inequalities.

Suppose $2 \nmid m$. Then

$$\begin{aligned}
[K(m):\mathbb{Q}] \geq 2h(m^2\Delta) &\geq 2\frac{h(\Delta)m}{\left[\mathcal{O}_K^* : \mathcal{O}^*\right]} \prod_{p|m}\left(1-\left(\frac{\Delta}{p}\right)\frac{1}{p}\right) \\
&= 4\frac{h(\Delta)m}{w_K} \prod_{p|m}\left(1-\left(\frac{\Delta}{p}\right)\frac{1}{p}\right) \\
&= 4\frac{h(\Delta)m}{w_K} \prod_{\substack{p|m \\ p \text{ inert}}}\left(1-\left(\frac{\Delta}{p}\right)\frac{1}{p}\right) \prod_{\substack{p|m \\ p \text{ ramifies}}}\left(1-\left(\frac{\Delta}{p}\right)\frac{1}{p}\right) \\
&\geq 4\frac{h(\Delta)m}{w_K}.
\end{aligned}$$

Suppose $2|m$. Then

$$\begin{aligned}
[K(m):\mathbb{Q}] \geq 2h(m^2\Delta) &\geq 2\frac{h(\Delta)m}{\left[\mathcal{O}_K^* : \mathcal{O}^*\right]} \prod_{p|m}\left(1-\left(\frac{\Delta}{p}\right)\frac{1}{p}\right) \\
&= 4\frac{h(\Delta)m}{w_K}\left(1-\left(\frac{\Delta}{2}\right)\frac{1}{2}\right)\prod_{\substack{p|m \\ p\neq 2}}\left(1-\left(\frac{\Delta}{p}\right)\frac{1}{p}\right) \\
&= 4\frac{h(\Delta)m}{w_K}\left(1-\left(\frac{\Delta}{2}\right)\frac{1}{2}\right) \prod_{\substack{p|m \\ p \text{ inert} \\ p\neq 2}}\left(1-\left(\frac{\Delta}{p}\right)\frac{1}{p}\right) \prod_{\substack{p|m \\ p \text{ ramifies} \\ p\neq 2}}\left(1-\left(\frac{\Delta}{p}\right)\frac{1}{p}\right) \\
&\geq 4\frac{h(\Delta)m}{w_K}\left(1-\left(\frac{\Delta}{2}\right)\frac{1}{2}\right).
\end{aligned}$$

Altogether we have

$$[K(m):\mathbb{Q}] \geq \begin{cases} \frac{2h(\Delta)m}{w_K} & \text{if 2 splits in } K \\ \frac{4h(\Delta)m}{w_K} & \text{if 2 ramifies in } K \text{ or } 2 \nmid m \\ \frac{6h(\Delta)m}{w_K} & \text{if 2 is inert in } K. \end{cases}$$

The lower bounds on the denominator do not change. If we put these estimates together, we get

the bounds below. Recall that r is the number of odd primes dividing the discriminant $m^2\Delta$ in this case.

$$[K(m) : K(m) \cap \mathbb{Q}^{\text{cyc}}] = \frac{[K(m) : \mathbb{Q}]}{[K(m) \cap \mathbb{Q}^{\text{cyc}} : \mathbb{Q}]} \geq \begin{cases} \frac{4h(\Delta)m/w_K}{2^r} = \frac{4h(\Delta)m}{2^{r-2}w_K} & 2 \nmid m, d \not\equiv 0 \bmod(4) \\ \frac{4h(\Delta)m/w_K}{2^{r+2}} = \frac{h(\Delta)m}{2^r w_K} & 2 \nmid m, d \equiv 0 \bmod(4) \\ \frac{4h(\Delta)m/w_K}{2^{r+2}} = \frac{h(\Delta)m}{2^r w_K} & 2|m, \left(\frac{\Delta}{2}\right) = 0 \\ \frac{6h(\Delta)m/w_K}{2^{r+2}} = \frac{3h(\Delta)m}{2^{r+1}w_K} & 2|m, \left(\frac{\Delta}{2}\right) = -1 \\ \frac{2h(\Delta)m/w_K}{2^{r+2}} = \frac{h(\Delta)m}{2^{r+1}w_K} & 2|m, \left(\frac{\Delta}{2}\right) = 1 \end{cases}$$

3.4 Inert and Split Cases

Suppose p is inert in O_K, i.e. $\left(\frac{\Delta_K}{p}\right) = -1$, and let $a \in \mathbb{Z}^+$. Then there is a prime ideal $(p) = pO_K$ of O_K. Then, $E[p^a] \cong O_K/(p)^a$. The O_K-submodules of $E[p^a]$ are thus all of the form $(p)^b$ for $b \in \mathbb{Z}$ such that $0 \leq b \leq a$, where

$$(p)^b/(p)^a \cong_{O_K} O_K/(p)^{a-b} \cong_{\mathbb{Z}} \mathbb{Z}/p^{a-b}\mathbb{Z} \oplus Z/p^{a-b}\mathbb{Z}$$

Then if a torsion point P of E has order p^a, then $\langle\langle P\rangle\rangle = E[p^a]$ and thus

$$K(j(E), W(\langle\langle P\rangle\rangle)) = K^{(p)^a}.$$

Now suppose $K^{(p)^a}$ is abelian over $\mathbb{Q}$. Then we have that

$$K(p^a) \subset K^{(p)^a} \subset \mathbb{Q}^{ab}.$$

Therefore, $K(p^a) = K(j(\mathbb{C}/\mathcal{O}))$, where $\mathcal{O}$ is the ring class field of conductor p^a. Voight provides all possible imaginary quadratic orders with Picard group whose exponent divides two. Since $\mathrm{Aut}(K(m)/\mathbb{Q}) \cong \mathrm{Pic}\,\mathcal{O} \rtimes \mathbb{Z}/2\mathbb{Z}$, then ring class field is abelian if and only if $\mathrm{Pic}\,\mathcal{O}_m$ has an exponent dividing two. Therefore, using Voight's tables (see Appendix Tables), we get that $p^a \leq 8$, and so $a \leq 3$ and $p \leq 7$. For even torsion, see the section below on even torsion.

Suppose p is a prime which splits in $\mathcal{O}_K$, i.e. $\left(\frac{\Delta_K}{p}\right) = 1$. Then there is a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that

$$p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}} \text{ where } \mathfrak{p} \neq \overline{\mathfrak{p}}.$$

Then, for prime powers

$$p^a\mathcal{O}_K = \mathfrak{p}^a\overline{\mathfrak{p}}^a.$$

Thus,

$$E[p^a] \cong_{\mathcal{O}_K} \mathcal{O}_K/\mathfrak{p}^a\overline{\mathfrak{p}}^a \cong \mathcal{O}_K/\mathfrak{p}^a \oplus \mathcal{O}_K/\overline{\mathfrak{p}}^a.$$

Therefore, the $\mathcal{O}_K$-submodules of $\mathcal{O}_K/\mathfrak{p}^a\overline{\mathfrak{p}}^a$ are of the form $\mathfrak{p}^c\overline{\mathfrak{p}}^d/\mathfrak{p}^a\overline{\mathfrak{p}}^a$ where $c, d \in \mathbb{Z}$ and $0 \leq c, d \leq a$. Then, we have that

$$\mathfrak{p}^c\overline{\mathfrak{p}}^d/(p)^a \cong_{\mathcal{O}_K} \mathcal{O}_K/\mathfrak{p}^{a-c} \oplus \mathcal{O}_K/\mathfrak{p}^{a-d} \cong_{\mathbb{Z}} Z/p^{a-c}\mathbb{Z} \oplus Z/p^{a-d}\mathbb{Z}.$$

We have either $E[p] \supset E[\mathfrak{p}^a]$ or $E[p] \supset E[\overline{\mathfrak{p}}^a]$. Then, by the fundamental theorem of complex multiplication, we get that either

$$K(j(E), W(\langle\langle P\rangle\rangle)) \supset K^{\mathfrak{p}} \text{ or } K^{\overline{\mathfrak{p}}}$$

However, if complex conjugation does not fix $K^{\mathfrak{p}}$ or $K^{\overline{\mathfrak{p}}}$, it is not a Galois extension of $\mathbb{Q}$ and so it is certainly not abelian. If the two fields are equal, i.e. $K^{\mathfrak{p}} = K^{\overline{\mathfrak{p}}}$, then $K^{\mathfrak{p}}$ is an abelian extension of

K containing the Hilbert class field K^1. By definition, $K^{\mathfrak{p}} = K^{\overline{\mathfrak{p}}}$ has no primes that simultaneously ramify outside of $\mathfrak{p}$ and $\overline{\mathfrak{p}}$; however, $\mathfrak{p} \neq \overline{\mathfrak{p}}$, therefore $K^{\mathfrak{p}} = K^1$. Thus, since $[K^{\mathfrak{p}} : K^1] = \frac{p-1}{2} = 1$, there is no odd prime torsion in the split case except for possibly when the j-invariant is 0 or 1728. For the case of even torsion, see the section below on even torsion.

3.5 Ramified Case

Suppose p is ramified in $\mathcal{O}_K$, i.e. $\left(\frac{\Delta_K}{p}\right) = 0$, and let $a \in \mathbb{Z}^+$. Then there exists a unique prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ with $|\mathfrak{p}| = p$ and $(p) = \mathfrak{p}^2$. Then, for the p^a torsion, we have that

$$E[p^a] \cong \mathcal{O}_K/(p)^a \cong \mathcal{O}_K/\mathfrak{p}^{2a}.$$

The $\mathcal{O}_K$ submodules of $E[p^a]$ are of the form $\mathfrak{p}^b$ for $b \in \mathbb{Z}$ such that $0 \leq b \leq 2a$. The exponent of $\mathcal{O}_K/\mathfrak{p}^b$ is the largest power of $\mathfrak{p}^c \subset \mathfrak{p}^b$. Since $(p)^d = \mathfrak{p}^{2d}$, the exponent is $\mathfrak{p}^{\lceil \frac{b}{2} \rceil}$, and $\#\mathcal{O}_K/\mathfrak{p}^b = p^b$, we see that

$$\mathcal{O}_K/\mathfrak{p}^b \cong_{\mathbb{Z}} \mathbb{Z}/p^{\lceil \frac{b}{2} \rceil}\mathbb{Z} \oplus \mathbb{Z}/p^{\lfloor \frac{b}{2} \rfloor}\mathbb{Z}$$

Thus, we get that if a torsion point P of E has order p^a, then $\langle\langle P \rangle\rangle \supset E[\mathfrak{p}^{2a-1}]$, and

$$K(j(E), h(\langle\langle P \rangle\rangle)) = K^{\mathfrak{p}^{2a-1}} \supset K^{(p)^{a-1}}.$$

Again by [C15], in order for $K(p^{a-1})$ to be abelian over $\mathbb{Q}$, we must have that Pic $p^{a-1}\mathcal{O}$ has exponent dividing 2. In particular, $p^{2(a-1)}\Delta_K$ must appear on Voight's tables. Under the condition that $a > 1$, we can get the bound that $p^{a-1} \leq 8$, and so $a \leq 4$ and $p \leq 8$. In particular, if $a = 3, 4$ then $p = 2$. If $a = 2$ then $p = 3$ or 5. If $a = 4$, then $K(\mathfrak{p}^4) = K(p^2) \subset \mathbb{Q}^{ab}$ and so $p = 2$ and

$$\mathcal{O}_K/\mathfrak{p}^4 \cong \mathbb{Z}/2^2\mathbb{Z} \oplus \mathbb{Z}/2^2\mathbb{Z}.$$

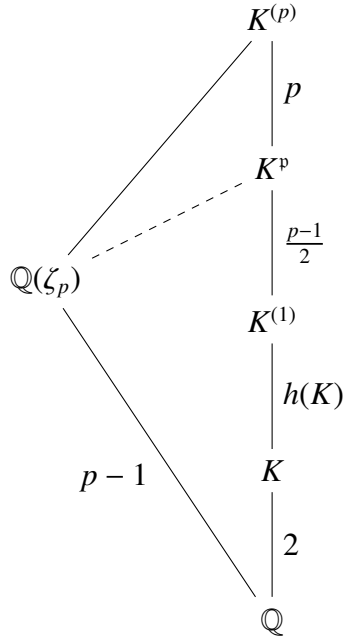
If $a = 3$, then $K(p) \subset K(\mathfrak{p}^3) \subset \mathbb{Q}^{ab}$ and so $p = 2, 3, 5, 7$ and

$$O_K/\mathfrak{p}^3 \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z}.$$

Hence, what is left is to check when $K^{\mathfrak{p}}$ is abelian over $\mathbb{Q}$.

Theorem 3.3. *Let $p > 2$ be an odd prime in $\mathbb{Z}$ and K be an imaginary quadratic field with $\Delta_K \neq -3, -4$ with its Hilbert class field K^1 abelian over $\mathbb{Q}$. If p is ramified in K, so that $(p) = \mathfrak{p}^2$, then $K^{\mathfrak{p}} = K^{(1)}(\zeta_p)$, the compositum of the Hilbert class field with the p-cyclotomic field, which is itself abelian over $\mathbb{Q}$.*

Proof. If $p \neq 2 \in \mathbb{Z}$ ramifies in K, then $(p) = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ of O_K of norm p. We wish to consider when the ray class field $K^{\mathfrak{p}}$ is contained in $\mathbb{Q}^{\text{cyc}}$. Consider the following diagram:



First we prove the dashed inclusion above: $\mathbb{Q}(\zeta_p) \subseteq K^{\mathfrak{p}}$. Indeed, suppose that $\zeta_p \notin K^{\mathfrak{p}}$. Then $K^{\mathfrak{p}} \subsetneq K^{\mathfrak{p}}(\zeta_p) \subseteq K^{(p)}$. However, this would imply that

$$[K^{\mathfrak{p}}(\zeta_p) : K^{\mathfrak{p}}] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p) \cap K^{\mathfrak{p}}]$$

with the left hand side dividing p and the right hand side dividing $p-1$. Thus, $\zeta_p \in K^{\mathfrak{p}}$.

In fact, $K^{\mathfrak{p}} = K^{(1)}(\zeta_p)$. We count the degree of each extension.

$$[K^{\mathfrak{p}} : \mathbb{Q}] = (p-1)h(K),$$

while

$$[K^{(1)}(\zeta_p) : \mathbb{Q}] = \frac{[K^{(1)} : \mathbb{Q}][\mathbb{Q}(\zeta_p) : \mathbb{Q}]}{[K^{(1)} \cap \mathbb{Q}(\zeta_p)]} = \frac{2h(K)(p-1)}{2},$$

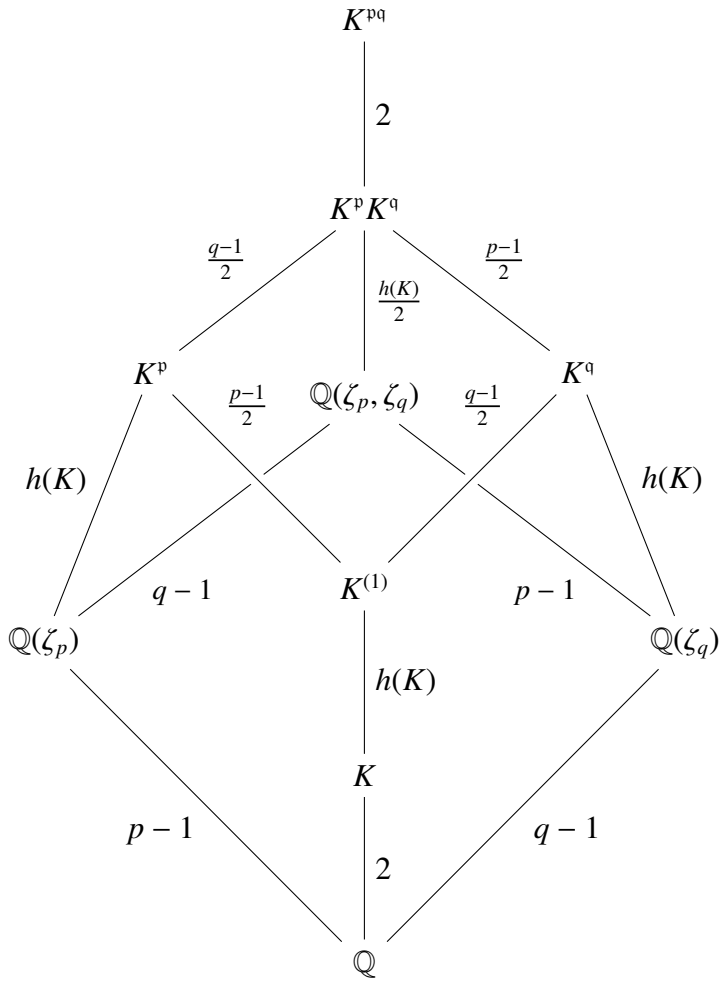
since $K^{(1)} \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$. Therefore, we can conclude that $K^{\mathfrak{p}} = K^{(1)}(\zeta_p)$. □

Hence, we have that $K(j(E), h(\langle\langle P\rangle\rangle)) = K^{(1)}(\zeta_p)$. Therefore, this result implies that for an elliptic curve E with complex multiplication by a maximal order $\mathcal{O}_K$, we have p-torsion in the ramified case.

3.6 Odd Ramified Composites

Theorem 3.4. *Let K be a quadratic field with discriminant $\Delta = -pq$ for odd primes $p, q \in \mathbb{Z}$. Then K ramifies precisely at the odd primes p, q, but not at 2. Let $\mathfrak{p}, \mathfrak{q}$ be prime ideals of K such that $\mathfrak{p}^2 = (p)$ and $\mathfrak{q}^2 = (q)$. Then, $K^{\mathfrak{pq}}/\mathbb{Q}$ is not abelian over $\mathbb{Q}$.*

Proof. Suppose that $K^{\mathfrak{pq}}/\mathbb{Q}$ is abelian over $\mathbb{Q}$. Now, consider the following field diagram.



By the conductor theorem [J73, Theorem 12.7 and Chapter V, §6] we know that a prime ramifies if and only if it divides the conductor $f = f(K^{\mathfrak{pq}}/\mathbb{Q})$. The only primes of $\mathbb{Q}$ that ramify in $K^{\mathfrak{pq}}$ are the ramified primes p, q. Therefore, by the Kronecker-Weber Theorem, we know that $K^{\mathfrak{pq}} \subset \mathbb{Q}(\zeta_N)$ the only primes that divide N are p, q since $N = f(K^{\mathfrak{pq}}/\mathbb{Q})$. Therefore $N = p^{e_p}q^{e_q}$. Thus we know that $\left[\mathbb{Q}(\zeta_N) : \mathbb{Q}(\zeta_p, \zeta_q)\right] = p^{e_p-1}q^{e_q-1}$ and $[K^{\mathfrak{pq}} : K^{\mathfrak{p}}K^{\mathfrak{q}}] = 2$ but $2 \nmid p^{e_p-1}q^{e_q-1}$. Thus, no such composite ray class field $K^{\mathfrak{pq}}$ that is abelian over $\mathbb{Q}$. □

Note that this does not rule out the case of when the quadratic field K has a discriminant of three primes, $\Delta_K = pqr$. However, we have strong computational evidence that there is no composite prime ramified torsion over abelian numberfields.

$K^{(2)}$ abelian	$K^{\mathfrak{p}_2^3}$ abelian	$K^{(4)}$ abelian
3		3
4	4	4
7		7
8	8	
15		15
24	24	
40	40	
88	88	
120	120	
168	168	
232	232	
280	280	
312	312	
408	408	
520	520	
760	760	
840	840	
1320	1320	
1848	1848	

Table 3.1: Fundamental discriminants Δ_K that have two-powered ray-class fields abelian over $\mathbb{Q}$

3.7 Even Case

If 2 ramifies in K, there exists a unique prime $\mathfrak{p}_2$ such that $\mathfrak{p}^2 = (2)$. Given that the Hilbert class field K^1 is abelian over $\mathbb{Q}$, we have computed that the K^2 Hilbert class field must also be abelian; therefore, all elliptic curves have 2-torsion. We also compute when the two powered ray class fields $K^{\mathfrak{p}_2^n}$ are abelian over the rationals. The following table shows which fundamental discriminant Δ_K have $K^{\mathfrak{p}_2^n}/\mathbb{Q}$ abelian for $n \geq 3$. We computed that $K^{\mathfrak{p}_2^5}$ and $K^{(8)}$ are never abelian. This table shows us precisely what $E(\mathbb{Q}^{\text{ab}})[2^\infty]$ is, according to the work in Clark's initial paper [C15]:

$$K^{(2)}/\mathbb{Q} \text{ abelian} \Rightarrow \text{ 2 powered torsion is of the form } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \tag{3.1}$$

$$K^{\mathfrak{p}_2^3}/\mathbb{Q} \text{ abelian} \Rightarrow \text{ 2 powered torsion is of the form } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \tag{3.2}$$

$$K^{(4)}/\mathbb{Q} \text{ abelian} \Rightarrow \text{ 2 powered torsion is of the form } \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \tag{3.3}$$

3.8 Conclusions and Future Work

Given an imaginary quadratic field K with discriminant Δ_K we have shown that, conditional under GRH, for ramified primes p such that $\mathfrak{p}^2 = (p)$, the ray class fields $K^{\mathfrak{p}}$ are abelian over $\mathbb{Q}$. We have shown that K^p is never abelian over $\mathbb{Q}$ for odd split primes, and that the composite ray class field $K^{\mathfrak{pq}}$ for odd ramified primes p, q is also never abelian over $\mathbb{Q}$ for quadratic fields K with discriminants of the form $\Delta_K = -pq$ where p, q are both primes in $\mathbb{Z}$. For two-powered ray class fields, we have computed the cases where $K^{\mathfrak{p}_2^n}$ is abelian over $\mathbb{Q}$, where $\mathfrak{p}_2$ is the prime ideal of K such that $\mathfrak{p}_2^2 = (2)$. We still need to show that the ray-class fields corresponding to composite even ideals $K^{\mathfrak{p}_2^n\mathfrak{p}}$ are abelian over $\mathbb{Q}$, and we need to finish the proof for odd composite ramified torsion. Our current computational approaches fail for ray-class fields of large degree. We have also only considered elliptic curves with complex multiplication by maximal orders $\mathcal{O}_K$, and have not yet addressed the case of non-maximal orders $\mathcal{O}$. The following recent result from Bourdon and Clark relates the torsion fields of elliptic curves with complex multiplication by a non-maximal order to an elliptic curve with complex multiplication by the corresponding maximal order.

Theorem 3.5. *(Isogeny Torsion Theorem)[BC16, Theorem 1.7] Let $\mathcal{O}$ be an order in an imaginary quadratic field K, of conductor $\mathfrak{f}$, and let $\mathfrak{f}'$ be a positive integer dividing $\mathfrak{f}$. Let $F \supset K$ be a number field, and let $E_{/F}$ be an $\mathcal{O}$-CM elliptic curve. Let $\iota_{\mathfrak{f}'} : E \to E_{\mathfrak{f}'}$ be the F-rational isogeny to an*

elliptic curve $E_{\mathfrak{f}'}$ with CM by the order in K of conductor $\mathfrak{f}'$, then we have

$$\#E(F)[\text{tors}] \mid \#E_{\mathfrak{f}'}(F)[\text{tors}].$$

If we take $\mathfrak{f}' = 1$, we see that $\#E(F)[\text{tors}]$ is bounded by $\#E_1(F)[\text{tors}]$, where $(E_1)_{/F}$ is an elliptic curve with CM by the maximal order in K. Therefore, with a classification in the case of maximal orders complete, we should be able to compute the case of non-maximal orders.

3.9 Appendix

3.9.1 Tables

The following tables come from Voight's appendix [Vo07]. The tables are captioned by the type of the class groups, e.g. if the class group is of type (2,2,2) then there must be an embedding of the class group into $(\mathbb{Z}/2\mathbb{Z})^3$.

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$
3	1	3	8	1	8
3	2	12	11	1	11
3	3	27	19	1	19
4	1	4	43	1	43
4	2	16	67	1	67
7	1	7	163	1	163
7	2	28			

Table 3.2: Orders of Quadratic Fields with Class Groups of Type (1) [Vo07][Table 7, p. 27]

$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$	$\lvert d\rvert$	f	$\lvert D\rvert$
3	4	48	15	1	15	115	1	115
3	5	75	15	2	60	123	1	123
3	7	147	20	1	20	148	1	148
4	3	36	24	1	24	187	1	187
4	4	64	35	1	35	232	1	232
4	5	100	40	1	40	235	1	235
7	4	112	51	1	51	267	1	267
8	2	32	52	1	52	403	1	403
8	3	72	88	1	88	427	1	427
11	3	99	91	1	91			

Table 3.3: Orders of Quadratic Fields with Class Groups of Type (2) [Vo07][Table 8, p. 27]

$\|d\|$	f	$\|D\|$	$\|d\|$	f	$\|D\|$	$\|d\|$	f	$\|D\|$
3	8	192	168	1	168	520	1	520
7	8	448	195	1	195	532	1	532
8	6	288	228	1	228	555	1	555
15	4	240	232	2	928	595	1	595
20	3	180	280	1	280	627	1	627
24	2	96	312	1	312	708	1	708
35	3	315	340	1	340	715	1	715
40	2	160	372	1	372	760	1	760
84	1	84	408	1	408	795	1	795
88	2	352	435	1	435	1012	1	1012
120	1	120	483	1	483	1435	1	1435
132	1	132						

Table 3.4: Orders of Quadratic Fields with Class Groups of Type $(2,2)$ [Vo07][Table 10, p. 28]

$\|d\|$	f	$\|D\|$	$\|d\|$	f	$\|D\|$
15	8	960	1092	1	1092
120	2	480	1155	1	1155
168	2	672	1320	1	1320
280	2	1120	1380	1	1380
312	2	1248	1428	1	1428
408	2	1632	1540	1	1540
420	1	420	1848	1	1848
520	2	2080	1995	1	1995
660	1	660	3003	1	3003
760	2	3040	3315	1	3315
840	1	840			

Table 3.5: Orders of Quadratic Fields with Class Groups of Type $(2,2,2)$ [Vo07][Table 12, p. 29]

$\|d\|$	f	$\|D\|$
840	2	3360
1320	2	5280
1848	2	7392
5460	1	5460

Table 3.6: Orders of Quadratic Fields with Class Groups of Type $(2,2,2,2)$ [Vo07][Table 14, p. 30]

3.9.2 Code

The following Magma code checks if the class field is abelian for inert primes.

```
P<x>:=PolynomialRing(Rationals());
load "~/cm/vlists";
AbInerts:=[* *];
for i:=1 to #InertPrimes do
d:=InertPrimes[i][1];
d;
K:=NumberField(x^2+d);
O:=Integers(K);
Inerts:=[];
for p in InertPrimes[i][2] do
G,m:=RayClassGroup(p*O);
A:=AbelianExtension(m);
AA:=NumberField(A);
Kp:=AbsoluteField(AA);
if IsAbelian(Kp) then
Append(~Inerts,p);
end if;
end for;
if #Inerts gt 0 then
Append(~AbInerts, [*d,Inerts*]);
end if;
end for;
print AbInerts;
```

The following code checks if K^n is abelian for composite n of p,q.

```
function CheckComp(p,q,d)
    P<x>:=PolynomialRing(Rationals());

    K<a>:=NumberField(x^2+d);
    O:=Integers(K);
    H<b>:=HilbertClassField(K);
    H:=AbsoluteField(H);

    fp:=x^2-p*pm(p);
    fq:=x^2-q*pm(q);
    K2:=NumberField([fp, fq]);

    frakp:=Factorization(p*O)[1][1];
    frakq:=Factorization(q*O)[1][1];

    Gpq, mpq := RayClassGroup(frakp*frakq);
    Apq := AbelianExtension(mpq);
    AApq:=NumberField(Apq);
    Kpq:=AbsoluteField(AApq);

    return Kpq;
end function;

//meant for input of list "PossiblePrimePowers"
```

```
function SmallRamifiedPrimesCheck(list)
    discriminants:=[* *];
    for i:=1 to #list do
        divs:=PrimeDivisors(list[i][1]);
        Append(~discriminants, [*list[i][1], divs*]);
    end for;
    for i:=1 to #discriminants do
        print discriminants[i];
        pairlist:=[];
//make all pairs of small primes
        if #discriminants[i][2] gt 1 then
            for j:=1 to #discriminants[i][2] do
            for k:=1 to #discriminants[i][2] do
                if j lt k then
                    pair:=[discriminants[i][2][j],discriminants[i][2][k]];
                    Append(~pairlist,pair);
                end if;
            end for;
            end for;
        end if;
        validcomposites:=[* *];
        print pairlist;
        for j:=1 to #pairlist do
//remove pairs with primes too large
            if Maximum(pairlist[j]) lt 10 then
//check if Kpq is abelian, if it is, add it to the list of possible composites
```

```
//if the degree is too large to check, then just give it the tag "999"
                C:=CheckComp(pairlist[j][1],pairlist[j][2],-discriminants[i][1]);
                if Degree(C) lt 80 then
                    if IsAbelian(C) then
                        Append(~validcomposites, [*pairlist[j], 1*]);
                    end if;
                else
                    Append(~validcomposites, [*pairlist[j], 999*]);
                end if;
            end if;
        end for;
        Append(~discriminants[i], validcomposites);
    end for;
    return discriminants;
end function;
```

The following code checks if there is $K^{p_2^n}$ is abelian.

```
load "~/cm/checkklabelian";
load "~/cm/vlists";

P<x>:=PolynomialRing(Rationals());

function pm(p)
    if (p mod 4) eq 1 then
        return 1;
```

```
    else
        return -1;
    end if;
end function;



Kfrak22ab:=[];
Kfrak23ab:=[];
Kfrak24ab:=[];

Possible2:=[];
Possible4:=[];

for entry in MaximalDs do
    if 2^2*entry in DTMaster then
        Append(~Possible2,entry);
    end if;
    if 4^2*entry in DTMaster then
        Append(~Possible4,entry);
    end if;
end for;

//check if K^(2) is abelian
for d in Possible2 do
    if IsAbelian(RayClassField(-d,2)) then
        Append(~Kfrak22ab, d);
```

```
    end if;
end for;
//check if K^(frak2^3) is abelian
for d in Possible2 do
    if d mod 2 eq 0 then
        K<a>:=NumberField(x^2+d);
        O:=Integers(K);
        frak2:=Factorization(2*O)[1][1];
        G2, m2:=RayClassGroup(frak2^3);
        A2 := AbelianExtension(m2);
        AA2:= NumberField(A2);
        K2:=AbsoluteField(AA2);
        if IsAbelian(K2) then
            Append(~Kfrak23ab, d);
        end if;
    end if;
end for;
//check if K^(4) is abelian
for d in Possible4 do
    if IsAbelian(RayClassField(-d,4)) then
        Append(~Kfrak24ab, d);
    end if;
end for;
```

The following code checks if $K^{p_2^n q}$ is abelian.

```
print "loaded function: pe(2composite(d, largestpower, ramifiedprime)";
print "Note: d should be negative, largest prime is the highest power of frak2";
print "loaded function: all2composites(MaximalD_facts_frak2bound)";
load "~/cm/vlists";

function p2composite(d, largestpower, ramifiedprime)
P<x>:=PolynomialRing(Rationals());
K:=NumberField(x^2-d);
O:=Integers(K);
p:=ramifiedprime;
if d mod 2 eq 0 then
    frak2:=Factorization(2*O)[1][1];
    a:=largestpower;
else
    frak2:=2*O;
    a:= largestpower div 2;
end if;
if d mod p eq 0 then
    frakp:=Factorization(p*O)[1][1];
    G, map:=RayClassGroup(frakp*frak2^a);
    A:=AbelianExtension(map);
    Kl:=AbsoluteField(NumberField(A));
    Degree(Kl);
    return IsAbelian(Kl);
```

```
else
    print "prime is not ramified";
    return "prime is not ramified";
end if;
end function;

function all2composites(list);
    newlist:=[* *];
    for i:=1 to #list do
        d:= list[i][1];
        print "Discriminant: ", -d;
        dplist:=[ ];
        for j:=1 to #list[i][2] do
            if list[i][2][j][1] ne 2 then
                p:=list[i][2][j][1];
                print "prime: ", p;
                if p lt 80 then
                    notyet:=true;
                    N:=list[i][3];
                    a:=0;
                    while notyet do
                        a:=a+1;
                        if a lt N+1 then
                            notyet:=p2composite(-d,a,p);
                        else
                            notyet:=false;
```

```
                        end if;
                    end while;
                    Append(~dplist, [p, a-1]);
                else
                    print "prime too large";
                end if;
            end if;
        end for;
        print dplist;
        Append(~newlist, [*-d, dplist*]);
    end for;
    return newlist;
end function;
all2composites(MaximalD_facts_frak2bound);
```

Bibliography

[BC16] A. Bourdon and P. Clark. *Torsion Points and Galois Representation on CM Elliptic Curves.* Pre-print (2018). http://alpha.math.uga.edu/~abourdon/Bourdon_Clark_8_17.pdf

[BCP17] A. Bourdon, P.L. Clark and P. Pollack, *Anatomy of torsion in the CM case*. Math. Z. 285 (2017), no. 3-4, 795-820.

[CCRS2014] P. Clark, P. Corn, A. Rice and J. Stankewicz, *Computation on elliptic curves with complex multiplication*, LMS Journal of Computation and Mathematics 17 (2014), 509-535.

[C15] P. Clark, *Acyclotomy of torsion in the CM case*, http://alpha.math.uga.edu/~pete/acyclotomy.pdf (2015).

[CMP2017] P. Clark, M. Milosevic, and P. Pollack, *Typically Bounding Torsion*, Journal of Number Theory, Volume 192, November (2018), Pages 150-167.

[CP2015] P. Clark and P. Pollack *The truth about torsion in the CM case* C.R. Math. Acad. Sci. Paris 353 (2015), 683-688.

[Cox] D. Cox, *Primes of the form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication*. John Wiley and Sons, New York, (1989).

[DLNS2018] H. Daniels, Á. Lozano-Robledo, F. Najman, and A. Sutherland, *Torsion subgroups of rational elliptic curves over the compositum of all cubic fields*, Math. Comp. 87 (2018), 425-458.

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

[Et16] A. Etropolski, *Local-global principles for certain images of Galois representations*. Preprint online at `http://math.rice.edu/~ae22/Papers/localglobal.pdf`.

[HS99] M. Hindry and J. Silverman, *Sur le nombre de points de torsion rationnels sur une courbe elliptique*. C. R. Acad. Sci. Paris SÂ´er. I Math. 329 (1999), no. 2, 97-100.

[J73] G. Janusz, *Algebraic Number Fields*, Academic Press, New York, (1973).

[K92] S. Kamienny *Torsion points on elliptic curves and q-coefficients of modular forms*. Invent. Math., 109 (1992), 221-229.

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

[LV14] E. Larson and D. Vaintrob, *Determinants of subquotients of Galois representations associated with abelian varieties*. Journal of the Institute of Mathematics of Jussieu, 13 (2014), 517-559.

[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.

[M77] B. Mazur, *Modular curves and the Eisenstein ideal* Publications Mathématiques de l'Institut des Hautes Études Scientifiques 47 (1977), no. 1, 33-186.

[M78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*. Invent. Math. 44 (1978), 129-162.

[Me96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math. 124 (1996), 437-449.

[Mo95] F. Momose, *Isogenies of prime degree over number fields.* Compositio Math. 97 (1995), 329-348.

[Mor1922] L.J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*. Proc Cam. Phil. Soc. 21 (1992). 179-192.

[P99] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, Journal für die Reine und Angewandte Mathematik 506 (1999), 85-116.

[HP1901] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, Journal de Mathématiques pures et appliquées 7, no. 3, (1901), 161-233.

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*. Ann. of Math. (2) 88 (1968), 492-517.

[S72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. 15 (1972), no. 4, 259-331.

[Sil86] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer Verlag, (1986).

[Sil94] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer-Verlag, (1994).

[Vo07] J. Voight, *Quadratic forms that represent almost the same primes*. Math. Comp. 76 (2007), 1589-1617.

[W1929] A. Weil, *L'arithmetique sur les courbes algebriques*. Acta Mathematica. 52 (1), (1929), 281-315.