5-5-2017

Torsion of Rational Elliptic Curves over Abelian Extensions of Q

Michael Y. Chou
University of Connecticut - Storrs, michael.chou@uconn.edu

Torsion of Rational Elliptic Curves over Abelian Extensions of $\mathbb{Q}$

Michael Chou, Ph.D.

University of Connecticut, 2017

ABSTRACT

Let E be an elliptic curve defined over $\mathbb{Q}$. We investigate $E(K)_{\text{tors}}$ for various abelian extensions K of $\mathbb{Q}$. For number fields, a theorem of Merel implies a uniform bound on the size of the torsion subgroup based on the degree of the number field. We discuss a number of results that classify torsion subgroups of elliptic curves over number fields of a fixed degree. We prove a classification of torsion subgroups for elliptic curves $E/\mathbb{Q}$ base extended to quartic Galois number fields. For infinite extensions of $\mathbb{Q}$, the Mordell-Weil theorem no longer applies, and so the torsion subgroup of $E/\mathbb{Q}$ is a priori not even finite. We prove that when base extended to $\mathbb{Q}^{ab}$, the size of the torsion subgroup of an elliptic curve $E/\mathbb{Q}$ is uniformly bounded. Moreover, we classify all groups that arise as $E(\mathbb{Q}^{ab})_{\text{tors}}$ for elliptic curve $E/\mathbb{Q}$.

Torsion of Rational Elliptic Curves over Abelian Extensions of $\mathbb{Q}$

Michael Chou

M.S. University of Connecticut

B.A. Wesleyan University

A Dissertation

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

at the

University of Connecticut

2017

APPROVAL PAGE

Doctor of Philosophy Dissertation

Torsion of Rational Elliptic Curves over Abelian Extensions of $\mathbb{Q}$

Presented by

Michael Chou, B.A. Math., M.S. Math.

Major Advisor _____
Álvaro Lozano-Robledo

Associate Advisor _____
Keith Conrad

Associate Advisor _____
Liang Xiao

University of Connecticut

2017

ACKNOWLEDGMENTS

First and foremost I would like to thank my Ph.D. advisor Dr. Álvaro Lozano-Robledo. His thoughts and ideas are littered throughout this thesis, and without his insights this project would never have been completed. His dedication to both my academic and professional development has been instrumental in my success as a graduate student. I cannot thank him enough for his patience and guidance.

I am very grateful to have had both Dr. Keith Conrad and Dr. Liang Xiao serve as my committee members. Keith's incredible collection of knowledge has guided my mathematics since before I was even a graduate student at the University of Connecticut. He has always been generous with his time and advice and no doubt is responsible for a many-fold increase in the quality of my mathematics. Many of the courses I've taken at UConn have been with Liang, who has always had a great eye for the big picture. I thank him for providing me with a good perspective on many topics. Moreover, I thank all of my committee members for their many comments and the care with which they have read through this thesis.

I would like to thank Dr. Pete Clark and Dr. Abbey Bourdon for the incredible opportunities they provided for me. In particular I'd like to thank Pete for inviting me to spend time at the University of Georgia collaborating with him and Marko Milosevic.

My time at the University of Connecticut was made all the brighter because of the wonderful graduate students I met during my time here. I would particularly

like to thank my academic older brother Dr. Harris Daniels for his care and concern throughout my years at UConn. I owe many thanks to my incoming cohort for the support to make it through tough times. Of course there are many more at UConn who have helped build a sense of community for me and I want to express my gratitude to them all. The friendly and supportive atmosphere at UConn made my time as a graduate student incredibly dear to me.

Of course, I would like to extend the greatest thanks to my family. My mother has always been such an extraordinary example for me to follow. Her passion and dedication to her own career is an inspiration for me. I am thankful to my brother for his love and support. Finally, I would like to express how grateful I am to my fiancée Leah. As a graduate school study-buddy, her orthogonal perspective helped me learn mathematics on a much richer level. As a partner, her unending love and brilliant humor always lifted my spirits throughout this thesis.

This thesis is dedicated to my father, Dr. Arthur Chou, whose love of mathematics inspired me to first begin my studies.

Contents

Chapter 1

Introduction

1.1 Rational Points on Elliptic Curves

We begin with the definition of an elliptic curve over a field.

Definition 1.1.1. *An **elliptic curve** E over a field K, denoted E/K, is a smooth, projective algebraic curve of genus one defined over K on which there is a specified point $\mathcal{O}$ with coordinates in K.*

Definition 1.1.2. *Let K be an arbitrary field. A Weierstrass equation for an elliptic curve E defined over K is an equation of the form*

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

where $a_1, a_2, a_3, a_4, a_6 \in K$.

All elliptic curves have a Weierstrass model. In fact, if the characteristic of K is

neither 2 nor 3, any elliptic curve over K can be written in short Weierstrass form:

$$y^2 = x^3 + Ax + B$$

with $A, B \in K$. For our purposes we will be considering elliptic curves over algebraic fields, i.e., fields K such that $\mathbb{Q} \subseteq K \subseteq \overline{\mathbb{Q}}$, and thus it will always be possible to find a short Weierstrass model of our curves.

A remarkable fact of elliptic curves is the existence of a group structure on the points of the elliptic curve. Addition of points is defined so that any three collinear points add up to $\mathcal{O}$. We can also describe the addition completely algebraically. For a formula to add two points on an elliptic curve (x_1, y_1) and (x_2, y_2) see [33] (III.2.3). The formula is defined over the field of definition of the elliptic curve. Thus, for an elliptic curve defined over a field K, adding two K-rational points will result in a third K-rational point. Therefore, if we denote the points of E with K-rational coordinates by $E(K)$, then $E(K)$ is closed under the group law and thus is a group itself. In fact, if K is a number field we have the following theorem describing the structure of the group $E(K)$:

Theorem 1.1.3 (Mordell-Weil)**.** *Let E be an elliptic curve over a number field K. The group of K-rational points, $E(K)$, is a finitely generated abelian group.*

By the fundamental theorem of finitely generated abelian groups it follows that, for any elliptic curve E over K, there exists an integer $r > 0$ such that

$$E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^r,$$

where $E(K)_{\text{tors}}$ is a finite group. We call $r = r(E, K)$ the rank of E over K, and we

call $E(K)_{\text{tors}}$ the torsion subgroup of the E over K. Note that the rank and torsion of an elliptic curve can change as we consider the curve over different number fields.

Example 1.1.4. The elliptic curve $E : y^2 = x^3 - x$ has rank 0 over $\mathbb{Q}$, but over the field $K = \mathbb{Q}(\alpha)$, where α is a root of $x^3 - x - 1$, the curve has rank 1. The point $(\alpha, 1)$ is a point of infinite order. (By a later theorem, it has order at most 16, so we can test to see if any multiple of it up to 16 is $\mathcal{O}$ or not).

Example 1.1.5. The curve $E : y^2 = x^3 - 2$ has no torsion points over $\mathbb{Q}$, but if we look over the field $K = \mathbb{Q}(\sqrt[3]{2})$ we see that

$$E(K)_{\text{tors}} = \langle(\sqrt[3]{2}, 0)\rangle \cong \mathbb{Z}/2\mathbb{Z}.$$

The study of ranks of elliptic curves is a rich field with many interesting open questions. For instance, it is still an open conjecture on whether ranks of elliptic curves are bounded over $\mathbb{Q}$. See [29] for an interesting discussion on this topic. We will, however, restrict our attention to studying the torsion subgroups that arise over various algebraic fields.

1.2 Torsion of Elliptic Curves Over Number Fields

1.2.1 Background

The classification of torsion structures of elliptic curves over $\mathbb{Q}$ was done by Mazur [26] who proved the following theorem on the torsion of an elliptic curve over $\mathbb{Q}$.

Theorem 1.2.1 (Mazur [26]). *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following 15 groups:*

$$\begin{aligned} &\mathbb{Z}/N_1\mathbb{Z}, && 1 \leq N_1 \leq 12, N_1 \neq 11, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, && 1 \leq N_2 \leq 4. \end{aligned}$$

Each of these groups actually appears infinitely often as the torsion subgroup of elliptic curves over the rationals. Here, and throughout the rest of the thesis, the phrase "appears infinitely often" means "appears for infinitely many non-isomorphic elliptic curves over $\overline{K}$".

In fact, Merel proved that there is a bound for the size of the torsion subgroup of an elliptic curve defined over any number field depending only on the degree of the number field.

Theorem 1.2.2 (Merel [27]). *For all $d \in \mathbb{Z}$, $d \geq 1$, there exists a constant $B(d) \geq 0$ such that for all elliptic curves E over a number field K with $[K : \mathbb{Q}] = d$,*

$$\#E(K)_{\text{tors}} \leq B(d).$$

Given that the size of the torsion subgroup of an elliptic curve over a number field is bounded strictly by a function of the degree of the number field, there are only a finite number of possible torsion subgroups that can appear over any number field K of a fixed degree and any elliptic curve E defined over K. A natural question is to classify precisely which torsion subgroups appear over number fields of a fixed degree.

Definition 1.2.3. *Let d be a positive integer. Let $\Phi(d)$ denote the set of groups (up to isomorphism) that appear as $E(K)_{\text{tors}}$ for some elliptic curve E/K as K ranges*

over all number fields of degree d over $\mathbb{Q}$.

In particular, in [26] Mazur determined $\Phi(1)$. Not many other values of $\Phi(d)$ have been determined. The set $\Phi(2)$ was classified by Kamienny ([18] 1992), Kenku, and Momose ([20] 1988).

Theorem 1.2.4 (Kamienny [18], Kenku, Momose [20])**.** *Let K be a quadratic number field, and let E be an elliptic curve defined over K. Then $E(K)_{\text{tors}}$ is isomorphic to one of the following groups:*

$$\begin{aligned}
&\mathbb{Z}/N_1\mathbb{Z}, && 1 \leq N_1 \leq 18, N_1 \neq 17,\\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, && 1 \leq N_2 \leq 6,\\
&\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, && N_3 = 1, 2,\\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.
\end{aligned}$$

Again, each of these groups actually appears infinitely often for elliptic curves over quadratic number fields.

The torsion subgroups of elliptic curves defined over cubic number fields appearing infinitely often have been classified by Jeon, Kim, and Schweizer.

Theorem 1.2.5 (Jeon, Kim, Schweizer [17])**.** *Let K be a cubic number field, and let E be an elliptic curve defined over K. The groups appearing as $E(K)_{\text{tors}}$ infinitely often are precisely*

$$\begin{aligned}
&\mathbb{Z}/N_1\mathbb{Z}, && 1 \leq N_1 \leq 20, N_1 \neq 17, 19,\\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, && 1 \leq N_2 \leq 7.
\end{aligned}$$

From the case over $\mathbb{Q}$ and over quadratic number fields, we might expect this to be a full list of all torsion subgroups of elliptic curves over cubic number fields. However,

Najman showed that the curve

$$y^2 + xy + y = x^3 - x^2 - 5x - 5$$

has torsion subgroup isomorphic to $\mathbb{Z}/21\mathbb{Z}$ over the cubic field $\mathbb{Q}(\zeta_9)^+$, i.e., the maximal real subfield of $\mathbb{Q}(\zeta_9)$, so the above list must be incomplete.

The set $\Phi(3)$ was finally classified by Derickx, Etropolski, Morrow, van Hoeij, Zureick-Brown ([8] 2016) by demonstrating that $\mathbb{Z}/21\mathbb{Z}$ is the only group that does not appear infinitely often.

Theorem 1.2.6 (Etropolski, Morrow, Zureick-Brown [8])**.** *Let K be a cubic number field, and let E be an elliptic curve defined over K. The groups appearing as $E(K)_{\text{tors}}$ are precisely*

$$\begin{aligned} &\mathbb{Z}/N_1\mathbb{Z}, && 1 \leq N_1 \leq 21, N_1 \neq 17, 19, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, && 1 \leq N_2 \leq 7. \end{aligned}$$

Each of these groups appear infinitely often except $\mathbb{Z}/21\mathbb{Z}$. Here we see the first example of a torsion subgroup that does not appear infinitely often.

Jeon, Kim, and Park also determined which groups appear as $E(K)_{\text{tors}}$ infinitely often for quartic number fields K but, as in the cubic case, there may be other torsion subgroups appearing only finitely many times.

Theorem 1.2.7 (Jeon, Kim, Park, [16] Theorem 3.6)**.** *If K varies over all quartic number fields and E varies over all elliptic curves defined over K, the group structures that appear infinitely often as $E(K)_{\text{tors}}$ are exactly the following:*

$$\begin{aligned}
&\mathbb{Z}/N_1\mathbb{Z}, && N_1 = 1, \ldots, 18, 20, 21, 22, 24 \\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, && N_2 = 1, \ldots, 9 \\
&\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, && N_3 = 1, 2, 3 \\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N_4\mathbb{Z}, && N_4 = 1, 2 \\
&\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, \\
&\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.
\end{aligned}$$

In fact, all of these torsion structures already occur infinitely often if K varies over quadratic extensions of quadratic number fields, that is, all quartic Galois number fields.

One may also ask a more refined question. If E is an elliptic curve defined over $\mathbb{Q}$, but we consider its K-rational points for some field K, what groups appear as $E(K)_{\text{tors}}$? We have the following definition.

Definition 1.2.8. *Let d be a positive integer. Let $\Phi_{\mathbb{Q}}(d)$ denote the set of groups (up to isomorphism) that appear as $E(K)_{\text{tors}}$ for some elliptic curve $E/\mathbb{Q}$ as K ranges over all number fields of degree d over $\mathbb{Q}$.*

Notice that necessarily $\Phi_{\mathbb{Q}}(d) \subseteq \Phi(d)$ since we are restricting the set of elliptic curves we are considering. Of course, $\Phi_{\mathbb{Q}}(1) = \Phi(1)$. The classification of $\Phi_{\mathbb{Q}}(2)$ and $\Phi_{\mathbb{Q}}(3)$ was determined by Najman ([28] 2015).

Theorem 1.2.9 (Najman, [28], Theorem 2)**.**

$$\Phi_{\mathbb{Q}}(2) = \left\{ \begin{array}{ll} \mathbb{Z}/N_1\mathbb{Z}, & N_1 = 1, \ldots, 10, 12, 15, 16, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, & 1 \leq N_2 \leq 6, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, & N_3 = 1, 2, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. & \end{array} \right\}$$

Each of these groups, except for $\mathbb{Z}/15\mathbb{Z}$*, appears as a torsion subgroup over a quadratic field for infinitely many rational elliptic curves.*

Theorem 1.2.10 (Najman, [28], Theorem 1)**.**

$$\Phi_{\mathbb{Q}}(3) = \left\{ \begin{array}{ll} \mathbb{Z}/N_1\mathbb{Z}, & N_1 = 1, \ldots, 10, 12, 13, 14, 18, 21, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 1, 2, 3, 4, 7. \end{array} \right\}$$

The author put forth the first steps in determining $\Phi_{\mathbb{Q}}(4)$ by determining which groups appear as torsion subgroups of elliptic curves over quartic Galois number fields, i.e. number fields $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ (which we call a cyclic quartic extension of $\mathbb{Q}$) or $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ (which we call a biquadratic extension of $\mathbb{Q}$).

A complete classification of $\Phi_{\mathbb{Q}}(4)$ was later determined by González-Jiménez and Najman ([13] preprint).

Theorem 1.2.11 (González-Jiménez, Najman, [13], Corollary 8.7)**.**

$$\Phi_{\mathbb{Q}}(4) = \left\{ \begin{array}{ll} \mathbb{Z}/N_1\mathbb{Z}, & N_1 = 1, \ldots, 10, 12, 13, 15, 16, 20, 24, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 1, \ldots, 6, 8, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, & N_3 = 1, 2, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N_4\mathbb{Z}, & N_4 = 1, 2, \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. & \end{array} \right\}$$

More generally, in [24] there is a conjectural formula, for each $d > 0$, for the set of primes that divide the size of $E(K)_{\text{tors}}$, where K is a number field of degree d and E is an elliptic curve defined over $\mathbb{Q}$.

1.2.2 Results

As mentioned before, the author proved a classification of torsion subgroups of elliptic curves $E/\mathbb{Q}$ in quartic number fields that were Galois over $\mathbb{Q}$.

Theorem 1.2.12 (C., [3], Theorem 1.2)**.** *Let $E/\mathbb{Q}$ be an elliptic curve, and let K be a quartic Galois extension of $\mathbb{Q}$. Then $E(K)_{\text{tors}}$ is isomorphic to one of the following groups:*

$$\begin{array}{ll} \mathbb{Z}/N_1\mathbb{Z}, & N_1 = 1, \ldots, 16, N_1 \neq 11, 14, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 1, \ldots, 6, 8, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, & N_3 = 1, 2, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N_4\mathbb{Z}, & N_4 = 1, 2, \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. & \end{array}$$

Each of these groups, except for $\mathbb{Z}/15\mathbb{Z}$*, appears as the torsion structure over some quartic Galois field for infinitely many (non-isomorphic) elliptic curves defined over* $\mathbb{Q}$*.*

The proof of this theorem is broken up based on the structure of $\mathrm{Gal}(K/\mathbb{Q})$ and so, in fact, we have the following more specialized theorems:

Theorem 1.2.13 (C., [3], Theorem 1.3)**.** *Let* $E/\mathbb{Q}$ *be an elliptic curve, and let* K *be a quartic Galois extension with* $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$*. Then* $E(K)_{\mathrm{tors}}$ *is isomorphic to one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/N_1\mathbb{Z}, && N_1 = 1, \ldots, 10, 12, 13, 15, 16, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, && N_2 = 1, \ldots, 6, 8, \\ &\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}. \end{aligned}$$

Theorem 1.2.14 (C., [3], Theorem 1.4)**.** *Let* $E/\mathbb{Q}$ *be an elliptic curve, and let* K *be a quartic Galois extension with* $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$*. Then* $E(K)_{\mathrm{tors}}$ *is isomorphic to one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/N_1\mathbb{Z}, && N_1 = 1, \ldots, 10, 12, 15, 16, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, && N_2 = 1, \ldots, 6, 8, \\ &\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, && N_3 = 1, 2, \\ &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N_4\mathbb{Z}, && N_4 = 1, 2, \\ &\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. \end{aligned}$$

The proof of Theorem 1.2.14 is simply a collection of known results, and so we give a simple explanation of the proof in Section 3.2. The proof of Theorem 1.2.13 is more involved. Section 3.3 will show the tools involved in the proof, and Section 3.4 will

contain the actual proof. Finally, Section 3.5 will contain examples and references of infinite families for each torsion subgroup appearing in Theorem 1.2.12 to finish the proof.

1.3 Torsion of Elliptic Curves over Infinite Algebraic Extensions

1.3.1 Background

One can also consider torsion over an infinite extension L of $\mathbb{Q}$.

Definition 1.3.1. *Let L be an algebraic extension of $\mathbb{Q}$. Let $\Phi_{\mathbb{Q}}(L)$ denote the set of groups (up to isomorphism) that appear as $E(L)_{\text{tors}}$ that appear as E varies over all elliptic curves defined over $\mathbb{Q}$.*

Note that if L is an infinite extension of $\mathbb{Q}$ then the Mordell-Weil Theorem no longer applies, and so a priori it is not guaranteed that the size of $E(L)_{\text{tors}}$ is finite, let alone uniformly bounded as E varies. Even so, in certain infinite extensions the number of torsion points is finite and, in fact, uniformly bounded as E varies. For instance, denoting the maximal abelian extension of $\mathbb{Q}$ by $\mathbb{Q}^{ab}$, we have the following.

Theorem 1.3.2 (Ribet [30])**.** *Let $A/\mathbb{Q}$ be an abelian variety. Then the torsion subgroup of $A(\mathbb{Q}^{ab})$ is finite.*

Since an elliptic curve is simply a one-dimensional abelian variety, this implies that for any abelian extension, including infinite abelian extensions, the torsion subgroup of an elliptic curve is finite. Note that this theorem is not effective, and it does not imply there is a uniform bound for the size of such torsion subgroups.

Fujita determined $\Phi_{\mathbb{Q}}(\mathbb{Q}(2^\infty))$ where $\mathbb{Q}(2^\infty)$ is the compositum of all degree 2 extensions of $\mathbb{Q}$, i.e., $\mathbb{Q}(2^\infty) := \mathbb{Q}(\{\sqrt{m} : m \in \mathbb{Z}\})$.

Theorem 1.3.3 (Fujita, [10], Theorem 2)**.**

$$\Phi_{\mathbb{Q}}(\mathbb{Q}(2^\infty)) = \left\{ \begin{array}{ll} \mathbb{Z}/N_1\mathbb{Z}, & N_1 = 1,3,5,7,9,15, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 1,2,3,4,5,6,8, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4N_4\mathbb{Z}, & N_4 = 1,2,3,4, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, & \\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}. & \end{array} \right\}$$

Note that $\mathbb{Q}(2^\infty) \subseteq \mathbb{Q}^{ab}$, and so Theorem 1.3.2 guarantees that the torsion subgroup is finite, but this theorem shows that, in fact, there exists a uniform bound on the size of the torsion subgroup as E varies over all elliptic curves defined over $\mathbb{Q}$.

Torsion over a similar infinite extension, $\mathbb{Q}(3^\infty)$, the compositum of all cubic number fields, was studied by Daniels, Lozano-Robledo, Najman, and Sutherland in [7]. They classify $\Phi_{\mathbb{Q}}(\mathbb{Q}(3^\infty))$. Moreover they determine which of these torsion structures appear infinitely often and which appear for only finitely many isomorphism classes of elliptic curves.

Theorem 1.3.4 (Daniels, Lozano-Robledo, Najman, Sutherland, [7], Theorem 1.8)**.**

$$\Phi_{\mathbb{Q}}(\mathbb{Q}(3^\infty)) = \left\{ \begin{array}{ll} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 1,2,4,5,7,8,13, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4N_4\mathbb{Z}, & N_4 = 1,2,4,7, \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6N_6\mathbb{Z}, & N_6 = 1,2,3,5,7, \\ \mathbb{Z}/2M\mathbb{Z} \times \mathbb{Z}/2M\mathbb{Z}, & M = 4,6,7,9. \end{array} \right\}$$

All but 4 of the torsion subgroups T listed above appear infinitely often; for $T = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z}$, and $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ there are only 2, 2, 4, and 1 (respectively) $\overline{\mathbb{Q}}$-isomorphism classes of $E/\mathbb{Q}$ with $E(\mathbb{Q}(3^\infty))_{\text{tors}} \cong T$.

Note that $\mathbb{Q}(3^\infty) \not\subseteq \mathbb{Q}^{ab}$, and so one cannot use Theorem 1.3.2 to show that the torsion subgroup is finite. Nevertheless, the Theorem 1.3.4 shows that indeed the torsion subgroup is finite over $\mathbb{Q}(3^\infty)$ and that there is a uniform bound on the size of the torsion subgroup as E varies over all elliptic curves defined over $\mathbb{Q}$.

1.3.2 Results

We closely examine the torsion subgroup of elliptic curves over $\mathbb{Q}^{ab}$. In fact, we determine $\Phi_{\mathbb{Q}}(\mathbb{Q}^{ab})$:

Theorem 1.3.5.

$$\Phi_{\mathbb{Q}}(\mathbb{Q}^{ab}) = \left\{ \begin{array}{ll} \mathbb{Z}/N_1\mathbb{Z}, & N_1 = 1,3,5,7,9,11,13,15,17, \\ & \quad 19,21,25,27,37,43,67,163, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 1,2,\ldots,9, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3N_3\mathbb{Z}, & N_3 = 1,3, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4N_4\mathbb{Z}, & N_4 = 1,2,3,4, \\ \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, & \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, & \\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}. & \end{array} \right\}$$

A uniform bound on the size of $E(\mathbb{Q}^{ab})_{\text{tors}}$ for all elliptic curves $E/\mathbb{Q}$ is a direct consequence of the classification.

Corollary 1.3.6. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $\#E(\mathbb{Q}^{ab})_{\text{tors}} \leq 163$. This bound is sharp, as the curve $26569a1$ has a point of order 163 over $\mathbb{Q}^{ab}$.*

In Section 4.2 we discuss what is known about isogenies of elliptic curves over $\mathbb{Q}$. We then discuss the intimate connection between isogenies and torsion points over $\mathbb{Q}^{ab}$. In Section 4.3 we use the results from Section 4.2 to prove bounds on the group $E(\mathbb{Q}^{ab})_{\text{tors}}$ based on the isogenies E has over $\mathbb{Q}$. In Section 4.4 we further refine the bounds to eliminate the possibility of any group not appearing in Theorem 1.3.5. Finally, Section 4.5 has, for each subgroup T appearing in Theorem 1.3.5, an example of an elliptic curve $E/\mathbb{Q}$ such that $E(\mathbb{Q}^{ab})_{\text{tors}} \cong T$ completing the proof of Theorem 1.3.5.

Chapter 2

Background

2.1 Isogenies

First we investigate maps between elliptic curves. The following discussion is a paraphrasing of [33] Section III.4.

Definition 2.1.1 ([33], p. 66)**.** *Let E_1 and E_2 be elliptic curves. An* ***isogeny*** *from E_1 to E_2 is a non-constant morphism*

$$\phi : E_1 \to E_2 \quad \textit{satisfying} \quad \phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}.$$

Two elliptic curves E_1 and E_2 are called ***isogenous*** *if there exists an isogeny ϕ from E_1 to E_2.*

Since elliptic curves are smooth projective varieties, any birational map between elliptic curves is a morphism. We denote the set of all isogenies defined over $\overline{\mathbb{Q}}$ from

E_1 to E_2 by $\mathrm{Hom}(E_1, E_2)$ and we denote the endomorphisms defined over $\overline{\mathbb{Q}}$ of E, $\mathrm{Hom}(E_1, E_1)$, by $\mathrm{End}(E_1)$. We denote the invertible elements of $\mathrm{End}(E_1)$ by $\mathrm{Aut}(E_1)$.

Example 2.1.2. Let E be an elliptic curve. For each positive $m \in \mathbb{Z}$ the **multiplication-by-m** map

$$[m] : E \to E$$

defined by

$$[m](P) = \underbrace{P + P + \cdots + P}_{m \text{ times}}$$

for all $P \in E$ is an isogeny from E to itself. We extend this definition to all $m \in \mathbb{Z}$ by defining $[0](P) = \mathcal{O}$ and for $m < 0$

$$[m](P) = [-m](-P).$$

Suppose E is an elliptic curve defined over the field K. Since addition is defined over K, the multiplication-by-m isogenies are also defined over K. In general, we denote the set of isogenies defined over a field K by $\mathrm{Hom}_K(E_1, E_2)$ and similarly define $\mathrm{End}_K(E_1)$ and $\mathrm{Aut}_K(E_1)$.

Let K be a field of characteristic 0. For any elliptic curve E the multiplication-by-m map is an endomorphism of E. Generally, these maps comprise all of $\mathrm{End}(E)$, i.e., $\mathrm{End}(E) \cong \mathbb{Z}$. However, if $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, we say that E has *complex multiplication* (or simply CM). For an elliptic curve E defined over a number field K, if $\mathrm{End}(E) \ncong \mathbb{Z}$ then $\mathrm{End}(E) \cong \mathcal{O}_F$ where $\mathcal{O}_F$ is an order in an imaginary quadratic field F. If this is the case, we say E has *complex multiplication by $\mathcal{O}_F$*.

Example 2.1.3 ([33], p70)**.** Let $K = \mathbb{Q}(i)$ and E/K be the elliptic curve with

Weierstrass model

$$E : y^2 = x^3 - x.$$

Then the map $[i] : E \to E$ defined by

$$[i](x, y) = (-x, iy)$$

is an automorphism of E. We can compute that for any $(x, y) \in E$

$$[i] \circ [i](x, y) = [i](-x, iy) = (x, -y) = -(x, y) = [-1](x, y).$$

Thus $[i] \circ [i] = [-1]$ and there is a ring homomorphism

$$\mathbb{Z}[i] \to \mathrm{End}(E), \quad m + ni \mapsto [m] + [n] \circ [i].$$

Since K has characteristic 0 this map is an isomorphism, and so $\mathrm{End}(E) \cong \mathbb{Z}[i]$, and E has complex multiplication by $\mathbb{Z}[i]$.

An important property of isogenies is that they preserve the group structure of E.

Theorem 2.1.4 ([33] Theorem 4.8)**.** *Let*

$$\phi : E_1 \to E_2$$

be an isogeny. Then $\phi(P + Q) = \phi(P) + \phi(Q)$ *for all* $P, Q \in E_1$.

However, it should be noted that not every group homomorphism from E_1 to E_2 is an isogeny, as it may not be a rational map.

This leaves us with an important corollary

Corollary 2.1.5 ([33] Corollary 4.9)**.** *Let $\phi : E_1 \to E_2$ be a nonzero isogeny. Then*

$$\ker \phi = \phi^{-1}(\mathcal{O}_{E_2})$$

is a finite group.

In fact, the converse is true.

Proposition 2.1.6 ([33] Proposition 4.12)**.** *Let E be an elliptic curve and let Φ be a finite subgroup of E defined over an algebraic extension K of $\mathbb{Q}$. There is a unique elliptic curve and an isogeny defined over K*

$$\phi : E \to E' \quad \textit{satisfying} \quad \ker \phi = \Phi.$$

Thus, we have a one-to-one correspondence between finite subgroups of E and isogenies out of E. In fact, more can be said by examining the action of Galois on E. We define the action of Galois and describe some of its properites in the following proposition.

Proposition 2.1.7. *Let E be an elliptic curve defined over a field K of characteristic 0. There is a natural action by the group $\mathrm{Gal}(\overline{K}/K)$ on the points of E defined by*

$$(x, y)^\sigma = (x^\sigma, y^\sigma)$$

for all $(x, y) \in E$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$. This action commutes with the group structure

on E, i.e. for any $P, Q \in E$

$$(P+Q)^\sigma = P^\sigma + Q^\sigma.$$

Since addition on E is defined over K which is fixed by $\mathrm{Gal}(\overline{K}/K)$, the proposition follows. Further, an immediate corollary is that the action of Galois commutes with the multiplication-by-m isogenies.

Corollary 2.1.8. *Let K be a field of characteristic 0. Let E/K be an elliptic curve. For all $\sigma \in \mathrm{Gal}(\overline{K}/K)$, any $m \in \mathbb{Z}$, and any $P \in E$ we have*

$$[m](P^\sigma) = ([m]P)^\sigma.$$

Now we have an important remark concerning the field of definition of isogenies.

Remark 2.1.9 ([33], Remark 4.13.2)**.** Suppose that E is defined over K and that Φ is $\mathrm{Gal}(\overline{K}/K)$-invariant. In other words, if $T \in \Phi$, then $T^\sigma \in \Phi$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then the curve E' and isogeny ϕ described in Proposition 2.1.6 can be defined over K.

This shows that the one-to-one correspondence between finite subgroups of E and isogenies out of E can be refined to a one-to-one correspondence between finite $\mathrm{Gal}(\overline{K}/K)$-invariant subgroups of E and isogenies ϕ out of E defined over K. This idea will be crucial in examining torsion in the following sections.

Finally, we give the definition of a special type of isogeny.

Definition 2.1.10. *Let K be a number field and E_1, E_2 be elliptic curves over K. Let $\phi : E_1 \to E_2$ be an isogeny with $\ker\phi \cong \mathbb{Z}/n\mathbb{Z}$. Then we call ϕ an **n-isogeny** over K.*

Much is known about such isogenies. For instance we have a classification of n-isogenies over $\mathbb{Q}$, see [24] for more info.

Theorem 2.1.11 (Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, and Ogg, among others)**.** *If $E/\mathbb{Q}$ has an n-isogeny, $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$. If E does not have complex multiplication, then $n \leq 18$ or $n \in \{21, 25, 37\}$.*

Moreover, there is a detailed bound on the number of $\mathbb{Q}$-isogenies an elliptic curve can have. The following theorem is from [19], combining Theorem 2 and the surrounding discussion.

Theorem 2.1.12 (Kenku, [19])**.** *There are at most eight $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$ isogeny class.*

Let $C_p(E)$ denote the number of distinct $\mathbb{Q}$-rational cyclic subgroups of order p^n for any n of E. Let $C(E) = \prod_p C_p(E)$. Then, we have the following table for bounds on C_p for any elliptic curve over $\mathbb{Q}$

p	2	3	5	7	11	13	17	19	37	43	67	163	*else*
C_p	8	4	3	2	2	2	2	2	2	2	2	2	1

In particular, fix a $\mathbb{Q}$-isogeny class and a representative E of that class.

- *If $C_p(E) = 2$ for some prime $p \geq 11$, then $C_q(E) = 1$ for all other primes q. So $C(E) = 2$.*
- *If $C_7(E) = 2$, then $C_5(E) = 1$ and either $C_3(E) \leq 2$ and $C_2(E) = 1$ or $C_3(E) = 1$ and $C_2(E) \leq 2$. All these yield $C(E) \leq 4$.*
- *If $C_5(E) = 3$, then $C_p(E) = 1$ for all primes $p \neq 5$.*

- *If* $C_5(E) = 2$, *then either* $C_3(E) \leq 2$ *and* $C_2(E) = 1$ *or* $C_3(E) = 1$ *and* $C_2(E) \leq 2$. *Hence* $C(E) \leq 4$.

- *If* $C_3(E) = 4$, *then there exists a representative of the class of* E *with a* $\mathbb{Q}$*-rational cyclic subgroup of order 27, and* $C_2(E) = 1$ *so* $C(E) \leq 4$.

- *If* $C_3(E) = 3$, *then* $C_2(E) \leq 2$ *so that* $C(E) \leq 6$.

- *If* $C_3(E) \leq 2$, *then* $C_2(E) \leq 4$ *so that* $C(E) \leq 8$.

Note the fact that $C(E) = 8$ *is possible only if* $C_2(E) = 8$ *or* $C_3(E) = 2$ *and* $C_2(E) = 4$.

As we will see, isogenies are connected to torsion of elliptic curves, and knowing precisely what isogenies an elliptic curve can have over $\mathbb{Q}$ will be an instrumental tool in the proofs of our classification theorems.

2.2 Structure of $E(K)_{\text{tors}}$

We now define the torsion of an elliptic curve.

Definition 2.2.1 ([33], p. 69)**.** *Let* E *be an elliptic curve and let* $m \in \mathbb{Z}$ *with* $m \geq 1$. *The* m***-torsion subgroup of*** E, *denoted* $E[m]$, *is the set of points of* E *of order dividing* m,

$$E[m] := \{P \in E : [m]P = \mathcal{O}\}.$$

The ***torsion subgroup of*** E, *denoted* E_{tors}, *is the set of points of finite order,*

$$E_{\text{tors}} = \bigcup_{m=1}^{\infty} E[m].$$

If E is defined over the field K, then $E(K)_{\text{tors}}$ denotes the points of finite order in $E(K)$.

In the following section we will discuss the basic structure of $E(K)_{\text{tors}}$ for elliptic curves E defined over K, an algebraic extension of $\mathbb{Q}$. We follow much of [23] Section 3.2 for our discussion in this section.

Definition 2.2.2 ([23], Definition 3.1.1)**.** *A **lattice** L in the complex plane is an additive discrete subgroup of $\mathbb{C}$, such that $L \otimes \mathbb{R} = \mathbb{C}$.*

An alternative way to view a lattics in $\mathbb{C}$ is as a free $\mathbb{Z}$-submodule of $\mathbb{C}$ of rank 2. That is, there exist $\omega_1, \omega_2 \in \mathbb{C}$ such that

$$L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

with $\mathbb{C} = \mathbb{R}\omega_1 \oplus \mathbb{R}\omega_2$. The lattice generated by $\omega_1, \omega_2 \in \mathbb{C}$ will be denoted $\langle \omega_1, \omega_2 \rangle$. Without loss of generality we may assume that our lattices are *positively oriented*, i.e. the quotient $\frac{\omega_1}{\omega_2}$ has positive imaginary part, i.e. $\frac{\omega_1}{\omega_2} \in \mathbb{H}$, where $\mathbb{H}$ is the upper half complex plane

$$\mathbb{H} := \{a + bi : a, b \in \mathbb{R}, b > 0\}.$$

Definition 2.2.3 ([23], Definition 3.1.4)**.** *Let L be a lattice in $\mathbb{C}$ with generators $\omega_1, \omega_2 \in \mathbb{C}$. The group $\mathbb{C}/L$, the **quotient of** $\mathbb{C}$ **by the lattice** L, is the quotient of $\mathbb{C}$ as an additive group by the subgroup L.*

It is a classical result that $\mathbb{C}/L$ is a torus when considered as a surface. We will show that for any elliptic curve $E/\mathbb{C}$, there exists a lattice L such that $E \cong \mathbb{C}/L$ as complex analytic abelian groups, a result known as the *uniformization theorem.*

We first begin by defining functions on $\mathbb{C}/L$.

Definition 2.2.4 ([23], Definition 3.2.1)**.** *An* ***elliptic function*** *relative to a lattice $L \subseteq \mathbb{C}$ is a meromorphic function $f : \mathbb{C} \to \mathbb{C}$ such that $f(z+w) = f(z)$ for all $z \in \mathbb{C}$ and all $w \in L$. The set of all elliptic functions for L is denoted $\mathbb{C}(L)$.*

Elliptic functions are invariant under translation by elements $w \in L$, and thus define functions on the quotient $\mathbb{C}/L$. An important example of an elliptic function is the Weierstrass $\wp$-function.

Definition 2.2.5 ([23], Definition 3.2.2)**.** *Let L be a lattice. The* ***Weierstrass $\wp$-function*** *relative to L is the function*

$$\wp(z, L) = \frac{1}{z^2} + \sum_{0 \neq w \in L} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

We also define an important function on lattices: the Eisenstein series.

Definition 2.2.6 ([23], Definition 3.2.3)**.** *Let $k \geq 2$ and L be a lattice. The* ***Eisenstein series of weight*** *$2k$ is the series*

$$G_{2k}(L) = \sum_{0 \neq w \in L} \frac{1}{w^{2k}}.$$

The Weierstrass $\wp$-function is an elliptic function that has double poles at each lattice point $w \in L$. With the Eisenstein series in hand, we are now ready to state the uniformization theorem:

Theorem 2.2.7 (Uniformization Theorem, [23], Theorem 3.2.5)**.** *Let L be a lattice in $\mathbb{C}$. Let E_L be the elliptic curve over $\mathbb{C}$ given by the short Weierstrass equation*

$$E_L : y^2 = x^3 - 15G_4(L)x - 35G_6(L).$$

Let $\Phi : \mathbb{C}/L \to E_L$ *be the map defined by*

$$\Phi(z \bmod L) = \left(\wp(z, L), \frac{\wp'(z, L)}{2}\right)$$

where $\wp'(z, L)$ *denotes the derivative of* $\wp$ *with respect to* z*. Then*

1. Φ *is a complex analytic isomorphism of abelian groups.*

2. *Let* $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ *be an elliptic curve. Then there exists a lattice* $L \subseteq \mathbb{C}$ *such that* $A = -15G_4(L)$*,* $B = -35G_6(L)$*, and* $\mathbb{C}/L$ *is isomorphic to* $E(\mathbb{C})$ *via* Φ*.*

This deep result immediately demonstrates the structure of torsion points of E over $\mathbb{C}$. Points of order m in $\mathbb{C}/\langle\omega_1, \omega_2\rangle$ are points of form (up to equivalence) $\frac{a}{m}\omega_1 + \frac{b}{m}\omega_2$ for $0 \leq a, b \leq m - 1$. Thus, for any algebraic extension K of $\mathbb{Q}$ by fixing an embedding $K \to \mathbb{C}$ we have the following corollary:

Corollary 2.2.8. *Let* E *be an elliptic curve defined over an algebraic extension* K *of* $\mathbb{Q}$*. Then*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Thus, since $E(K)[m] \subseteq E[m]$, it follows that $E(K)[m] \subseteq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Definition 2.2.9. *Let* E *be an elliptic curve over an algebraic extension* K *of* $\mathbb{Q}$*. If*

$$E(K)[m] = E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

then we say E *has* ***full*** m***-torsion over*** K*.*

Now we mention a consequence of an elliptic curve having full m-torsion over a field K. Let μ_m denote the set of all m^{th}-roots of unity. There is a pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

called the **Weil pairing** that is alternating, bilinear, nondegenerate, compatible, and Galois invariant (see [33], Proposition 8.1 for more details). A consequence of the existence of such a pairing is the following corollary:

Corollary 2.2.10. *Let E be an elliptic curve over a field K of characteristic 0. If $E[m] \subseteq E(K)$, then $\mu_m \subseteq K$.*

This result restricts what possible full-m-torsion can appear over a field K, and will be important in ruling out possible torsion structures in our classifications.

2.3 Galois Representation

The following section draws from [33] Section III.7.

Fix a number field K and let E/K be an elliptic curve. Fix an integer $m > 1$. Recall from Corollary 2.1.8 that there exists an action of $\mathrm{Gal}(\overline{K}/K)$ on the points of E, and in fact this action commutes with the multiplication-by-m map. Thus, this action restricts to an action on $E[m]$, since for any point $P \in E[m]$ and any $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we have

$$[m](P^\sigma) = ([m]P)^\sigma = \mathcal{O}^\sigma = \mathcal{O}.$$

Therefore, there is a map

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m]).$$

Definition 2.3.1. *Let K be a number field and let E/K be an elliptic curve. For any integer $m > 1$ we define the Galois representation*

$$\rho_{E,m} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m]).$$

by $\sigma \mapsto (P \mapsto \sigma(P))$.

In fact, since $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, if we fix a $\mathbb{Z}/m\mathbb{Z}$-basis of $E[m]$, say $\{P, Q\}$, then $\mathrm{Aut}(E[m]) \cong \mathrm{GL}(2, \mathbb{Z}/m\mathbb{Z})$, and the map

$$\rho_{E,m} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2, \mathbb{Z}/m\mathbb{Z})$$

is given by $\sigma \mapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where

$$P^\sigma = aP + cQ \quad \text{and} \quad Q^\sigma = bP + dQ.$$

Note that since the isomorphism $\mathrm{Aut}(E[m]) \cong \mathrm{GL}(2, \mathbb{Z}/m\mathbb{Z})$ depends on a choice of basis of $E[m]$, the image of $\rho_{E,m}$ is only well-defined up to conjugation in $\mathrm{GL}(2, \mathbb{Z}/m\mathbb{Z})$.

The mod m representations can be fit together using the inverse limit construction.

Definition 2.3.2 ([33], p87)**.** *Let E be an elliptic curve and let $l \in \mathbb{Z}$ be a prime.*

*The **(l-adic) Tate module of** E is the group*

$$T_l(E) = \varprojlim_n E[l^n],$$

the inverse limit being taken with respect to the natural maps

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n].$$

Since the action of $\mathrm{Gal}(\overline{K}/K)$ commutes with the multiplication-by-l map used in the inverse limit definition of $T_l(E)$, we can extend the action of $\mathrm{Gal}(\overline{K}/K)$ to $T_l(E)$.

Definition 2.3.3 ([33], p88)**.** *The l-adic representation (of $\mathrm{Gal}(\overline{K}/K)$ associated to E) is the homomorphism*

$$\rho_{E,l^\infty} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_l(E))$$

induced by the action of $\mathrm{Gal}(\overline{K}/K)$ on the l^n torsion points of E.

Similar to before, by choosing a $\mathbb{Z}_l$-basis of $T_l(E)$ we get a representation

$$\rho_{E,l^\infty} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2, \mathbb{Z}_l)$$

which pieces together all of the ρ_{E,l^n} defined earlier. That is,

$$\rho_{E,l^\infty}(\mathrm{Gal}(\overline{K}/K)) \bmod l^n = \rho_{E,l^n}(\mathrm{Gal}(\overline{K}/K))$$

(up to conjugation).

Now, given a number field K and an elliptic curve E/K, we wish to investigate

what the possible images of $\rho_{E,l^\infty}(\mathrm{Gal}(\overline{K}/K))$ in $\mathrm{GL}(2,\mathbb{Z}_l)$ for various primes l.

Theorem 2.3.4 (Serre, [32]). *Let K be a number field and let E/K be an elliptic curve without complex multiplication.*

1. *$\rho_{E,l^\infty}(\mathrm{Gal}(\overline{K}/K))$ is of finite index in $\mathrm{Aut}(T_l(E))$ for all primes $l \neq \mathrm{char}(K)$.*
2. *$\rho_{E,l^\infty}(\mathrm{Gal}(\overline{K}/K)) = \mathrm{Aut}(T_l(E))$ for all but finitely many primes l.*

Moreover, Serre classifies precisely which maximal subgroups the image of $\rho_{E,l}$ can land in.

Theorem 2.3.5 (Serre, [32]). *Let $E/\mathbb{Q}$ be an elliptic curve. Let G be the image of $\rho_{E,l}$ in $\mathrm{GL}(2,\mathbb{Z}/l\mathbb{Z})$ for a prime l, and suppose $G \neq \mathrm{GL}(2,\mathbb{Z}/l\mathbb{Z})$. Then one of the following possibilities holds:*

1. *A conjugate of G is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}(2,\mathbb{Z}/l\mathbb{Z})$.*
2. *A conjugate of G is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}(2,\mathbb{Z}/l\mathbb{Z})$.*
3. *The projective image of G in $\mathrm{PGL}(2,\mathbb{Z}/l\mathbb{Z})$ is isomorphic to A_4, S_4, or A_5, where S_n is the symmetric group and A_n is the alternating group on n elements.*
4. *A conjugate of G is contained in a Borel subgroup of $\mathrm{GL}(2,\mathbb{Z}/l\mathbb{Z})$.*

Rouse and Zureick-Brown in fact classified all possible 2-adic images of elliptic curves $E/\mathbb{Q}$:

Theorem 2.3.6 (Rouse, Zureick-Brown, [31], Corollary 1.2). *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. There are exactly 1208 possibilities*

for the 2*-adic image* $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$*, up to conjugacy in* $\mathrm{GL}(2,\mathbb{Z}_2)$*. The index of* $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ *divides 64 or 96; all such indices occur. Moreover, the image of* $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ *is the inverse image in* $\mathrm{GL}_2(\mathbb{Z}_2)$ *of the image of* $\rho_{E,32}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$*.*

Understanding the Galois representations is crucial to understanding torsion of elliptic curves. We will see many applications of these representations in the proofs of our main results.

2.4 Modular Curves

In this section, we follow the discussion presented in [23] sections 3.4, 3.5, and 3.6. See also [33] Appendix C.13 for more detail on the theory of modular curves.

2.4.1 The Modular Curve $X(1)$

Recall that Theorem 2.2.7 shows that every elliptic curve is isomorphic to $\mathbb{C}/L$ for some lattice L in $\mathbb{C}$. In fact, we can always take the lattice L to be of the form $L = \langle \tau, 1\rangle$ for some $\tau \in \mathbb{H}$, where $\mathbb{H}$ denotes the upper half plane of $\mathbb{C}$, because of the following proposition:

Proposition 2.4.1 ([23] Proposition 3.1.10)**.** *Let* L *be a lattice in* $\mathbb{C}$*.*

1. *There is a* $\tau \in \mathbb{H}$ *such that* $\mathbb{C}/L \cong \mathbb{C}/\langle \tau, 1\rangle$*.*

2. *Let* $\tau, \tau' \in \mathbb{H}$*. Then* $\mathbb{C}/\langle \tau, 1\rangle \cong \mathbb{C}/\langle \tau', 1\rangle$ *if and only if there is a matrix* $M =$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \textit{ such that}$$

$$\tau' = M\tau = \frac{a\tau + b}{c\tau + d}.$$

Thus, we may identify every point $\tau \in \mathbb{H}$ to some elliptic curve $E/\mathbb{C}$, and vice versa via Theorem 2.2.7. Moreover, two elliptic curves E_τ and $E_{\tau'}$ are isomorphic over $\mathbb{C}$ if and only if $\tau' = M\tau$ for some $M \in \mathrm{SL}(2,\mathbb{Z})$ by the above proposition. For reasons that will become clear in the following sections, let $\Gamma(1) := \mathrm{SL}(2,\mathbb{Z})$. From our discussion, it is natural to take the quotient $\mathbb{H}/\Gamma(1)$, as points in this quotient are in bijective correspondence with the set of all isomorphism classes of elliptic curves $E/\mathbb{C}$. Moreover, the map Φ in Theorem 2.2.7 gives us a precise way to move back and forth between these sets.

Let $Y(1) := \mathbb{H}/\Gamma(1)$. This quotient is homeomorphic to a sphere missing one point. To compactify this space, we add a "point at infinity" called a cusp. The resulting space we call $X(1) := Y(1) \cup \{\infty\}$. In fact, $X(1)$ is a complex curve, and is our first example of a modular curve. This curve parametrizes all elliptic curves over $\mathbb{C}$ up to isomorphism, i.e., every non-cuspidal point on $X(1)$ corresponds to an elliptic curve $E/\mathbb{C}$.

In the rest of the chapter, we will construct other modular curves as quotients of $\mathbb{H}$ by subgroups of $\mathrm{SL}(2,\mathbb{Z})$ that will parametrize elliptic curves with additional information (depending on the subgroup).

2.4.2 General Modular Curves

We define some important subgroups of $\mathrm{SL}(2,\mathbb{Z})$.

Definition 2.4.2 ([23], Definition 3.5.1)**.** *Let $N \geq 1$ be an integer. We define subgroups of $\mathrm{SL}(2,\mathbb{Z})$ by:*

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : c \equiv 0 \bmod N \right\},$$

$$\Gamma_1(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : c \equiv 0, a \equiv d \equiv 1 \bmod N \right\},$$

$$\Gamma(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : b \equiv c \equiv 0, a \equiv d \equiv 1 \bmod N \right\}.$$

*We say that a subgroup G of $\mathrm{SL}(2,\mathbb{Z})$ is a **congruence subgroup** if G contains $\Gamma(N)$ for some integer $N \geq 1$.*

Indeed, each of the above groups is a congruence subgroup. In fact, $\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N)$.

Given a fixed congruence subgroup Γ, we can construct a modular curve in a similar way that we constructed $X(1)$. Let $Y := \mathbb{H}/\Gamma$, and then let $X = Y \cup \{\text{cusps}\}$ be the compactification of Y by adjoining a finite number of cusps. The precise definition of compactification is given by taking $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. Notice that $\Gamma(1)$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$. Thus, any finite index subgroup of $\Gamma(1)$ has finitely many orbits in $\mathbb{P}^1(\mathbb{Q})$. Each orbit is called a "cusp". See [9] Chapter 1.2 for more information.

We denote by $X_0(N)$, $X_1(N)$, and $X(N)$ the modular curves obtained by taking the quotient of $\mathbb{H}^*$ by $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma(N)$ respectively. Just as points on $X(1)$

had an interpretation as corresponding to elliptic curves, the points on a general modular curve correspond to elliptic curves with additional conditions. Let $\mathbb{H}^*$ denote $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, that is, the upper half plane union cusps. We summarize these results in the following theorem:

Theorem 2.4.3 ([33], Theorem 13.1)**.** *Let $N \geq 1$ be an integer.*

1. *There exist a smooth projective curve $X_0(N)/\mathbb{Q}$ and a complex analytic isomorphism*

$$j_{N,0} : \mathbb{H}^*/\Gamma_0(N) \to X_0(N)(\mathbb{C})$$

such that the following holds:

Let $\tau \in \mathbb{H}/\Gamma_0(N)$ and let $K = \mathbb{Q}(j_{N,0}(\tau))$. Then τ corresponds to an equivalence class of pairs (E, C) where E is an elliptic curve and $C \subseteq E$ is a cyclic subgroup of order N. Then this equivalence class contains a pair such that both E and C are defined over K, i.e., E is an elliptic curve over K and $C \subseteq E(\overline{K})$ is $\mathrm{Gal}(\overline{K}/K)$-invariant.

2. *There exist a smooth projective curve $X_1(N)/\mathbb{Q}$ and a complex analytic isomorphism*

$$j_{N,1} : \mathbb{H}^*/\Gamma_1(N) \to X_1(N)(\mathbb{C})$$

such that the following holds:

Let $\tau \in \mathbb{H}/\Gamma_1(N)$ and let $K = \mathbb{Q}(j_{N,1}(\tau))$. Then τ corresponds to an equivalence class of pairs (E, P) where E is an elliptic curve and $P \in E$ is point of exact order N. Then this equivalence class contains a pair such that E is defined over K and $P \in E(K)$.

3. *Fix a primitive N^{th} root of unity $\zeta \in \mathbb{C}$. There exist a smooth projective curve $X(N)/\mathbb{Q}$ and a complex analytic isomorphism*

$$j_N : \mathbb{H}^*/\Gamma(N) \to X(N)(\mathbb{C})$$

such that the following holds:

Let $\tau \in \mathbb{H}/\Gamma(N)$ and let $K = \mathbb{Q}(j_N(\tau))$. Then τ corresponds to an equivalence class of triples (E, P_1, P_2) where E is an elliptic curve and $\{P_1, P_2\}$ are generators for $E[N]$ satisfying $e_N(P_1, P_2) = \zeta$, where e_N is the Weil pairing. Then this equivalence class contains a triple such that E is defined over K and $P_1, P_2 \in E(K)$.

With this theorem, we see the important role modular curves play in understanding torsion of elliptic curves in algebraic extensions of $\mathbb{Q}$. For instance, the fact that there does not exist an elliptic curve $E/\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/11\mathbb{Z}$ (see Theorem 1.2.1) can be interpreted as the fact that $X_1(11)(\mathbb{Q})$ has no non-cuspidal points.

Another important interpretation of the above theorem comes from what was discussed in Remark 2.1.9. The cyclic Galois-stable subgroups C of order N described in part (b) imply that there is another curve E' and an N-isogeny $\varphi : E \to E'$ with kernel precisely C. Thus, K-rational points on $X_0(N)$ can be interpreted as triples (E, E', φ) where E, E', and φ are all defined over K, and the kernel of φ is cyclic of order N.

The proof of the results in this thesis will often times resort to the construction of a modular curve parametrizing a particular torsion structure we are interested in, and then classifying the rational points on that curve.

Chapter 3

Quartic Galois Number Field Classification

3.1 Overview

In this chapter we will present the proof of Theorem 1.2.12 via Theorem 1.2.13 and Theorem 1.2.14.

The proof of Theorem 1.2.14 is simply a collection of known results, and so we give a simple explanation of the proof in Section 3.2. The proof of Theorem 1.2.13 is more involved. Section 3.3 will show the tools involved in the proof, and Section 3.4 will contain the actual proof. Finally, Section 3.5 will contain examples and references of infinite families for each torsion subgroup appearing in Theorem 1.2.12 to finish the proof.

3.2 Torsion over Biquadratic Number Fields

Recall that $\Phi_{\mathbb{Q}}(\mathbb{Q}(2^\infty))$ was determined by Fujita, see Theorem 1.3.3. Certainly, if E is an elliptic curve over $\mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ for some square-free $m, n \in \mathbb{Z}$, then $E(K)_{tors} \leq E(\mathbb{Q}(2^\infty))_{tors}$, and so this gives the following list of possibilities for $E(K)_{tors}$:

$$\begin{aligned}
&\mathbb{Z}/N\mathbb{Z} && N = 1, \ldots, 10, 12, 15, 16.\\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, && N = 1, 2, 3, 4, 5, 6, 8,\\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N\mathbb{Z}, && N = 1, 2, 3, 4,\\
&\mathbb{Z}/2N\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, && N = 3, 4,\\
&\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z},\\
&\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.
\end{aligned}$$

First we wish to show that any group in Najman's classification in Theorem 1.2.9 must also appear over a biquadratic extension of $\mathbb{Q}$ by adjoining a square root that will not add any torsion points. This is done with the following lemma:

Lemma 3.2.1. *Let E be an elliptic curve defined over $\mathbb{Q}$. Given a quadratic field $F_1/\mathbb{Q}$, there is a quadratic field $F_2/\mathbb{Q}$ such that $E(F_1F_2)_{tors} \cong E(F_1)_{tors}$.*

Proof. Let E be an elliptic curve defined over $\mathbb{Q}$, and let F_1 be a quadratic field. Let L denote the maximal elementary 2-abelian extension of $\mathbb{Q}$. Then, $E(F_1)_{\text{tors}} \subseteq E(L)_{\text{tors}}$. Let M be the field of definition of all the points in $E(L)_{\text{tors}}$. Since by Theorem 1.3.3 there are only finitely many points in $E(L)_{\text{tors}}$, it follows that M is a finite extension of $\mathbb{Q}$ with $E(M)_{\text{tors}} \cong E(L)_{\text{tors}}$. Pick a $d \in \mathbb{Z}$ such that $\sqrt{d} \notin M$. Then

$$E(L)_{\text{tors}} \cong E(M)_{\text{tors}} \cong E(M(\sqrt{d}))_{\text{tors}},$$

since $M(\sqrt{d}) \subseteq L$. Now suppose $P \in E(F_1(\sqrt{d}))_{\text{tors}}$. Then P is defined over $F_1(\sqrt{d}) \cap M = F_1$. That is, no torsion points are gained by adjoining $\sqrt{d}$. Thus, setting $F_2 = \mathbb{Q}(\sqrt{d})$, we have that $E(F_1)_{\text{tors}} \cong E(F_1F_2)_{\text{tors}}$. □

This leaves us with six cases to verify:

$$\begin{aligned}
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N\mathbb{Z}, \quad N = 2, 3, 4, \\
&\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \\
&\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.
\end{aligned}$$

In [15] Theorem 4.10 and Theorem 4.11, Jeon, Kim, Lee construct an infinite family of curves defined over $\mathbb{Q}$ such that $E(K)_{tors} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ and $E(K)_{tors} \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ for biquadratic fields K (see section **??** for infinite families of such curves). Further, in Fujita's paper [10] he gives an example of a curve $E : y^2 = x(x^2 - 47x + 16^3)$ such that $E(L)_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$, but in fact already over a biquadratic extension $K = \mathbb{Q}(\sqrt{-7}, \sqrt{-15})$, we have $E(K)_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$.

Thus, we need only to verify three cases:

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}, \ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}, \ \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Proposition 3.2.2. *Let E be an elliptic curve defined over $\mathbb{Q}$, and let K be a biquadratic number field. Then, $E(K)_{tors}$ is not isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.*

Proof. Let L denote the maximal elementary 2-abelian extension of $\mathbb{Q}$. Suppose $E(K)_{tors} \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. From [10], Proposition 11, if $E(\mathbb{Q})_{\text{tors}}$ is cyclic, then we have $E(L)_{\text{tors}} \not\supseteq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Since $E(K)_{\text{tors}} \subseteq E(L)_{\text{tors}}$, this implies that if $E(\mathbb{Q})_{\text{tors}}$ is cyclic, then $E(K)_{\text{tors}} \not\supseteq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Thus, we may assume that $E(\mathbb{Q})_{\text{tors}}$ is not

cyclic. From [10] in his closing remarks shows that $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ occurs in number fields of degree 16 or greater if E is an elliptic curve over $\mathbb{Q}$ with non-cyclic torsion over $\mathbb{Q}$. □

Finally Najman and Bruin show in [2] that $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ do not appear as torsion subgroups for any elliptic curves over any quartic number fields K (not just elliptic curves defined over $\mathbb{Q}$).

Theorem 3.2.3 (Bruin, Najman, [2], Theorem 7)**.** *The following groups do not occur as subgroups of elliptic curves over quartic fields:*

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/27\mathbb{Z},$$
$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/33\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/39\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z},$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/44\mathbb{Z},$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/52\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/68\mathbb{Z}, \quad \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

3.3 Auxiliary Results

In this section we show a series of results needed to in the proof of Theorem 1.2.13. We begin by proving a lemma for determining when a quartic extension is cyclic.

Lemma 3.3.1. *Let K be a quartic Galois number field. Then K can be written in the form $K = \mathbb{Q}(\sqrt{m})(\sqrt{\alpha})$ for some square free $m \in \mathbb{Q}$ and some $\alpha \in \mathbb{Q}(\sqrt{m})$. Writing $\alpha = a + b\sqrt{m}$ for some $a, b \in \mathbb{Q}$, we have the following:*

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \Leftrightarrow \frac{a^2}{m} - b^2 = 1 \text{ for some } a \neq 0, b \neq 0$$

Proof. Notice that if $b = 0$ then K is a biquadratic extension of $\mathbb{Q}$ and so $\mathrm{Gal}(K/\mathbb{Q}) \cong V_4$. If $a = 0$, then $K = \mathbb{Q}(\sqrt[4]{m})$ which is not a Galois extension of $\mathbb{Q}$. Suppose $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$, i.e. K is cyclic Galois over $\mathbb{Q}$. Then the field K must contain both $\sqrt{a+b\sqrt{m}}$ and $\sqrt{a-b\sqrt{m}}$ since they are conjugates. For ease of notation we will call $\sqrt{a+b\sqrt{m}} = \beta$ and $\sqrt{a-b\sqrt{m}} = \overline{\beta}$. The other two conjugates differ only by a negative sign so we may claim that K is a Galois extension if and only if $\overline{\beta} \in K$. So we have that K is Galois if and only if $\mathbb{Q}(\beta) = \mathbb{Q}(\overline{\beta})$. This holds if and only if

$$\sqrt{a+b\sqrt{m}} = c^2\sqrt{a-b\sqrt{m}}$$

for some $c \in \mathbb{Q}(\sqrt{m})$, i.e.

$$\frac{\sqrt{a+b\sqrt{m}}}{\sqrt{a-b\sqrt{m}}} = \frac{(a+b\sqrt{m})^2}{a^2-b^2m} = c^2$$

so if and only if $a^2 - b^2m$ is a square in $\mathbb{Q}(\sqrt{m})$. Writing this out we have:

$$a^2 - b^2m = (d+e\sqrt{m})^2 = d^2 + 2ed\sqrt{m} + e^2m$$

for some $d, e \in \mathbb{Q}$. Either $d = 0$ or $e = 0$. If $e = 0$, then we have $a^2 - b^2m = d^2$. Then $\beta\overline{\beta} = \sqrt{a^2-b^2m} = d$, and some $\overline{\beta} = \frac{d}{\beta}$. However, then any σ in the Galois group of K has order at most 2, since either σ sends β to $-\beta$ in which case it is clear that σ has order two, or σ sends β to $\overline{\beta}$ in which case

$$\sigma^2(\beta) = \sigma(\overline{\beta}) = \sigma\left(\frac{d}{\beta}\right) = \frac{d}{\sigma\beta} = \beta.$$

Thus K is Galois cyclic if and only if $a^2 - b^2m = e^2m$ for some $e \in \mathbb{Q}, a \neq 0, b \neq 0$.

Dividing through by e^2 and absorbing it into a^2 and b^2 we get a nicer criterion:

$$\frac{a^2}{m} - b^2 = 1.$$

□

We use this to prove the next lemma, which in turn limits the amount of n-torsion that appears in $E(K)$.

Lemma 3.3.2. *Let K be a cyclic quartic extension of $\mathbb{Q}$. Let F be the (unique) intermediate quadratic subfield of K. Then, F is a real quadratic extension of $\mathbb{Q}$.*

Proof. From above, if $F = \mathbb{Q}(\sqrt{m})$, then a quadratic extension of F, say $F(\sqrt{a + b\sqrt{m}})$ for some $a, b \in \mathbb{Q}$, is quartic cyclic if and only if $\frac{a^2}{m} - b^2 = 1$. Suppose $m < 0$, then there are no solutions over the reals to $\frac{a^2}{m} - b^2 = 1$, and so there is no quadratic extension of F that is a cyclic quartic number field. Therefore, if F is contained in a cyclic quartic extension, $F = \mathbb{Q}(\sqrt{m})$ for some $m > 0$, i.e. F is totally real. □

Lemma 3.3.3. *Let K be a cyclic quartic extension of $\mathbb{Q}$, and let E be an elliptic curve over $\mathbb{Q}$. If $E(K)_{tors} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, then $n = 1, 2, 5,$ or 10.*

Proof. Suppose $E(K)_{\text{tors}} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. By the existence of the Weil pairing, full n-torsion is defined over a number field K only if the n^{th} roots of unity are defined over K. In particular we have $\mathbb{Q}(\zeta_n) \subseteq K$. where ζ_n denotes a primitive n^{th} root of unity. Thus we have

$$[K : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [K : \mathbb{Q}] = 4$$

and so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ divides 4. However, notice that $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_3) =$

$\mathbb{Q}(\sqrt{-3})$ are not contained in any cyclic quartic number field because of Lemma 3.3.2. Therefore, n is not divisible by 3 or 4. Now examining values of $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ shows that the only possibilities for n are $1, 2, 5,$ or 10. □

In fact, Bruin and Najman in [2] show that it is impossible for full 10-torsion to be defined over a quartic number field (see Theorem 3.4.2).

The following lemma helps us understand the 2-torsion of an elliptic curve over $\mathbb{Q}$.

Lemma 3.3.4. *Let K be a number field of degree not divisible by 3, and let E be an elliptic curve over $\mathbb{Q}$. If $E(\mathbb{Q})[2] = \{\mathcal{O}\}$, then $E(K)[2] = \{\mathcal{O}\}$.*

Proof. Suppose $E(\mathbb{Q})[2]$ is trivial. We may find a model for E in the form $y^2 = f(x)$ for some cubic polynomial f. Since the 2-torsion points of E are all of the form $(\alpha, 0)$ for a root α of f, it follows that f is irreducible over $\mathbb{Q}$. Thus, the field of definition of any 2-torsion point of E is $\mathbb{Q}(\alpha)$ for some root α of f, which is a degree 3 number field. Since K is of degree not divisible by 3, it follows that $\mathbb{Q}(\alpha) \not\subseteq K$ for any root α of f, and thus, $E(K)$ contains no non-trivial points of order 2. □

The following Lemma gives a criterion for a point to be halved:

Lemma 3.3.5 (Knapp [21], Theorem 4.2, p. 85)**.** *Let K be a field of characteristic not equal to 2 or 3, and let E be an elliptic curve over K given by $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ with α, β, γ in K. For $P = (x, y) \in E(K)$, there exists a K-rational point $Q = (x', y')$ on E such that $[2]Q = P$ if and only if $x - \alpha, x - \beta,$ and $x - \gamma$ are all squares in K. In this case, if we fix the sign of $\sqrt{x-\alpha}, \sqrt{x-\beta},$ and $\sqrt{x-\gamma}$, then x' equals one of the following:*

$$\sqrt{x-\alpha}\sqrt{x-\beta} \pm \sqrt{x-\alpha}\sqrt{x-\gamma} \pm \sqrt{x-\beta}\sqrt{x-\gamma} + x$$

or

$$-\sqrt{x-\alpha}\sqrt{x-\beta} \pm \sqrt{x-\alpha}\sqrt{x-\gamma} \mp \sqrt{x-\beta}\sqrt{x-\gamma} + x$$

where the signs are taken simultaneously.

The following lemma gives a bound on when full p-torsion may appear over a number field. Note that the Landau function is the function $g(n)$ which for a given n outputs the largest order element in S_n.

Lemma 3.3.6. *Let $E/\mathbb{Q}$ be an elliptic curve and let $K/\mathbb{Q}$ be a number field of degree n such that E has full p-torsion defined over the Galois closure of K. Then $p-1 \leq g(n)$ where $g(n)$ denotes the Landau function.*

Proof. Let L be the Galois closure of K. If full p-torsion is defined over $E(L)$, then by the existence of the Weil pairing, $\mathbb{Q}(\zeta_p) \subseteq L$. Since L is the Galois closure of a degree n number field, $\mathrm{Gal}(L/\mathbb{Q}) \leq S_n$. By Galois theory we have that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is a quotient of $\mathrm{Gal}(L/\mathbb{Q})$. Thus, we must have an element of order $p-1$ in S_n. Since the highest order element in S_n is given by $g(n)$, it follows that $p-1 \leq g(n)$. □

Here is a table of the first couple values for $g(n)$:

n	1	2	3	4	5	6	7	8
$g(n)$	1	2	3	4	6	6	12	15

The following proposition shows when torsion points over a quartic field K are actually defined over an intermediate quadratic field.

Proposition 3.3.7. *Let $p \equiv 3 \bmod 4$ be a prime with $p \geq 7$. Let $E/\mathbb{Q}$ be an elliptic curve and let $K/\mathbb{Q}$ be a quartic field such that $E(K)_{tors}$ contains a point P of order*

p.

Then either:

- *P is defined over $\mathbb{Q}$, i.e., $P \in E(\mathbb{Q})[p]$*
- *There is $F/\mathbb{Q}$, $F \subseteq K$, $[F:\mathbb{Q}] = 2$ such that $P \in E(F)[p]$.*

Proof. Let L denote the Galois closure of K. Now, consider the Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[p]$ by fixing a basis $\{P, Q\}$ of $E[p]$:

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p).$$

Without loss of generality let P be the point defined over K. Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Then $P^\sigma = \alpha P + \beta Q$ for some $\alpha, \beta \in \mathbb{F}_p$. But since $P^\sigma - \alpha P = P^\sigma + (p-\alpha)P = \beta Q \in E(L)$, it follows that $\beta = 0$ otherwise $E(L)$ would have full p-torsion, which is impossible by Lemma 3.3.6 (notice that $g(4) = 4$). Thus, we have that $P^\sigma \in \langle P \rangle$ for all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. In fact, since $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ it follows that

$$P^\sigma \in \langle P \rangle \text{ for all } \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

Thus, the image of ρ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Suppose

$$\rho(\sigma) = \begin{pmatrix} \varphi(\sigma) & \tau(\sigma) \\ 0 & \psi(\sigma) \end{pmatrix}$$

where φ, ψ are $\mathbb{F}_p$-valued characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\tau : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p$. Notice that if $P^\sigma = aP$, then $\varphi(\sigma) = a$. Thus, we have that the field of definition $\mathbb{Q}(P) = F$ where F is defined by $\ker(\varphi) = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$.

Now we claim that $[\mathbb{Q}(P) : \mathbb{Q}] = \#\operatorname{im}\varphi$ which can be seen as follows: Let H be the subgroup of $G = \operatorname{Gal}(L/\mathbb{Q})$ fixing $\mathbb{Q}(P)$. Then

$$\#\operatorname{im}\varphi = \#\{P^\sigma : \sigma \in G\} = \frac{|G|}{|H|} = [\mathbb{Q}(P) : \mathbb{Q}]$$

Now, since $\operatorname{im}\varphi \leq \mathbb{F}_p^\times$, we have that

$$\#\operatorname{im}\varphi \mid p - 1.$$

Also since $\mathbb{Q}(P) \subseteq K$ we have that

$$\#\operatorname{im}\varphi = [\mathbb{Q}(P) : \mathbb{Q}] \mid [K : Q] = 4.$$

Now, since $p \not\equiv 1 \bmod 4$, it follows that $\#\operatorname{im}\varphi = 1$ or 2, proving the proposition. □

Notice we can make use of this proposition to narrow the list of possible torsion subgroup structures.

Proposition 3.3.8. *The following subgroups do not appear as torsion subgroups over any quartic number field of any elliptic curve defined over* $\mathbb{Q}$*:*

$$\mathbb{Z}/14\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$$

Proof. Let E be an elliptic curve over $\mathbb{Q}$, and let K be a quartic number field. Suppose $E(K) \cong \mathbb{Z}/14\mathbb{Z}$. Suppose further that $E(\mathbb{Q})[2] \neq 0$. If $E(\mathbb{Q})[7] \neq 0$, then E has a rational torsion point of order 14, impossible by the classification of Mazur. Thus,

since $E(K)[7] \neq 0$, Proposition 3.3.7 gives that there exists a quadratic field $F \subseteq K$ such that $E(F)[7] = E(K)[7] \neq 0$. But $E(\mathbb{Q})[2] \neq 0$ implies that $E(F)[2] \neq 0$ implying that $E(F)[14] \neq 0$ which is impossible by the classification of torsion subgroups of elliptic curves defined over $\mathbb{Q}$ over quadratic number fields.
Thus, $E(\mathbb{Q})[2] = 0$. But this contradicts 3.3.4, since $E(K)[2] \neq 0$. Suppose $E(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. By the same argument as above we will reach the same contradiction. □

When the field K is Galois over $\mathbb{Q}$ the following lemma helps to determine when an elliptic curve defined over $\mathbb{Q}$ has an n-isogeny defined over $\mathbb{Q}$:

Lemma 3.3.9. *Let K be a Galois extension of $\mathbb{Q}$, and let E an elliptic curve over $\mathbb{Q}$. If $E(K)[n] \cong \mathbb{Z}/n\mathbb{Z}$, then E has an n-isogeny over $\mathbb{Q}$.*

Proof. Let $\{P, Q\}$ be a $\mathbb{Z}/n\mathbb{Z}$-basis for $E[n]$. Without loss of generality we may assume $P \in E(K)$ and $Q \notin E(K)$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since K is Galois over $\mathbb{Q}$, and $P \in E(K)[n]$, it follows that $P^\sigma \in E(K)[n]$. By assumption, $E(K)[n] = \langle P \rangle$ and thus $P^\sigma \in \langle P \rangle$. Therefore $\langle P \rangle$ is stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, which implies E has an n-isogeny over $\mathbb{Q}$. □

This combined with the complete classification of rational n-isogenies limits the possible torsion subgroups for elliptic curves over $\mathbb{Q}$ in Galois extensions of $\mathbb{Q}$.

Corollary 3.3.10. *Let E be an elliptic curve over $\mathbb{Q}$, and K a Galois extension of $\mathbb{Q}$. If $E(K)$ has a point of order n= 39, 49, 81, 91, 169, then $E(K)[n]$ is not cyclic.*

If we further limit that K is cyclic quartic, then we obtain the following proposition:

Proposition 3.3.11. *Suppose K is a cyclic quartic number field and E is an elliptic curve over $\mathbb{Q}$. Suppose $E(K)$ has a point of order n for some odd n relatively prime to 5. Then $E/\mathbb{Q}$ has an n-isogeny over $\mathbb{Q}$.*

Proof. Choose a basis $\{P, Q\}$ of $E[n]$ such that $P \in E(K)$. Let $G = \mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$. Then $P^\sigma = \alpha P + \beta Q$ for some $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$. Then $(n-\alpha)P + P^\sigma = \beta Q \in E(K)$ so $\beta = 0$, otherwise $E(K)$ would contain full l-torsion for some $l \mid n$, which is impossible since K does not contain any l^{th} roots of unity by Lemma 3.3.3. So, $\langle P\rangle$ is fixed by the action of G, and since the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ factors through G, we have that $\langle P\rangle$ is fixed by the action of the entire group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus, $E/\mathbb{Q}$ has an n-isogeny over $\mathbb{Q}$. □

The following two theorems are useful in looking at how specifically the torsion can grow from $\mathbb{Q}$ to F to K, where F is the intermediate quadratic number field. See the references given for more detail on them.

Theorem 3.3.12 (González-Jiménez, Tornero [11], Theorem 2)**.** *Let $\Phi(1)$ be the set of isomorphism classes of torsion subgroups for an elliptic curve over $\mathbb{Q}$. For a given group $G \in \Phi(1)$, let $\Phi_{\mathbb{Q}}(2, G)$ denote the possible isomorphism classes of $E(F)_{tors}$ for an elliptic curve E such that $E(\mathbb{Q})_{tors} \cong G$ and F a degree 2 extension of $\mathbb{Q}$. For*

$G \in \Phi(1)$, *the set* $\Phi_{\mathbb{Q}}(2, G)$ *is the following:*

G	$\Phi_{\mathbb{Q}}(2, G)$
$\mathcal{C}_1$	$\{\mathcal{C}_1, \mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_7, \mathcal{C}_9\}$
$\mathcal{C}_2$	$\{\mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_8, \mathcal{C}_{10}, \mathcal{C}_{12}, \mathcal{C}_{16}, \mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_{10}\}$
$\mathcal{C}_3$	$\{\mathcal{C}_3, \mathcal{C}_{15}, \mathcal{C}_3 \times \mathcal{C}_3\}$
$\mathcal{C}_4$	$\{\mathcal{C}_4, \mathcal{C}_8, \mathcal{C}_{12}, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_2 \times \mathcal{C}_{12}, \mathcal{C}_4 \times \mathcal{C}_4\}$
$\mathcal{C}_5$	$\{\mathcal{C}_5, \mathcal{C}_{15}\}$
$\mathcal{C}_6$	$\{\mathcal{C}_6, \mathcal{C}_{12}, \mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_3 \times \mathcal{C}_6\}$
$\mathcal{C}_7$	$\{\mathcal{C}_7\}$
$\mathcal{C}_8$	$\{\mathcal{C}_8, \mathcal{C}_{16}, \mathcal{C}_2 \times \mathcal{C}_8\}$
$\mathcal{C}_{10}$	$\{\mathcal{C}_{10}, \mathcal{C}_2 \times \mathcal{C}_{10}\}$
$\mathcal{C}_{12}$	$\{\mathcal{C}_{12}, \mathcal{C}_2 \times \mathcal{C}_{12}\}$
$\mathcal{C}_2 \times \mathcal{C}_2$	$\{\mathcal{C}_2 \times \mathcal{C}_2, \mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_2 \times \mathcal{C}_{12}\}$
$\mathcal{C}_2 \times \mathcal{C}_4$	$\{\mathcal{C}_2 \times \mathcal{C}_4, \mathcal{C}_2 \times \mathcal{C}_8, \mathcal{C}_4 \times \mathcal{C}_4\}$
$\mathcal{C}_2 \times \mathcal{C}_6$	$\{\mathcal{C}_2 \times \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_{12}\}$
$\mathcal{C}_2 \times \mathcal{C}_8$	$\{\mathcal{C}_2 \times \mathcal{C}_8\}$

The next theorem limits the number of $\mathbb{Q}$-isogenies a particular elliptic curve over $\mathbb{Q}$ can have.

Theorem 3.3.13 (Kenku [19] Theorem 2)**.** *There are at most 8* $\mathbb{Q}$*-isomorphism classes of elliptic curves in each* $\mathbb{Q}$*-isogeny class.*

In particular, the various combinations of isogenies are classified in that paper. For example there are only 8 $\mathbb{Q}$-isogeny classes of an elliptic curve if there are eight 2-powered isogenies or four 2-powered isogenies and two 3-powered isogenies (see the

reference for more detail).

The final lemma in this section relate torsion in a quadratic extension to torsion over the base field.

Lemma 3.3.14. *Let E be an elliptic curve defined over F, α square-free in F, $K = F(\sqrt{\alpha})$. If n is odd, then there exists an isomorphism*

$$E(K)[n] \cong E(F)[n] \oplus E^{\alpha}(F)[n].$$

Proof. See Corollary 1.3 (ii) and Lemma 1.4 (ii) in [22] □

3.4 Torsion over Cyclic Quartic Number Fields

In this section we give the proof of Theorem 1.2.13 in a series of propositions and lemmas. We will first bound the structure of the p-Sylow subgroups of $E(K)_{\text{tors}}$ for cyclic quartic number fields K and elliptic curves $E/\mathbb{Q}$. Then, we will prove certain order torsion points cannot appear in $E(K)$. Finally, we will provide examples of elliptic curves over $\mathbb{Q}$ that achieve each prescribed torsion subgroup over a cyclic quartic number field K.

We narrow down the possible torsion subgroups for $E(K)$ with the next proposition:

Proposition 3.4.1. *Let E be an elliptic curve over $\mathbb{Q}$. Let K a cyclic quartic extension of $\mathbb{Q}$. Then*

$$E(K)_{tors} \subseteq (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}) \oplus \mathbb{Z}/9\mathbb{Z} \oplus (\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}) \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z}.$$

Proof. Let $E(K)[p^\infty]$ denote the p-Sylow subgroup of $E(K)$. From [24], we have that

$$S_{\mathbb{Q}}(4) = \{2, 3, 5, 7, 13\}$$

where $S_{\mathbb{Q}}(d)$ is the set of primes p for which there exists a number field K of degree $\leq d$ and an elliptic curve $E/\mathbb{Q}$ such that the order of the torsion subgroup of $E(K)$ is divisible by p. Thus, we have $E(K)[p^\infty] = \{\mathcal{O}\}$ for all primes not in $S_{\mathbb{Q}}(4)$. (Recall that $E(\overline{\mathbb{Q}})[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ for all $m \in \mathbb{N}$.) We will proceed by examining the p-Sylow subgroup for each prime $p = 2, 3, 5, 7, 13$.

$\underline{p = 2}$

From Lemma 3.3.3 we see that full 4-torsion cannot be defined over K. Thus, $E(K)[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^m\mathbb{Z}$ for some m. Notice that if $E(K)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^m\mathbb{Z}$, then $2E(K)[2^\infty] \cong \mathbb{Z}/2^{m-1}\mathbb{Z}$ and so E has a $\mathbb{Q}$-rational isogeny of degree 2^{m-1}. Thus, by Theorem 2.1.11, $m - 1 \leq 4$, and so $m \leq 5$. Thus, we have that $E(K)[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$.

Now, suppose $E(K)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$. Fix a basis $\{P, Q\}$ of $E[32]$ such that $P \in E(K)$. Let

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/32\mathbb{Z})$$

be the Galois representation induced by the action of Galois on $E[32]$. Consider the image of the subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ under ρ, call this image H. Notice that $P^\sigma = P$ for all $\sigma \in H$ since P is defined over K. Further, for $\sigma \in H$, $Q^\sigma = aP + bQ$ for some $a, b \in \mathbb{Z}/32\mathbb{Z}$. Notice however, that $\{16P, 16Q\}$ is a basis for $E[2]$ which is contained in $E(K)$. Thus, for all $\sigma \in H$:

$$16Q = (16Q)^\sigma = 16Q^\sigma = 16aP + 16bQ$$

so we must have that $a \equiv 0 \bmod 2$ and $b \equiv 1 \bmod 2$. Therefore

$$H \subseteq \left\{ \begin{pmatrix} 1 & 2x \\ 0 & y \end{pmatrix} : x \in \mathbb{Z}/32\mathbb{Z}, y \in \mathbb{Z}/32\mathbb{Z}^\times \right\}.$$

Denote $\mathcal{H} := \left\{ \begin{pmatrix} 1 & 2x \\ 0 & y \end{pmatrix} : x \in \mathbb{Z}/32\mathbb{Z}, y \in \mathbb{Z}/32\mathbb{Z}^\times \right\}$.

Now let us consider the full image of ρ, call this image G. Since E has a 16-isogeny over $\mathbb{Q}$, for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ it must be that

$$\rho(\sigma) \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \bmod 16.$$

In fact, $a, d \in (\mathbb{Z}/32\mathbb{Z})^\times$ since $E[2] \subseteq E(K)$ and so

$$\rho(\sigma) \equiv \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \bmod 2.$$

Therefore:

$$\rho(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = G \subseteq \left\{ \begin{pmatrix} a & b \\ 16c & d \end{pmatrix} : a, d \in \mathbb{Z}/32\mathbb{Z}^\times, b, c \in \mathbb{Z}/32\mathbb{Z} \right\}.$$

Denote $\mathcal{G} := \left\{ \begin{pmatrix} a & b \\ 16c & d \end{pmatrix} : a, d \in \mathbb{Z}/32\mathbb{Z}^\times, b, c \in \mathbb{Z}/32\mathbb{Z} \right\}$.

Suppose there exist an elliptic curve E defined over $\mathbb{Q}$ such that $H \leq \mathcal{H}$ and $G \leq \mathcal{G}$, with H normal in G, and G/H isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

If $E/\mathbb{Q}$ does not have CM, then Theorem 2.3.6 shows that the index of G in $\mathrm{GL}(2,\mathbb{Z}/32\mathbb{Z})$ has index dividing 64 or 96. However,

$$1536 = [\mathrm{GL}(2,\mathbb{Z}/32\mathbb{Z}) : \mathcal{H}] \leq [\mathrm{GL}(2,\mathbb{Z}/32\mathbb{Z}) : H]$$

and since $[G : H] = 4$ this gives a lower bound on the index of G:

$$[\mathrm{GL}(2,\mathbb{Z}/32\mathbb{Z}) : G] = [GL(2,\mathbb{Z}/32\mathbb{Z}) : H]/[G : H] \geq \frac{1536}{4} = 384$$

and so such a curve does not exist.

If $E/\mathbb{Q}$ does have CM, then [5] gives a list of all possible isomorphism classes for $E(K)_{\mathrm{tors}}$ for K a quartic field (note that this list is for E/K not necessarily $E/\mathbb{Q}$, and K is any quartic field not necessarily cyclic quartic):

$$E(K)_{\mathrm{tors}} \in \begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{for } N_1 = 1,\ldots,8,10,12,13,21, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z} & \text{for } N_2 = 1,\ldots,5, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z} & \text{for } N_3 = 1,2, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \end{cases}$$

and notice that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$ is not on that list.

Therefore, no such elliptic curve exists, and so $E(K)[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$.

$\underline{p = 3}$

Full 3-torsion cannot be defined over K by Lemma 3.3.3. By Corollary 3.3.10 it follows that $E(K)[3^\infty] \subseteq \mathbb{Z}/27\mathbb{Z}$. By Lemma 3.3.14, we have that $E(K)[27] \cong$

$E(F)[27] \oplus E^\alpha(F)[27]$ for the quadratic intermediate field $F \subseteq F(\sqrt{\alpha}) = K$ for some square-free $\alpha \in F$. The curve E^α may not be defined over $\mathbb{Q}$, but it is certainly defined over F. By the classification of torsion subgroups of elliptic curves defined over quadratics (Theorem 1.2.4), it follows that neither $E^\alpha(F)$ nor $E(F)$ have any points of order 27. Thus, $E(K)$ does not have any points of order 27, and so $E(K)[3^\infty] \subseteq \mathbb{Z}/9\mathbb{Z}$.

$\underline{p = 5}$

It is possible for full 5-torsion to be defined over K in the case that $K = \mathbb{Q}(\zeta_5)$. By Lemma 3.3.14, we have $E(K)[25] \cong E(F)[25] \oplus E^\alpha(F)[25]$ for the quadratic intermediate field $F \subseteq F(\sqrt{\alpha}) = K$ for some square-free $\alpha \in F$. The curve E^α may not be defined over $\mathbb{Q}$, but it is certainly defined over F. By the classification of torsion subgroups of elliptic curves defined over quadratics (Theorem 1.2.4), we have that $E^\alpha(F)[25] \cong \mathbb{Z}/5\mathbb{Z}$ or 0. Similarly, $E(F)[25] \cong \mathbb{Z}/5\mathbb{Z}$ or 0, and thus $E(K)[5^\infty] = E(K)[25] \subseteq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

$\underline{p = 7}$

Again notice that we cannot have full 7-torsion defined over K by Lemma 3.3.3. Now, from Corollary 3.3.10, it follows that $E(K)$ has no points of order 49. Therefore, $E(K)[7^\infty] \subseteq \mathbb{Z}/7\mathbb{Z}$.

$\underline{p = 13}$

Again notice that we cannot have full 13-torsion defined over K by Lemma 3.3.3. Again, from Corollary 3.3.10, it follows that $E(K)$ has no points of order 169, so in fact $E(K)[13^\infty] \subseteq \mathbb{Z}/13\mathbb{Z}$.

□

We wish to see what torsion subgroups are possible when $\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z} \subseteq E(K)_{tors}$, but notice this is only possible when $K = \mathbb{Q}(\zeta_5)$. The following theorem of Bruin and Najman classifies all torsion subgroups that appear over $\mathbb{Q}(\zeta_5)$:

Theorem 3.4.2 (Bruin, Najman, [2], Theorem 5)**.** *Let E be an elliptic curve over $\mathbb{Q}(\zeta_5)$. Then $E(\mathbb{Q}(\zeta_5))_{tors}$ is isomorphic to a subgroup included in Mazur's list over $\mathbb{Q}$ or:*

$$\mathbb{Z}/15\mathbb{Z}, \mathbb{Z}/16\mathbb{Z}, \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}.$$

In particular, if $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \subseteq E(K)_{\text{tors}}$ then, in fact, they are equal. Now we rule out torsion points of certain order.

Lemma 3.4.3. *Let K be a Galois cyclic degree 4 number field, E an elliptic curve over $\mathbb{Q}$. Then $E(K)$ has no points of order 14 or 18.*

Proof. Suppose E has a point of order 18 over K. By Lemma 3.3.4 it follows that E has a point of order 2 over $\mathbb{Q}$. From Proposition 3.4.1, we see that $E(K)[18] \cong \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/18\mathbb{Z}$ or $\mathbb{Z}/18\mathbb{Z}$. In either case, E has a 9-isogeny over $\mathbb{Q}$. Let P be a point of order 9 in $E(K)$ and let $\sigma \in \text{Gal}(K/\mathbb{Q})$. Since $E(K)[9] = \langle P \rangle$ it follows that $P^\sigma = aP$ for some $a \in (\mathbb{Z}/9\mathbb{Z})^\times$. Thus, the orbit of P under $\text{Gal}(K/\mathbb{Q})$ has size dividing 6, and by the Orbit-Stabilizer Theorem and Galois theory, it follows that $[\mathbb{Q}(P) : \mathbb{Q}]$ divides 6. However, since K is degree 4 over $\mathbb{Q}$, and $\mathbb{Q}(P) \subseteq K$, it follows that the field of definition of P is either 1 or 2. In either case, we have a point of order 9 and a point of order 2 in a quadratic extension of $\mathbb{Q}$, giving us a point of order 18 in a quadratic extension of $\mathbb{Q}$. By Theorem 1.2.9, the classification of torsion of elliptic curves defined over $\mathbb{Q}$ over quadratic number fields, we see that this is impossible.
A similar proof shows that $E(K)$ has no points of order 14 (notice $|(\mathbb{Z}/14\mathbb{Z})^\times| = 6$). □

Lemma 3.4.4. *Let K be a Galois cyclic degree 4 number field, E an elliptic curve over $\mathbb{Q}$. Then $E(K)$ has no points of order 21, 26, 35, 39, 40, 45, 48, 63, 65, or 91.*

Proof. Notice that since full 3-torsion and full 13-torsion are not defined over K, Corollary 3.3.10 shows that it is impossible for $E(K)$ to contain a point of order 39 or 91. In this proof we will make repeated use Theorem 2.1.11.

$\underline{n = 21}$

If $E(K)$ has a point of order 21, then $E(K)[21] \cong \mathbb{Z}/21\mathbb{Z}$. Thus, by Lemma 4.2.4 E has a 21-isogeny over $\mathbb{Q}$. There are only finitely many isomorphism classes of elliptic curves with a 21-isogeny over $\mathbb{Q}$. Using division polynomials, we see that none of these curves have an x-coordinate of a 21-torsion point defined in a quadratic or quartic number field. Thus, it is impossible for E to have 21-torsion over a quartic number field.

$\underline{n = 26}$

If $E(K)$ has a point of order 26, then $E(K)[26]$ is isomorphic to either $\mathbb{Z}/26\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$. The first case implies the existence of a 26-isogeny over $\mathbb{Q}$, which is impossible. If $E(K)[26] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$, then by Lemma 3.3.4 the curve E has a 2-isogeny over $\mathbb{Q}$. Further, E has a 13-isogeny over $\mathbb{Q}$. This implies there is an elliptic curve over $\mathbb{Q}$ with a 26-isogeny over $\mathbb{Q}$, which again is impossible.

$\underline{n = 35}$

If $E(K)$ has a point of order 35, then $E(K)[35]$ is isomorphic to either $\mathbb{Z}/35\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/35\mathbb{Z}$. The first case implies the existence of a 35-isogeny over $\mathbb{Q}$, which is impossible, and the second case is ruled out by 3.4.2.

$\underline{n = 40}$

If $E(K)$ has a point of order 40, then $E(K)[40]$ is isomorphic to either $\mathbb{Z}/40\mathbb{Z}$ or

$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/40\mathbb{Z}$. In either case, this implies a 20-isogeny over $\mathbb{Q}$, which is impossible.

$\underline{n = 45}$

If $E(K)$ has a point of order 45, then $E(K)[45]$ is isomorphic to either $\mathbb{Z}/45\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/45\mathbb{Z}$. The first case implies the existence of a 45-isogeny over $\mathbb{Q}$, which is impossible, and the second case is ruled out by 3.4.2.

$\underline{n = 48}$

If $E(K)$ has a point of order 48, then $E(K)[48]$ is isomorphic to either $\mathbb{Z}/48\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/48\mathbb{Z}$. In either case, this implies a 24-isogeny over $\mathbb{Q}$, which is impossible.

$\underline{n = 63}$

If $E(K)$ has a point of order 63, then $E(K)[63]$ is isomorphic to $\mathbb{Z}/63\mathbb{Z}$, but this implies the existence of a 63-isogeny over $\mathbb{Q}$, which is impossible.

$\underline{n = 65}$

If $E(K)$ has a point of order 65, then $E(K)[65]$ is isomorphic to either $\mathbb{Z}/65\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/65\mathbb{Z}$. The first case implies the existence of a 65-isogeny over $\mathbb{Q}$, which is impossible, and the second case is ruled out by 3.4.2.

□

We separate the next two lemmas from the above because their proofs are more involved.

Lemma 3.4.5. *Let K be a cyclic quartic 4 number field, and let E an elliptic curve over $\mathbb{Q}$. Then $E(K)$ has no points of order 20.*

Proof. Notice that, as a consequence of Theorem 4.2.4 and Lemma 2.1.11, it is impossible for $E(K)[20] \cong \mathbb{Z}/20\mathbb{Z}$. Thus, if $E(K)$ has a point of order 20, then by Proposition 3.4.1, $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$.

Let $\mathbb{Q} \subset F \subset K$ denote the chain of number fields in K, where F is the unique intermediate quadratic number field. To prove that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$ torsion is impossible, we will break up the argument into different cases based on $E(F)_{\text{tors}}$ and subsequently $E(\mathbb{Q})_{\text{tors}}$.

Suppose $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$. Notice, since $E(K)[5] \cong \mathbb{Z}/5\mathbb{Z}$ we have by Lemma 4.2.4 that E has a 5-isogeny over $\mathbb{Q}$. Kenku's classification of $\mathbb{Q}$-isomorphism classes of elliptic curves (Theorem 3.3.13) states that if E has a 5-isogeny over $\mathbb{Q}$, then E has at most one $\mathbb{Q}$-rational subgroup of order 2. Therefore, $E(\mathbb{Q})[2] \subseteq \mathbb{Z}/2\mathbb{Z}$. Further, since $E(K)[2] \neq \{\mathcal{O}\}$, Lemma 3.3.4 gives that in fact $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. Thus given that $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$ we have that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/10\mathbb{Z}$.

Theorem 3.3.12 classifies precisely how certain torsion over $\mathbb{Q}$ can grow in a quadratic extension of $\mathbb{Q}$. So given that $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$, we have the following five possibilities for $E(F)_{\text{tors}}$:

$$\mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/10\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}.$$

Notice that if full 2-torsion is not defined over F, then the field extension adjoining the second 2-torsion point is $K = F(\sqrt{\triangle_E})$, which is a biquadratic extension, not a cyclic quartic extension. Therefore we need only consider when $F = \mathbb{Q}(\sqrt{\triangle_E})$ and

$$E(F)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \text{ or } \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}.$$

In either case, $E(F)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and so E gains a point of order 4 in K.

Since $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$, there exists a model for E of the form

$$E : y^2 = x(x^2 + bx + c).$$

Suppose first that the point of order 4 is Q, and $2Q = P = (0, 0)$. By Lemma 4.4.7, we have that the following are squares in K:

$$0, \frac{b + \sqrt{b^2 - 4c}}{2}, \frac{b - \sqrt{b^2 - 4c}}{2}.$$

That is, $K = F(\sqrt{\frac{b+\sqrt{b^2-4c}}{2}}, \sqrt{\frac{b-\sqrt{b^2-4c}}{2}}) = F(\sqrt{2b + 2\sqrt{m}}, \sqrt{2b - 2\sqrt{m}})$ where $m = b^2 - 4c \neq 0$ since $\triangle_E \neq 0$. By Lemma 3.3.1 we must have

$$\frac{(2b)^2}{m} - 2^2 = 1$$

and so $(2b)^2 = 5m$. Thus $m = 2^2 \cdot 5 \cdot t^2$ for some $t \in \mathbb{Q}$ and so $b = 5t$. Further, $m = 2^2 \cdot 5 \cdot t^2$ and so $25t^2 - 4c = 20t^2$. Thus, $4c = 5t^2$. Substituting $t = 2s$ gives $b = 10s$ and $c = 5s^2$. That is, we obtain a 1-parameter family of elliptic curves such that the 2-power-torsion grows:

$$\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

over $\mathbb{Q} \to F \to K$. However, all the curves in this 1-parameter family have the same j-invariant, namely $j(E) = 78608$, and thus are all isomorphic over $\mathbb{Q}$. Now, if one of them acquired $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$ over a cyclic quartic, then, in particular, there would be a 5-isogeny over $\mathbb{Q}$ for said curve. But 5-isogenies is an isomorphism invariant property, and so the entire family of curves would posses a 5-isogeny over

$\mathbb{Q}$. However, we can check that $\Phi_5(X, 78608)$ has no rational roots, where $\Phi_5(X, Y)$ is the 5^{th} classical modular polynomial, so this family does not have a 5-isogeny over $\mathbb{Q}$.

Now, suppose one of the other 2-torsion points is halved. Then, $2Q = P = (\frac{-b\pm\sqrt{b^2-4c}}{2}, 0)$. By Lemma 4.4.7 we have that the following are squares in K:

$$\frac{-b \pm \sqrt{b^2-4c}}{2}, \pm\sqrt{b^2-4c}.$$

However, it is easy to see by Lemma 3.3.1 that the field $K = F(\sqrt{\pm\sqrt{b^2-4c}})$ is not a cyclic quartic number field. Therefore, it is impossible for E to have torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$ over a cyclic quartic number field. □

Lemma 3.4.6. *Let K be a Galois cyclic degree 4 number field, E an elliptic curve over $\mathbb{Q}$. Then $E(K)$ has no points of order 24.*

Proof. Notice that by a simple consequence of Theorem 4.2.4 and Lemma 2.1.11 it is impossible for $E(K)[24] \cong \mathbb{Z}/24\mathbb{Z}$. Thus, if $E(K)$ has a point of order 24, then by Proposition 3.4.1, $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$.

Let $\mathbb{Q} \subset F \subset K$ denote the chain of number fields in K, where F is the unique intermediate quadratic number field. To prove that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$ torsion is impossible, we will break up the argument into different cases based on $E(F)_{\text{tors}}$ and subsequently $E(\mathbb{Q})_{\text{tors}}$.

Suppose $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$. Notice, since $E(K)[3] \cong \mathbb{Z}/3\mathbb{Z}$ we have by Lemma 4.2.4 that E has a 3-isogeny over $\mathbb{Q}$. Kenku's classification of $\mathbb{Q}$-isomorphism classes of elliptic curves (Theorem 3.3.13) states that if E has a 3-isogeny over $\mathbb{Q}$, then E has at most four $\mathbb{Q}$-rational subgroups of order a power of 2 (including $\{\mathcal{O}\}$).

Further, given that $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$ it follows that

$$E(\mathbb{Q})[2^\infty] \cong \begin{cases} \{\mathcal{O}\}, \\ \mathbb{Z}/2\mathbb{Z}, \\ \mathbb{Z}/4\mathbb{Z}, \\ \mathbb{Z}/8\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}. \end{cases}$$

We can rule out $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ because it has six subgroups of order a power of 2 and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ because it has eight. We can further rule of $E(\mathbb{Q})[2^\infty] \cong \mathbb{Z}/8\mathbb{Z}$ since then E would have an 8-isogeny over $\mathbb{Q}$, and thus a 24-isogeny over $\mathbb{Q}$, which is impossible. We can rule out $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ because this yields four cyclic-subgroups defined over $\mathbb{Q}$ of 2-power order (three of order 2 and the trivial subgroup), but since we know $E(K)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, it follows that E has a 4-isogeny over $\mathbb{Q}$, and therefore at least one more cyclic-subgroup defined over $\mathbb{Q}$. Finally, Lemma 3.3.4 rules out $E(\mathbb{Q})[2^\infty] \cong \{\mathcal{O}\}$. Thus,

$$E(\mathbb{Q})[2^\infty] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, \\ \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

Theorem 3.3.12 classifies precisely how certain torsion over $\mathbb{Q}$ can grow in a

quadratic extension of $\mathbb{Q}$. This gives the following possibilities for $E(F)[2^\infty]$:

$$\mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Again, notice that if full 2-torsion is not defined over F, then $K = F(\sqrt{\triangle_E})$, and so K is a biquadratic number field, not a cyclic quartic number field. Thus we need only consider

$$E(F)[2^\infty] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \end{cases} .$$

Case 1: Suppose $E(F)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then it must follow that $E(\mathbb{Q})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z}$, and so we have a model for E of the form

$$y^2 = x(x^2 + bx + c).$$

Following an identical argument to that of Lemma 3.4.5, it must be that the point that is halved in K is (0,0). We again find a 1-parameter family of curves with torsion $E(\mathbb{Q})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z}$ and $E(F)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ that gains a point of order 4 in a cyclic quartic extension K all with j-invariant 78608. We check that $\Phi_3(X, 78608)$ has no rational roots, where $\Phi_3(X, Y)$ is the 3^{rd} classical modular polynomial, and therefore these curves have no 3-isogeny over $\mathbb{Q}$.

Case 2: Suppose $E(F)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. From Theorem 3.3.12 we have $E(\mathbb{Q})[2^\infty] \cong \mathbb{Z}/4\mathbb{Z}$.

Since $E(\mathbb{Q})[2^\infty] \cong \mathbb{Z}/4\mathbb{Z}$, we have a model for E of the form:

$$y^2 = x(x^2 + bx + c)$$

and $F = \mathbb{Q}(\sqrt{m})$, where $m = b^2 - 4c$, and $E(\mathbb{Q})[4] = \{\mathcal{O}, (\sqrt{c}, y'), (0,0), (-\sqrt{c}, y'')\}$. Let $P = (d, y_0) \in E(\mathbb{Q})$ be the point of order 4 that is halved in K ($d = \sqrt{c}$ or $-\sqrt{c}$). Then by lemma 4.4.7 it follows that $K = F(\sqrt{d}, \sqrt{2d + 2b - 2\sqrt{m}}, \sqrt{2d + 2b + 2\sqrt{m}})$. Now using lemma 3.3.1, K is quartic cyclic if and only if

$$\frac{(2d + 2b)^2}{m} - 4 = 1$$

We see that $(2d + 2b)^2 = 5m$ so $4(d + b)^2 = 5m$ and thus $m = 2^2 \cdot 5 \cdot t^2$ for some $t \in \mathbb{Q}$. Thus $b^2 - 4c = 20t^2$. Further, $d + b = 5t$, and so $b = 5t - d = 5t \pm \sqrt{c}$, and so $(5t \pm \sqrt{c})^2 - 4c = 20t^2$ simplifying to

$$3c \pm 10t\sqrt{c} - 5t^2 = 0$$

or

$$3d^2 \pm 10td - 5t^2 = 0.$$

Solving for d yields:

$$d = \frac{\pm 5t \pm 2t\sqrt{10}}{3}.$$

Further, $d \neq 0$, since otherwise $t = 0$, implying $\triangle_E = 0$. So, this contradicts that $d \in \mathbb{Q}$. Therefore, it is impossible for $E(F)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Case 3: Suppose $E(F)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. From Theorem 3.3.12 we have

$E(\mathbb{Q})[2^\infty] \cong \mathbb{Z}/4\mathbb{Z}$.

Notice that since full 2-torsion is defined over F but not $\mathbb{Q}$ that $F = \mathbb{Q}(\triangle_E)$ where $\triangle_E$ is the discriminant of E. We may search the Rouse, Zureich-Brown database [31] for all families of elliptic curves (without CM) whose 2-adic image satisfies $E(\mathbb{Q})[2^\infty] \cong \mathbb{Z}/4\mathbb{Z}$ and $E(\mathbb{Q}(\triangle_E))[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. These families are:

X102k, X195h, X197f, X202e, X213k, X223b, X230h, X235f

Now, taking a representative from these families and computing the isogenies of the curve shows that all of the curves in each of these families has an 8-isogeny over $\mathbb{Q}$. But since we are assuming $E(K)[3] \cong \mathbb{Z}/3\mathbb{Z}$, these curves have both an 8-isogeny and a 3-isogeny over $\mathbb{Q}$, thus giving a curve with a 24-isogeny over $\mathbb{Q}$, which is impossible by Theorem 2.1.11.

If $E/\mathbb{Q}$ does have CM, then [5] gives a list of all possible isomorphism classes for $E(K)_{\text{tors}}$ for K a quartic field (note that this list is for E/K not necessarily $E/\mathbb{Q}$, and K is any quartic field not necessarily cyclic quartic):

$$E(K)_{\text{tors}} \in \begin{cases} \mathbb{Z}/m\mathbb{Z} & \text{for } N_1 = 1, \ldots, 8, 10, 12, 13, 21, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z} & \text{for } N_2 = 1, \ldots, 5, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z} & \text{for } N_3 = 1, 2, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, & \end{cases}$$

and notice that none of these groups have a point of order 24.

Therefore, it is impossible for an elliptic curve defined over $\mathbb{Q}$ to have a point of order 24 in a cyclic quartic extension of $\mathbb{Q}$.

□

Thus, the possible isomorphism classes for $E(K)_{tors}$ for an elliptic curve over $\mathbb{Q}$ and a cyclic quartic number field K is a subset of

$$\begin{aligned} &\mathbb{Z}/N_1\mathbb{Z}, && N_1 = 1, \ldots, 16, N_1 \neq 11, 14, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, && N_2 = 1, \ldots, 6, 8, \\ &\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}. \end{aligned}$$

and the examples given in the next section show that precisely all of these groups occur.

3.5 Examples

In this section we provide examples of an elliptic curve E defined over $\mathbb{Q}$ with prescribed torsion over a quartic Galolis number field.

The first table gives an elliptic curve E defined over $\mathbb{Q}$ and a polynomial f such that $K = \mathbb{Q}(\alpha)$ is a cyclic quartic number field for α a root of f, and $E(K)_{tors} \cong G$ for each group G appearing in Theorem 1.2.13 not appearing in Mazur's list completing the proof of Theorem 1.2.13.

G	E	$f(x)$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$	[1,0,0,-828,9072]	$x^4 - 20x^2 + 10$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$	[1,0,0,-5557266,-3547208700]	$13x^4 - 26x^2 + 4$
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$	[1,1,1,-5,2], $15a3$	$x^4 - 3x^3 - 6x^2 + 18x - 9$
$\mathbb{Z}/13\mathbb{Z}$	[1, 0, 1, 266982, 42637516]	$x^4 + 5688x^3 - 187682160510x^2 + 3933601303888x - 6842546623573620597$
$\mathbb{Z}/15\mathbb{Z}$	[1,1,1,-3,1], $50b1$	$x^4 - 10x^2 + 5$
$\mathbb{Z}/16\mathbb{Z}$	[1,1,1,0,0], $15a8$	$x^4 + 3x^3 + 4x^2 + 2x + 1$
$\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$	[0,-1,1,-10,-20], $11a1$	$x^4 + x^3 + x^2 + x + 1$

Now we finish the proof of Theorem 1.2.12 by proving that each subgroup listed, except for $\mathbb{Z}/15\mathbb{Z}$ appears for infinitely many non-isomorphic rational elliptic curves over some quartic Galois number field.

First, notice that, by Lemma 3.2.1, any group appearing infinitely often over a quadratic number field, as in Theorem 1.2.9, must also appear infinitely often over quartic Galois number fields.

The following two theorems of Jeon, Kim, Lee give infinite families of elliptic curves defined over $\mathbb{Q}$ that have torsion subgroup $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, respectively, over a biquadratic field.

Theorem 3.5.1 ([15], Theorem 4.10)**.** *Let $K = \mathbb{Q}(\sqrt{-1}, \sqrt{t^4 - 6t^2 + 1})$ with $t \in \mathbb{Q}$ and $t \neq 0, \pm 1$, and let E be an elliptic curve defined by the equation*

$$y^2 + xy - (\nu^2 - \frac{1}{16})y = x^3 - (\nu^2 - \frac{1}{16})x^3,$$

where $\nu = \frac{t^4-6t^2+1}{4(t^2+1)^2}$. *Then the torsion subgroup of* E *over* K *is equal to* $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ *for almost all* t.

Theorem 3.5.2 ([15], Theorem 4.11)**.** *Let* $K = \mathbb{Q}(\sqrt{-3}, \sqrt{8t^3+1})$ *with* $t \in \mathbb{Q}$ *and* $t \neq 0, 1, -\frac{1}{2}$, *and let* E *be an elliptic curve defined by the equation*

$$y^2 = x^3 - 27\mu(\mu^3+8)x + 54(\mu^6 - 20\mu^3 - 9),$$

where $\mu = \frac{2t^3+1}{3t^2}$. *Then the torsion subgroup of* E *over* K *is equal to* $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ *for almost all* t.

We now prove that there are infinitely many elliptic curves defined over $\mathbb{Q}$ with non-trivial 13-torsion over some cyclic quartic field.

Proposition 3.5.3. *There exists infinitely many elliptic curves* $E/\mathbb{Q}$ *such that there exists a cyclic quartic field* K *such that* $E(K)$ *has a 13-torsion point.*

Proof. Let $\Delta = \{\pm 1, \pm 5\} \subseteq (\mathbb{Z}/13\mathbb{Z})^\times$. Let $X_\Delta(13)$ be the modular curve defined over $\mathbb{Q}$ associated to the congruence subgroup:

$$\Gamma_\Delta(13) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \ a \bmod 13 \in \Delta, 13 \mid c \right\}$$

Then by [14] (Theorem 1.1 and Table 1), $X_\Delta(13)$ has genus 0. The example of the curve achieving torsion subgroup $\mathbb{Z}/13\mathbb{Z}$ over a cyclic quartic field in the Table above shows that $X_\Delta(13)(\mathbb{Q})$ (and hence $Y_\Delta(13)(\mathbb{Q})$) has infinitely many points. Now let $(E, \langle P \rangle)$, where $E/\mathbb{Q}$ and $\langle P \rangle$ is a 13-cycle of E, be a point on $X_\Delta(13)(\mathbb{Q})$. Consider

the Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/13\mathbb{Z})$$

induced by the action of Galois on a basis $\{P, R\}$ of $E[13]$. Then we have, for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$\rho(\sigma) = \begin{pmatrix} \varphi(\sigma) & * \\ 0 & * \end{pmatrix}$$

Let K be the field of definition of P. Notice that $\ker\varphi = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, and so in particular we have Image $\varphi \cong \mathrm{Gal}(K/\mathbb{Q})$. By our choice of Δ it must be that for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$P^\sigma \in \{\pm P, \pm 5P\}.$$

Thus, σ acts on $\langle P \rangle$ by multiplication by an element of order dividing 4. In fact, there must exist a $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that acts on $\langle P \rangle$ by an element of order exactly 4, since otherwise Image φ has size 2 or 1, implying that the degree of K over $\mathbb{Q}$ is 2 or 1. However, by Theorem 1.2.9 it is impossible for an elliptic curve over $\mathbb{Q}$ to have a 13-torsion point defined over a quadratic number field. Thus, $\mathrm{Gal}(K/\mathbb{Q}) \cong$ Image $\varphi \cong \{\pm 1, \pm 5\} \cong \mathbb{Z}/4\mathbb{Z}$, and the proposition is complete. □

The group $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ appears for infinitely many non-isomorphic curves over the cyclic quartic field $\mathbb{Q}(\zeta_5)$, shown in Theorem 1.1 of [12].

Finally we show an infinite family of elliptic curves such that there exists a bi-quadratic number field K with $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ using the construction given in [10] Section 5.

Proposition 3.5.4. *Let E be the elliptic curve given by $y^2 = x(x+(t^2-1)^4)(x+(2t)^4)$,*

where $t > 1$ is an integer, and $K = \mathbb{Q}(\sqrt{t(t^2-1)}, \sqrt{(t^2-1)(t^2+1)(t^2+2t-1)})$. Then $E(K)_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$.

Proof. The curve E fulfills the criteria put forth in [10] Section 5 Case 1.(II) with $u = t^2 - 1$, $v = 2t$, and $w = t^2 + 1$. Notice that $\sqrt{-1} \notin K$ because, since $t > 1$, K is totally real. Therefore $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$. □

Finally it remains to be remarked as to why $\mathbb{Z}/15\mathbb{Z}$ only appears finitely often as the torsion subgroup of rational elliptic curves over quartic Galois number fields. This follows from Lemma 4.2.4 and the fact that there are only finitely many j-invariants of elliptic curves over $\mathbb{Q}$ having a $\mathbb{Q}$-rational15-isogeny.

Chapter 4

Maximal Abelian Extension of $\mathbb{Q}$ Classification

4.1 Overview

In this chapter we present the proof to the following theorem (Theorem 1.3.5)

Theorem 4.1.1. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}^{ab})_{\text{tors}}$ is isomorphic to one of the following groups:*

$$\begin{aligned}
&\mathbb{Z}/N_1\mathbb{Z}, && N_1 = 1,3,5,7,9,11,13,15,17,19,21,25,27,37,43,67,163,\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, && N_2 = 1,2,\ldots,9,\\
&\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3N_3\mathbb{Z}, && N_3 = 1,3,\\
&\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4N_4\mathbb{Z}, && N_4 = 1,2,3,4,\\
&\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},\\
&\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z},\\
&\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.
\end{aligned}$$

Each of these groups appear as $E(\mathbb{Q}^{ab})_{\text{tors}}$ for some elliptic curve over $\mathbb{Q}$.

As mentioned before, this implies the following Corollary:

Corollary 4.1.2. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $\#E(\mathbb{Q}^{ab})_{\text{tors}} \leq 163$. This bound is sharp, as the curve $26569a1$ has a point of order 163 over $\mathbb{Q}^{ab}$.*

In section 4.2 we discuss what is known about isogenies of elliptic curves over $\mathbb{Q}$. We then discuss the intimate connection between isogenies and torsion points over $\mathbb{Q}^{ab}$. In section 4.3 we use the results from section 4.2 to prove bounds on the group $E(\mathbb{Q}^{ab})_{\text{tors}}$ based on the isogenies E has over $\mathbb{Q}$. In section 4.4 we further refine the bounds to eliminate the possibility of any group not appearing in Theorem 1.3.5. Finally, section 4.5 has, for each subgroup T appearing in Theorem 1.3.5, an example of an elliptic curve $E/\mathbb{Q}$ such that $E(\mathbb{Q}^{ab})_{\text{tors}} \cong T$ completing the proof of Theorem 1.3.5.

4.2 Isogenies and Torsion

The classification of torsion of elliptic curves $E/\mathbb{Q}$ over $\mathbb{Q}^{ab}$ relies heavily on the classification of $\mathbb{Q}$-rational n-isogenies, Theorem 2.1.11 and Theorem 3.3.13.

The first connection between isogenies and points over $\mathbb{Q}^{ab}$ is shown in the following Lemma.

Lemma 4.2.1. *If $E/\mathbb{Q}$ has an n-isogeny defined over $\mathbb{Q}$ then $E(\mathbb{Q}^{ab})$ has a point of order n.*

Proof. Let φ denote the n-isogeny over $\mathbb{Q}$. Then $\ker(\varphi) = \langle P \rangle$ for some point $P \in E(\overline{\mathbb{Q}})$ of order n such that $\langle P \rangle^\sigma = \langle P \rangle$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This induces a character

$$\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

defined by $\sigma \mapsto a \bmod n$ where a is given by $\sigma(P) = aP$. The kernel of ψ is precisely $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(P))$, and thus we have that $\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, and hence abelian. Therefore, $P \in E(\mathbb{Q}^{ab})$. □

Given an elliptic curve $E/\mathbb{Q}$, due to Ribet's theorem we know that there exists $m, n \in \mathbb{Z}^{\geq 0}$ such that $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$. We wish to understand what possible m and n can occur together.

In regards to the values of m, normally one could use an argument via the Weil-pairing which implies that our field must contain ζ_m, however this is not very restrictive when looking at torsion over $\mathbb{Q}^{ab}$. Instead, we have the following Theorem:

Theorem 4.2.2 (González-Jiménez, Lozano-Robledo; [12], Theorem 1.1)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. If there is an integer $n \geq 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then*

$n = 2, 3, 4,$ *or* 5. *More generally, if* $\mathbb{Q}(E[n])/\mathbb{Q}$ *is abelian, then* $n = 2, 3, 4, 5, 6,$ *or* 8. *Moreover,* $\mathrm{Gal}(\mathbb{Q}(E[n]/\mathbb{Q})$ *is isomorphic to one of the following groups:*

n	2	3	4	5	6	8
$\mathrm{Gal}(\mathbb{Q}(E[n]/\mathbb{Q})$	$\{0\}$ $\mathbb{Z}/2\mathbb{Z}$ $Z/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$ $(\mathbb{Z}/2\mathbb{Z})^4$	$\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/4\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$	$(\mathbb{Z}/2\mathbb{Z})^4$ $(\mathbb{Z}/2\mathbb{Z})^5$ $(\mathbb{Z}/2\mathbb{Z})^6$

Furthermore, each possible Galois group occurs for infinitely many distinct j*-invariants.*

In fact, if $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$, both values m and n are controlled primarily by isogenies. For instance, in the proof of Theorem 4.2.2, González-Jiménez and Lozano-Robledo make use of a key corollary relating full-p-torsion over $\mathbb{Q}^{ab}$ to $\mathbb{Q}$-rational p-isogenies:

Corollary 4.2.3 (González-Jiménez, Lozano-Robledo; [12], Corollary 3.9)**.** *Let* $E/\mathbb{Q}$ *be an elliptic curve, let* $p > 2$ *be a prime, and suppose that* $\mathbb{Q}(E[p])/\mathbb{Q}$ *is abelian. Then, the* $\mathbb{Q}$*-isogeny class of* E *contains at least three distinct* $\mathbb{Q}$*-isomorphism classes, and* $C_p(E) \geq 3$*. In particular* $p \leq 5$*.*

In particular, the proof of Corollary 2.4 in [12] shows that for all ptimes $p > 2$ if $\mathbb{Q}(E[p])/\mathbb{Q}$ is abelian for some $E/\mathbb{Q}$, then E has two independent p-isogenies over $\mathbb{Q}$.

Note that we can see in ([12], Table 1) a complete table showing which CM curves can have $\mathbb{Q}(E[n])$ abelian for which n. We also have the following lemma to help understand the possible values of n.

Lemma 4.2.4. *Let K be a Galois extension of $\mathbb{Q}$, and let E an elliptic curve over $\mathbb{Q}$. If $E(K)_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$, then E has an n-isogeny over $\mathbb{Q}$.*

Proof. Suppose $E(K)_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z} = \langle P, Q \rangle$ where P has order m and Q has order mn. Then $[m]E(K)_{\text{tors}} = \langle mP, mQ \rangle = \langle mQ \rangle \cong \mathbb{Z}/n\mathbb{Z}$. Let $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since K is Galois over $\mathbb{Q}$ and E is defined over $\mathbb{Q}$, the action of Galois commutes with multiplication by m and n. It follows that $(mQ)^\sigma \in E(K)[n] = \langle mQ \rangle$. Thus, $\langle mQ \rangle$ is a cyclic subgroup of order n that is stable under the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, which implies E has an n-isogeny over $\mathbb{Q}$. □

Thus, the possible values for m (up to a power of 2) and n are controlled by the $\mathbb{Q}$-isogenies of the elliptic curve. In order to understand 2-powered torsion we use the database of Rouse and Zureick-Brown [31] to understand $E(\mathbb{Q}^{ab})[2^\infty]$. First we prove a lemma concerning quadratic twists.

Lemma 4.2.5. *Let $E/\mathbb{Q}$ be an elliptic curve, let d be a square-free integer, and let E_d denote the quadratic twist of E by d. Then $E(\mathbb{Q}^{ab})_{\text{tors}} \cong E_d(\mathbb{Q}^{ab})_{\text{tors}}$.*

Proof. Since E and E_d become isomorphic over $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}^{ab}$ for any d, the lemma follows immediately. □

Note that the minimal field of definition of the torsion for E and E_d may differ, but by the Lemma their torsion over $\mathbb{Q}^{ab}$ will always be isomorphic. In particular, when examining elliptic curves with j-invariant not equal to 0 or 1728, it suffices to fix a specific curve E, and examine $E(\mathbb{Q}^{ab})_{\text{tors}}$.

We now prove a proposition about 2-powered torsion

Proposition 4.2.6. *Let $E/\mathbb{Q}$ be an elliptic curve. Table 4.1 gives the possibilities for $E(\mathbb{Q}^{ab})[2^\infty]$, the 2-powered isogenies attached to each case, and also $C_2(E)$.*

$E(\mathbb{Q}^{ab})[2^\infty]$	Isogeny Degrees	$C_2(E)$
$\{\mathcal{O}\}$	1	1
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	1 1, 2	1 2
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	1, 2 1, 2, 4, 4	2 4
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	1, 2, 4, 4 1, 2, 4, 4, 8, 8	4 6
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	1, 2, 2, 2 1, 2, 4, 4	4 4
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$	1, 2, 4, 4, 8, 8, 16, 16	8
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	1, 2, 2, 2, 4, 4 1, 2, 4, 4, 8, 8, 8, 8	6 8
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$	1, 2, 2, 2, 4, 4, 8, 8	8
$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	1, 2, 2, 2, 4, 4, 4, 4	8

TABLE 4.1: Possible 2-primary torsion over $\mathbb{Q}^{ab}$

Proof. If E does not have CM, it must be in one of the families given in the Rouse, Zureick-Brown database [31]. We compute for each family the 2-powered torsion over $\mathbb{Q}^{ab}$. We do this as follows: for each family let G be the image of $\rho_{E,32}$, that is $G = \rho_{E,32}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$. In fact,

$$G = \rho_{E,32}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \cong \mathrm{Gal}(\mathbb{Q}(E[32])/\mathbb{Q})$$

since $\ker \rho_{E,32} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[32]))$. Then the commutator subgroup $[G, G]$ has fixed field equal to $\mathbb{Q}(E[32]) \cap \mathbb{Q}^{ab}$. We fix a $\mathbb{Z}/32\mathbb{Z}$-basis $\{P, Q\}$ of $E[32]$ and identify G with a subgroup of $\mathrm{GL}(2, \mathbb{Z}/32\mathbb{Z})$. We then compute the vectors fixed in $(\mathbb{Z}/32\mathbb{Z})^2$ by $[G, G]$ which gives the structure of the points on E defined over $\mathbb{Q}(E[32]) \cap \mathbb{Q}^{ab}$, that is the structure of $E(\mathbb{Q}^{ab})[32]$. Here, a vector $[a, b] \in (\mathbb{Z}/32\mathbb{Z})^2$ corresponds to a point $aP + bQ \in E[32]$. Since the largest order point found in $E(\mathbb{Q}^{ab})[32]$ has order 16, we see that $E(\mathbb{Q}^{ab})[2^\infty] = E(\mathbb{Q}^{ab})[16]$.

For elliptic curves with CM we examine the finitely many j-invariants over $\mathbb{Q}$ (see Table 1 [12]). Note that the table is broken up into quadratic twist families, and so by Lemma 4.2.5 it suffices to fix a single curve within each family and examine its torsion over $\mathbb{Q}^{ab}$.

Let E be such a curve. From that table we can see the largest m such that $\mathbb{Q}(E[2^m])$ is abelian, as well as the isogenies each $\mathbb{Q}$-isomorphism class has. Let 2^n denote the largest degree 2-powered isogeny E has. Then from Lemma 4.2.4 it follows that $E(\mathbb{Q}^{ab})[2^\infty] \subseteq \mathbb{Z}/2^m\mathbb{Z} \times \mathbb{Z}/2^{n+m}\mathbb{Z}$.

Thus, to find the structure of $E(\mathbb{Q}^{ab})[2^\infty]$ it simply remains to find the largest 2-powered torsion E has over some abelian number field, up to 2^{n+m}. We do this by using the division polynomial method. For each $0 < k \leq n+m$ we use MAGMA to compute the $(2^k)^{\text{th}}$-division polynomial of E, whose roots are the x-coordinates of the points of order 2^k on E. From the x-coordinates, we can compute the corresponding y-coordinates, and get a list of all points of order 2^k on E. Now we simply compute the field of definition of these points and check whether each field is abelian or not. If k_0 is the first value where no points of order 2^{k_0} are defined over an abelian extension, then $E(\mathbb{Q}^{ab})[2^\infty] \cong \mathbb{Z}/2^m \times \mathbb{Z}/2^{k_0-1}\mathbb{Z}$.

We run through each quadratic twist family. Once computed we find that we do not gain any new groups nor do we add any new 2-powered isogeny degree combinations to the list originally found for non-CM curves. Note that the code used to do these compositions is available on the author's website. □

From Table 4.1 we can make a simple observation

Lemma 4.2.7. *Let $E/\mathbb{Q}$ be an elliptic curve and suppose that $E(\mathbb{Q}^{ab})[2^\infty] \ncong \{\mathcal{O}\}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then E has at least one 2-isogeny, that is, $C_2(E) \geq 2$.*

4.3 Bounding Torsion

We begin with a proposition that bounds $E(\mathbb{Q}^{ab})[p^\infty]$ for all primes p.

Proposition 4.3.1. *Let $E/\mathbb{Q}$ be an elliptic curve, and $\mathbb{Q}^{ab}$ be the maximal abelian extension of $\mathbb{Q}$. Then the following table gives a bound on $E(\mathbb{Q}^{ab})[p^\infty]$ for all primes p, i.e., the p-power torsion is contained in the following subgroups:*

p	2	3	5	7, 11, 13, 17, 19, 37, 43, 67, 163,	else
$E(\mathbb{Q}^{ab})[p^\infty] \subseteq$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/p\mathbb{Z}$	$\{\mathcal{O}\}$

Proof. Note that $E(\overline{\mathbb{Q}})[p^n] \cong \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$, and thus $E(\mathbb{Q}^{ab})[p^n] \subseteq \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ for any n. However, by Theorem 4.2.2, if $\mathbb{Q}(E[p^n])$ is abelian, then $p = 2,\ 3,$ or 5, and therefore for any prime except 2, 3, and 5, we must have that E does not have full p torsion defined over $\mathbb{Q}^{ab}$. Thus, if $p > 5$ then $E(\mathbb{Q}^{ab})[p^\infty] \subseteq \mathbb{Z}/p^n\mathbb{Z}$ for some n. However, since $\mathbb{Q}^{ab}$ is a Galois extension of $\mathbb{Q}$, Lemma 4.2.4 shows that $E(\mathbb{Q}^{ab})[p^\infty] \subseteq \mathbb{Z}/p\mathbb{Z}$ for $p = 7$, 11, 13, 17, 19, 37, 43, 67, and 163, and for all other primes l larger than 5, $E(\mathbb{Q}^{ab})[l^\infty] \cong \{\mathcal{O}\}$.

For the prime $p = 2$, we simply refer to Table 4.1.

For the prime $p = 3$, first notice that E cannot have full 9-torsion over $\mathbb{Q}^{ab}$ because of Theorem 4.2.2. Thus, $E(\mathbb{Q}^{ab})[3^\infty] \subseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^e\mathbb{Z}$ for some natural number e. By Lemma 4.2.4 if $E(\mathbb{Q}^{ab})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^e\mathbb{Z}$ then E has a 3^{e-1} isogeny. By Theorem 2.1.11, the largest 3-power degree rational isogeny is 27, and so $e - 1 \leq 3$, i.e. $E(\mathbb{Q}^{ab})[3^\infty] \subseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/81\mathbb{Z}$. However, suppose that in fact $E(\mathbb{Q}^{ab})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/81\mathbb{Z}$. Then by the above argument, E has a rational 27-isogeny. However, the only elliptic curves over $\mathbb{Q}$ that have a 27-isogeny are CM curves

(those with j-invariant $-215 \cdot 3 \cdot 5^3$). By Table 1 in [12] we see that such a curve does not have $\mathbb{Q}(E[n])$ abelian for any $n \geq 2$. Thus, $E(\mathbb{Q}^{ab})[3^\infty] \subseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$.

For the prime $p = 5$, first notice that E cannot have full 25-torsion over $\mathbb{Q}^{ab}$ because of Theorem 4.2.2. By an identical argument as in the $p = 3$ case, we have that $E(\mathbb{Q}^{ab})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z}$, since the largest 5-power degree rational isogeny is 25. However, suppose that $E(\mathbb{Q}^{ab})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$. Consider the Galois representation $\rho_{E,25} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[25]) \cong \mathrm{GL}(2, 25)$. Let G denote the image of $\rho_{E,25}$. Since full 5-torsion is defined over $\mathbb{Q}^{ab}$, Theorem 4.2.2 says there is a basis of $E[5]$ such that G mod 5 is contained in a split Cartan subgroup of $\mathrm{GL}(2, 5)$. Thus, we have that

$$G \leq \mathcal{G} := \left\{ \begin{bmatrix} a & 5b \\ 5c & d \end{bmatrix} : a, d \in (\mathbb{Z}/25\mathbb{Z})^\times, b, c \in \mathbb{Z}/5\mathbb{Z} \right\}.$$

Now, let H denote the image $\rho_{E,25}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[25]) \cap \mathbb{Q}^{ab}))$. Notice that $H = [G, G]$ the commutator subgroup of G. Since E has a point of order 25 over $\mathbb{Q}^{ab}$, we have that H must fix a vector of order 25 in $(\mathbb{Z}/25\mathbb{Z})^2$, and therefore $[G, G]$ must also fix a vector of order 25 in $(\mathbb{Z}/25\mathbb{Z})^2$.

By the Weil-pairing the image of $\rho_{E,25}$ must have determinant equal to the full group $(\mathbb{Z}/25\mathbb{Z})^\times$, and therefore G must be a subgroup of $\mathcal{G}$ with full determinant, and whose commutator subgroup fixes a vector of order 25 in $(\mathbb{Z}/25\mathbb{Z})^2$. Using MAGMA we can compute all such subgroups of $\mathrm{GL}(2, 25)$, and further we can also compute, given a subgroup of $\mathrm{GL}(2, 25)$, the isogenies of an elliptic curve associated with that image.

We thus compute that in fact all subgroups of $\mathcal{G}$ with the described properties all

yield a 25-isogeny, and thus any elliptic curve with such an image must in fact have a 25-isogeny. However, since full 5-torsion was defined over $\mathbb{Q}^{ab}$, Corollary 4.2.3 gives two isogenies of degree 5 and thus it is impossible for E to have a 25-isogeny, otherwise $C_5(E) = 4$ contradicting Theorem 3.3.13. Thus, $E(\mathbb{Q}^{ab})[5^\infty] \subseteq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. □

To prove bounds on the structure of $E(\mathbb{Q}^{ab})_{\text{tors}}$ We will need a Lemma about full 6-torsion from [12]:

Lemma 4.3.2 ([12], Lemma 3.12)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. If $\mathbb{Q}(E[6])/\mathbb{Q}$ is abelian, then* $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

As has been noted upon in Section 4.2, the structure of torsion over $\mathbb{Q}^{ab}$ is closely tied to the $\mathbb{Q}$-isogenies an elliptic curve has. We now prove bounds on $E(\mathbb{Q}^{ab})_{\text{tors}}$ based on these isogenies.

Proposition 4.3.3. *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose E has no non-trivial isogenies over $\mathbb{Q}$. Then $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \{\mathcal{O}\}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. By Lemma 4.2.4 it follows that $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ for some $m \geq 1$. However, Corollary 4.2.3 implies that m is a power of 2. Combining that with Lemma 4.2.7 shows that $m = 1$ or 2. □

Proposition 4.3.4. *Let $E/\mathbb{Q}$ be an elliptic curve, let $p = 11, 17, 19, 37, 43, 67,$ or 163 and suppose that E has a p-isogeny. Then $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. By Lemma 4.2.1 we have that $E(\mathbb{Q}^{ab})_{\text{tors}} \supseteq \mathbb{Z}/p\mathbb{Z}$. For these values of p, note that there are no rational isogenies of degree divisible by p besides isogenies of degree exactly p, and therefore by Lemma 4.2.4 it follows that $E(\mathbb{Q}^{ab})_{\text{tors}} \subseteq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for some m with $(m, p) = 1$. However, from Theorem 3.3.13 it follows that E

has no other rational isogenies. Thus Corollary 4.2.3 implies that m is a power of 2. Combining that with Lemma 4.2.7 shows that $m = 1$ or 2.

For any given p in this list there are only finitely many j-invariants of elliptic curves having a p-isogeny, as $X_0(p)$ has genus greater than 0. Given that these j-invariants are not 0 or 1728, by Lemma 4.2.5 it suffices to fix a representative E_j and compute (via MAGMA) that E_j does not have full 2-torsion defined over $\mathbb{Q}^{ab}$. □

Proposition 4.3.5. *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose $C_p(E) = 1$ for all primes $p \neq 2$. Then $E(\mathbb{Q}^{ab})_{\text{tors}} = E(\mathbb{Q}^{ab})[2^\infty]$ and is contained in either $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ or $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$*

Proof. By Corollary 4.2.3 and Lemma 4.2.4 it follows that $E(\mathbb{Q}^{ab})_{\text{tors}} = E(\mathbb{Q}^{ab})[2^\infty]$. Thus $E(\mathbb{Q}^{ab})_{\text{tors}}$ is one of the groups on Table 4.1 from Proposition 4.2.6. □

Proposition 4.3.6. *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose E has a 3-isogeny and $C_p(E) = 1$ for all primes $p > 3$. Then*

$$E(\mathbb{Q}^{ab})_{\text{tors}} \subseteq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 12, 18, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}, & \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, & \text{or} \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}. & \end{cases}$$

Proof. By Theorem 3.3.13 we have either

- $C_3(E) = 4$ and $C_p(E) = 1$ for all primes $p \neq 3$,
- $C_3(E) = 3$ and $C_2(E) \leq 2$,
- or $C_3(E) = 2$ and $C_2(E) \leq 4$.

Suppose $C_3(E) = 4$ and $C_p(E) = 1$ for all primes $p \neq 3$. Then by Proposition 4.3.1 we know that $E(\mathbb{Q}^{ab})[3^\infty] \subseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$. Suppose that E has full 2-torsion over $\mathbb{Q}^{ab}$ and full 3-torsion over $\mathbb{Q}^{ab}$ and hence full 6-torsion over $\mathbb{Q}^{ab}$. Then by Lemma 4.3.2 we must have $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. This is possible only if E has a point of order 2 defined over $\mathbb{Q}$, but that would give a Galois stable subgroup of order 2, and hence $C_2(E) \geq 2$ a contradiction. Therefore by Lemma 4.2.7 we have that $E(\mathbb{Q}^{ab})[2^\infty] \cong \{\mathcal{O}\}$ and so $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \subseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$. If E does not have full 3-torsion over $\mathbb{Q}^{ab}$ then $E(\mathbb{Q}^{ab})[3^\infty] \subseteq \mathbb{Z}/27\mathbb{Z}$. If $E(\mathbb{Q}^{ab})[3^\infty] \cong \mathbb{Z}/27\mathbb{Z}$ then E has a 27-isogeny and all such curves have CM (for instance see [24] Table 4). By Table 1 in [12] we see that such a curve does not have full n torsion defined over $\mathbb{Q}^{ab}$ for any n. Thus, $E(\mathbb{Q}^{ab})_{\mathrm{tors}} = E(\mathbb{Q}^{ab})[3^\infty] \cong \mathbb{Z}/27\mathbb{Z}$ or $E(\mathbb{Q}^{ab})[3^\infty] \subseteq \mathbb{Z}/9\mathbb{Z}$ and $E(\mathbb{Q}^{ab})[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which yields $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$.

Suppose that $C_3(E) = 3$ and $C_2(E) \leq 2$. Then we have that $E(\mathbb{Q}^{ab})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$. The largest $E(\mathbb{Q}^{ab})[2^\infty]$ can be so that $C_2(E) = 2$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Therefore, $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \subseteq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$.

Suppose that $C_3(E) = 2$ and $C_2(E) \leq 4$. Then $E(\mathbb{Q}^{ab})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z}$. From Proposition 4.2.6 the largest $E(\mathbb{Q}^{ab})[2^\infty]$ can be so that $C_2(E) = 4$ is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Thus, $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \subseteq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$. □

Proposition 4.3.7. *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose E has a 5-isogeny. Then*

$$E(\mathbb{Q}^{ab})_{\mathrm{tors}} \subseteq \begin{cases} \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}, \ \textit{or} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}. \end{cases}$$

Proof. By Theorem 3.3.13 we have either

- $C_5(E) = 3$ and $C_p(E) = 1$ for all primes $p \neq 5$,
- $C_5(E) = 2$ and $C_3(E) \leq 2$ and $C_2(E) = 1$,
- or $C_5(E) = 2$ and $C_3(E) = 1$ and $C_2(E) \leq 2$.

Suppose $C_5(E) = 3$ and $C_p(E) = 1$ for all primes $p \neq 5$. By Corollary 4.2.3 we see that E does not have full 3-torsion over $\mathbb{Q}^{ab}$. By Lemma 4.2.7 we have $E(\mathbb{Q}^{ab})[2^\infty] \cong \{\mathcal{O}\}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $E(\mathbb{Q}^{ab})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, then $E(\mathbb{Q}^{ab})[2^\infty] \cong \{\mathcal{O}\}$, since otherwise E would have full 10-torsion over $\mathbb{Q}^{ab}$, contradicting Theorem 4.2.2. Thus if $E(\mathbb{Q}^{ab})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, then $E(\mathbb{Q}^{ab})_{\text{tors}} = E(\mathbb{Q}^{ab})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. If E does not have full 5-torsion over $\mathbb{Q}^{ab}$, then $E(\mathbb{Q}^{ab})[5^\infty] \cong \mathbb{Z}/25\mathbb{Z}$ in order for $C_5(E) = 3$. Then $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/25\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.

Suppose $C_5(E) = 2$ and $C_3(E) \leq 2$ and $C_2(E) = 1$. Then $E(\mathbb{Q}^{ab})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z}$ and $E(\mathbb{Q}^{ab})[3^\infty] \subseteq \mathbb{Z}/3\mathbb{Z}$ by Lemma 4.2.1. Again by Lemma 4.2.7 we have $E(\mathbb{Q}^{ab})[2^\infty] \cong \{\mathcal{O}\}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus, $E(\mathbb{Q}^{ab})_{\text{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$.

Suppose $C_5(E) = 2$ and $C_3(E) = 1$ and $C_2(E) \leq 2$. Then again $E(\mathbb{Q}^{ab})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z}$. By Table Proposition 4.2.6, the largest $E(\mathbb{Q}^{ab})[2^\infty]$ can be so that $C_2(E) = 2$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Further, E does not have full torsion of any order prime to 2 by Corollary 4.2.3. Thus, $E(\mathbb{Q}^{ab})_{\text{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$. □

Proposition 4.3.8. *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose E has a 7-isogeny. Then either $E(\mathbb{Q}^{ab})_{\text{tors}} \subseteq \mathbb{Z}/21\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$.*

Proof. By Theorem 3.3.13 we have $C_p(E) = 1$ for all primes $p \neq 2, 3, 7$ and either $C_3(E) \leq 2$ and $C_2(E) = 1$, or $C_3(E) = 1$ and $C_2(E) \leq 2$.

Suppose $C_3(E) = 2$ and $C_2(E) = 1$. Then E has a 7-isogeny and a 3-isogeny and so E has a 21-isogeny. Since there are only finitely many rational points on $X_0(21)$, there are only a finite number of j-invariants for elliptic curves over $\mathbb{Q}$ with a 21-isogeny. We can fix a model for each of these curves and explicitly check that none of these families have full m-torsion for any $2 \leq m \leq 8$. Thus by Lemma 4.2.1, Lemma 4.2.4, and Theorem 4.2.2 we have $E(\mathbb{Q}^{ab}) \cong \mathbb{Z}/21\mathbb{Z}$.

Suppose instead that $C_3(E) = 1$ and $C_2(E) = 2$. Since $C_3(E) = 1$, Corollary 4.2.3 tells us that E does not have full 3-torsion. Further, since $C_2(E) = 2$, by Proposition 4.2.6, it follows that $E(\mathbb{Q}^{ab})[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Therefore, by Lemma 4.2.4 we have that $E(\mathbb{Q}^{ab})_{\text{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$.

Finally if $C_3(E) = C_2(E) = 1$, then by Lemma 4.2.4, Corollary 4.2.3, and Lemma 4.2.7 we have that $E(\mathbb{Q}^{ab})_{\text{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$. □

Proposition 4.3.9. *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose E has a 13-isogeny. Then $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/13\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$.*

Proof. Since there are no curves over $\mathbb{Q}$ with rational isogenies of degree properly divisible by 13, it follows from Lemma 4.2.4 that $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ for some $m \geq 1$. However, by Theorem 3.3.13 we have that $C_p(E) = 1$ for all primes $p \neq 13$. Thus by Corollary 4.2.3 and Lemma 4.2.7 we have that $m = 1$ or 2. □

Note that from here a quick count of the possible sizes of the torsion subgroups here along with Lemma 4.2.1 for the example of 26569a1 having a point of order 163 over $\mathbb{Q}^{ab}$ is already enough to prove Corollary 1.3.6.

4.4 Eliminating Possible Torsion

We restate the classification theorem for convenience:

Theorem 4.4.1. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}^{ab})_{\text{tors}}$ is isomorphic to one of the following groups:*

$$
\begin{aligned}
&\mathbb{Z}/N_1\mathbb{Z}, && N_1 = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 37, 43, 67, 163,\\
&\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, && N_2 = 1, 2, \ldots, 9,\\
&\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3N_3\mathbb{Z}, && N_3 = 1, 3,\\
&\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4N_4\mathbb{Z}, && N_4 = 1, 2, 3, 4,\\
&\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},\\
&\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z},\\
&\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.
\end{aligned}
$$

Each of these groups appear as $E(\mathbb{Q}^{ab})_{\text{tors}}$ for some elliptic curve over $\mathbb{Q}$.

We now eliminate the possibility of many of the groups appearing in the previous propositions as possible torsion subgroups over $\mathbb{Q}^{ab}$ for some elliptic curve $E/\mathbb{Q}$. We begin with a simple observation about 2-torsion over $\mathbb{Q}^{ab}$ from Proposition 4.2.6.

Lemma 4.4.2. *Let $E/\mathbb{Q}$ be an elliptic curve. If $E(\mathbb{Q}^{ab})[2] \neq \{\mathcal{O}\}$ then $E(\mathbb{Q}^{ab})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus $E(\mathbb{Q}^{ab})\text{tors} \ncong \mathbb{Z}/2N\mathbb{Z}$ for any $N \geq 1$.*

This eliminates many possible torsion structures over $\mathbb{Q}^{ab}$. In particular, after we combine the possibilities for $E(\mathbb{Q}^{ab})_{\text{tors}}$ from Propositions 4.3.9, 4.3.8, 4.3.7, 4.3.6, and 4.3.5, and eliminate those groups ruled out by Lemma 4.4.2, we can compare them to the classification in Theorem 1.3.5 to see that it remains to rule out the following groups as possibilities for $E(\mathbb{Q}^{ab})_{\text{tors}}$:

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z}, \quad N_2 = 10, 12, 13, 14, 15, 18, 25,$$
$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z},$$
$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}.$$

Proposition 4.4.3. *Let $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathbb{Q}^{ab})_{\text{tors}}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$.*

Proof. In the case $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}$ the curve has a 14-isogeny by Lemma 4.2.4 of which there are only two possible isomorphism classes of curves given by the j-invariants $-3^3 5^3$ and $3^3 5^3 17^3$ (see for instance Table 4 of [24]). Using division polynomials we can check that in both cases there are no points of order 4 defined over an abelian extension of $\mathbb{Q}$.

In the case $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ the curve has a 15-isogeny by Lemma 4.2.4. Here there are four possible j-invariants, $-\frac{5^2}{2}$, $-\frac{5^2 \cdot 241^3}{2^3}$, $-\frac{5 \cdot 29^3}{2^5}$, and $\frac{5 \cdot 211^3}{2^{15}}$. Again using division polynomials we can check that none of these curves have a point of order 2 defined over an abelian extension of $\mathbb{Q}$. □

Proposition 4.4.4. *Let $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathbb{Q}^{ab})_{\text{tors}} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$.*

Proof. Suppose that $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$. Then E has a 13-isogeny, and so by [24] Table 3 the curve has a j-invariant of the form:

$$j(E) = \frac{(h^2 + 5h + 13)(h^4 + 7h^3 + 20h^2 + 19h + 1)^3}{h}$$

for some $h \in \mathbb{Q}$ with $h \neq 0$. Thus, E must be a twist of the curve

$$E' : y^2 + xy = x^3 - \frac{36}{j(E) - 1728}x - \frac{1}{j(E) - 1728}.$$

Since $E(\mathbb{Q}^{ab})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ but E does not have any 2-isogenies by Theorem 3.3.13, we must have $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$, implying that the discriminant of E is a square. Since E is a twist of E', the discriminant of E differs from the discriminant of E' by at most a square. Thus, we obtain a formula $y^2 = \mathrm{Disc}(E')$, which we compute in terms of h. By absorbing squares into the y^2 term we obtain a curve

$$C : Y^2 = h(h^2 + 6h + 13)$$

which is a modular curve describing precisely when E has a 13-isogeny and $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. This curve is actually an elliptic curve with $C(\mathbb{Q}) = \{(0 : 0 : 1), (0 : 1 : 0)\} \cong \mathbb{Z}/2\mathbb{Z}$, both points being cusps. Therefore there are no elliptic curves with $E(\mathbb{Q}^{ab}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$. □

Proposition 4.4.5. *Let $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.*

Proof. Suppose that $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$. Then E has a 25-isogeny, and so by [24] Table 3 the curve has a j-invariant of the form:

$$j(E) = \frac{(h^{10} + 10h^8 + 35h^6 - 12h^5 + 50h^4 - 60h^3 + 25h^2 - 60h + 16)^3}{(h-1)(h^4 + h^3 + 6h^2 + 6h + 11)}$$

for some $h \in \mathbb{Q}$ with $h \neq 1$ By a similar argument made in Proposition 4.4.4 we have that the discriminant of E must be a square. We again obtain a formula $y^2 = \mathrm{Disc}(E)$ and by absorbing squares into the y^2 term we obtain a curve

$$C : Y^2 = h^7 + 9h^5 + 25h^3 - 11h^2 + 20h - 44$$

which is a modular curve describing precisely when E has a 25-isogeny and $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong$

$\mathbb{Z}/3\mathbb{Z}$. This is a genus 3 hyperelliptic curve.

We can construct a map π from C to an elliptic curve $\tilde{C} : y^2 = x^3 + x^2 - x$ given by

$$(x : y : z) \mapsto (x^3 - x^2z + 4xz^2 - 4z^3 : yz^2 : x^2z - 2xz^2 + z^3). \qquad (*)$$

The curve $\tilde{C}$ has Cremona label 20a2 and rank 0 and torsion isomorphic to $\mathbb{Z}/6\mathbb{Z}$. It has rational points

$$\tilde{C}(\mathbb{Q}) = \{(0 : 1 : 0), (0 : 0 : 1), (-1 : -1 : 1), (1 : -1 : 1), (-1 : 1 : 1), (1 : 1 : 1)\}$$

and we can use $(*)$ to explicitly compute the preimage of each point under π to see that the only rational points on C are $(1 : 0 : 1)$ and $(0 : 1 : 0)$. Note that we have $h = \frac{X}{Z}$ for points $(X : Y : Z) \in C$. The first points corresponds to $h = 1$, which is a zero of the denominator of $j(E)$, and the second point is the point at infinity, which corresponds to $h = \infty$, which is not a value we can consider. Thus, both of these points are cusps, and therefore there are no elliptic curves with $E(\mathbb{Q}^{ab}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$. $\square$

We will make use of the following proposition found in [6]:

Proposition 4.4.6 ([6] Corollary 4.5)**.** *Let $f(X) = X^4 + bX^2 + d$ be irreducible in $K[X]$, where K does not have characteristic 2. Its Galois group over K, denoted G_f, is V, $\mathbb{Z}/4\mathbb{Z}$, or D_4 according to the following conditions.*

1. *If $d \in (K^\times)^2$ then $G_f = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*
2. *If $d \notin (K^\times)^2$ and $(b^2 - 4d)d \in (K^\times)^2$ then $G_f = \mathbb{Z}/4\mathbb{Z}$.*
3. *If $d \notin (K^\times)^2$ and $(b^2 - 4d)d \notin (K^\times)^2$ then $G_f = D_4$.*

The following lemma gives a criterion for a point to be halved:

Lemma 4.4.7 (Knapp [21], Theorem 4.2, p. 85)**.** *Let K be a field of characteristic not equal to 2 or 3, and let E be an elliptic curve over K given by $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ with α, β, γ in K. For $P = (x, y) \in E(K)$, there exists a K-rational point $Q = (x', y')$ on E such that $[2]Q = P$ if and only if $x - \alpha, x - \beta$, and $x - \gamma$ are all squares in K. In this case, if we fix the sign of $\sqrt{x-\alpha}, \sqrt{x-\beta}$, and $\sqrt{x-\gamma}$, then x' equals one of the following:*

$$\sqrt{x-\alpha}\sqrt{x-\beta} \pm \sqrt{x-\alpha}\sqrt{x-\gamma} \pm \sqrt{x-\beta}\sqrt{x-\gamma} + x$$

or

$$-\sqrt{x-\alpha}\sqrt{x-\beta} \pm \sqrt{x-\alpha}\sqrt{x-\gamma} \mp \sqrt{x-\beta}\sqrt{x-\gamma} + x$$

where the signs are taken simultaneously.

We combine these results to prove the following lemma:

Lemma 4.4.8. *Suppose E is an elliptic curve over $\mathbb{Q}$ with a point of order 4 defined over $\mathbb{Q}^{ab}$ but not full 4-torsion defined over $\mathbb{Q}^{ab}$. Then, there is a model of E of the form:*

$$E : y^2 = x(x^2 + bx + d)$$

and either d or $(b^2 - 4d)d$ is a non-zero perfect square in $\mathbb{Q}$.

Proof. By Lemma 4.2.7 if E has a point of order 4 defined over $\mathbb{Q}^{ab}$ then E has at least one 2-isogeny over $\mathbb{Q}$. Thus there exists a point P of order 2 defined over $\mathbb{Q}$, and by moving that point to $P = (0, 0)$ we obtain a model for E of the form $y^2 = x(x^2 + bx + d)$ with $b, d \in \mathbb{Q}$.

Over $\mathbb{Q}^{ab}$ we obtain a point of order 4, say Q. Suppose first that this point satisfies $2Q = P = (0,0)$. Writing $E : y^2 = x(x-\alpha)(x-\overline{\alpha})$, Lemma 4.4.7 says that we have that $\sqrt{-\alpha}$ and $\sqrt{-\overline{\alpha}}$ must be squares in $\mathbb{Q}^{ab}$. Notice that the minimal polynomial for both $\sqrt{-\alpha}$ and $\sqrt{-\overline{\alpha}}$ is in fact the polynomial

$$f = x^4 - bx^2 + d.$$

Thus, we must have that the Galois group of f over $\mathbb{Q}$ is abelian. Therefore $G_f = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. Now by Proposition 4.4.6 the two cases above follow.

Suppose instead that our point of order 4 is halving one of the other points of order 2. Without loss of generality we may assume $2Q = (\alpha, 0)$. By Lemma 4.4.7 we have that α and $\alpha - \overline{\alpha}$ are squares in $\mathbb{Q}^{ab}$. Notice that the minimal polynomial of $\sqrt{\alpha}$ is

$$f = x^4 + bx^2 + d$$

and the minimal polynomial of $\sqrt{\alpha - \overline{\alpha}}$ is

$$g = x^4 - (b^2 - 4d).$$

Note that $b^2 - 4d$ is not a square since $\alpha - \overline{\alpha} = \sqrt{b^2 - 4d}$ was was assumed to not be in $\mathbb{Q}$.

Let $L_1 = \mathbb{Q}(\sqrt{\alpha})$ and $L_2 = \mathbb{Q}(\sqrt{\alpha - \overline{\alpha}})$. We wish to consider when the composite $L_1 L_2 \subseteq \mathbb{Q}^{ab}$. For $L_2 \subseteq \mathbb{Q}^{ab}$ we must have $\mathrm{Gal}(L_2/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. Applying Proposition 4.4.6 to the defining polynomial g of L_2 gives us conditions for when this happens.

$$\mathrm{Gal}(L_2/\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } -(b^2-4d) \in (\mathbb{Q}^\times)^2 \\ \mathbb{Z}/4\mathbb{Z} & \text{if } -(b^2-4d) \notin (\mathbb{Q}^\times)^2 \text{ and } -4(b^2-4d)^2 \in (\mathbb{Q}^\times)^2 . \end{cases}$$

Notice that the second case $\mathrm{Gal}(L_2/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ cannot occur, since if $-4(b^2-4d)^2 \in (\mathbb{Q}^\times)^2$ then $-1 \in (\mathbb{Q}^\times)^2$.

Thus, suppose instead that $\mathrm{Gal}(L_2/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $-(b^2-4d) = s^2$ for some $s \in \mathbb{Q}$. Then $\alpha - \overline{\alpha} = \sqrt{b^2-4d} = \sqrt{-s^2} = |s|\sqrt{-1}$. Therefore, since $\alpha - \overline{\alpha} \in L_2$, we have that $\sqrt{-1} \in L_2$. Recall that $(0,0)$ is halved in the extension where $x^4 - bx^2 + d$ splits. By assumption, $x^4 + bx^2 + d$ is split in L_1, and thus it splits in L_1L_2. Further, we have shown that $\sqrt{-1} \in L_2 \subseteq L_1L_2$, and therefore $x^4 - bx^2 + d$ must also split. Thus the point $(0,0)$ is also halved in L_1L_2, and so full 4-torsion is defined over L_1L_2. Thus, if $L_1L_2 \subseteq \mathbb{Q}^{ab}$, we contradict our original assumption that E does not have full 4-torsion over $\mathbb{Q}^{ab}$.

□

Now we apply the above lemma to show that the torsion subgroups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ do not appear over $\mathbb{Q}^{ab}$.

Proposition 4.4.9. *Let $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.*

Proof. Suppose for the sake of contradiction that E is an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$. Then, E has a $\mathbb{Q}$-rational 10-isogeny, and so by [24] Table 3 the curve has a

$$j(E) = \frac{(h^6 - 4h^5 + 16h + 16)^3}{(h+1)^2(h-4)h}$$

for some $h \in \mathbb{Q}$ with $h \neq -1, 0, 4$. Thus, E must be a twist of the curve

$$E' : y^2 + xy = x^3 - \frac{36}{j(E) - 1728}x - \frac{1}{j(E) - 1728}.$$

Moving the 2-torsion point to (0,0) yields a model of E' of the form

$$E' : y^2 = x^3 + b(h)x^2 + d(h)x$$

for the rational functions

$$b(h) = \frac{-9h^{12} + 72h^9 - 144h^3 - 144}{h^{12} - 8h^9 - 8h^3 - 8},$$

$$d(h) = \frac{1296h^{27} - 19440h^{24} + 62208h^{21} + 124416h^{18} - 248832h^{15} - 622080h^{12} + 995328h^6 + 995328h^3 + 331776}{h^{36} - 24h^{33} + 192h^{30} - 464h^{27} - 720h^{24} + 2304h^{21} + 2112h^{18} + 5760h^{15} + 14400h^{12} + 11776h^9 + 12288h^6 + 12288h^3 + 4096}.$$

Note that $j(E) \neq 0, 1728$ since E has a 10-isogeny, and thus E is a quadratic twist of E'. By Lemma 4.2.5 we have that $E'(\mathbb{Q}^{ab})_{\text{tors}} \cong E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$. Now, since $E('\mathbb{Q}^{ab})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, Lemma 4.4.8 tells us that either

$$d(h) \in \left(\mathbb{Q}^\times\right)^2 \qquad \text{or} \qquad (b(h)^2 - 4d(h))d(h) \in \left(\mathbb{Q}^\times\right)^2.$$

Denote the 4-torsion point over $\mathbb{Q}^{ab}$ by Q.

Suppose $d(h) \in (\mathbb{Q}^\times)^2$. We obtain a formula $Y^2 = d(h)$ and by absorbing squares we obtain the curve

$$C : Y'^2 = h^3 + h^2 + 4h + 4$$

which is a modular curve describing precisely when E has a 10-isogeny and $\text{Gal}(\mathbb{Q}(x(Q))/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This is the elliptic curve with Cremona label 20a1

and rational points

$$C(\mathbb{Q}) = \{(0:1:0), (0:-2:1), (0:2:1), (4:-10:1), (4:10:1), (-1:0:1)\} \cong \mathbb{Z}/6\mathbb{Z}.$$

However, all of these points are cusps as they correspond to $h = 0, -1, 4$ which are all zeros of the denominator of $j(E)$. Therefore there are no such elliptic curves.

Suppose instead that $(b(h)^2 - 4d(h))d(h) \in (\mathbb{Q}^\times)^2$. Again we obtain a formula $Y^2 = (b(h)^2 - 4d(h))d(h)$ and by absorbing squares we obtain the curve

$$\hat{C} : Y'^2 = h^3 - 3h^2 - 4h$$

which is a modular curve describing precisely when E has a 10-isogeny and $\mathrm{Gal}(\mathbb{Q}(x(Q))/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. This is an elliptic curve with Cremona label 40a1 and rational points

$$\hat{C}(\mathbb{Q}) = \{(0:0:1), (0:1:0), (-1:0:1), (4:0:1)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Again, all of these points are cusps as they correspond to $h = 0, -1, 4$. Therefore there are no such elliptic curves. Thus we can conclude that no such a curve E exists. □

Proposition 4.4.10. *Let $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$.*

Proof. Suppose for the sake of contradiction that E is an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q}^{ab})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$. Then, E has a $\mathbb{Q}$-rational 18-isogeny, and so by [24] Table 3 the curve has a j-invariant of the form

$$j(E) = \frac{(h^3-2)^3(h^9-6h^6-12h^3-8)^3}{h^9(h^3-8)(h^3+1)^2}$$

for some $h \in \mathbb{Q}$ with $h \neq -1, 0, 2$. Thus, E must be a twist of the curve

$$E' : y^2 + xy = x^3 - \frac{36}{j(E) - 1728}x - \frac{1}{j(E) - 1728}.$$

Moving the 2-torsion point to (0,0) yields a model of E' of the form

$$E' : y^2 = x(x^2 + b(h)x + d(h))$$

for the rational functions

$$b(h) = \frac{(h^3 - 2)(h^9 - 6h^6 - 12h^3 - 8)}{h^{12} - 8h^9 - 8h^38},$$

$$d(h) = \frac{(h + 1)(h^2 - h + 1)(h^3 - 2)^2(h^9 - 6h^6 - 12h^3 - 8)^2}{(h^6 - 4h^3 - 8)^2(h^12 - 8h^9 - 8h^3 - 8)^2}.$$

Note that $j(E) \neq 0, 1728$ since E has an 18-isogeny, and thus E is a quadratic twist of E'. By Lemma 4.2.5 we have that $E'(\mathbb{Q}^{ab})_{\text{tors}} \cong E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$. Now, since $E('\mathbb{Q}^{ab})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, Lemma 4.4.8 tells us that either

$$d(h) \in \left(\mathbb{Q}^\times\right)^2 \qquad \text{or} \qquad (b(h)^2 - 4d(h))d(h) \in \left(\mathbb{Q}^\times\right)^2.$$

Denote the 4-torsion point over $\mathbb{Q}^{ab}$ by Q.

Suppose $d(h) \in (\mathbb{Q}^\times)^2$. We obtain a formula $Y^2 = d(h)$ and by absorbing squares we obtain the curve

$$C : Y'^2 = h^3 + 1$$

which is a modular curve describing precisely when E has a 18-isogeny and $\text{Gal}(\mathbb{Q}(x(Q))/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This is an elliptic curve with Cremona label 36a1

and rational points

$$C(\mathbb{Q}) = \{(0:1:0), (0:1:1), (0:-1:1), (2:3:1), (2:-3:1), (-1:0:1)\} \cong \mathbb{Z}/6\mathbb{Z}.$$

However, all of these points are cusps as they correspond to $h = -1, 0, 2$. Therefore there are no such elliptic curves.

Suppose instead that $(b(h)^2 - 4d(h))d(h) \in (\mathbb{Q}^\times)^2$. Again we obtain a formula $Y^2 = (b(h)^2 - 4d(h))d(h)$ and by absorbing squares we obtain the curve

$$\hat{C} : Y'^2 = h^7 - 7h^4 - 8h$$

which is a modular curve describing precisely when E has a 18-isogeny and $\mathrm{Gal}(\mathbb{Q}(x(Q))/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. This is a genus 3 hyperelliptic curve with an automorphism φ defined by

$$(x:y:z) \mapsto (2x^4 - 10x^3z + 12x^2z^2 + 8xz^3 - 16z^4 : 36yz^3 : x^4 - 8x^3z + 24x^2z^2 - 32xz^3 + 16z^4)$$

and taking the quotient of $\hat{C}$ by φ gives a map π from $\hat{C}$ to an elliptic curve $\hat{C}_\varphi$: $y^2 = x^3 - x^2 + x$ given by

$$(x:y:z) \mapsto (xz(x^2 - xz - 2z^2) : yz^3 : x^2(x+z)^2). \qquad (*)$$

The curve $\hat{C}_\varphi$ has Cremona label 24a4 and has rational points

$$\hat{C}_\varphi(\mathbb{Q}) = \{(0:1:0), (0:0:1), (1:1:1), (1:-1:1)\}.$$

We can use $(*)$ to explicitly compute the preimage of each point under π to compute the rational points on $\hat{C}$. We find that $\hat{C}(\mathbb{Q}) = \{(-1:0:1), (0:0:1), (2:0:1), (0:1:0)\}$. These points correspond to $h = 0, -1, 2$, which are zeros of the denominator of $j(E)$ and so are cusps. Thus we can conclude that no such a curve E exists. $\square$

Proposition 4.4.11. *Let $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathbb{Q}^{ab})_{\text{tors}} \ncong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.*

Proof. Suppose that $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. Then by Lemma 4.3.2 we have that $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, and thus E has a single non-trivial point P of order 2 over $\mathbb{Q}$. Take a model of E of the form $E : y^2 = x(x^2 + bx + c)$. Then $E[2] = \{\mathcal{O}, (0,0), (\alpha, 0), (\overline{\alpha}, 0)\}$ where α and $\overline{\alpha}$ are roots of $x^2 + bx + c$. Let $F = \mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(E[2])$.

Since $E(\mathbb{Q}^{ab})[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ we obtain a point of order 4 over $\mathbb{Q}^{ab}$. Suppose $(0,0)$ is halved in $E(\mathbb{Q}^{ab})_{\text{tors}}$. By Lemma 4.4.7 we have that the point of order 4 is defined over $K = F(\sqrt{2b + 2\sqrt{b^2 - 4c}})$. The field K must be an abelian extension of $\mathbb{Q}$ and so K is either cyclic or biquadratic, i.e. $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ respectively.

If K is cyclic quartic, then, as discussed in the proof of Lemma 4.5 in [3], E has j-invariant 78608. We can check that $\Phi_3(X, 78608)$ has no rational roots, where $\Phi_3(X, Y)$ denotes the third classical modular polynomial, and so no curve with j-invariant 78608 has a 3-isogeny, contradicting that $E(\mathbb{Q}^{ab})[3^\infty] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

If K is biquadratic, then $b^2 - 4c$ must be a square, but then E has full 2-torsion over $\mathbb{Q}$, contradicting the assumption that $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

Suppose instead that $(\alpha, 0)$ or $(\overline{\alpha}, 0)$ is halved over $\mathbb{Q}^{ab}$, without loss of generality suppose $(\alpha, 0)$ is halved. Then by Lemma 4.4.7 we have a point of order 4 defined over $K = F(\sqrt{-\alpha})$ which, as discussed in the proof of Lemma 4.5 in [3], is not a

cyclic extension. Also, K is not biquadratic unless $\alpha \in \mathbb{Q}$, again implying that E has full 2-torsion over $\mathbb{Q}$, a contradiction. Thus, there is no such curve E. □

Proposition 4.4.12. *Let $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathbb{Q}^{ab})_{\text{tors}} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$.*

Proof. Suppose for the sake of contradiction that E is an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$. Then, E has a $\mathbb{Q}$-rational 12-isogeny, and so by [24] Table 3 the curve has a j-invariant of the form

$$j(E) = \frac{(h^2-3)^3(h^6-9h^4+3h^2-3)^3}{h^4(h^2-9)(h^2-1)^3}$$

for some $h \in \mathbb{Q}$ with $h \neq 0, \pm 1, \pm 3$. Thus, E must be a twist of the curve

$$E' : y^2 + xy = x^3 - \frac{36}{j(E)-1728}x - \frac{1}{j(E)-1728}.$$

Moving the 2-torsion point to (0,0) yields a model of E' of the form

$$E' : y^2 = x(x^2 + b(h)x + d(h))$$

for the rational functions

$$b(h) = \frac{(h^2-3)(h^6-9h^4+3h^2-3)}{h^8-12h^6+30h^4-36h^2+9},$$

$$d(h) = \frac{h^2(h^2-3)^2(h^6-9h^4+3h^2-3)^2}{(h^4-6h^2-3)^2(h^8-12h^6+30h^4-36h^2+9)^2}.$$

For ease of notation going forward, we will write $b = b(h)$, $d = d(h)$, and it should be understood that many of the following variables are functions of h. From the proof of Lemma 4.4.8 we see that the point $Q \in E(\mathbb{Q}^{ab})$ of order 4 must satisfy $2Q = (0,0)$.

Let α and $\overline{\alpha}$ be roots of $x^2 + bx + d$ (over $\mathbb{Q}[h]$) so that $E' : y^2 = x(x-\alpha)(x-\overline{\alpha})$. Then, from Lemma 4.4.7 we have (without loss of generality) that Q has x-coordinate

$$(\sqrt{0-0})(\sqrt{0-\alpha}) \pm (\sqrt{0-0})(\sqrt{0-\overline{\alpha}}) \pm (\sqrt{0-\alpha})(\sqrt{0-\overline{\alpha}}) + 0 = \pm\sqrt{\alpha\overline{\alpha}} = \pm\sqrt{d}$$

Suppose that the x-coordinate of Q is $\sqrt{d}$. Since there is a point of order 8 in $E(\mathbb{Q}^{ab})$, there exists a point $R \in E(\mathbb{Q}^{ab})$ such that $2R = Q$. Denote

$$\alpha = \frac{-b + \sqrt{b^2 - 4d}}{2}$$

and

$$\overline{\alpha} = \frac{-b - \sqrt{b^2 - 4d}}{2}$$

so that we have

$$E' : y^2 = x(x-\alpha)(x-\overline{\alpha}).$$

For ease of notation we denote $\delta = \sqrt{d}$. We can apply Lemma 4.4.7 again to deduce that since such an R exists, we must have δ, $\delta - \alpha$, and $\delta - \overline{\alpha}$ are all squares in $\mathbb{Q}^{ab}$. Notice that through some simplification we have that $(\delta - \alpha)(\delta - \overline{\alpha}) = (b + 2\delta)\delta$ and so it suffices to prove that $\delta, (b+2\delta)\delta, \delta - \alpha$ are squares in $\mathbb{Q}^{ab}$.

For any $h \in \mathbb{Q}$ we have $\delta \in \mathbb{Q}$ and so clearly $\sqrt{\delta} \in \mathbb{Q}^{ab}$. Similarly, for all $h \in \mathbb{Q}$, we have that $(b+2\delta)\delta \in \mathbb{Q}$, and so $\sqrt{(b+2\delta)\delta} \in \mathbb{Q}^{ab}$.

To see when $\delta - \alpha$ is square in $\mathbb{Q}^{ab}$ we will find the minimal polynomial of $\delta - \alpha$ over $\mathbb{Q}$, and find when this defines an abelian extension of $\mathbb{Q}$. Notice that $\delta - \alpha = \frac{1}{2}(b - 2\delta - \sqrt{b^2 - 4d})$. Let $\xi = \sqrt{\delta - \alpha} = \sqrt{\dfrac{b - 2\delta - \sqrt{b^2 - 4d}}{2}}$. The minimal polynomial of

ξ is:

$$f(X) = X^4 - (b + 2\delta)X^2 + (b + 2\delta)\delta.$$

Now, we apply Proposition 4.4.6 and see that f defines an abelian extension of $\mathbb{Q}$ if and only if

$$(b + 2\delta)\delta \in \left(\mathbb{Q}^\times\right)^2$$

or

$$((b + 2\delta)^2 - 4(b + 2\delta)\delta)(b + 2\delta)\delta \in \left(\mathbb{Q}^\times\right)^2$$

which, by absorbing squares is equivalent to

$$(b - 2\delta)\delta \in \left(\mathbb{Q}^\times\right)^2.$$

These yield the curves

$$C_1 : y^2 = h^3 - 2h^2 - 3h \quad \text{and} \quad C_2 : y^2 = h^3 + 2h^2 - 3h$$

respectively.

Now it remains to classify all rational points on C_1 and C_2. These are curves with Cremona label 48a1 and 24a1 respectively and have rank 0 with rational points

$$C_1(\mathbb{Q}) = \{(0 : 0 : 1), (0 : 1 : 0), (3 : 0 : 1), (-1 : 0 : 1)\}$$

and

$$C_2(\mathbb{Q}) = \{(0:0:1), (0:1:0), (-1:-2:1), (3:-6:1),$$
$$(1:0:1), (3:6:1), (-1:2:1), (-3:0:1)\}.$$

Note that all of these points correspond to $h = 0, \pm 1, \pm 3$, which are zeros of the denominator of $j(E)$ and hence are cusps. Therefore there are no curves over $\mathbb{Q}$ with $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$.

□

The following result comes from a paper by Bourdon and Clark [1]. The theorem applies broadly to any elliptic curve over $\overline{\mathbb{Q}}$ with complex multiplication, but we will use it to show specifically that the torsion subgroup $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$ does not appear over $\mathbb{Q}^{ab}$.

Theorem 4.4.13 ([1], Theorem 2.7)**.** *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:*

(a) We have $M = E[\operatorname{ann} M]$. Hence:

(b) $M \cong \mathcal{O}_K/(\operatorname{ann} M)$.

(c) $\#M = |\operatorname{ann} M|$.

This gives us an understanding of $\mathcal{O}_K$-submodules of $E(\mathbb{C})$ for an elliptic curve with CM by the maximal order. We use these results to prove the following proposition:

Proposition 4.4.14. *Let $E/\mathbb{Q}$ be an elliptic curve, then $E(\mathbb{Q}^{ab})_{\text{tors}} \ncong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$.*

Proof. Suppose that $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$. Then by Lemma 4.2.4 the curve E has a 9-isogeny over $\mathbb{Q}$. By Corollary 4.2.3, E has an independent 3-isogeny as well. Thus we have the following isogeny graph:

$$E' \xleftarrow{\quad 3 \quad} E \xrightarrow{\qquad\qquad 9 \qquad\qquad} E''$$

Taking the dual isogeny also of degree 3 from E' to E and composing it with 9-isogeny from E to E'' shows that E' has a 27-isogeny. The modular curve $X_0(27)$ has genus one, and there is a unique 27-isogeny class of elliptic curves up to isomorphism. Examining the 27-isogeny class shows that E has CM by the maximal order of $K = \mathbb{Q}(\sqrt{-3})$.

Now, notice that $E(\mathbb{Q}^{ab})_{\text{tors}}$ is an $\mathcal{O}_K$-submodule of $E(\mathbb{C})$, since $K \subseteq \mathbb{Q}^{ab}$. Since the prime $p = 3$ ramifies in K, there is a unique prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ with $|\mathfrak{p}| = 3$ and we have $(3) = \mathfrak{p}^2$. By Theorem 4.4.13 (b) we have that $E[27] \cong \mathcal{O}_K/(3)^3 \cong \mathcal{O}_K/\mathfrak{p}^6$. Suppose I is an ideal of $\mathcal{O}_K/\mathfrak{p}^6$. Then $\mathfrak{p}^6 \subseteq I$ so $I|\mathfrak{p}^6$ and therefore $I = \mathfrak{p}^b$ for some $0 \leq b \leq 6$ by the unique factorization of ideals into prime ideals. Thus, the $\mathcal{O}_K$-submodules of $E[27]$ are all of the form $\mathfrak{p}^b/\mathfrak{p}^6$ for some $0 \leq b \leq 6$. Moreover, the exponent of $\mathcal{O}_K/\mathfrak{p}^b$ is the smallest power of 3 contained in $\mathfrak{p}^b$. Since $(3)^d = \mathfrak{p}^{2d}$, this smallest power is $3^{\lceil \frac{b}{2} \rceil}$. Further, by Theorem 4.4.13 (c) we have $\#\mathcal{O}_K/\mathfrak{p}^b = 3^b$, we deduce that

$$\mathcal{O}_K/\mathfrak{p}^b \cong_{\mathbb{Z}} \mathbb{Z}/3^{\lfloor \frac{b}{2} \rfloor}\mathbb{Z} \times \mathbb{Z}/3^{\lceil \frac{b}{2} \rceil}\mathbb{Z}$$

Notice that since $E(\mathbb{Q}^{ab})[27]$ is an $\mathcal{O}_K$-submodule of $E[27]$, we have that $\lfloor \frac{b}{2} \rfloor = 1$, implying $b = 2$ or $b = 3$, but also $\lceil \frac{b}{2} \rceil = 3$, implying $b = 5$ or $b = 6$, a contradiction. Thus no such curve exists. $\square$

4.5 Examples

Recall that Lemma 4.2.1 states that if an elliptic curve has an n-isogeny over $\mathbb{Q}$, then there is a point of order n in $E(\mathbb{Q}^{ab})_{\text{tors}}$. Thus, for the majority of the cyclic $\mathbb{Z}/n\mathbb{Z}$ torsion appearing over $\mathbb{Q}^{ab}$, it suffices to take a curve with an n-isogney over $\mathbb{Q}$ and simply check that it does not have full m-torsion over an abelian extension for any m. Given we know the classification of torsion subgroups over $\mathbb{Q}^{ab}$, in many cases it is unnecessary to check any values of m.

We first examine all examples of curves with an n-isogeny where $X_0(n)$ has finitely many non-cuspidal points over $\mathbb{Q}$ in Table 4.2. We refer to Table 4 of [24] for the j-invariants. We give the torsion subgroup over $\mathbb{Q}^{ab}$, the j-invariant, the cremona labels of the elliptic curves, and the Galois group of the field of definition of the abelian torsion. We then find examples for all the other torsion subgroups appearing in Theorem 1.3.5 in Table 4.3.

Note that counting isogenies only gives a piece of the torsion subgroup. Suppose that there is a subgroup H in our classification and we can show $E(\mathbb{Q}^{ab})_{\text{tors}} \supseteq H$. If there are subgroups $H' \geq H$ in our classification, then we can use isogeny counting or division polynomials to rule out the possibility of $E(\mathbb{Q}^{ab}) \cong H'$. For many cases there will not exist larger subgroups H', and so $E(\mathbb{Q}^{ab})_{\text{tors}} \supseteq H$ implies $E(\mathbb{Q}^{ab})_{\text{tors}} \cong H$. We will make note of the cases where we do indeed need to rule out larger subgroups.

For an exmaple of $E(\mathbb{Q}^{ab})_{\text{tors}} = \{\mathcal{O}\}$, we start with the curve E with Cremona Label 37a1 which has only a trivial isogeny. Thus by Lemma 4.2.4 $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ for some m. However, by Corollary 4.2.3, it follows that $m \leq 2$. Now by Proposition 4.2.6 we see that if $m = 2$ then, since E has no 2-isogenies, the discriminant of E must be a square. However, the discriminant of E is 37 and thus

$m = 1$.

For an example of $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/3\mathbb{Z}$, we start with the curve E with Cremona Label 44a1 with one isogeny of degree 3 and no other non-trivial isogenies. Thus by Lemma 4.2.4 $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z}$ for some m. However, by the classification in Theorem 1.3.5 it follows that $m \leq 3$. However, by Corollary 4.2.3, it follows that $m \neq 3$. Now by Proposition 4.2.6 we see that if $m = 2$ then, since E has no 2-isogenies, the discriminant of E must be a square. However, the discriminant of E is 44 and thus $m = 1$.

For an example of $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/5\mathbb{Z}$, we start with the curve E with Cremona Label 38b1 with one isogeny of degree 5 and no other non-trivial isogenies. Thus by Lemma 4.2.4 $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/5m\mathbb{Z}$ for some m. However, by the classification in Theorem 1.3.5 it follows that $m = 1$ or 2. Similar to before, since the discriminant of E is 38 which is not a square and E has no 2-isogenies, it follows that $m = 1$.

For an example of $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/7\mathbb{Z}$, we start with the curve E with Cremona Label 26b1 with one isogeny of degree 7 and no other non-trivial isogenies. Thus by Lemma 4.2.4 $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/7m\mathbb{Z}$ for some m. However, by the classification in Theorem 1.3.5 it follows that $m = 1$ or 2. Similar to before, since the discriminant of E is 26 which is not a square and E has no 2-isogenies, it follows that $m = 1$.

For an example of $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/9\mathbb{Z}$, we start with the curve E with Cremona Label 54b3 with isogenies of degrees 1, 3, and 9. We compute that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/9\mathbb{Z}$, and so $E(\mathbb{Q})^{ab}_{\text{tors}} \cong \mathbb{Z}/9\mathbb{Z}, \quad \mathbb{Z}/3/Z \times \mathbb{Z}/9\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$. Similar to before, since the discriminant of E is 54 which is not a square and E has no 2-isogenies, it follows that $E(\mathbb{Q}^{ab})_{\text{tors}} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$. Now using division polynomials we see that the second independent point of order 3 is defined over the extension given by $x^3 - 27x + 90$, which is not an abelian extension of $\mathbb{Q}$. Thus $E(\mathbb{Q}^{ab})_{\text{tors}} \cong \mathbb{Z}/9\mathbb{Z}$.

For examples with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, we use the information from Proposition 4.2.6 to find an elliptic curve with the correct 2-powered torsion, then use the isogeny information along with Lemma 4.2.4 and Lemma 4.2.1 to determine the rest of the structure.

TABLE 4.2: Torsion from n-isogenies with $X_0(n)$ genus > 0

$E(\mathbb{Q}^{ab})_{\text{tors}}$	$j(E)$	Cremona Label	$\text{Gal}(\mathbb{Q}(E(\mathbb{Q}^{ab})_{\text{tors}})/\mathbb{Q})$
$\mathbb{Z}/11\mathbb{Z}$	$-11 \cdot 131^3$	121A1	$\mathbb{Z}/10\mathbb{Z}$
		121C2	$\mathbb{Z}/5\mathbb{Z}$
	-2^{15}	121B1	$\mathbb{Z}/5\mathbb{Z}$
		121B2	$\mathbb{Z}/10\mathbb{Z}$
	-11^2	121C1	$\mathbb{Z}/10\mathbb{Z}$
		121A2	$\mathbb{Z}/5\mathbb{Z}$
$\mathbb{Z}/15\mathbb{Z}$	$-5^2/2$	50A1	$\mathbb{Z}/4\mathbb{Z}$
		50B3	$\mathbb{Z}/4\mathbb{Z}$
	$-5^2 \cdot 241^3/2^3$	50A2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
		50B4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
	$-5 \cdot 29^3/2^5$	50A3	$\mathbb{Z}/2\mathbb{Z}$
		50B1	$\mathbb{Z}/2\mathbb{Z}$
	$5 \cdot 211^3/2^{15}$	50A4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
		50B2	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/17\mathbb{Z}$	$-17^2 \cdot 101^3/2$	14450P1	$\mathbb{Z}/16\mathbb{Z}$
	$-17 \cdot 373^3/2^{17}$	14450P2	$\mathbb{Z}/8\mathbb{Z}$
$\mathbb{Z}/19\mathbb{Z}$	$-2^{15} \cdot 3^3$	361A1	$\mathbb{Z}/9\mathbb{Z}$
		361A2	$\mathbb{Z}/18\mathbb{Z}$
$\mathbb{Z}/21\mathbb{Z}$	$-3^2 \cdot 5^6/2^3$	162B1	$\mathbb{Z}/3\mathbb{Z}$
		162C2	$\mathbb{Z}/6\mathbb{Z}$
	$3^3 \cdot 5^3/2$	162B2	$\mathbb{Z}/6\mathbb{Z}$
		162C1	$\mathbb{Z}/6\mathbb{Z}$
	$-3^2 \cdot 5^3 \cdot 101^3/2^{21}$	162B3	$\mathbb{Z}/6\mathbb{Z}$
		162C4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
	$-3^3 \cdot 5^3 \cdot 383^3/2^7$	162B4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
		162C3	$\mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z}/27\mathbb{Z}$	$-2^{15} \cdot 3 \cdot 5^3$	27A2	$\mathbb{Z}/18\mathbb{Z}$
		27A4	$\mathbb{Z}/9\mathbb{Z}$
$\mathbb{Z}/37\mathbb{Z}$	$-7 \cdot 11^3$	1225H1	$\mathbb{Z}/12\mathbb{Z}$
	$-7 \cdot 137^3 \cdot 2083^3$	1225H2	$\mathbb{Z}/36\mathbb{Z}$
$\mathbb{Z}/43\mathbb{Z}$	$-2^{18} \cdot 3^3 \cdot 5^3$	1849A1	$\mathbb{Z}/21\mathbb{Z}$
		1849A2	$\mathbb{Z}/42\mathbb{Z}$
$\mathbb{Z}/67\mathbb{Z}$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	4489A1	$\mathbb{Z}/33\mathbb{Z}$
		4489A2	$\mathbb{Z}/66\mathbb{Z}$
$\mathbb{Z}/163\mathbb{Z}$	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	26569A1	$\mathbb{Z}/81\mathbb{Z}$
		26569A2	$\mathbb{Z}/162\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$	$-3^3 \cdot 5^3$	49A1	$\mathbb{Z}/6\mathbb{Z}$
		49A3	$\mathbb{Z}/6\mathbb{Z}$
	$-3^3 \cdot 5^3 \cdot 17^3$	49A2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
		49A4	$\mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$	0	27A1	$\mathbb{Z}/6\mathbb{Z}$
		27A3	$\mathbb{Z}/6\mathbb{Z}$

TABLE 4.3: Examples of remaining torsion subgroups

$E(\mathbb{Q}^{ab})_{\text{tors}}$	$j(E)$	Cremona Label	$\text{Gal}(\mathbb{Q}(E(\mathbb{Q}^{ab})_{\text{tors}})/\mathbb{Q})$
$\{\mathcal{O}\}$	$2^{12} \cdot 3^3/37$	37a1	$\{1\}$
$\mathbb{Z}/3\mathbb{Z}$	$2^{13}/11$	44a1	$\{1\}$
$\mathbb{Z}/5\mathbb{Z}$	$-1/2^5 \cdot 19$	38b1	$\{1\}$
$\mathbb{Z}/7\mathbb{Z}$	$3^3 \cdot 4^3/2^7 \cdot 13$	26b1	$\{1\}$
$\mathbb{Z}/9\mathbb{Z}$	$-3 \cdot 73^3/2^9$	54b3	$\{1\}$
$\mathbb{Z}/13\mathbb{Z}$	$-2^{12} \cdot 7/3$	147b1	$\mathbb{Z}/3\mathbb{Z}$
$\mathbb{Z}/25\mathbb{Z}$	$-2^{12}/11$	11a3	$\mathbb{Z}/5\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$-5^6/3^2 \cdot 23$	69a1	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$11^6/3 \cdot 5 \cdot 7$	315b1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$2^8 \cdot 7$	196a1	$\mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$12721^3/3 \cdot 5 \cdot 7 \cdot 11^2$	3465e1	$(\mathbb{Z}/2\mathbb{Z})^3$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$	$2161^3/2^{10} \cdot 3^5 \cdot 11$	66c1	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	$71^3/2^4 \cdot 3^3 \cdot 5$	30a1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$	$103681^3/3^4 \cdot 5$	15a5	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$	$-5^3 \cdot 1637^3/2^{18} \cdot 7$	14a3	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$-2^{18} \cdot 7^3/19^3$	19a1	$\mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$19^6/3^2 \cdot 5^2 \cdot 7^2$	315b2	$(\mathbb{Z}/2\mathbb{Z})^4$
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$37^3 \cdot 109^3/2^4 \cdot 3^4 \cdot 7^2$	162b2	$(\mathbb{Z}/2\mathbb{Z})^4$
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	$7^3 \cdot 127^3/2^2 \cdot 3^6 \cdot 5^2$	30a2	$(\mathbb{Z}/2\mathbb{Z})^4$
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$	$241^3/3^2 \cdot 5^2$	735e2	$(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$	$-2^{12} \cdot 31^3/11^5$	11a1	$\mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$5^3 \cdot 43^4/2^6 \cdot 7^3$	14a1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$13^3 \cdot 17^3/3^4 \cdot 5^4$	735e4	$(\mathbb{Z}/2\mathbb{Z})^5$

Bibliography

[1] A. Bourdon, P. Clark, *Torsion points and galois representations on CM elliptic curves*, preprint; `http://alpha.math.uga.edu/~pete/Bourdon_Clark_Abbey_12_18.pdf`.

[2] P. Bruin, F. Najman, *A criterion to rule out torsion groups for elliptic curves over number fields*, preprint.

[3] M. Chou, *Torsion of rational elliptic curves over quartic Galois number fields*, J. Number Theory 160 (2016), 603-628.

[4] P. Clark, *Notes on torsion kernels*; exposition, available at request.

[5] P. Clark, P. Corn, A. Rice, J. Stankewicz, *Computation on elliptic curves with complex multiplication*; arXiv:1307.6174v2 [math.NT]

[6] K. Conrad, *Galois groups of cubics and quartics (not characteristic 2)*, expository paper available at `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf`.

[7] H. Daniels, Á. Lozano-Robledo, F. Najman, A. Sutherland, *Torsion subgroups of rational elliptic curves over the compositum of all cubic fields*, submitted, to appear in Mathematics of Computation.

[8] M. Derickx, A. Etropolski, J. Morrow, M. van Hoeij, D. Zureick-Brown, *Sporadic torsion on elliptic curves*, in preparation.

[9] F. Diamond, J. Shurman, *A First Course in Modular Forms*, Springer-Verlag, New York, 2005.

[10] Y. Fujita, *Torsion subgroups of elliptic curves in elementary abelian 2-extensions of* $\mathbb{Q}$, J. Number Theory 114 (2005), 124-134.

[11] E. González-Jiménez, J. Tornero, *Torsion of rational elliptic curves over quadratic fields*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM 108 (2014), 923-934.

[12] E. González-Jiménez, Á. Lozano-Robledo, *Elliptic curves with abelian division fields*, preprint, available at `http://alozano.clas.uconn.edu/research-articles`.

[13] E. González-Jiménez, F. Najman, *Growth of torsion groups of elliptic curves upon base change*, preprint.

[14] D. Jeon, C. H. Kim, *On the arithmetic of certain modular curves*, Acta Arith. 112 (2004), 75-86.

[15] D. Jeon, C. H. Kim, Y. Lee, *Families of elliptic curves over quartic number fields with prescribed torsion subgroups*, Math. Comp. 80 (2011), pp. 2395-2410.

[16] D. Jeon, C. H. Kim, E. Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) 74 (2006), pp. 1-12.

[17] D. Jeon, C.H. Kim, A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. 113 (2004), 291-301.

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

[19] M.A. Kenku *On the number of* $\mathbb{Q}$*-isomorphism classes of elliptic curves in each* $\mathbb{Q}$*-isogeny class*, J. Number Theory 15 (1982), 199-202.

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

[21] A.W. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, NJ, 1992.

[22] M. Laska, M. Lorenz, *Rational points on elliptic curve over* $\mathbb{Q}$ *in elementary abelian 2-extensions of* $\mathbb{Q}$, J. Reine Angew Math. 355 (1985) 163-172.

[23] Á. Lozano-Robledo, *Elliptic Curves, Modular Forms, and their L-functions*, American Mathematical Society, Student Mathematical Library 058, 2011.

[24] Á. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Mathematische Annalen, Vol 357, Issue 1 (2013), 279-305.

[25] Á. Lozano-Robledo, *Uniform boundedness in terms of ramification*, preprint.

[26] B. Mazur, *Rational isogenies of prime degree*, Inventiones Math. 44 (1978), pp. 129 - 162.

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

[28] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$, Math. Res. Letters, to appear.

[29] J. Park, B. Poonen, J. Voight, M. Wood, *A heuristic for boundedness of ranks of elliptic curves*; arXiv:1602.01431 [math.NT].

[30] K. Ribet, *Torsion points of abelian varieties in cyclotomic extensions*, Enseign. Math. 27, pp. 315-319 (1981).

[31] J. Rouse, D. Zureick-Brown, *Elliptic curves over* $\mathbb{Q}$ *and 2-adic images of galois*; arXiv:1402.5997v2 [math.NT].

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

[33] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 2nd Edition, New York, 2009.