Spring 5-22-2021

# Torsion Subgroups Of Rational Elliptic Curves Over Odd Degree Galois Fields

Caleb Mcwhorter
*Syracuse University*, cgmcwhor@syr.edu

# Abstract

The Mordell-Weil Theorem states that if $K$ is a number field and $E/K$ is an elliptic curve that the group of $K$-rational points $E(K)$ is a finitely generated abelian group, i.e. $E(K) \cong \mathbb{Z}^{r_K} \oplus E(K)_{\text{tors}}$, where $r_K$ is the rank of $E$ and $E(K)_{\text{tors}}$ is the subgroup of torsion points on $E$. Unfortunately, very little is known about the rank $r_K$. Even in the case of $K = \mathbb{Q}$, it is not known which ranks are possible or if the ranks are bounded. However, there have been great strides in determining the sets $E(K)_{\text{tors}}$. Progress began in 1977 with Mazur's classification of the possible torsion subgroups $E(\mathbb{Q})_{\text{tors}}$ for rational elliptic curves, and there has since been an explosion of classifications.

Inspired by work of Chou, González-Jiménez, Lozano-Robledo, and Najman, the purpose of this work is to classify the set $\Phi_{\mathbb{Q}}^{\text{Gal}}(9)$, i.e. the set of possible torsion subgroups for rational elliptic curves over nonic Galois fields. We not only completely determine the set $\Phi_{\mathbb{Q}}^{\text{Gal}}(9)$, but we also determine the possible torsion subgroups based on the isomorphism type of $\text{Gal}(K/\mathbb{Q})$. We then determine the possibilities for the growth of torsion from $E(\mathbb{Q})_{\text{tors}}$ to $E(K)_{\text{tors}}$, i.e. what the possibilities are for $E(K)_{\text{tors}} \supseteq E(\mathbb{Q})_{\text{tors}}$ given a fixed torsion subgroup $E(\mathbb{Q})_{\text{tors}}$. Extending the techniques used in the classification of $\Phi_{\mathbb{Q}}^{\text{Gal}}(9)$, we then determine the possible structures over all odd degree Galois fields. Finally, we explicitly determine the sets $\Phi_{\mathbb{Q}}^{\text{Gal}}(d)$ for all odd $d$ based on the prime factorization for $d$ while proving a number of other related results.

# Torsion Subgroups of Rational Elliptic Curves over Odd Degree Galois Fields

by

**Caleb G. McWhorter**

B.A., Ithaca College, 2013

M.S., Syracuse University, 2017

Dissertation

Submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Mathematics

Syracuse University

May 2021

# Acknowledgements

This work is the culmination of a lifelong arc that would not have been possible without the support of many people, all of whom deserve many thanks. First, those who guided me along my mathematical journey: my high school teachers Donna Fallon, Karen Petramale, and Kevin Sullivan, among others, for their tremendous enthusiasm. Then my engaging and dedicated college professors: Dr. David Brown, Dr. James Conklin, Dr. Michael 'Bodhi' Rogers, Dr. Teresa Moore, Dr. Matthew Price, Dr. Scott Thompson, and Dr. Emilie Wiesner for their endless time and consideration, and especially Professor Victor Symonette without whom I may not be here today. Finally, the attentive faculty at Syracuse University: Dr. Uday Banerjee, Dr. Gerald Cargo, Dr. Steven Diaz, Dr. Duane Graysay, Dr. Thomas John, Dr. Leonid Kovalev, Dr. Loredana Lanzani, Dr. Graham Leuschke, Dr. Moira McDermott, Dr. Jeffrey Meyer, Dr. Claudia Miller, and Dr. Dan Zacharia, with a special thanks to my advisor Dr. Steven Diaz for putting up with me for so long. Moreover, thanks to the wonderful staff at Syracuse University: Kim Canino, Kelly Jarvi, Shawn Loner, Julie O'Connor, Sandra Ware, and Glenn Wright for all their time and guidance, excellent conversations, and for helping me to take advantage of so many transformative opportunities. I would also like to thank Professor John Voight and Professor David Zywina for our brief but helpful conversations.

Of course, I would not have had the perseverance to have made it through a Ph.D. program without all the amazing times that my colleagues and friends, especially at Syracuse University, brought to the process: Andrew and Morgan Ascanio, Mehmet Basarat, Will Carrara, Paul Casler, Adam V. D'Agostino, Jacob DeBlois, Ben Dows, Dr. Rachel and Holden Diethorn, Christopher Donohue, Samantha Epstein, Dr. Stephen Farnham, Joshua Fenton, Dr. Andrei Frimu, Ray Garzia, Dr. Stephen Gorgone, Dr. Erin and Ricci Griffin, Adam Harvey, Thomas Heath, Tamir Hemo, Patrick Kanzler, Dr. Nathan Lawless, Dr.

William Lippitt, Casey Necheles, Jessica Posega, Alan Robbins, Dr. Robert Roy, Dr. Eugenia Rosu, Timothy Tribone, Dr. Erin and Bess Tripp, and Nathan Uricchio, Dr. Heather Waymouth, and Ethan Wennberg. But a special thanks to Pablo Diaz and Krystina Lynn Drasher for putting up with me through all these years.

Finally and above all, I would like to thank my family for their endless support, both emotional and financial: Marie, Stephen, and Zachary McWhorter, Heather and Paul Lamos, Amy, Brian, Jeff, Patricia, and Kelly Gilchrist, Mike Patterson, Robert Gilchrist and Marlaine Burbank, Kelly and Michael DeCaprio, and the rest of the Gilchrist, Lamos, and McWhorter family as well as my honorary nieces and nephews. Without them, I would not have been able to accomplish any of this.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

The purpose of this dissertation is to study the possible torsion structures for rational elliptic curves over odd degree Galois fields. We begin this paper by motivating the study of Diophantine equations in Chapter 2. In particular, we will review a bit of the history of Diophantine equations and motivate why elliptic curves constitute perhaps the most interesting class of Diophantine equations—if only for their intrinsic beauty. Then in Chapter 3, we will give an overview of the theory of elliptic curves pertinent to the rest of the paper. For the expert, this chapter can be skipped. For the neophyte, we do not cover enough to have complete command of the theory—merely to make the subsequent results and discussions understandable. We do not assume much familiarity with elliptic curves, but we do assume the reader is familiar with Algebraic Geometry, Algebra, and some Number Theory. In Chapter 4, we review much of what is currently known about torsion subgroups of elliptic curves. Because results in this area are often scattered across dozens of papers and doing research in this area then often means juggling stacks of papers, we hope collecting a 'hefty' amount of results together will be of use.

Starting in Chapter 5, we begin the main purpose of this work—classifying torsion subgroups of rational elliptic curves over odd degree Galois fields. Chapter 5 begins by classifying the possibilities for $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(9)$, i.e. the set of isomorphism classes of torsion subgroups for rational elliptic curves, $E(K)_{\mathrm{tors}}$, where $E$ varies over all rational elliptic curves and $K/\mathbb{Q}$ varies over all nonic Galois fields. We also classify the possibilities for $E(K)_{\mathrm{tors}}$ based on the isomorphism type of $\mathrm{Gal}(K/\mathbb{Q})$, as well as classify the possibilities for torsion growth when base extending $E(\mathbb{Q})_{\mathrm{tors}}$ to a nonic Galois field. We give examples of each such possibility.

In Chapter 6, we begin work towards the main result of this paper, which is classifying the set $\bigcup_{k=0}^{\infty} \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(2k+1)$, i.e. the set of isomorphism classes of torsion subgroups for rational elliptic curves $E(K)_{\mathrm{tors}}$ as $E$ varies over all rational elliptic curves base extended to an odd degree Galois number field. We give examples of each such possibility. Furthermore, we are also able to classify the sets $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ for any odd integer $d$ based solely on the prime factorization of $d$. This result supersedes the result obtained in Chapter 5, in that the main result of Chapter 5 is a special case of our main result in Chapter 6. However, the classification obtained in Chapter 6 depends on the results and techniques developed in Chapter 5. Moreover in the classification of $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(9)$ in Chapter 5, we prove more specific results by classifying the possibilities for $E(K)_{\mathrm{tors}}$ by the isomorphism type of $\mathrm{Gal}(K/\mathbb{Q})$, as well as classifying the possibilities for torsion growth. Chapters 5 and 6 are fairly self-contained in that they often restate results required from previous chapters. Finally in Chapter 7, we discuss possible future research problems based on the work contained herein.

# Chapter 2

# Diophantine Equations

## 2.1 Historical Context

Number Theory is among the oldest fields of Mathematics. This fact is owed mostly to ancient culture's study of Diophantine equations, named in reference to the 3rd century mathematician Diophantus of Alexandria who systematically studied these equations.

**Definition** (Diophantine Equation)**.** A Diophantine equation is an equation of the form $f(x_1, \ldots, x_n) = 0$, where $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, where the only allowed solutions are integers (or more generally rational numbers).

Such equations arose naturally for ancient cultures, especially in the context of resource allocation. For example, Diophantine equations can be found in the Rhind Papyrus of Egypt, the Chinese Jiuzhang, the Babylonian Plimpton, and ancient Indian, Islamic, and Greek texts. As an explicit example, consider Problem 17 of the Jiuzhang found in

[Vog68]: "the price of 1 acre of good land is 300 pieces of gold; the price of 7 acres of bad land is 500. One has purchased altogether 100 acres; the price was 10,000. How much good land was bought and how much bad." This gives a system of equations

$$\begin{aligned} x + y &= 100 \\ 300x + \frac{500}{7} y &= 10,000, \end{aligned}$$

which of course is equivalent to the system of Diophantine equations

$$\begin{aligned} x + y &= 100 \\ 2100x + 500y &= 70,000, \end{aligned}$$

yielding solutions $x = 25/2$ acres and $y = 175/2$ acres. For more on this history with examples, see [Kat09]. Diophantine equations were also studied extensively in European mathematics, especially in the work of Euler, Gauss, Legendre, Dirichlet, Kummer, Sylvester, Weierstrass, Hermite, Eisenstein, Fermat, Kronecker, Dedekind, Germain, Poincaré, etc. The development of tools to study these equations led to enormous growth in Algebraic Geometry, Complex Analysis, Algebraic and Analytic Number Theory, Algebra, etc.

Of course, a Diophantine equation need not have any solutions. For example, the equation $x^2 + y^2 = 3$ has no integer solutions. A fortiori, there are no rational solutions to this equation. To see this, suppose that there were rational numbers satisfying the equation. Clearing denominators, we would then have integers $X, Y, Z$ such that $X^2 + Y^2 = 3Z^2$. Without loss of generality, by cancelling common factors, we assume that $\gcd(X, Y, Z) = 1$. Examining the equation modulo 3, we see that 3 divides $X^2 + Y^2$. But the only possible square values modulo 3 are 0 and 1 so that the only way for $X^2 + Y^2$ to be 0 modulo 3 is for $X^2$ and $Y^2$ to be 0 modulo 3. This implies that $X^2$ and $Y^2$, and hence $X$ and $Y$, are divisible by 3. But this implies that $Z^2$, and hence $Z$, is divisible by 3, a contradiction.

Such "modularity" conditions can be used to prove the nonexistence of rational solutions to equations such as $y^2 = 3x^2 + 2$, $3y = x^2 - 5$, $x^5 + y^5 + z^5 = 2021$, etc. The technique here can be generally summarized as follows: a (rational) solution to a Diophantine equation implies the existence of a real solution and a solution modulo every (prime) modulus. Showing that a certain modulus has no solutions proves the nonexistence of integer solutions.

However, the converse is not necessarily true. This naturally leads to a discussion of the local-to-global (or Hasse) principle, which essentially says that a Diophantine equation over $\mathbb{Q}$ has rational solutions "if and only if" it has a real solution and a solution modulo $n$ for $n \geq 2$. Using the Chinese Remainder Theorem, this is equivalent to the statement that a Diophantine equation over $\mathbb{Q}$ has rational solutions "if and only if" it has a real solution and a solution modulo $p^k$ for all $k$, i.e. a solution in $\mathbb{Q}_p$ for all primes $p$.[1] Of course, this "if and only if" is not an equivalence at all. Selmer gave the example of $3x^3 + 4y^3 + 5z^3 = 0$ in [Sel51], which has only the trivial solution over $\mathbb{Q}$ but possesses a nonzero real solution and a solution in $\mathbb{Q}_p$ for every $p$, see [Conc]. The famous theorem of Hasse-Minkowski states that the local-to-global principle holds for quadratic forms.

**Theorem 2.1** (Hasse-Minkowski)**.** *A homogeneous quadratic equation in several variables is solvable by rational numbers (not all zero) if and only if it is solvable in $\mathbb{Q}_p$ for all $p$, including $p = \infty$.*[2]

David Hilbert asked if there was an algorithm to determine if a given Diophantine equation has a solution. This was Hilbert's Tenth Problem of twenty-three proposed at the 1900 International Congress of Mathematicians in Paris. Matiyasevich, Putnam, and Robinson [Mat93] answered this question in the negative. Of course, one can ask a "Hilbert

[1] We are being intentionally vague and loose on the details here.
[2] $\mathbb{Q}_\infty = \mathbb{R}$.

Tenth Problem" type question for equations over rings other than $\mathbb{Z}$. This is a deep topic with connections to many different areas of Mathematics and is still an active area of research with several papers on the topic being released just this year, e.g. [MRUV20], [EMSW20], or [Spr20]. For more on this topic, see [Poo03].

Table 2.1: A table from [Poo03] indicating whether Hilbert's Tenth Problem holds for various fields of increasing arithmetic complexity (measured by $\mathrm{Gal}(\overline{K}/K)$)

| Ring | Hilbert's $10^{\text{th}}$ |
|---|---|
| $\mathbb{C}$ | ✓ |
| $\mathbb{R}$ | ✓ |
| $\mathbb{F}_q$ | ✓ |
| $p$-adic fields | ✓ |
| $\mathbb{F}_q(\!(t)\!)$ | ? |
| Number Fields | ? |
| $\mathbb{Q}$ | ? |
| Global Function Fields | ✗ |
| $\mathbb{F}_q(t)$ | ✗ |
| $\mathbb{C}(t)$ | ? |
| $\mathbb{C}(t_1, \ldots, t_n)$ | ✗ |
| $\mathbb{R}(t)$ | ✗ |
| $\mathcal{O}_K$ | ≈? |
| $\mathbb{Z}$ | ✗ |

## 2.2 Linear Diophantine Equations

For Diophantine equations in one variable, it is a simple matter to determine all the integer (or rational) solutions to the equation. Using the Rational Roots Theorem, there is a finite list of possible rational solutions (and hence possible integer solutions), which one then need only test.

**Theorem 2.2** (Rational Roots Theorem)**.** *If* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, *then the equation* $f(x) = 0$ *has a rational solution* $x = p/q$, $p, q \in \mathbb{Z}$ *with* $\gcd(p, q) = 1$, *only if* $p \mid a_0$ *and* $q \mid a_n$.

The case of linear Diophantine equations in $n$ variables $x_1, \ldots, x_n$ is also equally simple to

solve. Suppose we had an equation of the form $a_1x_1 + \cdots + a_nx_n = d$, where $a_i, d \in \mathbb{Q}$. Solving for one of the $x_i$, observe that there is always a rational solution (infinitely many if $n > 1$), and that we can parametrize the solutions. What about integer solutions? Clearing denominators, we obtain an equation $a_1'x_1 + \cdots + a_n'x_n = d'$, where $a_i', d' \in \mathbb{Z}$. This equation has integer solutions if and only if $\gcd(a_1', \ldots, a_n')$ divides $d'$, see [Nat00, Thm. 1.15]. Furthermore, it is equally simple to solve linear congruences (though a somewhat more difficult task for higher congruences) using the Chinese Remainder Theorem, the theory of primitive roots, and Quadratic Reciprocity, though we will not discuss this here, see Chapter 2 and 3 of [Nat00].

## 2.3 Quadratic Diophantine Equations

The study of quadratic Diophantine equations is really the study of conics. Of course, we assume our conics are nondegenerate.[3] Consider a conic given by a quadratic Diophantine equation

$$f(x, y) := a + bx + cy + dx^2 + exy + fy^2 = 0.$$

Note that the Hasse Principle does apply for conics. We have already seen in the example of the circle $x^2 + y^2 = 3$ that a conic need not possess any rational points whatsoever. However, when the conic does have a rational point, there is an easy method to find all the rational points on the curve. We will examine this method for the simple case of $x^2 + y^2 = 1$. We will need a theorem of Bézout:

**Theorem 2.3** (Bézout)**.** *Let $F, G \in K[x, y, z]$ be homogeneous curves of degree $m, n$, respectively. Then if $F(\overline{K}) \cap G(\overline{K})$ is nonempty and $F, G$ do not share a homogeneous polynomial of positive degree as a factor, then $F$ and $G$ intersect at precisely $nm$ points in projective space.*[4]

[3] The case of rational points on degenerate conics is not difficult to handle.

[4] We will always assume we count intersections with their multiplicity, which is required in Bézout's Theorem.

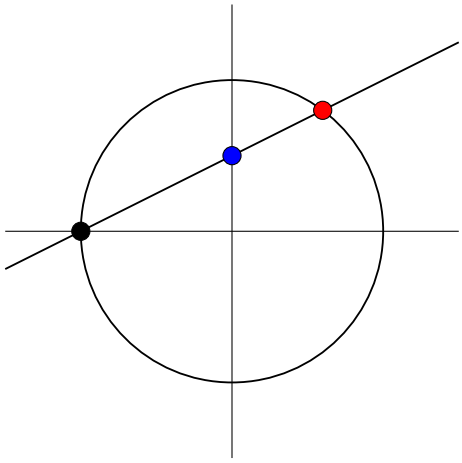


Figure 2.1: Finding the rational points on the circle $x^2 + y^2 = 1$.

The circle $x^2 + y^2 = 1$ has a rational point $(-1, 0)$ (the black point in Figure 2.1). Drawing the line through $(-1, 0)$ and a point $(0, q)$, where $q \in \mathbb{Q}$, this line intersects the circle at another point distinct from $(-1, 0)$ (the red point in Figure 2.1). Moreover, because the point $(-1, 0)$ is rational, this second point of intersection is rational. Conversely, choose a rational point distinct from $(-1, 0)$ on the circle. Drawing the line through this point and $(-1, 0)$, we see this line must intersect the line $x = 0$ at a rational point. With a bit of algebra, we can see that the set of rational points on this circle, $\mathcal{C}(\mathbb{Q})$, is the following:

$$\mathcal{C}(\mathbb{Q}) = \{(-1, 0)\} \cup \left\{ \left( \frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right) : t \in \mathbb{Q} \right\}.$$

The point $(-1, 0)$ corresponds to a vertical line through $(-1, 0)$ which intersects the conic with multiplicity two at $(-1, 0)$ in projective space. The vertical line through $(-1, 0)$ also intersects the line $x = 0$ at the point at infinity. It is then simple to see that $\mathcal{C}(\mathbb{Q})$ is isomorphic to the projective line $\mathbb{P}^1(\mathbb{Q})$.

There is nothing special about the case of the circle. We could have used this approach for any conic with a rational point. In the conic case, we are dealing with curves of degree 2,

so that the genus is 0 by the following well known formula:

$$g = \frac{(d-1)(d-2)}{2}.$$

In fact, a more general result is true.

**Theorem 2.4** ([HS00, Thm. A.4.2.7])**.** *Let $\mathcal{C}$ be a projective plane curve of degree $d$ with only ordinary singularities. Then its genus is given by*

$$g = \frac{(d-1)(d-2)}{2} - \sum_{P \in S} \frac{m_P(m_P-1)}{2},$$

*where $S$ is the set of singular points and $m_P$ is the multiplicity of $\mathcal{C}$ at $P$.*

The converse is true in a sense as well. Suppose $\mathcal{C}$ is a smooth projective curve of genus 0 over a field $F$. Let $K_{\mathcal{C}}$ be a canonical divisor over $F$ associated to $\mathcal{C}$. Using the Riemann-Roch theorem, it is simple to see that $-K_{\mathcal{C}}$ is a very ample divisor of degree 2 over $F$. Then the dimension of the associated embedding is $\ell(-K_C) = 3$. Therefore, $C$ can be embedded into $\mathbb{P}^2$ as a smooth curve of degree 2 defined over $F$, i.e. a conic over $F$. Then the above 'Circle Method' applies whenever this conic has a $F$-rational point. Thus, we have the following description of quadratic Diophantine equations:

**Theorem 2.5.** *Let $C$ be a smooth projective curve of genus 0 defined over a field $F$. Then*

*(i) the curve $\mathcal{C}$ is isomorphic over $F$ to a conic in $\mathbb{P}^2$.*

*(ii) the curve is isomorphic to $\mathbb{P}^1$ over $F$ if and only if it possess a $F$-rational point.*

## 2.4 Higher Diophantine Equations

For Diophantine equations given by polynomial functions of many variables with sufficiently high degree, we can see from Theorem 2.4 that the corresponding curves will have genus $g > 1$. We have already seen that rational points on linear Diophantine equations arise from divisibility conditions 'alone.' In the case of quadratic Diophantine equations, rational solutions arise from the fact (assuming $\mathcal{C}(\mathbb{Q}) \neq \emptyset$) that $\mathcal{C}(\mathbb{Q}) \cong \mathbb{P}^1(\mathbb{Q})$. As a 'moral argument,' one may summarize this as Diophantine equations 'have no business' having rational solutions at all unless there is a 'good reason.' For higher degree Diophantine equations, one might then expect them to have either no rational solutions at all or at most finitely many rational solutions. Indeed, this was Mordell's conjecture in 1922 (or the Mordell-Lang Conjecture). This conjecture was later proved by Gerd Faltings, earning him the Fields Medal.

**Theorem 2.6** (Faltings, [Fal84])**.** *Let $\mathcal{C}/K$ be a smooth, projective, and geometrically irreducible*[5] *curve of genus $g \geq 2$ over a number field $K$. Then the set $\mathcal{C}(K)$ is finite.*

For more on this amazing theorem, see [BS16]. Though Faltings' theorem proves there are at most finitely many rational solutions on higher degree Diophantine equations, it does not say how to actually compute this finite set. Faltings used Arakelov methods for his proof of Theorem 2.6. There are other proofs of Faltings' theorem by Vojta [Voj91] using Diophantine approximation, a proof of Bombieri [Bom90] altering Vojta's approach, and a proof of Lawrence-Vankatesh [LV20] using $p$-adic period maps. Perhaps more importantly, there is a method of Chabauty, using Coleman integration and an adaptation of the $p$-adic method of Skolem, that proves if the Jacobian of $\mathcal{C}$ satisfies $\dim J(\mathcal{C}) < g$ (or generally if $\dim \overline{J(C)} < g$), then $\mathcal{C}(K)$ is finite. Because computing all the $K$-rational points on higher genus curves is a necessity in many torsion classifications, we will give a small flavor of the

[5] The curve stays irreducible after extending to the algebraic closure of $K$.

approach by Chabauty-Coleman, following the description of Poonen [Poo20].

Let $\mathcal{C}/K$ be a smooth projective, geometrically integral curve of genus $g \geq 2$, and let $J$ be the Jacobian of $\mathcal{C}$—an abelian variety of dimension $g$ over $K$—with rank $r$. Let $K/\mathbb{Q}$ be a number field, and $\mathfrak{p}$ a prime above $p$ over which $\mathcal{C}$ has good reduction. Suppose we had a $K$-rational point $\mathcal{O} \in \mathcal{C}(K)$. Then we have an Abel-Jacobi embedding $\iota : \mathcal{C} \hookrightarrow J$ given by $P \mapsto [P - \mathcal{O}]$. If we do not have a $K$-rational point, we can always scale $P$ to find an effective divisor that can serve as a substitute for a $K$-rational point. The idea is to compute $J(\mathcal{C})$, and then determine which of the $K$-rational points in the Jacobian actually lie on $\mathcal{C}$.

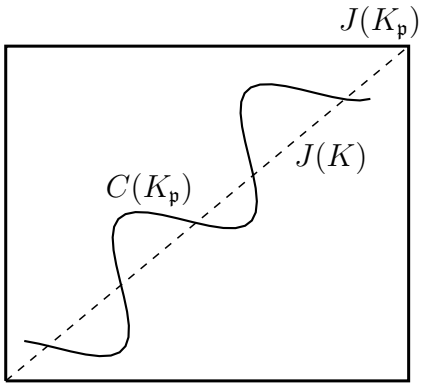



Figure 2.2: A graphical representation of the embedding $C(K_\mathfrak{p})$ into $J(K_\mathfrak{p})$.

Because we have more structure after completion, we will work with the $p$-adic Lie group $K_\mathfrak{p}$. The set $\mathcal{C}(K_\mathfrak{p})$ of local points on the curve $\mathcal{C}$ is an analytic submanifold of the Lie algebra of $J(K_\mathfrak{p})$. Because the $K$-rational points of $\mathcal{C}$ lie in both the Mordell-Weil group of $\mathcal{C}$ and $\mathcal{C}(K_\mathfrak{p})$, what we want to find is the intersection of the Mordell-Weil group of $\mathcal{C}$ (the dotted line in Figure 2.2) with $\mathcal{C}(K_\mathfrak{p})$. The Abel-Jacobi map takes rational points to rational points, so everything is happening inside the ambient Lie group $J(K_\mathfrak{p})$. So the $K$-rational points are in the intersection of the local points $\mathcal{C}(K_\mathfrak{p})$ and the group $J(K)$. We compute this intersection with the hope that this will just be the $K$-rational points with nothing 'extra.' Using the formal logarithm map, we base change from $J(K_\mathfrak{p})$ to

the local field obtained by integrating 1-forms $p$-adically. This takes the group law to an addition law in the vector space $K_{\mathfrak{p}}^g$, where intersections will be simpler to compute. Now assume that $r < g$. There then exists a nonzero functional $\lambda$ vanishing on $\operatorname{im} J(K)$. Now on each residue disk, $\lambda$ is represented by a (nonzero) power series in a 1-dimensional space. Therefore, $\lambda$ has at most finitely many zeros on each closed disk in this compact space. But then $\lambda$ pulls back to a nonzero locally analytic function on $\mathcal{C}(K_{\mathfrak{p}})$ that vanishes on $\mathcal{C}(K)$. Therefore, $\mathcal{C}(K)$ is finite.

**Theorem 2.7** ([Cha41], [Col85, Cor. 4a], [MP12, Thm. 5.3b]). *Let $\mathcal{C}$ be a smooth, projective, and geometrically integral scheme of dimension 1 over* $\operatorname{Spec}(\mathbb{Q})$ *with genus $g \geq 2$ over $\mathbb{Q}$, and let $J$ be its Jacobian variety. Let $p$ be a prime number. Suppose that the rank of $J(\mathbb{Q})$ is smaller than $g$, $p > 2g$, and $\mathcal{C}$ has good reduction at $p$. Then $\#\mathcal{C}(\mathbb{Q}) \leq \#\mathcal{C}(\mathbb{F}_p) + (2g-2)$.*

Obviously, Jacobians are difficult to work with. Moreover, one has the tedious restriction of $r < g$. The work of Minhyong Kim tries to replace Jacobians instead with homology groups of $\mathcal{C}$, developing a non-abelian Chabauty method which is much more powerful than ordinary Chabauty. We will not discuss this further. For more on this topic, see the notes from the 2020 Arizona Winter School at [Ari20]. Finally, we remark there is a much more 'high brow' approach to much of what we have discussed here in terms of general results from Algebraic Number Theory and Algebraic Geometry, see [HS00] and [Poo17].

## 2.5 Curves of Genus $g = 1$

We know (modulo technicalities) that curves of genus $g = 0$ have infinitely many $K$-rational points; moreover, we know how to find them. For curves of genus $g > 1$, we know there are at most finitely many $K$-rational solutions—though finding an effective way to

compute this set (especially in higher genus) is still a difficult open problem. This leaves the case of genus $g = 1$, which is the case of elliptic curves. In a sense, this is the most interesting case in that the set of $K$-rational points can be empty, finite, or infinite. We will not say anything more about elliptic curves here. An overview of the theory of elliptic curves is the purpose of Chapter 3. Instead, we will focus on giving examples of how elliptic curves and hyperelliptic curves (the higher genus 'cousin' of elliptic curves) arise 'in nature.'

## 2.6 Motivating Examples

We will now see a few scenarios in which elliptic (and hyperelliptic) curves naturally arise that highlight why one would be interested in elliptic curves as well as their connection to other areas in Mathematics. We begin with the classic cannonball arrangement.

**Example 2.1** (The Cannon Ball Problem, [Was03])**.** Suppose one has a square pyramid of cannonballs. No longer stable, the pile collapses and the balls scatter. For what size pyramid can these balls now instead be arranged into a square grid? It is clear that this is possible for the trivial pile with 0 cannon balls, as well as a pile with 1 cannon ball. Obviously, there are pile sizes that do not have this property. For instance, if the pile is 2 layers high, then there are 5 total cannon balls, which clearly cannot be arranged into a square grid as 5 is not a perfect square.

If the pyramid began with $x$ layers, then the total number of cannon balls is

$$1^2 + 2^2 + \cdots + x^2 = \frac{x(x+1)(2x+1)}{6}.$$

For these cannonballs to be arranged into a square grid, their total must be a perfect

square; that is, there is a $y \in \mathbb{Z} \subset \mathbb{Q}$ with

$$y^2 = \frac{x(x+1)(2x+1)}{6}. \tag{2.1}$$

A method of Diophantus finds us more points: we know the points $(0,0)$ and $(1,1)$ are on this curve. The line through these points is $y = x$. Intersecting this line with $y^2 = (x(x+1)(2x+1))/6$, we obtain the solution $(1/2, 1/2)$. Clearly, if $(x, y)$ is a solution to the equation, then so is $(x, -y)$. Then we have an additional solution $(1/2, -1/2)$. We can repeat this procedure using the points $(1/2, -1/2)$ and $(1, 1)$. This gives a solution of $(24, 70)$. One can repeat this method of Diophantus to produce more rational solutions—though none of them will be integer valued.

This secant line process of finding rational points is really addition of points on an elliptic curve. After multiplication by 6 in (2.1) and making a substitution of $Y = 72y$ and $X = 12x + 6$, we see that the curve in (2.1) is isomorphic to the elliptic curve $E : Y = X^3 - 36X$ with Cremona label `576h2`. We have $E \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By a theorem of Siegel, c.f. Theorem 3.7, there are only finitely many integer valued points on $E$. In this case, the only integral points are $(0,0)$, $(1, \pm 1)$, and $(24, \pm 70)$. ◁

**Example 2.2** (Fermat's Last Theorem)**.** In a marginal note in Fermat's copy of the *Arithmetica*, Pierre de Fermat noted,

> *"Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."*

That is, he has a truly marvelous proof that $x^n + y^n = z^n$ has no nontrivial solutions for $n > 2$, but the margins were too narrow to contain it. In fact, Fermat's copy of the *Arithmetica* contained many unproven marginal notes, which mathematicians took upon themselves to prove (or in some cases disprove). The problem stated above was the last of these marginal notes to be dealt with and became known as Fermat's Last Theorem (though Fermat's Last Conjecture would have been more appropriate). It would take 329 years for someone to prove this statement, although many tried. For a history of this problem, see [Sin12] or [Rib95]. Fermat's Last Theorem was ultimately proven by Wiles and Taylor-Wiles. In fact, Wiles did not prove Fermat's Last Theorem directly. Instead, Wiles proved a statement about elliptic curves.

In 1984, Gerhard Frey assumed that there was a nontrivial solution $(a, b, c)$ for exponent $p > 2$ to Fermat's equation.[6] He then conjectured that the (semistable) elliptic curve, now called the 'Frey curve',

$$y^2 = x(x - a^p)(x + b^p)$$

would not be modular, although he was unable to prove this, see [Fre86]. This gap became known as the $\epsilon$-conjecture (or epsilon-conjecture), now known as Ribet's Theorem. Serre gave a near proof which was completed in 1986 by Ribet [Rib90]. However, a famous conjecture of Taniyama-Shimura stated that all elliptic curves were modular. Hence to prove Fermat's Last Theorem, it sufficed to prove the Taniyama-Shumura conjecture. Using ideas of Iwasawa Theory, modular forms, and new techniques in Euler systems developed by Flach and Kolyvagin, Wiles gave a near proof of Fermat's Last Theorem in 1993 by proving that all semistable elliptic curves are modular. The proof contained a small gap that was filled in the following year by Wiles and Richard Taylor, a former Ph.D. student of Wiles, see [Wil95] and [TW95]. This was enough to establish Fermat's Last Theorem.

[6] To prove Fermat's Last Theorem, it suffices to prove the theorem for prime $p > 2$.

Later work of Breuil, Conrad, Diamond, Taylor in [CDT99] and [BCDT01] would fully prove the Taniyama-Shimura conjecture (now known as the Modularity Theorem) that all rational elliptic curves are modular. There exist other generalizations of Fermat's Last Theorem: the Generalized Fermat Equation (or Beal conjecture), the Inverse Fermat Equation, etc. ◁

**Example 2.3** (Congruent Number Problem)**.** What natural numbers $n$ are the areas of rational right triangles? We call integers $n$ with this property congruent. An integer $n$ is congruent if and only if there is a rational triplet $(x, y, z)$ with

$$x^2 + y^2 = z^2 \quad \text{and} \quad n = \frac{xy}{2}.$$

The history of this problem dates back to at least the year 972, see [Dic71]. Clearly, 6 is congruent because $3^2 + 4^2 = 5^2$ and $6 = \frac{3(4)}{2}$. However, restricting to integer sides is not sufficient. Observe that the triangle with sides 3/2, 20/3, and 41/6 has area 5, showing that 5 is congruent. Furthermore, 157 is a congruent number, as Zagier proved in [Zag90] with the following example:

$$\begin{aligned} x &= \frac{411340519227716149383203}{21666555693714761309610} \\ y &= \frac{680329848782643505121754 0}{411340519227716149383203} \\ z &= \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}. \end{aligned}$$

It is not known in general which integers are congruent, and given an integer $n$ it is not always a simple task to tell if $n$ is congruent or not. Certainly, if $n$ is congruent, then so too is $m^2 n$ for all natural numbers $m$. Not all integers are congruent numbers. Fermat showed that 1 was not a congruent number using his method of infinite descent. A vast generalization of this type of argument is used in the proof of the Mordell-Weil Theorem.

Now suppose that $n$ is a congruent number, i.e. there is a rational triplet $(X, Y, Z)$ with $X^2 + Y^2 = Z^2$ and $XY = 2n$. Setting $x := (Z/2)^2$ and $y := Z(X - Y)(X + Y)/8$, there is a rational point on the elliptic curve $E_n : y^2 = x^3 - n^2x$. Note that $E_n$ is a twist by $n$ of the elliptic curve $y^2 = x^3 - x$, which is the elliptic curve with Cremona label 32a2. Furthermore, given a rational point $(x, y) \in E_n$, we can define

$$X := \left|\frac{(x-n)(x+n)}{y}\right|, \quad Y := 2n\left|\frac{x}{y}\right|, \quad Z := \left|\frac{x^2+n^2}{y}\right|.$$

It is routine to verify that $X^2 + Y^2 = Z^2$ and that $2n = XY$, so that $n$ is congruent. Therefore, finding congruent numbers is equivalent to finding elliptic curves $E_n$ with rank $r > 0$. While many congruent numbers are known, it is still an open problem to determine which integers $n$ are congruent. However, assuming the Birch and Swinnerton-Dyer conjecture, an amazing theorem of Tunnell gives an effective sufficient and necessary condition for a square-free integer $n$ to be congruent [Tun83]. For more on this problem, see [Kob93]. ◁

**Example 2.4** (A Diophantine Equation)**.** What are the integer solutions to $y^2 = x^3 - 2$? One can 'easily' find the solutions $(3, \pm 5)$, but are these all the solutions? We choose instead to work over the UFD $\mathbb{Z}[\sqrt{-2}]$ in order to make use of the 'extra factorization' it has available. Then over $\mathbb{Z}[\sqrt{-2}]$, we have the factorization

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Writing $x = u_1\pi_1^{e_1} \cdots \pi_r^{e_r}$, where each $\pi_i$ is irreducible, $e_i \geq 1$, and $\pi_i \neq \pm\pi_j$ for $i \neq j$, we then have

$$u_1^3\pi_1^{3e_1} \cdots \pi_r^{3e_r} = (y + \sqrt{-2})(y - \sqrt{-2}).$$

We claim that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are relatively prime. To prove this, choose an irreducible dividing both $y \pm \sqrt{-2}$, say $\pi$. Then $\pi \mid \big((y+\sqrt{-2}) - (y-\sqrt{-2})\big) = 2\sqrt{-2} = (\sqrt{-2})^3$.

By unique factorization in $\mathbb{Z}[\sqrt{-2}]$, up to a unit $u$, we must have $\pi = u\sqrt{-2}$. But the only units in $\mathbb{Z}[\sqrt{-2}]$ are $\{\pm 1\}$. So after scaling by a unit, we have $\pi = \sqrt{-2}$. Now as $\pi \mid (y+\sqrt{-2})$, we have $y+\sqrt{-2} = \pi(a+b\sqrt{-2}) = \sqrt{-2}(a+b\sqrt{-2}) = -2b+a\sqrt{-2}$ for some $a, b \in \mathbb{Z}$. But then as $\pi \mid (y+\sqrt{-2})$, we have $y+\sqrt{-2} = \sqrt{-2}(a+b\sqrt{-2}) = -2b+a\sqrt{-2}$ for some $a, b \in \mathbb{Z}$. Therefore, $y = -2b$, which implies $x^3 = y^2+2 = 4b^2+2 \equiv 2 \mod 4$, a contradiction as no cube has residue 2 mod 4. This shows that $y+\sqrt{-2}$ and $y-\sqrt{-2}$ are relatively prime.

Then $\pi_i^{3e_i}$ divides $y+\sqrt{-2}$ or $y-\sqrt{-2}$ (but not both) for each $1 \leq i \leq r$. Then $y+\sqrt{-2} = u\prod_{i\in\mathcal{I}} \pi_i^{3e_i}$ for some $\mathcal{I} \subseteq \{1,\ldots,r\}$ and $u \in \mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$. This implies

$$y+\sqrt{-2} = u\prod_{i\in\mathcal{I}} \pi_i^{3e_i} = \left(u\prod_{i\in\mathcal{I}} \pi_i^{e_i}\right)^3 = (a+b\sqrt{-2}\,)^3$$

for some $a, b \in \mathbb{Z}$. Expanding yields $y+\sqrt{-2} = (a^3-6ab^2)+(3a^2b-2b^3)\sqrt{-2}$. This forces $y = a^3-6ab^2$ and $1 = 3a^2b-2b^3 = b(3a^2-2b^2)$. Now as $b(3a^2-2b^2) = 1$ with $a, b \in \mathbb{Z}$, it must be that $b \in \{\pm 1\}$. If $b = 1$, we have $3a^2-2 = 1$, which gives $a = \pm 1$. Using $a = \pm 1$ and $b = 1$, we have solutions $(3, \pm 5)$. If $b = -1$, then $3a^2(-1)-2(-1)^3 = 1$, which implies $3a^2 = 1$, a contradiction to the irrationality of $\sqrt{3}$. Therefore, the only integer solutions to $y^2 = x^2+3$ are $(3, \pm 5)$.

This proof is indeed tedious. Moreover, it only proves there are only finitely many integer solutions but says nothing of rational solutions. Worse yet, this approach does not necessarily apply to other quadratic rings. For instance, applying this same argument to $y^2 = x^3-61$ over the ring $\mathbb{Z}[\sqrt{-61}]$, one would 'prove' there are no integer solutions, despite the existence of solutions $(5, \pm 8)$. What fails in this argument is unique factorization in the ring $\mathbb{Z}[\sqrt{-61}]$, which is not a UFD. Generally, this unique factorization argument will not hold for number fields having class number $h_K \neq 1$.

How does one cope with the loss of unique factorization? Kummer (in approximately 1846) said that there should be a further factorization into "ideal numbers" in order to recover unique factorization. This led Dedekind to define ideals of a ring. He later gave the correct notion of factorization using (prime) ideals rather than factorization with elements. While elements may or may not factor uniquely in $\mathcal{O}_K$, the ring of integers of $K$, every ideal of $\mathcal{O}_K$ factors uniquely as a product of prime ideals. In the case of $y^2 = x^3 - 61$, while elements 5, $8 + \sqrt{-61}$, and $8 - \sqrt{-61}$ may not factor uniquely into irreducibles, the ideals generated by these elements will factor uniquely into a product of prime ideals $\mathfrak{p}$, $\mathfrak{q}$:

$$(5) = \mathfrak{pq}, \quad (8 + \sqrt{-61}) = \mathfrak{p}^3, \quad (8 - \sqrt{-61}) = \mathfrak{q}^3.$$

One can avoid all of this by appealing to the theory of elliptic curves. The curve $E : y^2 = x^3 - 2$ is the elliptic curve with Cremona label 1728v1, and $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}$. Hence, there are infinitely many rational solutions. By Siegel's theorem, there are only finitely many integer solutions. Indeed, there are precisely two—namely, $(3 \pm 5)$. ◁

**Example 2.5** (Isosceles Triangle Problem)**.** Does there exist a rational right triangle and a rational isosceles triangle that have the same area and the same perimeter? Supposing that the answer was in the affirmative, we could construct the triangles in Figure 2.3, where $k, t, u \in \mathbb{Q}$, $0 < t < 1$, $0 < u < 1$, and $k > 0$.

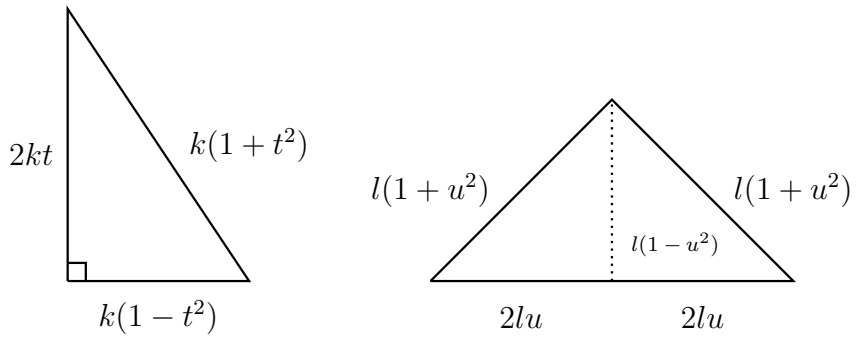



Figure 2.3: A hypothetical pairing of a rational right triangle and rational isosceles triangle with the same area and perimeter.

Rescaling each triangle by the same factor preserves the equality of the area and the perimeter. Therefore without loss of generality, we may assume that $l = 1$. Equating the areas and perimeters, we find the following simultaneous system of equations:

$$\begin{cases} k^2t(1-t^2) = 2u(1-u^2) \\ k + kt = 1 + 2u + u^2. \end{cases}$$

Define $x := u + 1$. Then reframing these equations using $x$, we obtain

$$\begin{cases} k^2t(1-t^2) = 2x(x-1)(x-2) \\ k(1+t) = x^2. \end{cases}$$

Writing the first line as $kt(1-t)\cdot k(1+t)$ and solving for $t$ and $1-t$ in the second equation, we can make the substitutions

$$k(1+t) = x^2, \quad t = \frac{x^2-k}{k}, \quad 1-t = \frac{2k-x^2}{k},$$

to obtain the equation

$$x^2(x^2-k)(2k-x^2) = 2kx(x-1)(x-2).$$

Noting that $0 < u < 1$, we know that $x > 0$. Dividing both sides of the equation by $x$, expanding, and writing this equation as a quadratic polynomial in $k$, we see there exists $x \in \mathbb{Q}$, $1 < x < 2$, such that

$$2xk^2 + (-3x^2 - 2x^2 + 6x - 4)k + x^5 = 0.$$

For there to be a rational solution to this equation, the discriminant of this polynomial in

$k$ must be a rational square. But then for some $y \in \mathbb{Q}$, we have

$$y^2 = (-3x^2 - 2x^2 + 6x - 4)^2 - 4(2x)x^5 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16.$$

We can then define a curve $\mathcal{C}(\mathbb{Q})$ by

$$\mathcal{C}: \quad y^2 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16.$$

Now $\mathcal{C}$ is a genus 2 hyperelliptic curve (a higher genus 'cousin' to the elliptic curve), and we would like to determine $\mathcal{C}(\mathbb{Q})$. By Theorem 2.6, we know that the set $\mathcal{C}(\mathbb{Q})$ is finite. The Jacobian of $\mathcal{C}$, $J(\mathcal{C})$, has rank $J(\mathbb{Q}) = 1$. Also, the Chabauty-Coleman bound gives $\#\mathcal{C}(\mathbb{Q}) \leq 10$. However, we have yet to actually find any rational points! In fact, we can find

$$\{\infty^{\pm}, (0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3)\} \subseteq \mathcal{C}(\mathbb{Q}).$$

Therefore, we have completely determined $\mathcal{C}(\mathbb{Q})$. Furthermore, the solution corresponding to the rational point $(12/11, 868/11^3)$ gives us a unique pair of such triangles. It was Hirakawa and Matsumura in 2018 that answered this discriminant question (and hence the triangle question), using generalizations of the method of Chabauty-Coleman, in the affirmative. They showed that there is exactly one pair of such triangles.

**Theorem 2.8** ([HM19])**.** *Up to similitude, there exists a unique pair of rational right triangles and a rational isosceles triangle which have the same perimeter and the same area. The unique pair consists of the right triangle with sides* $(377, 135, 352)$ *and isosceles triangle with sides* $(366, 366, 132)$*.*

# Chapter 3

# Elliptic Curves

In this chapter, we will as briefly as possible cover the core background of elliptic curves that one needs to understand the main results and follow the references therein. We do not assume much familiarity with elliptic curves. However, we do assume the reader is familiar with Algebra and Algebraic Geometry, along with at least passing knowledge of some Number Theory. The primary reference used here is standard reference for elliptic curves, namely [Sil09]. Although, we have diverged from the presentation in [Sil09] whenever necessary. Throughout, unless otherwise specified, all fields will have characteristic 0. We will not discuss the theory elliptic curves over finite, local, or function fields. Should the reader want to go further (and there is a vast ocean we have ignored), one can see [Sil09] or any number of other common references on the topic: [ST15], [Was03], [Kna92], [Mil06], etc. The author particularly recommends [Hus04] for its readability.

## 3.1 The Group Law & Weierstrass Equations

Suppose we begin with a smooth homogenous polynomial of degree 3 over a field $K$ with a $K$-rational point. We write $F(X, Y, Z)$ as in (3.1) and examine the curve defined by $F(X, Y, Z) = 0$. Note that any smooth cubic curve with a $K$-rational point can be put into this form via homogenization. Call the given $K$-rational point $P$.

$$\begin{aligned} F(X, Y, Z) := aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z \\ + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3 \end{aligned} \tag{3.1}$$

Because $F(X, Y, Z)$ is smooth, we can form the tangent line to $F$ at $P$. Now choose coordinates so that this tangent line is the line $Z = 0$. By Bézout's Theorem, c.f. Theorem 2.3, we know that this new line $Z = 0$ intersects the curve at another point, say $Q$. Again because the curve is smooth, we can form the tangent line to the curve at $Q$ and choose coordinates so that this tangent line is the line $X = 0$. Finally, choose any line through $P$ distinct from the tangent line at $P$ and choose coordinates so that this is the line $Y = 0$. With this new coordinate system, we have a curve $\widetilde{F}(X, Y, Z) = 0$ given by a smooth homogenous polynomial of degree 3 containing $P = [1, 0, 0]$ and $Q = [0, 1, 0]$. Routine verification checks that we have

$$\widetilde{F}(X, Y, Z) := rXY^2 + sZ\phi(X, Y, Z),$$

where $\phi(X, Y, Z)$ is a homogenous polynomial of degree 2 and $r, s \in K$. Dehomogenizing the curve $\widetilde{F}$, we have a smooth cubic curve

$$f(x, y) := xy^2 + ax^2 + bxy + cy^2 + dx + ey + g = 0, \tag{3.2}$$

where the $a, b, c, d, e, g \in K$ in (3.2) are not necessarily those in (3.1). By abuse of notation, make the change of variables $x := x + c$ to obtain an equation

$$xy^2 + (ax + b)y = cx^2 + dx + e,$$

for a possibly new set of $a, b, c, d, e$. Multiplying by $x$, we have

$$(xy)^2 + (ax + b)xy = cx^3 + dx^2 + ex.$$

Again by abuse of notation, make the change of variables $y := yx$ to obtain the equation

$$y^2 + axy + by = cx^3 + dx^2 + ex,$$

which is the Weierstrass form of an elliptic curve.[1] Completing the square by making the substitution $y := y - \frac{1}{2}(ax + b)$, one obtains an equation of the form $y^2 = f(x)$, where $f(x)$ is a cubic polynomial (not necessarily monic). Say that $\alpha$ is the leading coefficient of $f(x)$. As one final abuse of the notation, after making the change of variables $x := x/\alpha$ and $y := y/\alpha^2$, we obtain an equation

$$y^2 = x^3 + ax^2 + bx + c$$

for some $a, b, c \in K$. Following all these substitutions, the resulting transformation by taking the composite of all the substitutions is not linear, but the transformation is rational, which will preserve the underlying elliptic curve. If one desires, making the additional substitution $x := x - \alpha$ (for some carefully chosen $\alpha \in K$) eliminates the $x^2$-term to obtain

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

[1] Generally, the Weierstrass form is $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, where $a_1, a_2, a_3, a_4, a_6 \in K$.

which is again called the (short) Weierstrass form of the elliptic curve. Given that we have studied linear and quadratic (homogeneous) polynomial equations, homogeneous cubic polynomial equations was the next natural step. After the transformations above, we see that this is the same as studying a polynomial $y^2 = x^3 + Ax + B$, which will be one of the many equivalent definitions for an elliptic curve.

**Definition** (Elliptic Curve)**.** An elliptic curve defined over a field $K$, denoted $E/K$, is any of the following equivalent objects:

(i) A smooth projective curve of genus 1 over $K$ with a distinguished $K$-rational point.

(ii) The set $\{(x, y) \colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \Delta_E \neq 0\} \cup \{\infty\}$ with an addition structure given by the Chord-Tangent Law.

(iii) The set $\{(x, y) \colon y^2 = x^3 + Ax + B, -16(4A^3 + 27B^2) \neq 0\} \cup \{\infty\}$ with an addition structure given by the Chord-Tangent Law.

(iv) A compact Riemann surface of genus 1.[2]

(v) An abelian variety of dimension 1 over $K$.

We will only briefly describe how these definitions are equivalent. For a thorough discussion of these equivalencies, see any "standard" elliptic curve reference, e.g. [Hus04], [Sil09], [Was03], [Kna92], [Mil06], etc. Before discussing the addition law on an elliptic curve, we examine their "set structure." We begin with the equation in (ii), called the (general) Weierstrass form of an elliptic curve:

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

[2]For this isomorphism, we need $K = \mathbb{C}$.

Denote by $\{\infty\}$ the point at infinity, $\mathcal{O} := [0, 1, 0]$. If $\operatorname{char} \overline{K} \neq 2$, we can complete the square by making the substitution

$$y \mapsto \frac{1}{2}(y - a_1 x - a_3),$$

which gives an equation of the form $y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$, where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1 a_3$, $b_6 = a_3^2 + 4a_5$. Define

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \qquad \Delta_E = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$$

$$c_4 = b_2^2 - 24b_4 \qquad j = \frac{c_4^3}{\Delta_E}$$

$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6 \qquad \omega = \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y}.$$

We call $\Delta_E$, or just $\Delta$, the discriminant of $E$, $j$ the $j$-invariant of $E$, and $\omega$ the invariant differential associated to the equation for $E$. It is routine to verify that $4b_8 = b_2 b_6 - b_4^2$ and $1728\Delta = c_4^3 - c_6^2$. Assume also that $\operatorname{char} \overline{K} \neq 2, 3$. Then we can make the substitution

$$(x, y) \mapsto \left( \frac{x - 3b_2}{36}, \frac{y}{108} \right),$$

which eliminates the $x^2$ term, so that we obtain $y^2 = x^3 - 27c_4 x - 54c_6$—which is also referred to as the (short) Weierstrass form for $E$. Of course, there are many different equations that give the same elliptic curve. However, if one assumes that the line $Z = 0$ in projective space intersects $E$ only at $\mathcal{O}$, the only change of variables fixing $\mathcal{O}$ and preserving the Weierstrass form is $x = u^2 x' + r$ and $y = u^3 y' + u^2 s x' + t$, where $u, r, s, t \in \overline{K}$ and $u \neq 0$.

One can compute the new $a_i$'s obtained after such a substitution:

$$
\begin{aligned}
ua_1' &= a_1 + 2s & u^6 b_6' &= b_6 + 2rb_4 + r^2 b_2 + 4r^3 \\
u^2 a_2' &= a_2 - sa_1 + 3r - s^2 & u^8 b_8' &= b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \\
u^3 a_3' &= a_3 + ra_1 + 2t & u^4 c_4' &= c_4 \\
u^4 a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st & u^6 c_6' &= c_6 \\
u^6 a_6' &= a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1 & u^{12}\Delta' &= \Delta \\
u^2 b_2' &= b_2 + 12r & j' &= j \\
u^4 b_4' &= b_4 + rb_2 + 6r^2 & u^{-1}\omega' &= \omega.
\end{aligned}
$$

For more on all this, see [Sil09, III.1]. Take note that after such a substitution, $\Delta$ differs from $\Delta'$ by a square in $K$, while $j$ remains invariant—hence the name.

**Proposition 3.1** ([Sil09, III.1, Prop. 1.4])**.**

*(a) The curve given by a Weierstrass equation satisfies:*

*(i) It is nonsingular if and only if* $\Delta \neq 0$.

*(ii) It has a node if and only if* $\Delta = 0$ *and* $c_4 \neq 0$.

*(iii) It has a cusp if and only if* $\Delta = c_4 = 0$.

*In cases (ii) and (iii), there is only one singular point.*

*(b) Two elliptic curves are isomorphic over* $\overline{K}$ *if and only if they both have the same* $j$*-invariant.*

*(c) Let* $j_0 \in \overline{K}$*. There exists an elliptic curve defined over* $K(j_0)$ *whose* $j$*-invariant is equal to* $j_0$.

If $E$ has a singularity, essentially, it is a node if has two distinct tangent lines at the singular point, and otherwise the singularity is a cusp. Now assuming $\operatorname{char} \overline{K} \neq 2, 3$, we can write our elliptic curve in short Weierstrass form $y^2 = x^3 + Ax + B$, in which case we can rewrite $\Delta$ and $j$ as

$$\Delta = -16(4A^3 + 27B^2) \quad \text{and} \quad j = -1728\,\frac{(4A)^3}{\Delta}.$$

The only change of variables preserving this form is $x = u^2x'$, $y = u^3y'$ for some $u \in \overline{K}^\times$, in which case $u^4A' = A$, $u^6B' = B$, $u^{12}\Delta' = \Delta$. Under this change of variables, we have

$$y^2 + (a_1u)xy + (a_3u^3)y = x^3 + (a_2u^2)x^2 + (a_4u^4)x + a_6u^6,$$

which explains the peculiar numbering in definition (ii) for an elliptic curve. Now for $j \neq 0, 1729$, a (nonsingular) elliptic curve with $j$-invariant $j_0$ is given by

$$E\colon y^2 + xy = x^3 - \frac{36}{j_0 - 1728}\,x - \frac{1}{j_0 - 1728}.$$

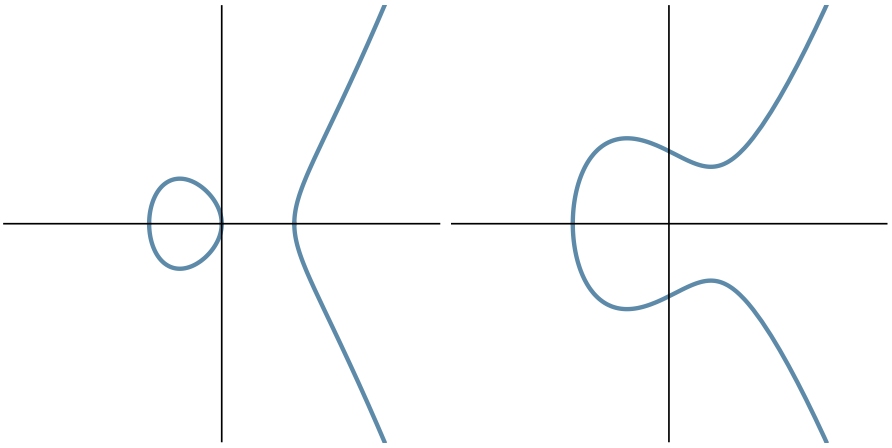
One calculates that for an elliptic curve with this model that $\Delta = j_0^3/(j_0 - 1728)^3$ and $j = j_0$. The elliptic curve with model $y^2 + y = x^3$ has $j$-invariant 0, and the elliptic curve with model $y^2 = x^3 + x$ has $j$-invariant 0. The $j$-invariant completely characterizes elliptic curves over $\overline{\mathbb{Q}}$ up to isomorphism, hence the name. Certainly, if $E$ and $E'$ are elliptic curves with $j(E) \neq j(E')$, then $E \ncong E'$. However, elliptic curves over a number field $K$ with the same $j$-invariant need not be isomorphic. They are isomorphic over $\overline{\mathbb{Q}}$, but the isomorphism might not be defined over $K$.

**Example 3.1.** The elliptic curve with Cremona label `64a4`, i.e. $y^2 = x^3 + x$, and elliptic curve with Cremona label `3136t1`, i.e. $y^2 = x^3 + 49x$, both have $j$-invariant 1728. However, these cannot be isomorphic as `64a4` has rank 0 while `3136t1` has rank 1. ◁

However, using the fact that an isomorphism must take the form $x = u^2x' + r$ and $y = u^3y' + u^2sx' + t$, where $u, r, s, t \in \overline{K}$, and applying Galois cohomology, one can classify elliptic curves with a given $j$-invariant over an arbitrary field $K$. Although, one will not always need such "heavy machinery" if one makes more specifications about the field(s) involved. For instance, consider elliptic curves over $\mathbb{Q}$ with $j \neq 0, 1728$. Any elliptic curve with the same $j$-invariant as $E : y^2 = x^3 + Ax + B$ must take the form $y^2 = x^3 + d^2Ax + d^3B$ for some nonzero $d \in \mathbb{Q}$ (or equivalently, the form $dy^3 = x^3 + Ax + B$ for a nonzero $d$). We call the curve $E^d : y^2 = x^3 + d^2Ax + d^3B$ the twist of $E$ by $d$. The curve $E^d$ will be isomorphic to $E$ over $\mathbb{Q}$ if and only if $d \in (\mathbb{Q}^\times)^2$, i.e. if $d$ is a nonzero square. Thus, the $\mathbb{Q}$-isomorphism classes of elliptic curves with a given $j$-invariant is isomorphic to $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Suppose that $K$ is an odd degree number field and $d \in K^\times/(K^\times)^2$. If $E/\mathbb{Q}$ is a rational elliptic curve, then for $E^d$ to be rational, clearly $d^2A \in \mathbb{Q}$ and $d^3B \in \mathbb{Q}$. But if $d^2A = q$ for some $q \in \mathbb{Q}$, then $d$ satisfies the polynomial equation $Ax^2 - q = 0$, which implies that $d$ is defined either over a quadratic extension of $\mathbb{Q}$ (impossible as $\mathbb{Q} \subseteq \mathbb{Q}(Ax^2 - q) \subseteq K$ and $K/\mathbb{Q}$ is odd) or that $d \in \mathbb{Q}$.

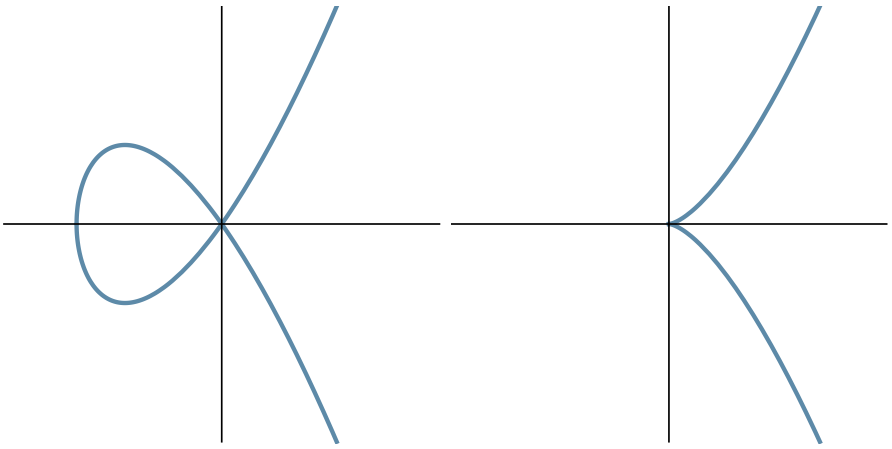
Write an elliptic curve $E$ in short Weierstrass form $y^2 = x^3 + Ax + B$. We know that the equation $x^3 + Ax + B = 0$ has at least one real root. If there is only one real root, then $E$ has one connected real component; otherwise, the equation has three real roots and $E$ has two connected real components. We show some examples of non-singular and singular elliptic curves in Figure 3.1 and Figure 3.2, respectively.

We now define the addition law on an elliptic curve, which is given by the so-called Chord-Tangent Law. We will also refer to as the geometric group law. Say $P$, $Q$ are two (distinct) $K$-rational points on an elliptic curve $E$, where for simplicity we say that $E$ has the form $y^2 = x^3 + Ax + B$. Draw a line through $P$ and $Q$. By Bézout's Theorem, this line will intersect the elliptic curve at another point, say $\widetilde{R}$. Reflect $\widetilde{R}$ across the $x$-axis (noting



(a) $y^2 = x(x^2 + 1)$ (b) $y^2 = x^3 - x + 1$

Figure 3.1: An elliptic curve $y^2 = x^3 + Ax + B$ with 3 real roots, (a), and 1 real root, (b).



(a) $y^2 = x^2(x + 2)$ (b) $y^2 = x^3$

Figure 3.2: An elliptic curve $y^2 = x^3 + Ax + B$ with a node, (a), and a cusp, (b).

that in this form $(x, y) \in E$ if and only if $(x, -y) \in E$), and call this reflected point $R$. We then define $P +_E Q := R$. If $P = Q$, then form the tangent line to $E$ at $P$. This tangent line will intersect $E$ at a point $\widetilde{R}$. Reflecting the point $\widetilde{R}$ across the $x$-axis, we obtain a point $R$ on $E$. We again define $P +_E P := R$. All of these constructions only involve ring operations in $K$, so that $R \in K \times K$, modulo a few minor technical difficulties, and the point $R$ is clearly on $E$. We take the identity under this 'group law' (we have not proved that this is an addition law) to be $\mathcal{O}$, the point at infinity. It is also immediately obvious from this construction that this 'group law' is abelian. Moreover, inverses are clear: $P = (x, y)$

has inverse $-P = (x, -y)$. It only remains to show that the law is associative—which is a tour de force in case work and algebra too gratuitous to go into here. Indeed, in any case, one should prove the law is associative using Algebraic Geometry. A visualization of the Chord-Tangent Law is given in Figure 3.3, where the sum of the red and blue point is the yellow point. One can work out these operations explicitly, see [Sil09, III.2], where one can also see how to handle the singular cases.

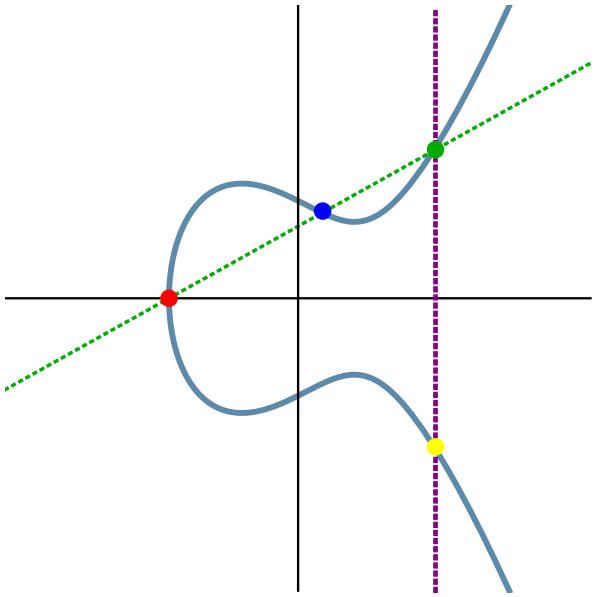


Figure 3.3: The Chord-Tangent Law.

All this discussion has (approximately) shown that definitions (ii) and (iii) for an elliptic curve are equivalent. But why is (i) equivalent to (ii)? Let $C$ be a smooth projective curve of genus 1 with a distinguished $K$-rational point $\mathcal{O}$. There are functions $x, y \in K(C)$ such that the map $\phi : C \to \mathbb{P}^2$ given by $\phi(x, y) = [x, y, 1]$ is an isomorphism to the definition of en elliptic curve $E$ of the form given in definition (ii), see [Sil09, III.3, Prop. 3.1]. This essentially follows from abstract nonsense involving examining the vector space $\mathcal{L}(n\mathcal{O})$ for $n \in \mathbb{N}$, and applying the Riemann-Roch Theorem to find an appropriate basis. Then if $P$, $Q \in E$, we have $(P) \sim (Q)$ if and only if $P = Q$.

**Proposition 3.2** ([Sil09, III.3, Prop. 3.4])**.** *Let $(E, \mathcal{O})$ be an elliptic curve.*

*(i)* *For every degree-0 divisor $D \in \mathrm{Div}^0(E)$ there exists a unique point $P \in E$ satisfying $D \sim (P) - (\mathcal{O})$. Define $\sigma : \mathrm{Div}^0(E) \to E$ to be the map that sends $D$ to its associated $P$.*

*(ii)* *The map $\sigma$ is surjective.*

*(iii)* *Let $D_1, D_2 \in \mathrm{Div}^0(E)$. Then $\sigma(D_1) = \sigma(D_2)$ if and only if $D_1 \sim D_2$. Thus $\sigma$ induces a bijection of sets (which we also denote by $\sigma$), $\sigma : \mathrm{Pic}^0(E) \xrightarrow{\sim} E$.*

*(iv)* *The inverse to $\sigma$ is the map*

$$\begin{aligned} \kappa : E &\xrightarrow{\sim} \mathrm{Pic}^0(E), \\ P &\mapsto \big(\textit{divisor class of } (P) - (\mathcal{O})\big) \end{aligned}$$

*(v)* *If $E$ is given by a Weierstrass equation, then the "geometric group law" on $E$ and the "algebraic group law" induced from $\mathrm{Pic}^0(E)$ using $\sigma$ are the same.*

**Corollary 3.3** ([Sil09, III.3, Cor. 3.5])**.** *Let $E$ be an elliptic curve and let $D = \sum n_p(P) \in \mathrm{Div}\, E$. Then $D$ is a principal divisor if and only if*

$$\sum_{P \in E} n_P = 0 \quad \textit{and} \quad \sum_{P \in E} [n_P]P = \mathcal{O}.$$

*(Note that the first sum is of integers, while the second is addition on $E$.)*

Using the fact that $E \cong \mathrm{Pic}^0(E)$, the associativity of the geometric group law then easily follows. This shows the equivalence of definitions (i) and (ii) for an elliptic curve. Note that of course the equivalence of (i) and (ii) in the definition of an elliptic curve requires choosing a specific affine chart. Choosing different affine charts will result in different forms for the elliptic curve, but these will all be isomorphic. We will be vague on the

equivalence of (i) and (v) for an elliptic curve. Essentially, if $\mathcal{C}$ is a curve of genus 1 and $P \in \mathcal{C}(K)$ is a $K$-rational point, we form the Jacobian variety of $\mathcal{C}$ and the regular map $\phi : \mathcal{C} \to J$ with $\phi(P) = 0$. 'Extending linearly', the natural map from $\mathrm{Div}^0(\mathcal{C}(K))$ to $J(K)$ is an isomorphism.

Perhaps the most interesting equivalence for the definitions of an elliptic curve is between definitions (iii) and (iv). We define a lattice, $\Lambda$, in $\mathbb{C}$ to be an additive subgroup of $\mathbb{C}$ generated by two $\mathbb{R}$-linearly independent complex periods $\omega_1, \omega_2 \in \mathbb{C}$, i.e. $\Lambda = \{a\omega_1 + b\omega_2 \colon a, b \in \mathbb{Z}\}$, where $\omega_1 := a + ci$, $\omega_2 := b + di$ with $a, b, c, d \in \mathbb{R}$ are such that

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0.$$

We say that two lattices $\Lambda$, $\Lambda'$ are homothetic if there is $u \in \mathbb{C}^\times$ such that $\Lambda' = u\Lambda$, i.e. one lattice can be scaled and rotated such that it then coincides with the other lattice. This implies that one can always choose $\omega_1 = 1 \in \mathbb{R}$ by replacing $\Lambda$ with $\frac{1}{\omega_1}\Lambda$. We define a fundamental domain (or a fundamental parallelogram) and its compactification for a lattice to be

$$\mathcal{F}_\Lambda = \{a\omega_1 + b\omega_2 \colon 0 \leq a < 1, 0 \leq b < 1\}$$
$$\overline{\mathcal{F}}_\Lambda = \{a\omega_1 + b\omega_2 \colon 0 \leq a \leq 1, 0 \leq b \leq 1\},$$

respectively. Now as $\Lambda$ is an additive subgroup of $\mathbb{C}$, we can form the quotient $\mathbb{C}/\Lambda$. One can easily write down an isomorphism $\mathbb{C}/\Lambda \cong \mathcal{F}_\Lambda$. One can also obtain this via "gluing" in $\overline{\mathcal{F}}_\Lambda$, i.e. one can find an isomorphism $\mathbb{C}/\Lambda \cong \overline{\mathcal{F}}_\Lambda/\sim$, where $\sim$ the identification of the opposite sides of the parallelogram $\overline{\mathcal{F}}_\Lambda$. But of course, $\mathcal{F}_\Lambda$ is isomorphic to $T := S^1 \times S^1$, i.e. a complex torus. Routine verification checks that $\mathbb{C}/\Lambda$ inherits the topology induced from $\mathbb{C}$, and is homeomorphic to a torus via its identification with $\mathcal{F}_\Lambda$. Moreover, $\mathbb{C}/\Lambda$ inherits the structure of a 1-dimensional complex manifold, so that $\mathbb{C}/\Lambda$ is a Riemann surface of genus 1, i.e. a complex torus. Two such tori, $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$, are isomorphic as Riemann

surfaces if and only if $\Lambda$ and $\Lambda'$ are homothetic.

Now we identify $\mathbb{C}/\Lambda$ with periodic meromorphic functions on $\mathbb{C}$. Define the Weierstrass $\wp$-function, $\wp(z)$, as

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus 0} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Lengthy but routine computations show that the summation on the right above converges absolutely, $\wp(z)$ is meromorphic and periodic, and that the only poles for $\wp(z)$ are double poles at every lattice point $\omega \in \Lambda$. Furthermore,

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$$

has poles only at the lattice points $\omega \in \Lambda$, and these are all triple poles. Make the following definitions:

$$G_{2k} = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^{2k}}, \quad g_2 = 60 G_4, \quad \text{and} \quad g_3 = 140 G_6.$$

One then verifies that the function $\wp'(z)^2 - 4\wp(z)^3 + g_2 \wp(z) + g_3$ has no poles. Furthermore, the numbers $g_2 := g_2(\Lambda)$ and $g_3 := g_3(\Lambda)$ depend only on the choice of lattice, and the sum $G_{2k}$ converges absolutely. It turns out, c.f. [Sil09, VI.3], that any doubly periodic function over $\mathbb{C}$ is a rational function in $\wp(z)$ and $\wp'(z)$, and that the extension $\mathbb{C}(\wp, \wp')/\mathbb{C}(\wp)$ is a quadratic extension. One then shows that $g_2^3 - 27 g_3^2 \neq 0$. Then we define a mapping

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow E(\mathbb{C}) \\ z &\longmapsto (\wp(z), \wp'(z)), \end{aligned}$$

which is an (complex analytic) isomorphism of the complex Lie groups $\mathbb{C}/\Lambda$ and the elliptic curve $y^2 = 4x^3 - g_2 x - g_3$,[3] i.e. a map of complex Riemann surfaces that is also a group

[3] Precisely, its homogenization, so that the map is rightfully $[\wp(z), \wp'(z), 1]$.

homomorphism. One checks that homothetic lattices $\Lambda$, $\Lambda'$ yield isomorphic elliptic curves. For the reverse direction, given an elliptic curve $y^2 = 4x^3 - g_2x - g_3$, we can take $\Lambda$ to be the lattice with periods $\omega_1$, $\omega_2$ given by

$$\omega_1 = \int_\alpha \frac{dx}{y} \quad \text{and} \quad \omega_2 = \int_\beta \frac{dx}{y},$$

where $\alpha$, $\beta$ are closed paths on $E(\mathbb{C})$ that are a basis for $H_1(E, \mathbb{Z})$. This is the so-called Uniformization Theorem, see [Sil09, IV.5, Thm. 5.1]. The computation of $\omega_1$, $\omega_2$ is tedious and involves elliptic functions, choosing branch cuts, etc. However, if we can write $E$ in the form $y^2 = (x - r_1)(x - r_2)(x - r_3)$ over $\mathbb{C}$ with $r_1, r_2, r_3 \in \mathbb{R}$ and $r_1 < r_2 < r_3$, then ignoring technical difficulties, we can write

$$\omega_1 = \int_{r_1}^{r_2} \frac{dx}{\sqrt{(x - r_1)(x - r_2)(x - r_3)}}$$
$$\omega_2 = \int_{r_2}^{r_3} \frac{dx}{\sqrt{(x - r_1)(x - r_2)(x - r_3)}}.$$

This finally completes the equivalences of the definitions for an elliptic curve.

## 3.2 Mordell-Weil Theorem

Now that we know an elliptic curve is a smooth projective curve of genus 1 (with a specified $K$-rational point $\mathcal{O}$) with an addition structure, one might ask what this curve is as an abelian group. Poincaré conjectured in 1901 that the group of rational points on an elliptic curve, $E(\mathbb{Q})$, is a finitely generated abelian group [Poi01]. This conjecture was proved by Mordell in 1922 [Mor22].

**Theorem 3.4** (Mordell, 1922)**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then the group of*

*$\mathbb{Q}$-rational points on $E$, denoted $E(\mathbb{Q})$, is a finitely generated abelian group. In particular,*

$$E(\mathbb{Q}) \cong \mathbb{Z}^{r_{\mathbb{Q}}} \oplus E(\mathbb{Q})_{tors},$$

*where $r_{\mathbb{Q}} \geq 0$ is the rank of $E$ and $E(\mathbb{Q})_{tors}$ is the torsion subgroup of $E$.*

André Weil [Wei29] then generalized Mordell's result in 1929, proving that the group of $K$-rational points on an abelian variety defined over a number field is a finitely generated abelian group.

**Theorem 3.5** (Mordell-Weil, 1928)**.** *Let $K$ be a number field, and let $A/K$ be an abelian variety. Then the group of $K$-rational points on $A$, denoted $A(K)$, is a finitely generated abelian group. In particular,*

$$A(K) \cong \mathbb{Z}^{r_K} \oplus A(K)_{tors},$$

*where $r_K \geq 0$ is the rank of $A$ and $A(K)_{tors}$ is the torsion subgroup.*

This was further generalized by Néron in [Nér52].

**Theorem 3.6** (Mordell-Weil-Néron, 1952)**.** *Let $K$ be a field that is finitely generated over its prime field, and let $A/K$ be an abelian variety. Then the group of $K$-rational points on $A$, denoted $A(K)$, is a finitely generated abelian group. In particular,*

$$A(K) \cong \mathbb{Z}^{r_K} \oplus A(K)_{tors},$$

*where $r_K \geq 0$ is the rank and $A(K)_{tors}$ is the torsion subgroup.*

There exist further generalizations by Lang-Néron [LN59], see [Cona] for further discus-

sion.

From the Mordell–Weil Theorem, it follows that $E(K) \cong \mathbb{Z}^{r_K} \oplus E(K)_{\text{tors}}$, where $r_K$ is the rank of the elliptic curve (depending on $K$) and $E(K)_{\text{tors}}$ is the torsion subgroup of $E$. Though vastly studied, there are very few concrete results on the ranks of elliptic curves $E/K$. Although, there is some progress in studying the growth of the rank over towers of number fields. Even in the case of $K = \mathbb{Q}$, it is not known which ranks are possible, or even if rank are unbounded, i.e. do there exist elliptic curves $E/\mathbb{Q}$ of arbitrary large rank. Note that Shafarevich and Tate [ST67] showed that the rank of elliptic curves over function fields is unbounded. The current rank record is at least 28, due to Elikes.[4] Table 3.1 summarizes historical rank records and can be found in the database [Duj].

Table 3.1: Rank records throughout history

| Rank | Year | Due To |
|---|---|---|
| 3 | 1938 | Billing |
| 4 | 1945 | Wiman |
| 6 | 1974 | Penney/Pomerance |
| 7 | 1975 | Penney/Pomerance |
| 8 | 1977 | Grunewald/Zimmert |
| 9 | 1977 | Brumer/Kramer |
| 12 | 1982 | Mestre |
| 14 | 1986 | Mestre |
| 15 | 1992 | Mestre |
| 17 | 1992 | Nagao |
| 19 | 1992 | Fermigier |
| 20 | 1993 | Nagao |
| 21 | 1994 | Nagao/Kouya |
| 22 | 1997 | Fermigier |
| 23 | 1998 | Martin/McMillen |
| 24 | 2000 | Martin/McMillen |
| 28 | 2006 | Elkies |

The greatest successes in the direction of studying ranks has come from examining how the ranks can grow in towers of number fields, where one employs techniques from Iwa-

[4] Subject to the GRH, the curve has rank exactly 28, see [KSW19].

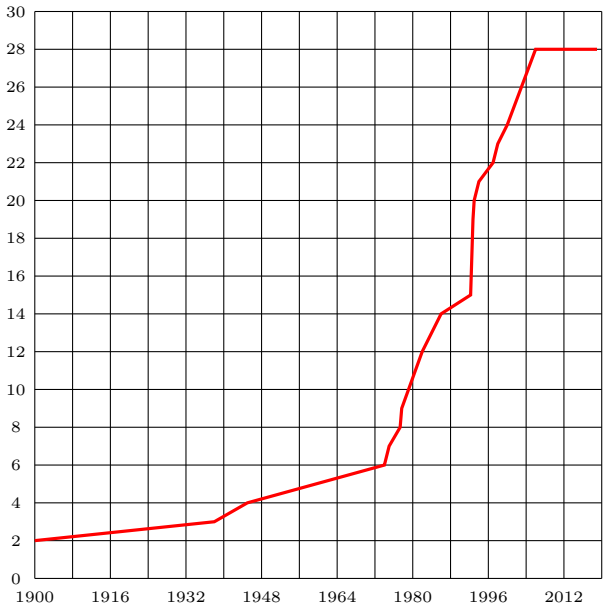



Figure 3.4: Rank records over time.

sawa Theory. However, this is far beyond our scope. There are suggestions that the ranks of elliptic curves over $\mathbb{Q}$ may be bounded. In a recent paper of Machett Wood, Park, Poonen, and Voight [PPVM19], by modeling Shafarevich-Tate groups using certain alternating matrices of specified ranks, they predict that there are only finitely many elliptic curves (up to isomorphism) with rank greater than 21. However, data analyzed by Lozano-Robledo in [LR21] using statistical modeling suggests that there still may be infinite families with large rank. In any case, the rank of an elliptic curve is "typically" small. Specifically, "most" elliptic curves have either rank 0 or rank 1. This is commonly referred to as the minimalist conjecture. We will only comment on this briefly.

To prove the Mordell-Weil Theorem (there is essentially only one proof, they all boil down to the same idea), one must prove that $E(\mathbb{Q})/nE(\mathbb{Q})$ is finite for some $n \geq 2$—typically $n = 2$. This is a vast generalization of the descent technique of Fermat. Let $\mathbb{Q}_p$ be the $p$-adic numbers, where we allow $p = \infty$, i.e. $\mathbb{Q}_\infty = \mathbb{R}$, and fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Denote by $H^1(\mathbb{Q}, E)$ the profinite cohomology group $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E(\overline{\mathbb{Q}}))$. We take

Galois cohomology of the exact sequence

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow 0$$

over $\mathbb{Q}$ and $\mathbb{Q}_p$ for each prime $p$, which gives a long exact sequence (the Kummer sequence), from which we can obtain the following commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, E[n]) & \longrightarrow & H^1(\mathbb{Q}, E)[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \iota_1} & & \downarrow & & \\
0 & \longrightarrow & \prod_{p\leq\infty} E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) & \xrightarrow{\iota_2} & \prod_{p\leq\infty} H^1(\mathbb{Q}_p, E[n]) & \longrightarrow & \prod_{p\leq\infty} H^1(\mathbb{Q}_p, E)[n] & \longrightarrow & 0
\end{array}$$

Because the group $H^1(\mathbb{Q}, E[n])$ is cumbersome to work with, we choose to work locally over $\mathbb{Q}_p$. We then define the $n$-Selmer group

$$\mathrm{Sel}_n(E) := \{x \in H^1(\mathbb{Q}, E[n]) \colon \operatorname{im} \iota_1 \in \operatorname{im} \iota_2\}.$$

Then $\mathrm{Sel}_n E \subseteq H^1(\mathbb{Q}, E[n])$ bounds $E(\mathbb{Q})/nE(\mathbb{Q})$. The group $\mathrm{Sel}_n E$ is finite and computable—though this computation is non-trivial. We then define the Shafarevich-Tate group

$$Ш_E := \ker\left(H^1(\mathbb{Q}, E) \longrightarrow \prod_{p\leq\infty} H^1(\mathbb{Q}_p, E)\right),$$

which then gives an exact sequence

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow \mathrm{Sel}_n E \longrightarrow Ш[n] \longrightarrow 0.$$

It is not known whether $Ш_E$ is finite—although it is conjectured to be finite. Measuring the "average" size of Selmer groups, Bhargava and Shankar [BS15] prove that the "aver-

age" rank of elliptic curves is at most 7/6 in the sense that

$$\lim_{X\to\infty} \frac{\sum_{\mathrm{ht}\, E<X} \operatorname{rank} E}{\sum_{\mathrm{ht}\, E<X} 1} \leq \frac{7}{6},$$

which we shall not make any more precise. Again, this limit is conjectured to be $\frac{1}{2}$—the so-called "50-50 conjecture." Goldfeld has also conjectured that

$$\lim_{D\to\infty} \frac{\#\{E^d \colon d \leq D,\, \operatorname{rank} E^d \geq 1\}}{\#\{E^d \colon d \leq D\}} = \frac{1}{2}.$$

This is typically referred to as Goldfeld's conjecture. We will not make this any more precise. For more on both of these problems, see [BMSW07] and [Poo15]. There is a conjectural formula to compute the rank of an elliptic curve, namely the $1 million prize problem of Birch and Swinnerton-Dyer:

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^{r_E}} \stackrel{?}{=} \frac{\Omega_E \operatorname{Reg}(E) \#Ш(E/\mathbb{Q}) \prod_p c_p}{\#E(\mathbb{Q})^2_{tors}},$$

where $L(E,s)$ is the $L$-function associated to $E$, $r_E$ is the rank of $E$, $\Omega_E = \int_{E(\mathbb{R})} \left|\frac{dx}{y}\right|$, $\operatorname{Reg}(E)$ is the regulator of $E$, and $c_p$ is Tamagawa number of $E$ at $p$, i.e. the cardinality of $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, where $E_0(\mathbb{Q}_p)$ is the set of points in $E(\mathbb{Q}_p)$ whose mod $p$ reduction is nonsingular in $E(\mathbb{F}_p)$.

While the ranks of elliptic curves are quite intractable, the torsion subgroups are much better understood. Treating an elliptic curve $E$ as $\mathbb{C}/\Lambda$, we can easily see that the subgroup of points of order $n$,[5] denoted $E[n]$, is isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. This is demonstrated for $n = 4$ in Figure 3.5.

If instead we restrict to the points of order $n$ defined over a number field $K$ (rather than

[5]By abuse of language, we will say points of order $n$ to mean points $P \in E$ such that $nP = \mathcal{O}$; that is, in more traditional language, points whose order divides $n$.

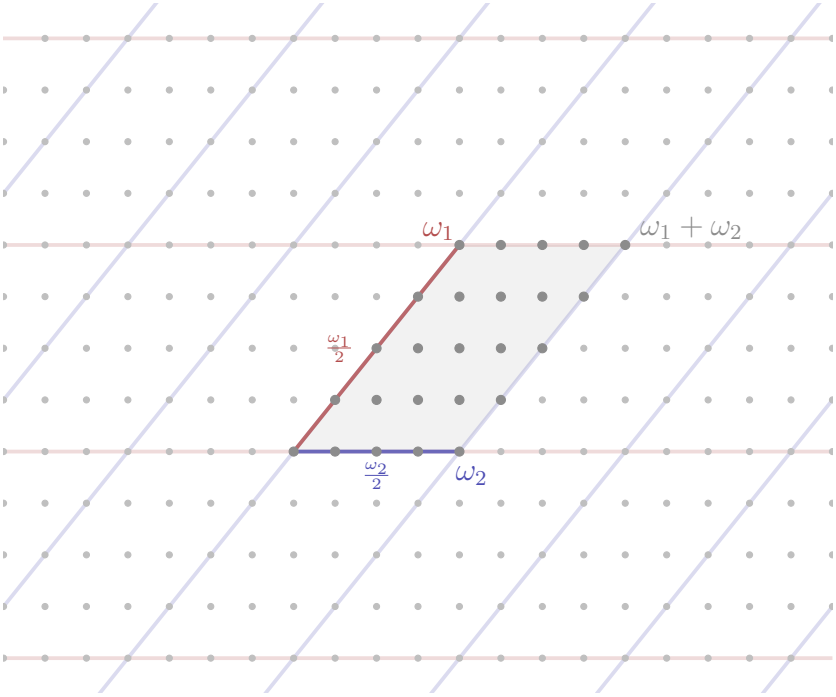



Figure 3.5: The subgroup $E[4]$ via the period parallelogram.

over $\mathbb{C}$), it is well-known (see [Sil09]) that $E(K)_{\text{tors}} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/nm\mathbb{Z}$, where $n, m \geq 1$ are positive integers. Generally, if $A/K$ is an abelian variety with genus $g$, $A(K)_{\text{tors}}$ is a $\mathbb{Z}/n\mathbb{Z}$-module of rank $2g$. Furthermore, fixing a genus $g$, given a finite abelian group with rank $2g$ as a $\mathbb{Z}/n\mathbb{Z}$-module, there is an abelian variety over some field with that specified torsion subgroup.

Finally, we mention in passing two amazing theorems concerning the structure of integral points on elliptic curves.

**Theorem 3.7** (Siegel,[Sil09, IX.3, Thm. 3.1])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the set of integral points on $E$ is finite.*

There are ineffective bounds on the size of these integral points due to Baker [Bak90] in

terms of $A, B$: if $(x, y)$ is an integral point on $E : y^2 = x^3 + Ax + B$, then

$$\max\{|x|, |y|\} \leq \exp\left(\left(10^6 \cdot \max\{|A|, |B|\}\right)^{10^6}\right).$$

**Theorem 3.8** (Nagell-Lutz, [Nag35, Lut37])**.** *Let $E/\mathbb{Q}$ be an elliptic curve with equation $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$. If $P = \big(x(P), y(P)\big) \in E(\mathbb{Q})$ is a nontrivial torsion point, then $x(P)$, $y(P) \in \mathbb{Z}$ and either $y = 0$, i.e. $[2]P = \mathcal{O}$, or $y(P)^2$ divides $\Delta_E$.*

## 3.3 Isogenies

Now that we have defined elliptic curves, we want to define maps between them. These will be isogenies. Note that one makes similar definitions for the case of abelian varieties $A/K$.

**Definition** (Isogeny)**.** Let $E_1$ and $E_2$ be elliptic curves. An isogeny from $E_1$ to $E_2$ is a morphism $\phi : E_1 \to E_2$ with $\phi(\mathcal{O}) = \mathcal{O}$. Two elliptic curves $E_1$ and $E_2$ are isogenous if there is an isogeny from $E_1$ to $E_2$ with $\phi(E_1) \neq \{\mathcal{O}\}$.

From routine Algebraic Geometry, a map of projective curves is either surjective or constant, see [Sil09, II.2.3]. Hence for an isogeny of elliptic curves, we either have $\phi(E_1) = \{\mathcal{O}\}$ or $\phi(E_1) = E_2$. But the only isogeny with $\phi(E_1) = \{\mathcal{O}\}$ is the zero isogeny given by $[0](P) = \mathcal{O}$ for all $P \in E_1$. Alhough it is not immediately obvious, isogenies form an equivalence relation (this follows from the existence of the dual isogeny). An isogeny between elliptic curves induces a map of function fields $\phi^* : \overline{K}(E_2) \to \overline{K}(E_1)$, which by our preceding comments must be an injection.

The degree of an isogeny $\phi$, which we will denote by $\deg \phi$, is the degree of the finite ex-

tension $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$. We define similarly the separable and inseparable degrees for $\phi$, denoted by $\deg_s \phi$ and $\deg_i \phi$, respectively. We also refer to the map $\phi$ as being separable, inseparable, or purely inseparable according to the corresponding property of the field extension $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$. By convention, we set $\deg[0] = 0$ so that $\deg(\psi \circ \phi) = \deg \psi \cdot \deg \phi$ for maps $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$. Because elliptic curves are abelian groups, one can then form $\mathrm{Hom}(E_1, E_2)$ to be the group of isogenies in the usual way. Similarly, one defines $\mathrm{End}\, E := \mathrm{Hom}(E, E)$ in the usual way, where addition in $\mathrm{End}\, E$ is addition on the elliptic curve and multiplication in $\mathrm{End}\, E$ is given by function composition. Then $\mathrm{Aut}\, E$ is the set of invertible endomorphisms. Of course, if $E$ is defined over some field $K$, one may restrict $\mathrm{Hom}(E_1, E_2)$, $\mathrm{End}\, E$, $\mathrm{Aut}\, E$ to just those maps defined over $K$.

Observe that the definition of an isogeny mentions nothing about the fact that the morphisms respect the group law on the elliptic curve. However, it is the case that every isogeny is a homomorphism of elliptic curves (the reverse is also true).

**Theorem 3.9** ([Sil09, III.4.8])**.** *Let $\phi : E_1 \to E_2$ be an isogeny. Then $\phi(P + Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E_1$.*

**Corollary 3.10** ([Sil09, III.4.9])**.** *Let $\phi : E_1 \to E_2$ be a nonzero isogeny. Then $\ker \phi = \phi^{-1}(\mathcal{O})$ is a finite group.*

For an isogeny $\phi : E_1 \to E_2$ with $\#\ker \phi = n$, we say that $E_1$ has a $n$-isogeny. If the map $\phi$ is defined over a field $K$, we say that $E_1$ has a $K$-rational $n$-isogeny. Finally, if $\ker \phi$ is cyclic, we say that $E$ has a cyclic isogeny. Throughout this work, whenever we refer to an isogeny, we will typically mean a $\mathbb{Q}$-rational cyclic isogeny.

**Example 3.2.** For each $m \in \mathbb{Z}$, we define the multiplication-by-$n$ isogeny, $[n] : E \to E$, in

the natural way, i.e. $[n](P)$ is the $n$-fold sum of $P$ on $E$. ◁

**Proposition 3.11** ([Sil09, III.4.2])**.** *Let $E_1/K$ and $E_2/K$ be elliptic curves, and let $n \in \mathbb{Z}$ with $n \neq 0$. Then the multiplication-by-$n$ map $[n] : E \to E$ is nonconstant. Furthermore, the group of isogenies $\operatorname{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module and $\operatorname{End} E$ is a ring of characteristic 0 with no zero divisors (not necessarily commutative).*

Typically, $\operatorname{End} E \cong \mathbb{Z}$ and is entirely composed of the multiplication-by-$n$ maps, i.e. the map $\mathbb{Z} \to \operatorname{End} E$ given by $n \mapsto [n]$ is an isomorphism. Over fields of characteristic 0, this map is always injective so that we can view $\mathbb{Z} \subseteq \operatorname{End} E$.[6] However, there are elliptic curves where this inclusion is strict.

**Example 3.3** ([Sil09, III.4.4])**.** Let $K$ be a field with $\operatorname{char} K \neq 2$, and let $i \in \overline{K}$ be a primitive fourth root of unity, i.e. $i^2 = -1$. Consider the elliptic curve $E/K$ given by $y^2 = x^3 - x$. Observe that we have a map $[i] : E \to E$ given by $(x, y) \mapsto (-x, iy)$. Note that $E$ is defined over $K$ but $[i]$ is defined over $K$ if and only if $i \in K$. Furthermore, observe that

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

so that $[i] \circ [i] = [-1]$. We then have a ring homomorphism $\mathbb{Z}[i] \to \operatorname{End} E$ given by $m + ni \mapsto [m] + [n] \circ [i]$. Assuming $\operatorname{char} K = 0$, this map is an isomorphism, i.e. $\mathbb{Z}[i] \cong \operatorname{End} E$. Then $\operatorname{Aut} E \cong \mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ is a cyclic group of order 4. Elliptic curves with $\operatorname{End} E \supsetneq E$ are said to have CM, or are simply called CM elliptic curves. It is no coincidence that in this example that the endomorphism ring was the ring of integers in an imaginary quadratic field. ◁

**Definition** (CM Elliptic Curve)**.** We say that an elliptic curve $E$ has complex multipli-

[6] Over finite fields, $\operatorname{End} E$ is always strictly larger than $\mathbb{Z}$.

cation, or CM, if $\operatorname{End} E \supsetneq \mathbb{Z}$. It turns out that in our case, $\operatorname{End} E$ will be an order in an imaginary quadratic field $K$ and $\operatorname{End} E \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$, c.f. Theorem 3.18. In this case, we say $E$ has CM by $K$.

With the multiplication-by-$n$ map defined, we can then properly define the $n$-torsion subgroup of $E$.

**Definition** ($n$-torsion subgroup)**.** Let $E$ be an elliptic curve, and let $n \in \mathbb{Z}$ with $n \geq 1$. The $n$-torsion subgroup of $E$, denoted by $E[n]$, is the set of points of $E$ of order $n$, $E[n] = \{P \in E \colon [n]P = \mathcal{O}\}$. The torsion subgroup of $E$, denoted by $E_{\text{tors}}$ is the set of points of finite order on $E$, i.e. $E_{\text{tors}} = \bigcup_{n=1}^{\infty} E[n]$. If $E$ is defined over $K$, then $E(K)_{\text{tors}}$ denotes the points of finite order in $E(K)$.

It is worth noting that one can construct isogenies from finite subgroups of $E$.

**Proposition 3.12** ([Sil09, III.4.12])**.** *Let $E$ be an elliptic curve and let $\Phi$ be a finite subgroup of $E$. There are a unique elliptic curve $E'$ and a separable isogeny $\phi : E \to E'$ satisfying* $\ker \phi = \Phi$.

If $E$ is defined over $K$ and $\Phi$ is $G_{\overline{K}/K}$-invariant, i.e. $T^{\sigma} \in \Phi$ for all $\sigma \in G_{\overline{K}/K}$,[7] then the curve $E'$ and isogeny $\phi$ can be defined over $K$. There are descriptions on how to construct equations for $E'$ and the isogeny $\phi : E \to E'$, c.f. [Vél71].

Finally, although we will not make much use of it, for every nonconstant isogeny of elliptic curves $\phi : E_1 \to E_2$ of degree $n$, there is an isogeny, called the dual isogeny and denoted $\widehat{\phi} : E_2 \to E_1$, with $\widehat{\phi} \circ \phi = [n]$. If $\phi = [0]$, we take $\widehat{\phi} = [0]$.

[7] Throughout, $G_{\overline{K}/K} := \operatorname{Gal}(\overline{K}/K)$, the absolute Galois group of $K$.

**Theorem 3.13** ([Sil09, III.6.2]). *Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves. Then*

*(a) Let $m = \deg \phi$. Then $\widehat{\phi} \circ \phi = [m]$ on $E_1$ and $\phi \circ \widehat{\phi} = [m]$ on $E_2$*

*(b) Let $\lambda : E_2 \to E_3$ be another isogeny. Then $\widehat{\lambda \circ \phi} = \widehat{\phi} \circ \widehat{\lambda}$.*

*(c) Let $\psi : E_1 \to E_2$ be another isogeny. Then $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$.*

*(d) For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ and $\deg[m] = m^2$.*

*(e) $\deg \widehat{\phi} = \deg \phi$*

*(f) $\widehat{\widehat{\phi}} = \phi$.*

For more on dual isogenies, especially its construction, see [Sil09, III.6].

## 3.4 Weil Pairing

Let $E/K$ be an elliptic curve, where $K$ is a field of characteristic $p$. Fix an integer $n \geq 2$, where if $p = \operatorname{char} K > 0$ we assume that $\gcd(n, p) = 1$. We know that the group of $n$-torsion points is $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Therefore, $E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank two. We will define an alternating, nondegenerate multilinear map on $E[n]$. Fix a $\mathbb{Z}/n\mathbb{Z}$-basis for $E[n]$, say $\{P, Q\}$. We then have a determinant map:

$$\det : E[n] \times E[n] \to \mathbb{Z}/n\mathbb{Z}$$
$$\det(aP + bQ, cP + dQ) := ad - bc.$$

Of course, the values of this map depend on the choice of basis. However, selecting a different basis simply scales all of the values of $\det : E[n] \times E[n] \to \mathbb{Z}/n\mathbb{Z}$ by an element of $(\mathbb{Z}/n\mathbb{Z})^\times$. Note also that this map is not Galois invariant: if $P$, $Q \in E[n]$ and $\sigma \in G_{\overline{K}/K}$, then $\det(P^\sigma, Q^\sigma)$ need not be the same as $\det(P, Q)^\sigma$. It would be advantageous to have a

'determinant' map which is Galois invariant. For this, we need the pairing to take values in the $n$th roots of unity. To create such a pairing, we make use of the fact that if $E$ is an elliptic curve and $D = \sum n_P(P) \in \mathrm{Div}(E)$, then $D$ is a principal divisor if and only if $\sum_{P\in E} n_P = 0$ and $\sum_{P\in E}[n_P]P = \mathcal{O}$.

Suppose that $T \in E[n]$. There is a function $f \in \overline{K}(E)$ with $\operatorname{div} f = n(T) - n(\mathcal{O})$. Let $T' \in E$ be a point with $[n]T' = T$. Similarly, we have a function $g \in \overline{K}(E)$ satisfying

$$\operatorname{div} g = [n]^*(T) - [n]^*(\mathcal{O}) = \sum_{R\in E[n]} \big((T' + R) - (R)\big).$$

It is routine to check that $f \circ [n]$ and $g^n$ have the same divisor. Scaling $f$, we can assume that $f \circ [n] = g^n$.

Now suppose that $S \in E[n]$ is an $n$-torsion point (not necessarily distinct from $T$). For $X \in E$,

$$g(X + S)^m = f([n]X + [n]S) = f([n]X) = g(X)^n.$$

Then the function $e_n(X) := g(X + S)/g(X)$ has finite image. But then for all $X$, $e(X)$ is an $n$th root of unity. The map of curves, $E \to \mathbb{P}$, given by $e_n(X)$ then cannot be surjective. But maps of curves are constant or surjective. Therefore, $e_n(X)$ is constant.

We then define a pairing $e_n\colon E[n] \times E[n] \to \mu_n$ by defining $e_n(S, T) = \dfrac{g(X + S)}{g(X)}$, where $X \in E$ is any point such that $g(X + S)$ and $g(X)$ are well-defined and nonzero. While the function $g$ is defined only up to multiplication by some $\alpha \in \overline{K}^\times$, the value of $e_n(S, T)$ is independent of the choice of $\alpha$.

**Definition** (Weil Pairing)**.** We define the map $e_n(S, T)$ described above is called the Weil ($e_n$-)pairing.

There is alternative construction of the Weil pairing: choose $X$, $Y \in E$ and $f_S$, $f_T \in \overline{K}(E)$ with $\operatorname{div} f_S = n(X+S) - n(X)$ and $\operatorname{div} f_T = n(Y+T) - n(Y)$. Then one can define the pairing

$$e_n(S,T) = \frac{f_S(Y+T)}{f_S(Y)} \Big/ \frac{f_T(X+S)}{f_T(X)},$$

though one need check that this map is well defined and is the same as the Weil pairing defined above.

**Proposition 3.14** ([Sil09, III.8.1])**.** *The Weil $e_n$-pairing has the following properties:*

*(a) It is bilinear:*

$$e_n(S_1+S_2,T) = e_n(S_1,T)\, e_n(S_2,T)$$
$$e_n(S,T_1+T_2) = e_n(S,T_1)\, e_n(S,T_2)$$

*(b) It is alternating: $e_n(T,T) = 1$.*

*(c) It is nondegenerate: if $e_n(S,T) = 1$ for all $S \in E[n]$, then $T = \mathcal{O}$.*

*(d) It is Galois invariant: $e_n(S,T)^\sigma = e_n(S^\sigma, T^\sigma)$ for all $\sigma \in G_{\overline{K}/K}$.*

*(e) It is compatible: $e_{nn'}(S,T) = e_n([n']S,T)$ for all $S \in E[nn']$ and $T \in E[n]$.*

The existence of the Weil pairing forces the following useful fact about fields over which full $n$-torsion can be defined.

**Corollary 3.15** ([Sil09, III.8.1.1])**.** *There exist points $S$, $T \in E[n]$ such that $e_n(S,T)$ is a primitive $m$th root of unity. In particular, if $E[n] \subset E(K)$, then $\mu_n \subset K^\times$.*

*Proof.* We give the proof in [Sil09]. As $S$ and $T$ range over $E[n]$, the image of $e_n(S,T)$ is a

subgroup of $\mu_n$, the $n$th roots of unity, say equal to $\mu_d$. It follows that

$$1 = e_n(S,T)^d = e_n([d]S,T) \text{ for all } S,T \in E[n].$$

The nondegeneracy of the $e_n$-pairing implies that $[d]S = \mathcal{O}$, and since $S$ is arbitrary, it follows from [Sil09, III.6.4] that $d = n$. Finally, if $E[n] \subset E(K)$, then the Galois invariance of the $e_n$-pairing implies that $e_n(S,T) \in K^*$ for all $S$, $T \in E[n]$. Hence, $\mu_n \subset K^*$. □

If $\phi : E_1 \to E$ is an isogeny, and $\widehat{\phi}$ its corresponding dual isogeny, then $\phi$ and $\widehat{\phi}$ are dual (or adjoint) with respect to the Weil pairing, see [Sil09, III.8.2]

**Proposition 3.16.** *Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves. Then for all $n$-torsion points $S \in E_1[n]$ and $T \in E_2[n]$, $e_n(S, \widehat{\phi}(T)) = e_n(\phi(S), T)$.*

For a prime $\ell$, one can combine the various $e_{\ell^n}$-pairings compatibly to define a $\ell$-adic Weil pairing on the $\ell$-adic Tate module, $T_\ell(E) := \varprojlim E[\ell^n]$, where the limit is taken over the natural maps $E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n]$, which we will not go into here. But this turns out to be extremely useful. The resulting Weil pairing action on the $\ell$-adic Tate module $T_\ell$ gives a determinant and trace map. Viewing the Tate module as a homology group, we can then compute the degrees of isogenies topologically by examining its action on $H_1(E, \mathbb{Z}_\ell)$. This gives a way of computing points on elliptic curves over finite fields.

**Proposition 3.17** ([Sil09, III.8.6])**.** *Let $\phi \in \operatorname{End} E$ and $\phi_\ell : T_\ell(T) \to T_\ell(E)$ be the map that $\phi$ induces on the Tate module of $E$. Then*

$$\det \phi_\ell = \deg \phi \text{ and } \operatorname{tr}(\phi_\ell) = 1 + \deg \phi - \deg(1 - \phi),$$

*where $\phi_\ell$ comes from the representation $\operatorname{End} E \to \operatorname{End} T_\ell(E)$ given by $\phi \mapsto \phi_\ell$. In particu-*

*lar,* $\det \phi_\ell$ *and* $\operatorname{tr} \phi_\ell$ *are in* $\mathbb{Z}$ *and are independent of* $\ell$*.*

## 3.5 The Endomorphism and Automorphism Groups

Let $E$ be an elliptic curve. It is well known that $\operatorname{End} E$ has characteristic 0, no zero divisors, and rank at most 4 when viewed as a $\mathbb{Z}$-module; moreover, $\operatorname{End} E$ has an anti-involution: $\phi \mapsto \widehat{\phi}$. For $\phi \in \operatorname{End} E$, the product $\phi\,\widehat{\phi}$ is a non-negative integer, and $\phi\,\widehat{\phi} = 0$ if and only if $\phi = 0$, see [Sil09, §III]. Suppose that $\mathcal{K}$ is a (not necessarily commutative) $\mathbb{Q}$-algebra that is also finitely generated over $\mathbb{Q}$. We call $\mathcal{R}$ an order of $\mathcal{K}$ if it is a subring of $\mathcal{K}$ that is finitely generated as a $\mathbb{Z}$-module and satisfies $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$. To give the possibilities for $\operatorname{End} E$, we will need the following definition:

**Definition** ((Definite) Quaternion Algebra)**.** A (definite) quaternion algebra is an algebra of the form $\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$, whose multiplication satisfies $\alpha^2$, $\beta^2 \in \mathbb{Q}$, $\alpha^2 < 0$, $\beta^2 < 0$, and $\beta\alpha = -\alpha\beta$.

**Theorem 3.18** ([Sil09, III.9.3])**.** *Let* $\mathcal{R}$ *be a ring of characteristic 0 having no zero divisors, and assume that* $\mathcal{R}$ *has the following properties:*

*(i)* $\mathcal{R}$ *has rank at most four as a* $\mathbb{Z}$*-module.*

*(ii)* $\mathcal{R}$ *has an anti-involution* $\alpha \mapsto \widehat{\alpha}$ *satisfying* $\widehat{\alpha+\beta} = \widehat{\alpha} + \widehat{\beta}$, $\widehat{\alpha\beta} = \widehat{\beta}\widehat{\alpha}$, $\widehat{\widehat{\alpha}} = \alpha$, $\widehat{a} = a$ *for all* $a \in \mathbb{Z} \subset \mathcal{R}$*.*

*(iii) For* $\alpha \in \mathcal{R}$*, the product* $\alpha\widehat{\alpha}$ *is a nonnegative integer, and* $\alpha\widehat{\alpha} = 0$ *if and only if* $\alpha = 0$*.*

*Then* $\mathcal{R}$ *is one of the following types of rings*

*(a)* $\mathcal{R} \cong \mathbb{Z}$*.*

*(b) $\mathcal{R}$ is an order in an imaginary quadratic extension of $\mathbb{Q}$.*

*(c) $\mathcal{R}$ is an order in a quaternion algebra over $\mathbb{Q}$.*

**Corollary 3.19** ([Sil09, III.9.4])**.** *The endomorphism ring of an elliptic curve $E/K$ is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. If* $\operatorname{char} K = 0$*, then only the first two are possible.*

Complete descriptions of $\operatorname{End} E$ exist, but they are rather tedious. Moreover, it is generally difficult to determine $\operatorname{End} E$ precisely. However, the automorphism group of an elliptic curve $E$ is much simpler.

**Theorem 3.20** ([Sil09, III.10.1])**.** *Let $E/K$ be an elliptic curve. Then its automorphism group* $\operatorname{Aut} E$ *is a finite group of order dividing 24. More precisely, the order of* $\operatorname{Aut} E$ *is given in Table 3.2:*

Table 3.2: The order of $\operatorname{Aut} E$ depending on $j(E)$ and $\operatorname{char} K$

| $\#\operatorname{Aut} E$ | $j(E)$ | $\operatorname{char} K$ |
|---|---|---|
| 2 | $j(E) \neq 0, 1728$ | — |
| 4 | $j(E) = 1728$ | $\operatorname{char} K \neq 2, 3$ |
| 6 | $j(E) = 0$ | $\operatorname{char} K \neq 2, 3$ |
| 12 | $j(E) = 0 = 1728$ | $\operatorname{char} K = 3$ |
| 24 | $j(E) = 0 = 1728$ | $\operatorname{char} K = 2$ |

**Corollary 3.21** ([Sil09, III.10.2])**.** *Let $E/K$ be a curve over a field of characteristic not equal to 2 or 3, let*

$$n = \begin{cases} 2, & \text{if } j(E) \neq 0, 1728 \\ 4, & \text{if } j(E) = 1728 \\ 6, & \text{if } j(E) = 0. \end{cases}$$

*Then there is a natural isomorphism of $G_{\overline{K}/K}$-modules* $\operatorname{Aut} E \cong \mu_n$.

## 3.6 Division Polynomials

Let $E/K$ be a rational elliptic curve given by a model $y^2 = x^3 + Ax + B$, and say that $P = (x, y) \in E(K)$. Suppose that $P$ is a point of order 2, i.e. $2P = \mathcal{O}$. Then we know that $P = -P = (x, -y)$. This implies that $y = -y$ so that $y = 0$. But then $x^3 + Ax + B = 0$ so that $x$ is a root of $x^3 + Ax + B$. Now suppose instead that $P$ is a point of order 3, i.e. $3P = \mathcal{O}$. Then we know that $2P = P$. We can use the duplication formula to find $x(2P)$, i.e. the $x$-coordinate of $2P$. We find that $x(2P)(x)$ is

$$x(2P) = \frac{x^4 - 2Bx^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

Equating $x$ and $x(2P)$, we find that $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$, so that $x$ is a root of $3x^4 + 6Ax^2 + 12Bx - A^2$. We can repeat this process to find conditions for $x \in K$ for $P = (x, y)$ to be a point of order $n$. These conditions will be necessary, but not sufficient. If $x$ is defined over $K$, $y^2 = x^3 + Ax + B$ need not be defined over $K$. However, $y$ will be defined over at most a quadratic extension of $K$. Of course, these polynomials could be reducible, e.g. in the case of a point of order 3, $x$ need not be a root of $3x^4 + 6Ax^2 + 12Bx - A^2$ but rather an irreducible factor of $3x^4 + 6Ax^2 + 12Bx - A^2$. We wish to formalize this process, which will result in the division polynomials for $E$.

Generally speaking, suppose $E$ is an elliptic curve with model $y^2 = x^3 + Ax + B$. By Riemann-Roch, any function with a pole of order 1 at $\mathcal{O}$ is a polynomial in $X$, $Y$, and can be written uniquely as a polynomial in $K[x] \oplus YK[x]$. Then for each integer $n > 0$, we define a polynomial $\psi_{E,n} \in \mathbb{Z}[A, B, x] \oplus y\mathbb{Z}[A, B, x]$, called the $n$-division polynomial for $E$.

We have

$$\operatorname{div}\psi_n = \sum_{Q\in E[n]\setminus\{\mathcal{O}\}} (Q) - (n^2-1)(\mathcal{O}).$$

This shows that if $n$ is odd that $\psi_{E,n} \in \mathbb{Z}[A,B,x]$, and if $n$ is even that $\psi_{E,n} \in y\mathbb{Z}[A,B,x]$. We define the first few $n$-division polynomials as follows:

$$\psi_{E,n} = \begin{cases} 1, & \text{for } n=1, \\ 2y, & \text{for } n=2, \\ 3x^4+6Ax^2+12Bx-A^2, & \text{for } n=3, \\ 4y(x^6+5Ax^4+20Bx^3-5A^2x^2-4ABx-8B^2-A^3), & \text{for } n=4. \end{cases}$$

We define $\psi_n$ for $n>4$ using the recursive relations

$$\begin{cases} \psi_{E,2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, & \text{if } n\geq 2 \\ 2y\psi_{E,2n} = \psi_m(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), & \text{if } n\geq 3. \end{cases}$$

For some polynomials $\phi_n(x)$ and $\omega_n(x,y)$, we have

$$[n]P = \left(\frac{\phi_n(x)}{\psi_{E,n}^2(x)}, \frac{\omega_n(x,y)}{\psi_{E,n}(x,y)^2}\right).$$

Let $E/\mathbb{Q}$ be a rational elliptic curve given by $y^2 = x^3+Ax+B$, and let $P=(x,y)\in E(\overline{\mathbb{Q}})$ be a point of order $n$. If $n$ is odd, then the $x$-coordinate of $P$ is a root of $\psi_{E,n}$ and we can write

$$\frac{1}{n}\psi_{E,n} = \prod \big(x - x(P)\big),$$

where the product is over the nontrivial $n$-torsion points with distinct coordinates.

If $n$ is even (and not 2), the $x$-coordinate of $P\in E[n]\setminus E[2]$ is a root of $\psi_{E,n}/\psi_{E,2}$ and we

can write

$$\frac{2}{n\psi_{E,2}}\psi_{E,n} = \prod \big(x - x(P)\big),$$

where the product is taken over the nontrivial $n$-torsion points ($n \neq 2$) with distinct $x$-coordinates. The polynomial $\psi_{E,n}$ has degree $(n^2-1)/2$.[8] From these equations, we see that if $d \mid n$, then $\psi_{E,d} \mid \psi_{E,n}$. Let $f_{E,n}$ denote the primitive $n$-division polynomial associated to $\psi_{E,2}$, i.e. a polynomial whose roots are the $x$-coordinates of points $P \in E[n]$ of exact order $n$. Note that if $p$ is prime, then $\psi_{E,n} = f_{E,n}$. For composite $n$, we have

$$f_{E,n} = \frac{\psi_{E,n}}{\prod_{\substack{d \mid n \\ d \neq n}} f_{E,d}}.$$

There is an important relation between the division polynomials for $E$ and it's twists by $d$, $E^d$. Let $E^d$ be a quadratic twist of $E/\mathbb{Q}$. Then $\psi_{E,n} = p_d \psi_{E^d,n}$ and $f_{E,n} = q_d f_{E^d,n}$ for some $p_d$, $q_d \in \mathbb{Q}$, depending on $d$. Then the roots of $\psi_{E,n}, \psi_{E^d,n}$ and $f_{E,n}, f_{E^d,n}$ are the same, respectively.

When asking if $E(K)$ contains a point of exact order $n$ over $K$, we (vaguely) define the "method of division polynomials" as follows: if $E/\mathbb{Q}$ is an elliptic curve with $j$-invariant $j_E$ (or a twist of an elliptic curve with $j$-invariant $j_E$), to determine if $E(K)$ contains a point of exact order $n$ over a field $K$, one computes and factors the primitive $n$-division polynomial $f_{E,n} \in \mathbb{Q}[x]$. Suppose that $f_{E,n} = f_1^{n_1} \cdots f_i^{n_i}$, where the $f_i$ are the irreducible factors of $f_{E,n}$ over $\mathbb{Q}[x]$ and $n_i \in \mathbb{Z}^+$. The $x$-coordinate of a point of exact order $n$ is then a root of one of the $f_i$. We can then check if $\mathbb{Q}(f_i) \subseteq K$ for some $i$. If not, there cannot be a point of exact order $n$ on $E$ defined over $K$. For instance, it may be that $K/\mathbb{Q}$ is an odd degree number field and that $\mathbb{Q}(f_i)/\mathbb{Q}$ is an even degree number field. Then it cannot be the case that $\mathbb{Q}(f_i) \subseteq K$. There can be any number of conditions that $\mathbb{Q}(f_i)$ might violate

[8] This is obvious when $n$ is odd. When $n$ is even, this is true so long as we think of $y$ has having 'degree' 3/2 in $x$ from the fact that $y^2 = x^3 + Ax + B$.

to preclude $K \supseteq \mathbb{Q}(f_i)$. Note that even if $\mathbb{Q}(f_i) \subseteq K$ for some $i$, a point of order $n$ may still not be possible as the $y$-coordinate need not be defined over $\mathbb{Q}(f_i) \subseteq K$, but rather defined over a quadratic extension of $\mathbb{Q}(f_i)$ because $y^2 = x^3 + Ax + B$.

## 3.7 Galois Representations

Let $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group. One can use Class Field Theory to understand one-dimensional Galois representations. Let $\rho\colon G_{\mathbb{Q}} \longrightarrow \mathbb{C}^\times \cong \mathrm{GL}_1(\mathbb{C})$ be the one-dimensional Galois representation corresponding to Dirichlet characters $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ via identifying abelian extensions of $\mathbb{Q}$ with cyclotomic extensions obtained by adjoining $n$th roots of unity. We have an isomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, where $\zeta_n$ denotes a primitive $n$th root of unity, taking $k$ with $\gcd(k, N) = 1$ to their $k$th power in a fixed algebraic closure $\overline{\mathbb{Q}}$. There is then a maximal abelian quotient, $G_{\mathbb{Q}}^{\mathrm{ab}} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q})$, where $\zeta_\infty$ denotes the set of all roots of unity in $\overline{\mathbb{Q}}$. Fix a prime $\ell$. We have representations $\chi_n : G_{\mathbb{Q}} \to \mathrm{Aut}(\zeta_{\ell^n}) \cong (\mathbb{Z}/\zeta_n)^\times$. Taking the inverse limit over the $\ell$-power map, we obtain the Tate module, $T_\ell$. The absolute Galois group acts on this limit, and we obtain a representation $\chi : G_{\mathbb{Q}} \to \mathrm{Aut}(T_\ell(\zeta_\infty)) \cong \mathbb{Z}_\ell^\times$.

Similarly, we can use elliptic curves to create 2-dimensional Galois representations, which in return gives us information about the elliptic curve. Let $E/\mathbb{Q}$ be a rational elliptic curve, and fix an integer $n \geq 2$. As usual, let $E[n]$ denote the subgroup of $E(\overline{\mathbb{Q}})$ consisting of points of order $n$, i.e. $E[n] = \{P \in E(\overline{\mathbb{Q}})\colon [n]P = \mathcal{O}\}$. The absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts coordinate-wise on the points of $E[n]$. We then obtain a representation

$$\rho_{E,n}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]).$$

But $E[n]$ is a free rank two $\mathbb{Z}/n\mathbb{Z}$-module. Fixing a basis, say $\{P, Q\}$, for $E[n]$, we know

that $\mathrm{Aut}(E[n])$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. We then have a map

$$\rho_{E,n}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[n]) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Denote by $G_E(n)$ the image of $\rho_{E,n}$ under this composition. While the exact image of this composition depends on the choice of basis, the image is unique up to conjugacy. Denote by $\mathbb{Q}(E[n])$ the field of definition for $E[n]$, i.e. $\mathbb{Q}(E[n]) := \mathbb{Q}(\{x, y\}\colon (x, y) \in E[n]\})$. This is always a finite extension of $\mathbb{Q}$. Furthermore, the extension $\mathbb{Q}(E[n])$ is a Galois extension of $\mathbb{Q}$. It is routine to verify that $\ker \rho_{E,n} = \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(E[n])\right)$. But then by the Galois correspondence, we have $G_E(n) \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. Suppose that $P = (x, y) \in E[n]$. We denote by $x(P)$ and $y(P)$ the $x$ and $y$ coordinates of $P$, respectively. In this notation, we have $\mathbb{Q}(P) = \mathbb{Q}(x(P), y(P))$. Let $H$ be the subgroup of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ corresponding to $\mathbb{Q}(E[n])^H = \mathbb{Q}(P)$ via the Galois correspondence, i.e. $\mathbb{Q}(P)$ is the subfield of $\mathbb{Q}(E[n])$ fixed by $H$. Now define $\widetilde{H} := \rho_{E,n}(H)$. We then have $[\mathbb{Q}(P)\colon \mathbb{Q}] = |G_E(n)\colon \widetilde{H}|$.

A natural question is what are the possible images of $\rho_{E,p}$, where $p$ is a prime. This question was answered by Serre.

**Theorem 3.22** (Serre, [Ser72])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $G_E(p)$ denote the image of $\rho_{E,p}$. Supposing that $G_E(p) \neq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, then there is a $\mathbb{Z}/p\mathbb{Z}$=basis of $E[p]$ such that one of the following possibilities is true:*

*(i) $G_E(p)$ is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, or*

*(ii) $G_E(p)$ is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, or*

*(iii) the projective image of $G$ in $\mathrm{PGL}(E[p])$ is isomorphic to $A_4$, $S_4$, or $A_5$, where $A_n, S_n$ are the alternating and symmetric group, respectively, or*

*(iv)* $G_E(p)$ *is contained in a Borel subgroup of* $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Note that the first case can only occur $p \leq 13$ with $p \neq 11$, the third for $p \leq 13$, and the last for $p = 2$, 3, 5, 7, 11, 13, 17, or 37. We will take care to define the last case in Theorem 3.22, as it will be the case of interest to us. We say that a subgroup $B$ of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ is Borel if every matrix in $B$ is upper triangular, i.e.

$$B \leq \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, c \in \mathbb{Z}/p^n\mathbb{Z}, a, c \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}.$$

Note that if $P \in E(\overline{\mathbb{Q}})$ is a point of order $n$ and $P \in E(K)$, where $K$ is a number field, then we can extend $P$ to a basis of $\{P, Q\}$ for $E[p]$. In particular, $\rho_{E,p}$ is contained in a Borel subgroup. Sutherland computed the mod-$p$ image of all non-CM elliptic curves in the Cremona and Stein-Watkins database—around 140 million elliptic curves. Zywina has also described conjecturally all the proper subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ which occur as images of $\rho_{E,p}$, including all known cases.

**Conjecture 3.23** ([Sut16, Zyw15])**.** *Let* $E/\mathbb{Q}$ *be a rational elliptic curve without CM, and let* $p$ *be a prime. Then there is a set* $S_p$ *formed by* $s_p = |S_p|$ *isomorphism types of subgroups of* $\mathrm{GL}_2(\mathbb{F}_p)$*, where such that if* $G$ *is the image of* $\rho_{E,p}$*, then* $G$ *is conjugate to one*

| $p$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 37 | else |
|---|---|---|---|---|---|---|---|---|---|
| $s_p$ | 3 | 7 | 15 | 16 | 7 | 11 | 2 | 2 | 0 |

*of the subgroups in* $S$*, or* $G \cong \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

## 3.8 Modular Curves

Let the modular group be the group of 2-by-2 matrices with integer entries and determinant 1, i.e. $\mathrm{SL}_2(\mathbb{Z})$. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half plane, $\mathcal{H}$, via fractional

transformations. Let $N$ be a positive integer. We define the principal congruence subgroup of level $N$ to be

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

We say that a subgroup $\Gamma$ of $\mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup if $\Gamma(N) \subseteq \Gamma$ for some $N$, in which case we call $\Gamma$ a congruence subgroup of level $N$. We define also

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} \star & \star \\ 0 & \star \end{pmatrix} \mod N \right\}$$
$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix} \mod N \right\},$$

where $\star$ indicates that the element is unspecified. One can recognize each of these subgroups as the kernel of certain projection maps, and hence are all normal subgroups of $\mathrm{SL}_2(\mathbb{Z})$. Hence, we form the quotient space $Y(\Gamma) := \Gamma \setminus \mathcal{H}$. This quotient space is a Riemann surface—though not necessarily compact. A non-obvious, but nevertheless true, fact is that we can adjoin to $Y(\Gamma)$ finitely many points, called cusps, to form a compact Riemann surface $X(\Gamma)$ (which itself can be recognized as a quotient space). The space $X_0(N)$ is a compact algebraic curve defined over $\mathbb{C}$ with a model over $\mathbb{Q}$.

Now $X_0(N)$ is a moduli space of isomorphism classes of ordered pairs $(E, C)$, where $E$ is an elliptic curve and $C$ is a cyclic subgroup of $E$ with order $N$. Thus, the non-cuspidal $\mathbb{Q}$-rational points of $X_0(N)$ have the following (equivalent) moduli interpretations:

- Isomorphism classes of pairs $(E, C)$, where $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational cyclic subgroup of $E$ with order $n$.

- Isomorphism classes of pairs $(E, \langle P \rangle)$, where $E/\mathbb{Q}$ is an elliptic curve and $P$ is a point of exact order $N$ on $E$.
- Isomorphism classes of triples $(E_1, E_2, \phi)$, where $E_1/\mathbb{Q}$, $E_2/\mathbb{Q}$ are elliptic curves and $\phi : E_1 \to E_2$ is an isogeny with cyclic kernel of cardinality $N$.

Similarly, $X(N)$ classifies the pairs $(E, \{P, Q\})$, where $E$ is an elliptic curve over $K$ and $\{P, Q\}$ is a basis for $E[n]$, and $X_1(N)$ classifies the pairs $(E, P)$, where $E$ is an elliptic curve over $K$ and $P$ is a point of exact order $n$ on $E$.

**Example 3.4** ([Kna92])**.** Let $K$ be a field and $E/K$ be an elliptic curve. Suppose $P \in E(K)$ is a point of exact order 4. Translating the elliptic curve so that $P$ is at the origin, we can write $E$ as $y^2 + cxy + by = x^3 + bx^2$, i.e. the Tate normal form for $E$. Observing that $-2P = (-b, 0)$ and performing some other brief calculations, including a transformation, we find that $E$ is given by $y^2 + xy + by = x^3 + bx^2$. This is a (universal) elliptic curve for $X_1(4)$. The discriminant of this elliptic curve is $-16b^5 + b^4$, so the value $b = 1/16$ corresponds to a cusp on $X_1(4)$. Then for all $b \in K^\times \setminus \{1/16\}$, $Y_1(4)(K)$ is the resulting elliptic curve. The curve $X_1(4)$ is the projective line over $K$, and the complete set of cusps of $X_1(4)$ is $\{\mathcal{O}, 0, 1/16\}$. Of course, $X_1(N)$ need not always be an elliptic curve, and it could be that the genus of $X_1(N)$ is $g = 0$ or $g > 1$. ◁

One of the significant advantages of working with rational elliptic curves is that there is a complete classification of the possible $\mathbb{Q}$-rational points on $X_0(N)$. We do not have such a classification for elliptic curves over any other number field. By the equivalence above, this restricts the possible $\mathbb{Q}$-rational $n$-isogenies a rational elliptic curve can have. This classification was the result of decades of work due to Fricke, Kenku, Kubert, Ligozat, Mazur, Ogg, among others, with Mazur completing the critical classification of $p$-isogenies, where $p$ is a prime, see [LR13] for more detailed references.

**Theorem 3.24.** *Let $N \geq 2$ be such that $X_0(N)$ has a non-cuspidal $\mathbb{Q}$-rational point. Then*

*(i) $N \leq 10$ or $N = 12, 13, 16, 18,$ or $25$. In this case, $X_0(N)$ is a curve of genus 0, and the $\mathbb{Q}$ rational points on $X_0(N)$ form an infinite 1-parameter family, or*

*(ii) $N = 11, 14, 15, 17, 19, 21,$ or $27$, i.e. $X_0(N)$ is a rational elliptic curve (in each case $X_0(N)(\mathbb{Q})$) is finite, or*

*(iii) $N = 37, 43, 67,$ or $163$. In this case, $X_0(N)$ is a curve of genus $\geq 2$ and by Faltings' Theorem has only finitely many $\mathbb{Q}$-rational points.*

*In particular, a rational elliptic curve may only have a rational cyclic $n$-isogeny for $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$. Furthermore, if $E$ does not have CM, then $n \leq 18$ or $n \in \{21, 25, 37\}$.*

For more on all of these topics, see [DS05].

## 3.9 CM Elliptic Curves

The theory of elliptic curves with CM is a deep subject area, making extensive use of the theory of complex multiplication and Class Field Theory. Obviously, going too deep is far beyond the scope of this work. We will only give an overview for the extra structure afforded to elliptic curves with CM. For more on this topic, see [Sil94].

Recall that $E/K$ has CM if $\operatorname{End} E \supsetneq \mathbb{Z}$. In this case, $\operatorname{End} E$ is isomorphic to an order in an imaginary quadratic extension of $\mathbb{Q}$, say $K$, and $\operatorname{End} E \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$. Let $K/\mathbb{Q}$ be a number field (or in more general cases, a global field). We define the modulus $\mathfrak{m}$ of $K$ to be $\prod_{\mathfrak{p}} \mathfrak{p}^{m(p)}$, where the product is taken over all real and finite places of $\mathfrak{p}$. Note that

$m(\mathfrak{p}) \geq 0$ for all $\mathfrak{p}$, with all but finitely many $m(\mathfrak{p}) = 0$, and $m(\mathfrak{p}) < 1$ if $\mathfrak{p}$ is a real place. We denote by $K_{\mathfrak{m},1}$ the set of all $a \in K^\times$ so that $\mathrm{ord}_p(a-1) \geq m(\mathfrak{p})$ for all finite $\mathfrak{p} \mid \mathfrak{m}$ and $\sigma(a) > 1$ for all real $\mathfrak{p} \mid \mathfrak{m}$, where $\sigma$ is the real embedding given by the real place $\mathfrak{p}$.

Let $S$ be a finite set of primes dividing $\mathfrak{m}$, and let $S(\mathfrak{m})$ denote the set of primes dividing $\mathfrak{m}$. We write $I^S$ for the group of fractional ideals of $K$ that are relatively prime to $S$. We have a map $\iota : K_{\mathfrak{m},1} \to I^{S(\mathfrak{m})}$ given by mapping $a$ to the ideal that it generates. Then $\iota(K_{\mathfrak{m},1})$ is a subgroup of $I^{S(\mathfrak{m})}$. We then define the ray class group (modulo $\mathfrak{m}$) to be $C_\mathfrak{m} := I^{S(\mathfrak{m})}/\iota(K_{\mathfrak{m},1})$. Note that if $\mathfrak{m} = 1$, then $C_\mathfrak{m}$ is simply the usual ideal class group $\mathrm{Cl}(K)$. It is known that each class of $C_\mathfrak{m}$ has infinitely many representatives that are primes of $K$.

Now let $L/K$ be a finite abelian extension of global fields, with $G$ its Galois group. There are only finitely many primes of $K$ which ramify in $L$—those dividing the discriminant ideal $\mathfrak{d}_{L/K}$. Let $S$ be the set of primes dividing $\mathfrak{d}_{L/K}$. The Artin reciprocity map $\omega_{L/K} : I^S \to \mathrm{Gal}(L/K)$ associates to each prime $\mathfrak{p} \in I^S$ the unique element of the decomposition group, $D(\mathfrak{p})$, that acts as the Frobenius map on the residue field tower $\mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\right)$, where $\mathfrak{P}$ is a prime of $K$ lying above $\mathfrak{p}$. We extend this map linearly so that we have $\omega_{L/K}\left(\prod_i \mathfrak{p}_i^{n_i}\right) = \prod_i (\omega_{L/K}(\mathfrak{p}_i))^{n_i}$. Denote by $I_L^S$ the set of fractional ideals of $L$ relatively prime to $S$, where $S$ is a finite set of primes of $L$. Then $\ker \omega_{L/K}$ contains $\mathrm{Nm}_{L/K}(I_L^S)$. The Artin global reciprocity law states that if $S$ is the set of primes ramifying in $L$, then $\omega_{L/K}$ admits a modulus, say $\mathfrak{m}$, with $S(\mathfrak{m}) = S$, and that there is an isomorphism

$$\mathrm{Gal}(L/K) \cong I^S/\left(\iota(K_{m,1})\mathrm{Nm}_{K/L}(I_L^S)\right).$$

A congruence subgroup (modulo $\mathfrak{m}$) is a group $G$ with $\iota(K_{\mathfrak{m},1}) \subseteq G \subseteq I^{S(\mathfrak{m})}$. If $G$ is a congruence subgroup, then there exists a finite abelian extension $L/K$ such that $G =$

$\iota(K_{\mathfrak{m},1})\mathrm{Nm}_{L/K} I_L^{S(\mathfrak{m})}$. Then if $G = \iota(K_{\mathfrak{m},1})$, we have a finite abelian extension $L/K$ with $\iota(K_{\mathfrak{m},1}) = \iota(K_{\mathfrak{m},1})\mathrm{Nm}_{L/K} I_L^{S(\mathfrak{m})}$. But by the Artin Reciprocity Theorem, this is isomorphic to $\mathrm{Gal}(L/K)$. Indeed in a sense, classifying abelian extensions of a global field is precisely the goal of Class Field Theory. We then define the ray class field (modulo $\mathfrak{m}$) to be the finite abelian extension $L_{\mathfrak{m}}/K$ with $C_{\mathfrak{m}} \cong \mathrm{Gal}(L_{\mathfrak{m}}/K)$, and define the Hilbert class field of $K$, $H_K$, to be the ray class field of $K$ with $\mathfrak{m} = 1$. That is, the Hilbert class field $H_K/K$ is the unique abelian extension of $K$ with $\mathrm{Gal}(H_K/K) = \mathrm{Cl}(K)$, meaning that it is the maximal unramified abelian extension of $K$. Finally, we define the conductor, $\mathfrak{c}$, of an abelian extension $L/K$ to be the smallest modulus for $L/K$, i.e. $\mathfrak{c}$ divides $\mathfrak{m}$ for all moduli of $L$. We now state some of the main results of the theory of elliptic curves with CM.

**Theorem 3.25** ([Sil94, Thm. 4.1, 4.3])**.** *Let $K/\mathbb{Q}$ be an imaginary quadratic field with ring of integers $\mathcal{O}_K$, and let $E/\mathbb{C}$ be an elliptic curve with $\operatorname{End} E \cong \mathcal{O}$. Then $K(j(E))$, i.e. the field of definition for $E$, is the Hilbert class field $H_K$ of $K$. Furthermore, $[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = h_K$, where $h_K$ is the class number of $K$.*

**Theorem 3.26** ([Sil94, Thm. 6.1])**.** *Let $E/\mathbb{C}$ be an elliptic curve with CM. Then $j(E)$ is an algebraic integer.*

Indeed, the theory of elliptic curves with CM is very deep and beautiful. For instance, using the theory of elliptic curves with CM, one discovers, see [Sil94], that

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999250072597\ldots$$

is very nearly an integer.

# Chapter 4

# Currently Known Results

Throughout this chapter, when convenient, we will make use of the following notation:

- Let $\Phi(d)$ denote the set of isomorphism classes of torsion subgroups $E(K)_{\text{tors}}$, where $K$ varies over all number fields of degree $d$ and $E$ varies over all elliptic curves defined over $K$. Similarly, let $\Phi_{\mathbb{Q}}(d)$ denote the set of isomorphism classes of torsion subgroups $E(K)_{\text{tors}}$, where $K$ varies over all number fields of degree $d$ and $E$ varies over all rational elliptic curves, i.e. elliptic curves $E/\mathbb{Q}$ base extended to $K$.

- Let $\Phi^{\text{Gal}}(d)$ denote the set of isomorphism classes of torsion subgroups $E(K)_{\text{tors}}$, where $K$ varies over all Galois number fields of degree $d$ and $E$ varies over all elliptic curves defined over $K$. Similarly, let $\Phi_{\mathbb{Q}}^{\text{Gal}}(d)$ denote the set of isomorphism classes of torsion subgroups $E(K)_{\text{tors}}$, where $K$ varies over all Galois number fields of degree $d$ and $E$ varies over all rational elliptic curves, i.e. elliptic curves $E/\mathbb{Q}$ base extended to $K$.

- Let $\Phi^G(d)$ denote the set of isomorphism classes of torsion subgroups $E(K)_{\text{tors}}$, where $K$ varies over all number fields of degree $d$ with $\text{Gal}(\widehat{K}/\mathbb{Q}) \cong G$, where $\widehat{K}$ is the Galois closure of $K$, and $E$ varies over all rational elliptic curves, i.e. elliptic curves $E/\mathbb{Q}$ base extended to $K$. Note that if $K$ is Galois, then $\widehat{K} \cong K$. Similarly, let $\Phi^G_{\mathbb{Q}}(d)$ denote the set of isomorphism classes of torsion subgroups $E(K)_{\text{tors}}$, where $K$ varies over all number fields of degree $d$ with $\text{Gal}(\widehat{K}/\mathbb{Q}) \cong G$, where $\widehat{K}$ is the Galois closure of $K$, and $E$ varies over all rational elliptic curves, i.e. elliptic curves $E/\mathbb{Q}$ base extended to $K$. Note that if $K$ is Galois, then $\widehat{K} \cong K$.

- Let $\Phi^\infty(d)$ denote the subset of $\Phi(d)$ of isomorphism classes of torsion subgroups $E(K))_{\text{tors}}$ which occur for infinitely many non-isomorphic elliptic curves. That is, the set torsion subgroups $T$ such that there are infinitely many elliptic curves, not isomorphic over $\overline{\mathbb{Q}}$, such that there is a field $K$ of degree $d$ with $E(K)_{\text{tors}} \cong T$. Similarly, let $\Phi^\infty_{\mathbb{Q}}(d)$ denote the subset of $\Phi_{\mathbb{Q}}(d)$ of isomorphism classes of torsion subgroups $E(K)_{\text{tors}}$ which occur for infinitely many non-isomorphic rational elliptic curves. That is, the set torsion subgroups $T$ such that there are infinitely many rational elliptic curves, not isomorphic over $\overline{\mathbb{Q}}$, such that there is a field $K$ of degree $d$ that, when $E$ is base extended to $K$, $E(K)_{\text{tors}} \cong T$.

- Let $\Phi_{j\in\mathbb{Q}}(d)$ denote the set of isomorphism classes of torsion subgroups $E(K)_{\text{tors}}$, where $K$ varies over all number fields of degree $d$ and $E$ runs over all elliptic curves with $j_E \in \mathbb{Q}$. Generally, let $\Phi_{j\in\mathcal{O}_K}(d)$ denote the set of isomorphism classes of torsion subgroups $E(K)_{\text{tors}}$, where $K$ varies over all number fields of degree $d$ and $E$ runs over all elliptic curves with $j_E \in \mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of $K$.

- If $G \in \Phi(1)$, let $\Phi_{\mathbb{Q}}(d, G)$ denote the set of isomorphism classes of torsion subgroups $E(K)_{\text{tors}}$ as $E/\mathbb{Q}$ runs over all rational elliptic curves and $K/\mathbb{Q}$ runs over all number fields of degree $d$.

- Let $S(d)$ denote the set of primes such that there exists a number field of degree $\leq d$ and an elliptic curve $E/K$ such that there is a point of order $p$ on $E(K)$. Similarly, let $S_{\mathbb{Q}}(d)$ denote the set of primes such that there exists a number field of degree $\leq d$ and a rational elliptic curve $E/K$ such that, when $E$ is base extended to $K$, there is a point of order $p$ on $E(K)$.

- Let $R(d)$ denote the set of primes such that there exists a number field of exact degree $d$ and an elliptic curve $E/K$ such that there is a point of order $p$ on $E(K)$. Similarly, let $R_{\mathbb{Q}}(d)$ denote the set of primes such that there exists a number field of exact degree $d$ and a rational elliptic curve $E/K$ such that, when $E$ is base extended to $K$, there is a point of order $p$ on $E(K)$.

Note that $\Phi_{\mathbb{Q}}(d) \subseteq \Phi(d)$ for all $d$. However, it is worth noting that $\Phi_{\mathbb{Q}}^{\infty}(d) \subseteq \Phi_{\mathbb{Q}}(d) \cap \Phi^{\infty}(d)$ can be distinct sets. Clearly, we have $\Phi_{\mathbb{Q}}^{\infty}(d) \subseteq \Phi^{\infty}(d)$. However, a torsion subgroup which appears infinitely often for elliptic curves $E/K$ may only occur for finitely many rational elliptic curves; that is, there may only be finitely many rational elliptic curves that when base extended to a number field of degree $d$ have a specified torsion subgroup. Furthermore for all $d$, we have $R(d) \subseteq S(d)$ and $R_{\mathbb{Q}}(d) \subseteq S_{\mathbb{Q}}(d)$. If one knows $R(d')$ for all $d' \leq d$, then one can recover $S(d)$ via $S(d) = \cup_{k \leq d} R(k)$. However, knowledge of $S(d')$ for all $d' \leq d$ does not allow one to recover $R(d)$. The same observations are true for $S_{\mathbb{Q}}(d)$ and $R_{\mathbb{Q}}(d)$, mutatis mutandis.

Even in the cases where $\Phi(d)$ or $\Phi_{\mathbb{Q}}(d)$ are unknown, they are known to be finite sets. Merel [Mer96] showed that the sets $\Phi(d)$ (and hence $\Phi_{\mathbb{Q}}(d)$) are uniformly bounded, now known as the Uniform Boundedness Theorem. However, Merel's result was not effective. Instead, Merel merely proved that there existed a constant $B(d)$, depending only on $d$, such that $|G| \leq B(d)$ for all $G \in \Phi(d)$. Merel's result was later made effective in work by Parent [Par99], and Oesterlé (unpublished but can be found in [DKSS17]). Both Merel

and Parent's work was based on extending Kamienny and Mazur's work in Jacobian varieties and Hecke algebras, see [Edi93]. In particular, along with Oesterlé's work, they prove:

**Theorem 4.1** ([Mer96],[Par99])**.** *Let $K$ be a number field of degree $d > 1$. Then*

*(i) (Merel) Let $E/K$ be an elliptic curve. If $E(K)$ contains a point of exact prime order $\ell$, then $\ell \leq d^{3d^2}$.*

*(ii) (Parent) If $P$ is a point of exact prime power order $\ell^n$, then*

*(a) $\ell^n \leq 65(3^d - 1)(2d)^6$, if $\ell \geq 5$*

*(b) $\ell^n \leq 65(5^d - 1)(2d)^6$, if $\ell = 3$*

*(c) $\ell^n \leq 129(3^d - 1)(3d)^6$, if $\ell = 2$*

*In particular, $\ell^p \leq 129(5^d - 1)(3d)^6$ for all primes $\ell$.*

*(iii) (Oesterlé) If $p \in S(d)$, then $p \leq (1 + 3^{d/2})^2$.*

The first classification of torsion subgroups of elliptic curves came with Mazur's classification of the possibilities for $E(\mathbb{Q})_{\text{tors}}$ in 1977. The next full classification would not come until Kammieny, Kenku, and Momose's classification of $\Phi(2)$. There has been an explosion of results since 2000. We now give an overview of the progress in the classification of torsion subgroups for elliptic curves in various settings.

## 4.1 The Case of $E(\mathbb{Q})_{\text{tors}}$

The possible structures for $E(\mathbb{Q})_{\text{tors}}$ was originally conjectured by Beppo Levi, see [SS96]. Later Trygve Nagell and Andrew Ogg independently arrived at Levi's conjecture. Drawing on Ogg's work connecting torsion subgroups of elliptic curves, modular forms, and isoge-

nies of elliptic curves, work of Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, Ogg, et al. classified the possible $\mathbb{Q}$-rational points on $X_0(N)$. Mazur's work on the Eisenstein ideal classified the possible $\mathbb{Q}$-rational points on $X_0(N)$ in the case where $N$ was prime. Hence, Mazur was able to classify the possible torsion subgroups for $E(\mathbb{Q})_{\text{tors}}$.

**Theorem 4.2** ([Maz77, Maz78])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(\mathbb{Q})_{tors}$ is isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4. \end{cases}$$

*Moreover, each possibility occurs for infinitely many distinct elliptic curves.*

One can prove Mazur's Theorem as follows: the modular curve $Y_1(N)$ classifies the pairs $(E, P)$, where $E/\mathbb{C}$ is an elliptic curve and $P \in E$ is a point of exact order $N$; that is, the set of rational points on $Y_1(N)$, denoted $Y_1(N)(\mathbb{Q})$, corresponds to the set of (isomorphism classes) of pairs $(E, P)$. The proof then reduces to showing that $Y_1(N)(\mathbb{Q})$ is empty for $N > 7$. One then naturally considers the map of algebraic curves $Y_1(N) \to Y_0(N)$, where $Y_0(N)$ is the affine curve parametrizing the set of pairs $(E, G)$, where $E/\mathbb{C}$ is an elliptic curve and $G \subseteq E$ is a cyclic subgroup of order $N$. Let $X_0(N)$ denote the compactification of $Y_0(N)$.

One then proves for a rational abelian variety $A$ and a rational map $f : X_0(N) \to A$ that if $A$ has good reduction away from $N$, $f(0) \neq f(\infty)$, and $A(\mathbb{Q})$ has rank 0, then no rational elliptic curve has a point of order $N$. Furthermore, one must prove the following: let $A/\mathbb{Q}$ be an abelian variety and let $N$ and $p$ be distinct primes, with $N$ odd. If $A$ has good reduction away from $N$, $A$ has completely toric reduction at $N$, and the Jordan-Hölder constituents of $A[p](\overline{\mathbb{Q}})$ are 1-dimensional, and either trivial or cyclotomic, then

$A(\mathbb{Q})$ has rank 0.

But of course, one must first find such an abelian variety $A$ of rank 0. Embedding a curve into its Jacobian, one can find the abelian variety $A$ by recognizing it as a quotient of the Jacobian $J_0(N)$ of $X_0(N)$. Studying the Hecke operators $T_p$ on $J_0(N)$, one can identify $A$ using the Hecke algebra. For the details on all of this, see [Sno13].

## 4.2 Torsion Subgroups of Elliptic Curves over General Number Fields

Of course, one need not restrict to rational elliptic curves. Instead, one could consider elliptic curves over a number field, $E/K$. The first progress in this direction was work begun by Kenku and Momose, later finished by Kamienny.

**Theorem 4.3** ([KM88, Kam92a, Kam92b]). *Let $K/\mathbb{Q}$ be a quadratic number field, and let $E/K$ be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 16, 18 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

*Moreover, there exist infinitely many $\overline{\mathbb{Q}}$-isomorphism classes for each possible torsion subgroup.*

Rabarison [Rab10] gives many interesting parametrizations for the torsion subgroups in Theorem 4.3. Of course, Theorem 4.3 does not say over which quadratic fields the listed

torsion subgroups appear. In fact, Bosman, Bruin, Dujella, and Najman are able to classify the possibilities for $E(K)_{\text{tors}}$ based on the type of quadratic field.

**Theorem 4.4** ([BBDN13b]). *Let $K/\mathbb{Q}$ be a real quadratic number field $K$, and let $E/K$ be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 16, 18 \text{or} \\ \mathbb{Z}2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4. \end{cases}$$

*Moreover, each torsion subgroup occurs for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes.*

**Theorem 4.5** ([BBDN13b]). *Let $K/\mathbb{Q}$ be an imaginary quadratic number field $K$, and let $E/K$ be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 12, 14, 15, 16 \text{ or} \\ \mathbb{Z}2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

*Moreover, each torsion subgroup occurs for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes.*

Of course, fixing a quadratic field $K/\mathbb{Q}$ and possible torsion subgroup $G \in \Phi(2)$, Theorems 4.3, 4.4, and 4.5 say nothing about whether there is an elliptic curve $E(K)$ with $E(K)_{\text{tors}} \cong G$. Najman classified the possibilities if $K$ a quadratic cyclotomic field in [Naj11] and [Naj10]. Moreover, Kamienny and Najman describe a method in [KN11] to determine all the possible torsion subgroups $E(K)_{\text{tors}}$ over a fixed quadratic field, and they find examples of the smallest quadratic field (measured by the absolute discriminant) over which that torsion subgroup occurs. They also examine an interplay between rank

and torsion for the groups $E(K)$ and give some results concerning the density of torsion subgroups.

The first progress for the case of cubic number fields came with Jeon, Kim, and Schweizer, who determined the possible torsion structures which appear infinitely often over cubic fields.

**Theorem 4.6** ([JKS04])**.** *Let $K/\mathbb{Q}$ be a cubic number field, and let $E/K$ be an elliptic curve. Then the possibilities for $E(K)_{tors}$ occurring for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes are precisely:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 16, 18, 20 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 7. \end{cases}$$

Furthermore by finding certain trigonal modular curves, Jeon, Kim, and Lee [JKL11a] constructed infinite families of elliptic curves realizing each of these torsion structures. Jeon [Jeo16] constructs other families of examples in the case of cyclic cubic number fields. Extending Najman's work in [Naj12b], Maarten Derickx and Filip Najman classified the torsion subgroups of elliptic fields over Galois cubic fields, complex cubic fields, and totally real cubic fields with Galois group $S_3$.

**Theorem 4.7** ([DN19])**.** *Let $K/\mathbb{Q}$ be a cyclic cubic field, and let $E/K$ be an elliptic curve. Then $E(K)_{tors}$ is precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 16, 18, 21 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 7. \end{cases}$$

*Each such possibility occurs for some elliptic curve $E/K$ over some cyclic cubic field $K$.*

Furthermore, the only elliptic curve with $\mathbb{Z}/16\mathbb{Z}$ torsion over a cyclic cubic field $K$ is $y^2 + axy + by = x^3 + bx^2$, where

$$a = \frac{-11\alpha^2 + 2543\alpha + 2240}{2232}, \quad b = \frac{481\alpha^2 - 2465\alpha - 376}{155682},$$

and $\alpha$ is a root of $x^3 - 8x^2 - x + 8/9$ and $K = \mathbb{Q}(\alpha)$, c.f. [DN19, Lemma 4.13].

**Theorem 4.8** ([DN19])**.** *Let $K/\mathbb{Q}$ be a complex cubic field, and let $E/K$ be an elliptic curve. Then $E(K)_{tors}$ is precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 16, 18, 20 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6. \end{cases}$$

*Moreover, there are infinitely many distinct $\overline{\mathbb{Q}}$-isomorphism classes such that $E(K)_{tors}$ is isomorphic to one of the groups above for some complex cubic field.*

**Theorem 4.9** ([DN19])**.** *Let $K/\mathbb{Q}$ be a totally real cubic field with Galois group $S_3$, and let $E/K$ be an elliptic curve. Then $E(K)_{tors}$ is precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 16, 18, 20 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6. \end{cases}$$

*Moreover, there are infinitely many distinct $\overline{\mathbb{Q}}$-isomorphism classes such that $E(K)_{tors}$ is isomorphic to one of the groups above for some totally real cubic field with* $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

Their method, in part, relies on a process called Mordell-Weil sieving, which is useful in finding all rational points on a curve $C$ by examining the Mordell-Weil group of its Jacobian. For more on this topic, see [BS10]. Their work was later extended by Jeon and Schweizer, who determined in [JS20] over which types of cubic number fields each possible torsion subgroup can occur, and if the torsion subgroup occurs infinitely often over that type of field or not. Finally, Bruin and Najman [BN17] show that all elliptic curves over quadratic fields with $E(K)_{\text{tors}} \supseteq \mathbb{Z}/16\mathbb{Z}$ and elliptic curves over cubic fields with $E(K)_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ are base changes of elliptic curves defined over $\mathbb{Q}$. In fact, they show, [BN17, Thm. 1.2], if $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, then $K$ is cyclic.

However despite all this work, the list from Theorem 4.6 cannot be complete. In [Naj16], Najman found that the rational elliptic curve with Cremona label `162b1` has 21-torsion over a cubic field, namely $E(\mathbb{Q}(\zeta_9)^+) \cong \mathbb{Z}/21\mathbb{Z}$, and that this is the unique elliptic curve with 21-torsion over a cubic field. This was the first known example of a sporadic point on a modular curve, i.e. sporadic torsion. Today, there are many other known sporadic torsion groups over number fields, c.f. [vH14] where examples of sporadic torsion subgroups $\mathbb{Z}/28\mathbb{Z}$ and $\mathbb{Z}/30\mathbb{Z}$ are given in the case of quintic number fields and $\mathbb{Z}/25\mathbb{Z}$ and $\mathbb{Z}/37\mathbb{Z}$ are given in the sextic case. Until recently, all of the known cases of sporadic torsion corresponded to cyclic torsion subgroup. However in a recent paper of González-Jiménez and Najman [GJN20a], they give an example of a sextic number field $K$ such that (using Theorem 4.38) $E(K)_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$—first known example of sporadic torsion for a non-cyclic torsion subgroup.

The full classification for torsion subgroups of elliptic curves over cubic number fields (though announced much earlier) was only submitted this year in a paper of Derickx, Etropolski, van Hoeij, Morrow, and Zureick-Brown. The result relies on the work of many mathematicians such as Bruin, Jeon, Kato, Kim, Lee, Momose, Najman, Parent, Schweizer,

Wang, among others. The classification relies on a number of techniques: local arguments, Abel-Jacobi maps, quotients of modular curves, modular units, etc. and a vast amount of computation. Of course, there is a lot of other related work in this general area. For instance, see [BGRW20]. The final result is that the only possible torsion subgroups are those from the list of Jeon, Kim, and Schweizer along with Najman's example of $\mathbb{Z}/21\mathbb{Z}$-torsion.

**Theorem 4.10** ([DEvH+20])**.** *Let $K/\mathbb{Q}$ be a cubic number field, and let $E/K$ be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 16, 18, 20, 21 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 7. \end{cases}$$

*Moreover, there exist infinitely many $\overline{\mathbb{Q}}$-isomorphism classes for each torsion subgroup except in the case $E(K) \cong \mathbb{Z}/21\mathbb{Z}$. In this case, the base change of the curve with Cremona label `162b1` to $\mathbb{Q}(\zeta_9)^+$ is the unique elliptic curve over a cubic field with 21-torsion.*

All these results, especially the work involved in proving Theorem 4.10, are entangled with concepts from Algebraic Geometry, e.g. gonality. Recall that the gonality of an algebraic curve $X$, denoted $\gamma(X)$, is the lowest degree of a nonconstant rational map from $X$ to the projective line. Points of degree $d$ on the modular curves $Y_1(m, n)$, when $d < \gamma(Y_1(m, n))$, are called sporadic. The torsion structures in $\Phi(1)$ are all parametrized by modular curves of genus 0 and all have infinitely many rational points. All these curves have gonality 1. The modular curves parametrizing the torsion structures in $\Phi(2)$ are of gonality 1 or 2. Therefore, there are no sporadic points of degree 1 or 2 on these curves. The modular curves $X_1(21)$ has gonality 4 and is the unique rational elliptic curve with 21-torsion over a cubic field giving a degree three sporadic point. We will not comment further on the

connection between gonality, sporadic points, and torsion subgroups of elliptic curves further here.

For elliptic curves $E/K$, where $K$ is a number field of degree $d$, the case of $d = 3$ is the last case where a complete classification is known. There are partial results in the cases of $d = 4, 5, 6$. In particular, the possible torsion structures occurring for infinitely many non-isomorphic elliptic curves is known.

**Theorem 4.11** ([JKP16])**.** *Let $K/\mathbb{Q}$ be a quartic number field, and $E/K$ an elliptic curve. The possible torsion subgroups occurring for infinitely many distinct $\overline{\mathbb{Q}}$-isomorphism classes are precisely:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 18, 20, 21, 22, 24 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 9 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2, 3 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \text{or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. \end{cases}$$

*Moreover, all these torsion structures already occur infinitely often if $K$ varies over all quadratic extensions of all quadratic number fields, i.e. all biquadratic number fields.*

Jeon, Kim, and Lee construct (infinite) families of elliptic curves with cyclic torsion subgroups over quartic number fields $K$ such that the Galois closure of $K$ is a dihedral quartic number field, see [JKL15] and [JKL13]. For other related results, see also [JKL11b] and [Naj12a].

**Theorem 4.12** ([DS17]). *Let $K/\mathbb{Q}$ be a quintic number field, and $E/K$ an elliptic curve. The possible torsion subgroups occurring for infinitely many distinct $\overline{\mathbb{Q}}$-isomorphism classes are precisely:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 22, 24, 25 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 7, 8. \end{cases}$$

**Theorem 4.13** ([DS17]). *Let $K/\mathbb{Q}$ be a sextic number field, and $E/K$ an elliptic curve. The possible torsion subgroups occurring for infinitely many distinct $\overline{\mathbb{Q}}$-isomorphism classes are precisely:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 22, 24, 26, 27, 28, 30 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. \end{cases}$$

Of course, there are other related results. For instance, Dey and Roy classified the possible torsion subgroups of Mordell curves, i.e. elliptic curves of the form $E : y^2 = x^3 + n$ for $n \in \mathbb{Q}$, over (cubic and) sextic fields, see [DR19].

## 4.3 Torsion Subgroups of CM Elliptic Curves

Though amazing results have been achieved in classifying $\Phi(d)$, progress is still rather limited. However in the case where $E/K$ has CM, there is much more progress. This is primarily due to the fact that one has the Theory of Complex Multiplication and especially the Class Field Theory interpretation of torsion points on elliptic curves, allowing

many more techniques to be at one's disposal. In particular, one often has powerful tools to bound the size of the torsion subgroup, which gives a finite set of possibilities for the possible torsion subgroups. For example, here are two well known results allowing one to bound torsion in specific cases, though there are refined bounds in [CCS13]:

**Theorem 4.14** (Silverberg, Prasad-Yogananda)**.** *Let $E$ be an elliptic curve over a number field $F$ of degree $d$, and suppose that $E$ has CM by the order $\mathcal{O}$ in the imaginary quadratic field $K$. Let $e$ be the exponent of the torsion subgroup of $E(F)$. Then*

*(a)* $\phi(e) \leq w(\mathcal{O})d$

*(b) If* $K \subseteq F$*, then* $\phi(e) \leq w(\mathcal{O})d/2$

*(c) If* $K \not\subseteq F$*, then* $\phi(\#E(F)_{tors}) \leq w(\mathcal{O})d$

*Proof.* See [Sil88] and [PY01]. □

**Theorem 4.15** ([Par89])**.** *Let $E/F$ be an elliptic curve with CM by an imaginary quadratic order $\mathcal{O}$, and suppose that $h(\mathcal{O}) = [F\colon \mathbb{Q}]$. Then $E(F)_{tors}$ has order 1, 2, 3, 4, or 6.*

Olson [Ols74] classified the set $\Phi^{\mathrm{CM}}(1)$, i.e. the set of possible torsion subgroups for CM elliptic curves over $\mathbb{Q}$, and determined that there were 6 possibilities (the so-called "Olson groups").[1] The sets $\Phi^{\mathrm{CM}}(2)$ and $\Phi^{\mathrm{CM}}(3)$ were determined by Fung, Müller, Petho, Ströher, Weis, Williams, and Zimmer [MSZ89, FSWZ90a, PWZ97]. Clark, Cook, Corn, Lane, Rice, Stankewicz, Walters, Winburn, and Wyser give a complete list of possible torsion subgroups of elliptic curves with complex multiplication over number fields of degree $d$, $1 \leq d \leq 13$, see [CCRS14]. Moreover, they give an algorithm to compute list of all tor-

[1] There are only 13 isomorphism classes of elliptic curves defined over $\mathbb{Q}$ with complex multiplication, see [Sil09, Appendix A, §3].

sion subgroups $E(K)_{\text{tors}}$ that occur for elliptic curves $E$ with CM over number fields $K$ of degree $d$. They give a list of the possible torsion subgroups $E(K)_{\text{tors}}$ with examples for number fields of degree $1 \leq d \leq 13$ in [CCRS14, Sec. 4], which are too long to include in full here. However, we will include two relevant results for our purposes here.

**Theorem 4.16** ([CCRS14, Sec. 4.3])**.** *Let $K/\mathbb{Q}$ be a cubic extension, and let $E/K$ be an elliptic curve with CM. Then the possible torsion subgroups $E(K)_{tors}$ that occur over $K$ are precisely*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 6, 9, 14 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \end{cases}$$

**Theorem 4.17** ([CCRS14, Sec. 4.9])**.** *Let $K/\mathbb{Q}$ be a nonic extension, and let $E/K$ be an elliptic curve with CM. Then the possible torsion subgroups $E(K)_{tors}$ that occur over $K$ are precisely*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 6, 9, 14, 18, 19, 27 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \end{cases}$$

Further work of Bourdon, Clark, and Stankewicz, [BCS17], gives a complete classification of torsion subgroups arising from CM elliptic curves over number fields of odd degree. They also study the torsion subgroups of elliptic curves with complex multiplication over number fields admitting at least one real embedding. Finally, they also answer a question of Schütt on whether there is an absolute bound on the size of torsion subgroups of all CM elliptic curves defined over all number fields of prime degree in the affirmative. In particular, they prove the following:

**Theorem 4.18** ([BCS17, Thm. 1.5,Odd Degree Theorem])**.** *Let $F$ be a number field of odd*

*degree, let $E/F$ be a $K$-CM elliptic curve, and let $T = E(F)_{tors}$. Then:*

*(i) One of the following occurs:*

*(a) $T$ is isomorphic to the trivial group, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$;*

*(b) $T \cong \mathbb{Z}/\ell^n\mathbb{Z}$ for a prime $\ell \equiv 3 \mod 8$ and $n \in \mathbb{Z}^+$ and $K = \mathbb{Q}(\sqrt{-\ell})$;*

*(c) $T \cong \mathbb{Z}/2\ell^n\mathbb{Z}$ for a prime $\ell \equiv 3 \mod 4$ and $n \in \mathbb{Z}^+$ and $K = \mathbb{Q}(\sqrt{-\ell})$.*

*(ii) If $E(F)_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then $\operatorname{End} E$ has discriminant $\Delta = -4$.*

*(iii) If $E(F)_{tors} \cong \mathbb{Z}/4\mathbb{Z}$, then $\operatorname{End} E$ has discriminant $\Delta \in \{-4, -16\}$.*

*(iv) Each of the groups listed in part (i) arises up to isomorphism as the torsion subgroup $E(F)$ of a CM elliptic curve $E$ defined over an odd degree number field $F$.*

Of course, Theorem 4.18 does not identify in which degrees $d$ the subgroups occur. Later, Bourdon and Pollack were able to extend the work in [BCS17]. In particular, letting $h_{\mathbb{Q}(\sqrt{-\ell})}$ denote the class number of $\mathbb{Q}(\sqrt{-\ell})$, they prove the following:

**Theorem 4.19** ([BP16b, Thm. 1.2,Strong Odd Degree Theorem])**.** *Let $\ell \equiv 4 \mod 4$ and $n \in \mathbb{Z}^+$. Define $\delta$ as follows:*

$$\delta = \begin{cases} \lfloor \frac{3n}{2} \rfloor - 1, & \ell > 3, \\ 0, & \ell = 3 \text{ and } n = 1, \\ \lfloor \frac{3n}{2} \rfloor - 2, & \ell = 3 \text{ and } n \geq 2. \end{cases}$$

*Then:*

*(1) For any odd positive integer $d$, the groups $\{\bullet\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ appear as the torsion subgroup of a CM elliptic curve defined over a number field of degree $d$.*

*(2)* $\mathbb{Z}/\ell^n\mathbb{Z}$ *appears as the torsion subgroup of a CM elliptic curve defined over a number field of odd degree* $d$ *if and only if* $\ell \equiv 3 \mod 8$ *and* $d$ *is a multiple of* $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$.

*(3)* $\mathbb{Z}/2\ell^n\mathbb{Z}$ *appears as the torsion subgroup of a CM elliptic curve defined over a number field of odd degree* $d$ *if and only if one of the following holds:*

*(a)* $\ell \equiv 3 \mod 8$, *where* $n \geq 2$ *if* $\ell = 3$, *and* $d$ *is a multiple of* $3 \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$, *or*

*(b)* $\ell = 3$ *and* $n = 1$ *and* $d$ *is any odd positive integer, or*

*(c)* $\ell \equiv 7 \mod 8$ *and* $d$ *is a multiple of* $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$.

For a given positive integer $d$, let $\mathscr{G}(d)$ denote the set of (isomorphism classes) of abelian groups that appear as $E(F)_{\text{tors}}$ for some elliptic curve $E$ defined over some degree $d$ number field $F$, and let $T_{\text{CM}}(d) = \max_{G \in \mathscr{G}(d)} \#G$. Theorem 4.19 can be used to algorithmically determine $\mathscr{G}(d)$ for any odd degree $d$. In particular in [BP16b, Table 7], Bourdon and Pollack give a table of groups arising for odd $1 \leq d \leq 99$. They state, "On a modern desktop computer, one can process all odd $d \leq 2 \cdot 10^8$ in about 12 hours." Their paper contains many interesting results, which would take too long to summarize here. We will comment that, under the Generalized Riemann Hypothesis, they prove that

$$\left(\frac{12e^\gamma}{\pi}\right)^{2/3} \leq \limsup_{\substack{d \to \infty \\ d \text{ odd}}} \frac{T_{\text{CM}}(d)}{(d \log\log d)^{2/3}} \leq \left(\frac{24e^\gamma}{\pi}\right)^{2/3}.$$

Work of Dieulefait, González-Jiménez, and Urroz, see [DGJU11], examined the fields of definition of torsion points for rational elliptic curves with CM by examining the image of the mod $p$ Galois representation attached to $E$. Denote by $E_{D,\mathfrak{f}}$ the elliptic curve $E/\mathbb{Q}$ having CM by an order $R = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ of conductor $\mathfrak{f}$ in a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$, where $\mathcal{O}_K$ is the ring of integers of $K$.

**Theorem 4.20** ([DGJU11, Thm. 1]). *Let $E/\mathbb{Q}$ be a rational elliptic curve with CM by an order $K = \mathbb{Q}(\sqrt{-D})$ of conductor $\mathfrak{f}$, and let $F$ be a Galois number field not containing $K$, then*

*(i)* $j(E) \neq 0, 1728$*:*

- *If $D \neq 8$ and $\mathfrak{f}$ odd, then $E(F)[2] = E(\mathbb{Q})[2]$.*
- *Otherwise, $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{p})$, where $p \mid D$; in particular, there are 2-torsion points in a quadratic field different from $K$.*

*(ii)* $j(E) = 1728$*: In this case, $E = E^d_{4,1}$ for $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^4$ and $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-d})$; in particular for $d \neq 1$, there are 2-torsion points in a quadratic field different from $K$.*

*(iii)* $j(E) = 0$*: In this case, $E = E^d_{3,1}$ for $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^6$ and $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2d})$. Moreover, $E(F)[2] = E(\mathbb{Q})[2]$.*

**Theorem 4.21** ([DGJU11, Thm. 2]). *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with CM by an order of $K = \mathbb{Q}(\sqrt{-D})$ and $p$ an odd prime not dividing $D$. Let $F$ be a Galois number field not containing $K$, then $E(F)[p]$ is trivial.*

Define $n(E)$ as follows:

$$n(E) = \begin{cases} 2, & \text{if } j(E) \neq 0, 1728 \\ 4, & \text{if } j(E) = 1728, \\ 6, & \text{if } j(E) = 0. \end{cases}$$

**Theorem 4.22** ([DGJU11, Thm. 3]). *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with CM by an order of $K = \mathbb{Q}(\sqrt{-D})$ of conductor $\mathfrak{f}$. We know that $E = E^d_{D,\mathfrak{f}}$ for some integer $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^{n(E)}$. Let $p$ be an odd prime dividing $D$.*

*(i)* *If $p > 7$, then there are $p$-torsion points of $E$ defined over $\mathbb{Q}(\zeta_p + \overline{\zeta}_p, \sqrt{d})$. Furthermore, $d = -p$ is the only case where any Galois number field containing $p$-torsion points contains $K$.*

*(ii)* *If $D = 7$:*

- *Case $\mathfrak{f} = 1$: There are 7-torsion points of $E$ defined over $\mathbb{Q}(\zeta_7 + \overline{\zeta}_7, \sqrt{-7d})$. Furthermore, $d = 1$ is the only case where any Galois number field containing 7-torsion points contains $K$.*

- *Case $\mathfrak{f} = 2$: There are 7-torsion points of $E$ defined over $\mathbb{Q}(\zeta_7 + \overline{\zeta}_7, \sqrt{7d})$. Furthermore, $d = -1$ is the only case where any Galois number field containing 7-torsion points contains $K$.*

*(iii)* *If $D = 3$:*

- *Case $\mathfrak{f} = 1$: $\mathbb{Q}(E[3]) = \mathbb{Q}(d^{1/6}, \sqrt{-3})$. There is a 3-torsion point in the field $\mathbb{Q}(\sqrt{d})$ and, except for $d = -3$, this quadratic field is different from $K$. Moreover, if $d = e^3$, there is a 3-torsion point on $\mathbb{Q}(\sqrt{-3e})$ which, except when $e$ is a square, is different from $K$.*

- *Case $\mathfrak{f} \neq 1$: There are 3-torsion points in the field $\mathbb{Q}(\sqrt{d})$. Except for $d = -3$, this quadratic field is different from $K$.*

Daniels and Lozano-Robledo have determined an upper bound on the number of isomorphism classes of CM elliptic curves defined over a number field of fixed odd degree $N$. For a number field $L$, define $\Sigma(L)$ to be the set of all CM $j$-invariants defined over $L$ but not defined over $\mathbb{Q}$.[2] This set was already known to be finite for any field $L$.

[2]Then the total number of CM $j$-invariants defined over $L$ is $13 + \#\Sigma(L)$.

**Theorem 4.23** ([DLR15, Thm. 1.1])**.** *Let $L$ be a number field of odd degree. Then $\#\Sigma(L) \leq 2\log_3([L\colon \mathbb{Q}])$. In particular, the number of distinct CM $j$-invariants defined over $L$ is bounded by $13 + 2\log_3([L\colon \mathbb{Q}])$.*

Daniels and Lozano-Robledo remark that this bound is essentially sharp, in a sense that we will not describe here. In fact, they actually prove a much stronger result depending on the factorization of $N$.

**Theorem 4.24** ([DLR15, Thm. 1.4])**.** *Let $L/\mathbb{Q}$ be a number field of odd degree $N = p_1^{e_1}\cdots p_r^{e_r}$, and let $K_1, \ldots, K_t$ be the list of imaginary quadratic fields such that there is $j(E) \in \Sigma(L)$, where $E$ has CM by an order of $K_i$ for some $i = 1, \ldots, t$. Further, let $h_i$ be the class number of $K_i$, and suppose that $h_i > 1$ for $i = 1, \ldots, s$ and $h_i = 1$ for $i = s+1, \ldots, t$. Then*

$$\#\Sigma(L) \leq 2s + 2\sum_{j=1}^{r}\left(e_j - \sum_{i=1}^{s} f_{i,j}\right),$$

*where $h_i = p_1^{f_{i,1}}\cdots p_r^{f_{i,r}}$. In particular, $\#\Sigma(L) \leq 2\sum_{j=1}^{r} e_j$.*

Observe that because $p_j \geq 3$, the quantity $\sum e_j$ is maximized if $r = 1$, $p_1 = 3$, and $e_1 = \log_3 N$, so that

$$\#\Sigma(L) \leq 2\sum_{j=1}^{r} e_j \leq 2\log_3 N,$$

which proves Theorem 4.23.

Results in the CM case are not limited to torsion subgroups of elliptic curves. In particular, building on their work in [BC20a] and establishing new results about rational cyclic isogenies for CM elliptic curves, Bourdon and Clark [BC20b] determine for positive integers $M \mid N$ the least degree of an $\mathcal{O}$-CM point on the modular curve $X(M,N)_{/K(\zeta_M)}$ and on the modular curve $X(M,N)_{/\mathbb{Q}(\zeta_M)}$.

**Theorem 4.25** ([BC20b, Thm. 1.1]). *Let $\mathcal{O}$ be an imaginary quadratic order of conductor $\mathfrak{f}$, and let $M \mid N$ be positive integers. There is a positive integer $T(\mathcal{O}, M, N)$, explicitly given, such that for all positive integers $d$, there is a field extension $F/K(\mathfrak{f})$ of degree $d$ and an $\mathcal{O}$-CM elliptic curve $E/F$ such that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$ if and only if $T(\mathcal{O}, M, N) \mid d$.*

**Theorem 4.26** ([BC20b, Thm. 1.2]). *Let $\mathcal{O}$ be an imaginary quadratic order, let $\ell$ be a prime number, and let $a \in \mathbb{Z}^+$. Let $m$ denote the maximum over all $i \in \mathbb{Z}^{\geq 0}$ such that there is an $\mathcal{O}$-CM elliptic curve $E/\mathbb{Q}(\mathfrak{f})$ with a $\mathbb{Q}(\mathfrak{f})$-rational $\ell^i$-isogeny, and let $M$ denote the supremum over all $i \in \mathbb{Z}^{\geq 0}$ such that there is an $\mathcal{O}$-CM elliptic curve $E/K(\mathfrak{f})$ with a $K(\mathfrak{f})$-rational cyclic $\ell^i$-isogeny. The least degree over $\mathbb{Q}(\mathfrak{f})$ in which there is an $\mathcal{O}$-CM elliptic curve with a rational point of order $\ell^a$ is as follows:*

*(i) If $a \leq m$, then the least degree is $T(\mathcal{O}, \ell^a)$.*

*(ii) If $m < a \leq M$, then $\ell^a > 2$ and the least degree is $2 \cdot T(\mathcal{O}, \ell^a)$.*

*(iii) If $a > M = m$, then the least degree is $T(\mathcal{O}, \ell^a)$.*

*(iv) If $a > M > m$, then $\ell = 2$ and the least degree is $2 \cdot T(\mathcal{O}, 2^a)$.*

Let $T^\circ(\mathcal{O}, N)$ denote the least degree over $\mathbb{Q}(\mathfrak{f})$ in which there is an $\mathcal{O}$-CM elliptic curve with a rational point of order $N$.

**Theorem 4.27** ([BC20b, Thm. 1.3]). *Let $\mathcal{O}$ be an imaginary quadratic order. Let $N \in \mathbb{Z}^+$ have prime power decomposition $\ell_1^{a_1} \cdots \ell_r^{a_r}$ with $\ell_1 < \cdots < \ell_r$. The least degree over $\mathbb{Q}(\mathfrak{f})$ in which there is an $\mathcal{O}$-CM elliptic curve with a rational point of order $N$ is $T(\mathcal{O}, N)$ if and only if $T^\circ(\mathcal{O}, \ell_i^{a_i}) = T(\mathcal{O}, \ell_i^{a_i})$ for all $1 \leq i \leq r$. Otherwise, the least degree is $2 \cdot T(\mathcal{O}, N)$.*

**Theorem 4.28** ([BC20b, Thm. 1.4]). *Let $\mathcal{O}$ be an imaginary quadratic order of discrimi-*

*nant* $\Delta$. *Let*

$$2 \leq M = \ell_1^{a_1} \cdots \ell_r^{a_r} \mid N = \ell_1^{b_1} \cdots \ell_r^{b_r} \text{ with } \ell_1 < \cdots < \ell_r.$$

*The least degree* $[F\colon \mathbb{Q}(\mathfrak{f})]$ *of a number field* $F \supset \mathbb{Q}(\mathfrak{f})$ *for which there is an* $\mathcal{O}$*-CM elliptic curve* $E/F$ *and an injective group homomorphism* $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$ *is* $T(\mathcal{O}, M, N)$ *if and only if all of the following conditions hold:* $M = 2$, $\Delta$ *is even, and* $T^\circ(\mathcal{O}, \ell_i^{a_i}, \ell_i^{b_i}) = T(\mathcal{O}, \ell_i^{a_i}, \ell_i^{b_i})$ *for all* $1 \leq i \leq r$. *Otherwise, the least degree is* $2 \cdot T(\mathcal{O}, M, N)$.

## 4.4 Torsion Subgroups of Rational Elliptic Curves

Like the case with CM elliptic curve, and unlike the case of elliptic curves over a general number field $K$, there has been tremendous progress in classifying the sets $\Phi_{\mathbb{Q}}(d)$ for various $d$. This is owed, in part, due to the fact that there is a complete classification of the possible $\mathbb{Q}$-rational isogenies for rational elliptic curves.

The initial progress was Najman's classification of $\Phi_{\mathbb{Q}}(2)$ and $\Phi_3(\mathbb{Q})$ in [Naj16], where he also found the example of the sporadic torsion subgroup on 162b2, which has 21-torsion over a cubic field, namely $E(\mathbb{Q}(\zeta_9)^+) \cong \mathbb{Z}/21\mathbb{Z}$.

**Theorem 4.29** ([Naj16, Thm. 2])**.** *Let* $E/\mathbb{Q}$ *be a rational elliptic curve, and let* $K/\mathbb{Q}$ *be a quadratic field. Then* $E(K)_{tors}$ *is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 15, 16 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

*Moreover, each of these groups, except for* $\mathbb{Z}/15\mathbb{Z}$*, occurs over some quadratic field for*

*infinitely many $\overline{\mathbb{Q}}$-isomorphism classes. The elliptic curves with Cremona labels* `50b1` *and* `50a3` *have 15-torsion over $\mathbb{Q}(\sqrt{5})$, and the curves with Cremona labels* `50b2` *and* `450b4` *have 15-torsion over $\mathbb{Q}(\sqrt{-15})$. These are the only rational elliptic curves having non-trivial 15-torsion over any quadratic field.*

**Theorem 4.30** ([Naj16, Thm. 2])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a cubic number field. Then $E(K)_{tors}$ is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7. \end{cases}$$

*Moreover, each of these groups, except for $\mathbb{Z}/21\mathbb{Z}$, occurs over some cubic field for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes. The elliptic curve* `162b1` *over $\mathbb{Q}(\zeta_9)^+$ is the unique rational elliptic curve with torsion $\mathbb{Z}/21\mathbb{Z}$.*

Najman gives examples of elliptic curves having each possible torsion structure—not already occurring over $\Phi(1)$—in Theorem 4.29 and Theorem 4.30 in his paper. Even in the cases when $\Phi_{\mathbb{Q}}(d)$ is known, it is generally an open problem to determine which types of fields of degree $d$ the various torsion subgroups $G \in \Phi_{\mathbb{Q}}(d)$ can occur. Najman classified the possibilities for $E(K)_{\text{tors}}$ for elliptic curves $E/K$, where $K$ is a quadratic cyclotomic field, see [Naj11] and [Naj10]. Furthermore as noted, Kamienny and Najman describe a method in [KN11] to determine all the possible torsion subgroups $E(K)_{\text{tors}}$ over a fixed quadratic field, and provide examples. Otherwise, results in these directions tend to be to classify the possibilities for $E(K)_{\text{tors}}$, where $\text{Gal}(\widehat{K}/\mathbb{Q})$ is of a fixed isomorphism type. For instance, see the results of Bosman, Bruin, Dujella, and Najman in [BBDN13b] or the work of Derickx and Najman in [DN19]. We shall also see examples of this in the classification of $\Phi_{\mathbb{Q}}(4)$ in [Cho16], [GJLR18], and [GJN20b]. But given a fixed field $K$ of degree $d$,

it is generally an open problem to determine what are the possibilities for $E(K)_{\text{tors}}$. There is some partial progress towards this in the case of quadratic fields, see [Trb18].

The classification of $\Phi_{\mathbb{Q}}(4)$ came in a series of papers, beginning with the paper which inspired this work. Chou began the classification of $\Phi_{\mathbb{Q}}(4)$ by determining the possibilities for $\Phi_{\mathbb{Q}}^{\text{Gal}}(4)$. Moreover, he determined the possible torsion subgroups based on the isomorphism type of $\text{Gal}(K/\mathbb{Q})$ and gives examples of each possible torsion subgroup not already occurring in $\Phi(1)$, along with a number of other interesting results.

**Theorem 4.31** ([Cho16, Thm. 1.2])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K$ be a quartic Galois extension of $\mathbb{Q}$. Then $E(K)_{tors}$ is isomorphic to one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, \ldots, 10, 12, 13, 15, 16 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, \ldots, 6, 8, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2, \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \text{or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. \end{cases}$$

*Moreover, each of these groups, except for $\mathbb{Z}/15\mathbb{Z}$, occurs over some quartic Galois field for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes.*

**Theorem 4.32** ([Cho16, Thm. 1.3])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K$ be a quartic cyclic Galois extension, i.e. $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. Then $E(K)_{tors}$ is isomorphic to*

*precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, \ldots, 10, 12, 13, 15, 16, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 8, \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}. \end{cases}$$

**Theorem 4.33** ([Cho16, Thm. 1.4])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K$ be a quartic bicyclic Galois extension, i.e.* $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$*. Then $E(K)_{tors}$ is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, \ldots, 10, 12, 15, 16, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 8, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2, \text{ or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. \end{cases}$$

The only elliptic curves $E(K)$ with $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/15\mathbb{Z}$ are those from Theorem 4.29, base extended to a quartic Galois field. González-Jiménez and Lozano-Robledo extended Chou's results to determine the set $\Phi_{\mathbb{Q}}^{\infty}(4)$.

**Theorem 4.34** ([GJLR18, Thm. 1])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a quartic number field. Then if $E(K)_{tors}$ occurs for infinitely many distinct $\overline{\mathbb{Q}}$-isomorphism classes (or is isomorphic to $\mathbb{Z}/15\mathbb{Z}$), then $E(K)_{tors}$ is isomorphic to precisely one of the*

*following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 15, 16, 20, 24 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 8 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} & \text{or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. \end{cases}$$

*Moreover, if $E/\mathbb{Q}$ is an elliptic curve with $E(K)_{tors} \cong \mathbb{Z}/15\mathbb{Z}$ over some quartic field $K$, then $j(E) \in \{-5^2/2, -5^2 \cdot 241^3/2^3, -5 \cdot 29^3/2^5, 5 \cdot 211^3/2^{15}\}$.*

Furthermore, González-Jiménez and Lozano-Robledo partially determine the possible torsion growths when base extending to $K$, i.e. if $E(\mathbb{Q})_{\text{tors}} \cong G$, they partially determine the possibilities for $E(K) \cong H$, where $H$ is a torsion subgroup listed in Theorem 4.34. They also provide examples of each such torsion subgroup. It is worth noting that by Theorem 4.11, $\mathbb{Z}/15\mathbb{Z}$ occurs infinitely often as a torsion subgroup for elliptic curves $E/K$, where $K$ is a quartic field. But when one begins with a rational elliptic curve $E/\mathbb{Q}$ and base extends to a quartic field, there are only finitely many elliptic curves that then gain a point of order 15—precisely the ones in Theorem 4.34. Finally, González-Jiménez and Najman complete the classification of $\Phi_{\mathbb{Q}}(4)$ in [GJN20b].

**Theorem 4.35** ([GJN20b, Cor. 8.7])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be*

*a quartic number field. Then* $E(K)_{tors}$ *is isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 15, 16, 20, 24 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 8 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \text{or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. \end{cases}$$

*Moreover, each of these groups, except for* $\mathbb{Z}/15\mathbb{Z}$*, occurs over some quartic field for infinitely many* $\overline{\mathbb{Q}}$*-isomorphism classes. If* $E/\mathbb{Q}$ *is an elliptic curve with* $E(K)_{tors} \cong \mathbb{Z}/15\mathbb{Z}$ *over some quartic field* $K$*, then* $j(E) \in \{-5^2/2, -5^2 \cdot 241^3/2^3, -5 \cdot 29^3/2^5, 5 \cdot 211^3/2^{15}\}$.

Furthermore, they determine the possible torsion structures based on the isomorphism type of $\mathrm{Gal}(\widehat{K}/\mathbb{Q})$. Note that in the cases where $\mathrm{Gal}(\widehat{K}/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ or $\mathrm{Gal}(\widehat{K}/\mathbb{Q}) \cong V_4$, the Klein-4 group, this is just Chou's result [Cho16].

**Theorem 4.36** ([GJN20b, Cor. 8.4,Thm. 8.5])**.** *Let* $E/\mathbb{Q}$ *be a rational elliptic curve, and let* $K/\mathbb{Q}$ *be a quartic number field. Let* $\widehat{K}$ *denote the Galois closure of* $K/\mathbb{Q}$*. Then*

$$\begin{aligned} \Phi_{\mathbb{Q}}^{\mathbb{Z}/4\mathbb{Z}}(4) &= \Phi(1) \cup \{\mathbb{Z}/n\mathbb{Z} \colon \ = 13, 15, 16\} \cup \{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \colon n = 6, 8\} \cup \{\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}\}, \\ \Phi_{\mathbb{Q}}^{V_4}(4) &= \Phi_{\mathbb{Q}}(2) \cup \{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}\}, \\ \Phi_{\mathbb{Q}}^{D_4}(4) &= \Phi_{\mathbb{Q}}(2) \cup \{\mathbb{Z}/20\mathbb{Z}, \mathbb{Z}/24\mathbb{Z}\}, \text{ and} \\ \Phi_{\mathbb{Q}}^{S_4}(4) &= \Phi_{\mathbb{Q}}^{A_4}(4) = \Phi(1). \end{aligned}$$

González-Jiménez determines the set $\Phi_{\mathbb{Q}}(5)$ in [GJ17]. González-Jiménez also determines

for a fixed possible torsion subgroup $G \cong E(\mathbb{Q})_{\text{tors}}$ the possible torsion subgroups $E(K)_{\text{tors}} \supseteq G$ with $E(\mathbb{Q})_{\text{tors}} \subsetneq E(K)_{\text{tors}}$, and the number of such fields there is torsion growth. In particular, he shows there is at most one quintic number field $K$ such that there is torsion growth.

**Theorem 4.37** ([GJ17, Thm. 1, Thm. 2])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a quintic number field. Then $E(K)_{tors}$ is isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 12, 25 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \end{cases}$$

*Moreover, each of these groups, except for $\mathbb{Z}/11\mathbb{Z}$, occurs over some quintic field for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes. The only elliptic curves $E/\mathbb{Q}$ with $E(K)_{tors} \cong \mathbb{Z}/11\mathbb{Z}$ over some quintic field $K$ have Cremona label `121a2`, `121c2`, `121b1`. For elliptic curves $E/\mathbb{Q}$ with CM, $\Phi_{\mathbb{Q}}^{\text{CM}}(5) = \{\mathcal{O}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/11\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\}$.*

The classification of the set $\Phi_{\mathbb{Q}}(6)$ began with work of Daniels and González-Jiménez in [DGJ20], where they classify the possible torsion subgroups $E(K)_{\text{tors}}$ which occur infinitely often, as well as a few other torsion possibilities which do not. They are also able to determine the possible growth of torsion subgroups $E(\mathbb{Q})_{\text{tors}}$ to $E(K)_{\text{tors}}$ in many cases, c.f. [DGJ20, Thm. 2].

**Theorem 4.38** ([DGJ20, Thm. 1])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a sextic number field. Then if $E(K)_{tors}$ occurs for infinitely many distinct $\overline{\mathbb{Q}}$-isomorphism classes (or is isomorphic to $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/21\mathbb{Z}$, or $\mathbb{Z}/30\mathbb{Z}$), then $E(K)_{tors}$ is isomorphic to*

*precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 21, 30,\ n \neq 11, 17, 19, 20 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 7, 9 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, & \text{or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. & \end{cases}$$

*Moreover, if $E/\mathbb{Q}$ is an elliptic curve with $E(K)_{tors} \cong H$ over some sextic field $K$, then if*

*(i) $H = \mathbb{Z}/15\mathbb{Z}$: then $E$ has Cremona label 50a3, 50a4, 50b1, 50b2, 450b4, or 450b3.*

*(ii) $H = \mathbb{Z}/21\mathbb{Z}$: $j(E) \in \{3^3 \cdot 5^3/2, -3^2 \cdot 5^3 \cdot 101^3/2^{21}, -3^3 \cdot 5^3 \cdot 382^3/2^7, -3^2 \cdot 5^6/2^3\}$.*

*(iii) $H = \mathbb{Z}/30\mathbb{Z}$: then $E$ has Cremona label 50a3, 50b1, 50b2, or 450b4.*

Moreover, Daniels and González-Jiménez give examples of each possible torsion structure and conjecture that $\Phi_{\mathbb{Q}}(6)$ is the set of possibilities given in Theorem 4.38 along with the group $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. Finally, they also make progress in determining the possible torsion growth from $E(\mathbb{Q})_{\text{tors}}$ to $E(K)_{\text{tors}}$, where $K$ is a sextic number field. The next progress in the classification of $\Phi_{\mathbb{Q}}(6)$ (including the near complete description of the possible growths for torsion subgroups) came shortly thereafter in work of Gužvoć.

**Theorem 4.39** ([Guž21, Thm. 1])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a*

*sextic number field. Then* $E(K)_{tors}$ *is isomorphic to one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 21, 30,\ n \neq 11, 17, 19, 20 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 7, 9 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, & \text{or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. & \end{cases}$$

*Furthermore, all but the group* $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$ *are known to occur.*

As Gužvoć remarks, the group $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$ is unlikely to actually occur, though he is unable to prove it entirely in the paper. If this group does not occur as the torsion subgroup $E(K)_{\text{tors}}$ for an elliptic curve over a sextic number field, then this would confirm the conjecture of Daniels and González-Jiménez.

There are currently no remaining "non-trivial" classifications for the sets $\Phi_{\mathbb{Q}}(d)$, in the sense that there is no $d > 6$ such that $\Phi_{\mathbb{Q}}(d)$ is known and $\Phi_{\mathbb{Q}}(d) \neq \Phi(1)$. A remarkable paper of González-Jiménez and Najman actually classify the set $\Phi_{\mathbb{Q}}(7)$ (along with the possible torsion growth) and the sets $\Phi_{\mathbb{Q}}(d)$ for an infinite set of $d$, namely those whose smallest prime divisor is at least 11.

**Theorem 4.40** ([[GJN20b, Prop7.7]]). *Let* $E/\mathbb{Q}$ *be an elliptic curve, and* $K$ *a number field of degree 7.*

*(i) If* $E(\mathbb{Q})_{tors} \not\simeq \{\mathcal{O}\}$, *then* $E(\mathbb{Q})_{tors} = E(K)_{tors}$.

*(ii) If* $E(\mathbb{Q})_{tors} \simeq \{\mathcal{O}\}$, *then* $E(K)_{tors} \simeq \{\mathcal{O}\}$ *or* $\mathbb{Z}/7\mathbb{Z}$. *Furthermore, if* $E(\mathbb{Q})_{tors} \simeq \{\mathcal{O}\}$ *and* $E(K)_{tors} \simeq \mathbb{Z}/7\mathbb{Z}$, *then* $K$ *is the unique degree 7 number field with this property*

*and $E$ is isomorphic to the elliptic curve*

$$\begin{aligned} E_t\colon y^2 = x^3 &+ 27(t^2-t+1)(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)x \\ &+ 54(t^{12}-522t^{11}-8955t^{10}+37950t^9-70998t_1^8 31562t^7 \\ &- 253239t^6+316290t^5-218058t^4+80090t^3-14631t^2+510t+1) \end{aligned}$$

*for some $t \in \mathbb{Q}$.*

**Theorem 4.41** ([GJN20b, Thm. 7.2])**.** *Let $d$ be a positive integer. Let $E/\mathbb{Q}$ be an elliptic curve, and let $K/\mathbb{Q}$ be a number field of degree $N$, where the smallest prime divisor of $N$ is $\geq d$. Then*

*(i) If $d \geq 11$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p$. In particular, $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

*(ii) If $d \geq 7$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 7$.*

*(iii) If $d \geq 5$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 5, 7, 11$.*

*(iv) If $d > 2$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 2, 3, 5, 7, 11, 13, 19, 43, 67, 163$.*

In particular, this proves the following

**Corollary 4.42** ([GJN20b, Cor 7.3])**.** *Let $d$ be a positive integer such that the smallest prime factor of $d$ is $\geq 11$. Then $\Phi_{\mathbb{Q}}(d) = \Phi(1)$.*

As González-Jiménez and Najman remark ([GJN20b, Rem. 7.4]), Corollary 4.42 is best

possible in the sense that for $p \in \{2, 3, 5, 7\}$, the set

$$\bigcup_{n=1}^{\infty} \Phi_{\mathbb{Q}}(p^n)$$

contains $\mathbb{Z}/p^k\mathbb{Z}$ for all positive integers $k$, and hence would be infinite. The positive integers whose smallest prime divisor is at least 11 are of the form $d = 210k + x$, where $1 \leq x < 210$ is an integer coprime to 210. But then

$$\frac{\phi(210)}{210} = \frac{48}{210} = \frac{8}{35} \approx 0.2286$$

of all integers satisfy this property. In fact, the methods applied in their paper also apply to infinite extensions of $\mathbb{Q}$.

**Corollary 4.43** ([GJN20b, Cor. 7.6]). *Let $p \geq 11$ be a prime, and let $K$ be the $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Then $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

## 4.5 Growth of Torsion Upon Base Extension

One approach to classifying $\Phi(d)$ or $\Phi_{\mathbb{Q}}(d)$, especially in the cases when the set $\Phi_{\mathbb{Q}}(d')$ is known for $d' \mid d$, is to study how torsion subgroups can grow when base extending from $E(F)_{\text{tors}}$ to $E(K)_{\text{tors}}$, where $\mathbb{Q} \subseteq F \subseteq K$ is a finite extension of fields. For instance, while studying torsion subgroups of elliptic curves defined over cubic fields, Najman proved the following:

**Lemma 4.44** ([Naj12b, Lemma 1]). *If the torsion subgroup of an elliptic curves $E$ over $\mathbb{Q}$ has a nontrivial 2-Sylow subgroup, then over any number field of odd degree the torsion of $E$ will have the same 2-Sylow subgroup as over $\mathbb{Q}$, i.e. $E(K)[2^\infty] = E(\mathbb{Q})[2^\infty]$.*

**Lemma 4.45** ([Naj16, Lemma 21]). *Let $K$ be a cubic field. Then the 5-Sylow groups of $E(\mathbb{Q})$ and $E(K)$ are equal.*

Furthermore while classifying the set $\Phi_{\mathbb{Q}}(3)$, Najman provided criterion for when one should not see torsion growth when base extending the elliptic curve based on the structure of $E(K)_{\text{tors}}$ and the Galois group of the number field.

**Lemma 4.46** ([Naj16, Lemma 16]). *Let $p, q$ be distinct odd primes, $F_2/F_1$ a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$ and $E/F_1$ an elliptic curve with no $p$-torsion over $F_1$. Then if $q$ does not divide $p-1$ and $\mathbb{Q}(\zeta_p) \not\subset F_2$, then $E(F_2)[p] = 0$.*

**Lemma 4.47** ([Naj16, Lemma 17]). *Let $p$ be an odd prime number, $q$ a prime not dividing $p$, $F_2/F_1$ a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$, $E/F_1$ an elliptic curve, and suppose $E(F_1) \supset \mathbb{Z}/p\mathbb{Z}$, $E(F_1) \not\supset \mathbb{Z}/p^2\mathbb{Z}$, and $\zeta_p \notin F_2$. Then $E(F_2) \not\supset \mathbb{Z}/p^2\mathbb{Z}$.*

These results were vastly generalized in the amazing paper of González-Jiménez and Najman [GJN20b].

**Theorem 4.48** ([GJN20b, Thm. 4.1]). *Let $L/F$ be a finite extension of number fields, $\widehat{L}$ denote the normal closure of $L$ over $F$, $G = \mathrm{Gal}(\widehat{L}/F)$, and suppose that $H = \mathrm{Gal}(\widehat{L}/L)$ is a non-normal maximal subgroup of $G$. Let $p$ be a prime, $a = [F(\zeta_p)\colon F]$, and suppose $G$ does not contain a cyclic quotient group of order $a$. Then for every elliptic curve $E/F$, it holds that $E(L)[p] = E(F)[p]$.*

**Theorem 4.49** ([GJN20b, Thm. 4.3]). *Let $E/F$ be an elliptic curve, $L/F$ be a finite extension of number fields with no intermediate fields, and let $G = \mathrm{Gal}(\overline{L}/F)$, where $\widehat{L}$ is the*

*normal closure of $L$ over $F$. If $G$ is not isomorphic to a quotient of* $\mathrm{Gal}(F(E[p])/F)$*, then* $E(L)[p] = E(F)[p]$.

**Theorem 4.50** ([GJN20b, Thm. 4.5])**.** *Let $L/F$ be a finite extension of number fields,* $G = \mathrm{Gal}(\widehat{L}/F)$*, where $\widehat{L}$ is the normal closure of $L$ over $F$, $n$ be a positive integer, and let $p$ be a prime co-prime to $[L\colon F]$. Suppose that $G$ is not isomorphic to a quotient of any subgroup of* $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ *and that* $\mathrm{Gal}(\overline{L}/L)$ *is maximal in $G$. Let $E/F$ be an elliptic curve such that it has a $F$-rational point of order $p^n$, but no $F$-rational points of order $p^{n+1}$. Then $E(L)$ has no points of order $p^{n+1}$.*

**Theorem 4.51** ([GJN20b, Prop. 4.6])**.** *Let $E/F$ be an elliptic curve over a number field $F$, $n$ a positive integer, $P \in E(\overline{F})$ be a point of order $p^{n+1}$. Then $[F(P)\colon F(pP)]$ divides $p^2$ or $(p-1)p$.*

**Theorem 4.52** ([GJN20b, Prop. 4.8])**.** *Let $E/F$ be an elliptic curve over a number field $F$, $n$ a positive integer, $P \in E(\overline{F})$ be a point of order $2^{n+1}$, and let $\widehat{F(P)}$ be the Galois closure of $F(P)$ over $F(2P)$. Then $[F(P)\colon F(2P)]$ divides 4 and* $\mathrm{Gal}(\widehat{F(P)}/F(2P))$ *is either trivial, isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or $D_4$.*

The results in Theorem 4.48–4.52 were based on a careful study of the mod $n$ Galois representation, building on work of Balakrishnan, Bilu, Dogra, Mazur, Müller, Parent, Rebolledo, Serre, Tuitman, Vonk, and Zywina, and the action of Galois on torsion points. But using these tools, one can do more than just determine criterion for when there is no torsion growth. González-Jiménez and Najman apply these same techniques to determine the degrees of the possible fields of definition for points of prime order.

**Theorem 4.53** ([GJN20b, Thm. 5.8])**.** *Let $E/\mathbb{Q}$ be an elliptic curve, $p$ a prime and $P$ a*

*point of order $p$ in $E$. Then all of the cases in table 4.1 occur for $p \leq 13$ or $p = 37$, and they are the only ones possible. The degrees in Table 4.1 with an asterisk occur only when $E$ has CM. For all other $p$, the possibilities for $[\mathbb{Q}(P)\colon \mathbb{Q}]$ are as is given below. The degrees in equations 4.3–4.5 occur only for CM elliptic curves $E/\mathbb{Q}$. Furthermore, the degrees in equation 4.5 occur only for elliptic curves with $j$-invariant 0. If a given conjecture is true, c.f.* [GJN20b, Conj. 3.5]*, then the degrees in equations 4.6 also occur only for elliptic curves with $j$-invariant 0.*

$$p^2 - 1 \qquad \text{for all } p, \tag{4.1}$$

$$8, 16, 32^*, 136, 256^*, 272, 288 \qquad \text{for } p = 17, \tag{4.2}$$

$$(p-1)/2, p-1, p(p-1)/2, p(p-1) \qquad \text{if } p \in \{19, 43, 67, 163\} \tag{4.3}$$

$$2(p-1), (p-1)^2 \qquad \text{if } p \equiv 1 \mod 3 \text{ or } \left(\frac{-D}{p}\right) = 1 \text{ for any } D \in CM \tag{4.4}$$

$$(p-1)^2/3, 2(p-1)^2/3 \qquad p \equiv 4, 7 \mod 9 \tag{4.5}$$

$$(p^2-1)/3, 2(p^2-1)/3 \qquad p \equiv 2, 5 \mod 9 \tag{4.6}$$

*where $CM = \{1, 2, 7, 11, 19, 43, 67, 163\}$. Apart from the cases above that have been proven to appear, the only other options that might be possible are:*

$$(p^2-1)/3, 2(p^2-1)/3 \quad \text{if } p \equiv 8 \mod 9. \tag{4.7}$$

**Corollary 4.54** ([GJN20b, Cor. 6.1 (i)–(iv)])**.**

*(i)* $11 \in R_{\mathbb{Q}}(d)$ *if and only if* $5 \mid d$.

*(ii)* $13 \in R_{\mathbb{Q}}(d)$ *if and only if* $3 \mid d$ *or* $4 \mid d$.

*(iii)* $17 \in R_{\mathbb{Q}}(d)$ *if and only if* $8 \mid d$.

Table 4.1: The possible degrees for the field of definitions for points of prime order $p = 2$, 3, 5, 7, 11, 13, 37

| $p$ | $[\mathbb{Q}(P)\colon \mathbb{Q}]$ |
|---|---|
| 2 | 1, 2, 3 |
| 3 | 1, 2, 3, 4, 6, 8 |
| 5 | 1, 2, 4, 5, 8, 10, 16, 20, 24 |
| 7 | 1, 2, 3, 6, 7, 9, 12, 14, 18, 21, 24*, 36, 42, 48 |
| 11 | 5, 10, 20*, 40*, 55, 80*, 100*, 110, 120 |
| 13 | 3, 4, 6, 12, 24*, 39, 48*, 52, 72, 78, 96, 144*, 156, 168 |
| 37 | 12, 36, 72*, 444, 1296*, 1332, 1368 |

*(iv)* $37 \in R_{\mathbb{Q}}(d)$ *if and only if* $12 \mid d$.

As they state in their paper, González-Jiménez and Najman are able to determine the possible degrees of the fields of definition for points of prime order $p$ for all primes with $p \not\equiv 8 \mod 9$ or $\left(\frac{-D}{p}\right) = 1$, which represents a set of primes of density $1535/1536 \approx 0.9993$. In particular, this computes the possible degrees for the fields of definition of points of prime order $p$ for all $p < 3167$. González-Jiménez and Najman are then able to determine the possible prime orders for points over all fields of degree $d \leq 3342296$. Furthermore, combing these results, given a number field $K$ of degree $d$, González-Jiménez and Najman are able to determine when there can be torsion growth when base extending an elliptic curve $E/\mathbb{Q}$ to $K$ based solely on the prime divisors of $d$, which we shall restate:

**Theorem 4.41** ([GJN20b, Thm. 7.2])**.** *Let $d$ be a positive integer. Let $E/\mathbb{Q}$ be an elliptic curve, and let $K/\mathbb{Q}$ be a number field of degree $N$, where the smallest prime divisor of $N$ is $\geq d$. Then*

*(i) If $d \geq 11$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p$. In particular, $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

*(ii) If $d \geq 7$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 7$.*

*(iii) If $d \geq 5$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 5, 7, 11$.*

*(iv) If $d > 2$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 2, 3, 5, 7, 11, 13, 19, 43, 67, 163$.*

In this same paper, González-Jiménez and Najman complete the classification of $\Phi_{\mathbb{Q}}(4)$ and also classify $\Phi_{\mathbb{Q}}(7)$. Moreover, using Theorem 4.41, they are able to determine $\Phi_{\mathbb{Q}}(d) = \Phi_{\mathbb{Q}}(1)$ for all degrees $d$ whose smallest prime divisor is at least 11. Obviously, Theorem 4.41 says that not only is $\Phi_{\mathbb{Q}}(d) = \Phi_{\mathbb{Q}}(1)$ for such $d$, but that actually $E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ for all such fields $K$.

If that was not enough, González-Jiménez and Najman do even more in a later paper. Suppose we wanted to determine when there can be torsion growth for elliptic curves over fields of degree $d$. By Merel's Theorem, see [Mer96], we know that the sets $\Phi_{\mathbb{Q}}(d)$ are uniformly bounded. Suppose that for the set $\Phi_{\mathbb{Q}}(d)$, we have an effective bound $B_d$, i.e. that $\#E(K)_{\text{tors}} \leq B_d$. For each prime power $\ell^n \leq B_d$, one can compute the $\ell^n$th division polynomial $\psi_{\ell^n}$. For each irreducible factor $f_i$ of $\psi_{\ell^n}$, one can check whether $\deg f_i$ divides $d$. If not, move onto the next prime or prime power. If so, then one checks whether the point of order $\ell^n$, say $P$, is defined over $\mathbb{Q}(f_i)$. If so, add this field to a list. If not, then the torsion is defined over a quadratic extension of $\mathbb{Q}(f_i)$, i.e. the field where $y$ is defined. Then if $2 \deg f_i$ divides $d$, add the field $\mathbb{Q}(P)$ (the field where both the $x, y$ coordinates of the $\ell^n$-torsion point are defined) to the list. This is exactly what González-Jiménez and Najman do in [GJN20a]. However, this is not a practical algorithm as the degree of $\psi_n$ is quadratic in $n$ and the prime powers needed to be checked grow exponentially in $d$. However, González-Jiménez and Najman apply information about the mod $n$ Galois representations attached to $E/\mathbb{Q}$ developed in [GJN20b] to avoid division polynomial computations when possible. They apply these techniques to all elliptic curves of conductor of less than 400,000 (a total of 2,483,649 curves) and all $d \leq 23$. They are then able to arrive at a number of interesting results. For instance, they show that there is no point of

order 49 on any elliptic curve $E/\mathbb{Q}$ for fields of degree less than 42, or points of order 125 over fields of degree less than 50. For a complete description of their results and data, see [GJN20a].

Of course, one can be more specific than just determining when there can or cannot be torsion growth. Instead, one could focus on exactly how the torsion structure grows or changes as one base extends the curve. That is, given $G \in \Phi(1)$ (or more generally, $G \in \Phi_{\mathbb{Q}}(d')$ for some $d'$), what are the possible torsion subgroups $H \in \Phi_{\mathbb{Q}}(d)$ such that there is an elliptic curve $E/\mathbb{Q}$ with $E(K)_{\text{tors}} \cong H$ and $E(\mathbb{Q})_{\text{tors}} \cong G$. Of course, one always has $E(\mathbb{Q})_{\text{tors}} \subseteq E(K)_{\text{tors}}$, but what are the possibilities for torsion growth? In [GJT14] and [GJT16], González-Jiménez and Tornero determine completely the sets $\Phi_{\mathbb{Q}}(2, G)$ for $G \in \Phi(1)$. They give examples of each such possible torsion growth, i.e. examples where $E(\mathbb{Q})_{\text{tors}} \subsetneq E(K)_{\text{tors}}$. Moreover, fixing an elliptic curve $E/\mathbb{Q}$, they are able to determine the maximum number of quadratic fields such that $E(K)_{\text{tors}} \ncong E(\mathbb{Q})_{\text{tors}}$. For all $G \in \Phi(1)$ except for $G \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, there are at most two quadratic fields such that $E(K)_{\text{tors}} \ncong E(\mathbb{Q})_{\text{tors}}$. In the case of $G \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $H \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, three such fields are possible. See [GJT16] for a complete description of their results with tables and examples. González-Jiménez also classifies these sets when restricting to CM elliptic curves in [GJ21]. In this case, González-Jiménez is also able to give an explicit characterization of the quadratic fields where the torsion grows in terms of invariants of the elliptic curve. The possible growths of torsion subgroups in the cubic case was completely characterized by González-Jiménez, Najman, and Tornero.

**Theorem 4.55** ([GJNT16, Thm. 1, Thm. 3])**.** *For $G \in \Phi(1)$, the set $\Phi_{\mathbb{Q}}(3, G)$ is given in Table 4.2. Furthermore, if $E/\mathbb{Q}$ is a rational elliptic curve, then*

*(i) There is at most one cubic number field $K$, up to isomorphism, such that $E(K)_{tors} \cong H \neq E(\mathbb{Q})_{tors}$ for a fixed $H \in \Phi_{\mathbb{Q}}(3)$.*

*(ii) There are at most three cubic number fields $K_i$, $i = 1, 2, 3$ (non-isomorphic pairwise), such that $E(K_i)_{tors} \neq E(\mathbb{Q})_{tors}$. Moreover, the elliptic curve 162b2 is the unique rational elliptic curve where the torsion grows over three non-isomorphic cubic fields.*

Table 4.2: A table of the sets $\Phi_{\mathbb{Q}}(3, G)$ for $G \in \Phi(1)$

| $G$ | $\Phi_{\mathbb{Q}}(3, G)$ |
|---|---|
| $\{\mathcal{O}\}$ | $\{\{\mathcal{O}\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/13\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}\}$ |
| $\mathbb{Z}/2\mathbb{Z}$ | $\{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/14\mathbb{Z}\}$ |
| $\mathbb{Z}/3\mathbb{Z}$ | $\{Z3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\}$ |
| $\mathbb{Z}/4\mathbb{Z}$ | $\{\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}\}$ |
| $\mathbb{Z}/5\mathbb{Z}$ | $\{\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/10\mathbb{Z}\}$ |
| $\mathbb{Z}/6\mathbb{Z}$ | $\{\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/18\mathbb{Z}\}$ |
| $\mathbb{Z}/7\mathbb{Z}$ | $\{\mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/14\mathbb{Z}\}$ |
| $\mathbb{Z}/8\mathbb{Z}$ | $\{\mathbb{Z}/8Z\}$ |
| $\mathbb{Z}/9\mathbb{Z}$ | $\{\mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/18\mathbb{Z}\}$ |
| $\mathbb{Z}/10\mathbb{Z}$ | $\{\mathbb{Z}/10\mathbb{Z}\}$ |
| $\mathbb{Z}/12\mathbb{Z}$ | $\{\mathbb{Z}/12\mathbb{Z}\}$ |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | $\{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\}$ |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ | $\{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\}$ |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ | $\{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\}$ |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ | $\{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}\}$ |

They give the number of possible fields over which there is torsion growth, along with examples of each such torsion growth, in their paper. It is worth noting that from their paper (as we will use this later) that if $H \cong \mathbb{Z}/18\mathbb{Z}$, there are only two possibilities for $G$—$\mathbb{Z}/6\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$—and in each case there is at most one cubic field where one can see that torsion growth. Again, González-Jiménez determines the possible torsion growths in the CM case in [GJ20], along with examples and explicit characterizations of the cubic fields over which there is growth in terms of invariants attached to the elliptic curve. The sets $\Phi_{\mathbb{Q}}(d, G)$ are determined for $d = 4$ in [GJLR18], $d = 5$ in [GJ17], and $d = 6$ in [DGJ20]. Finally from [GJN20b], we know that $\Phi_{\mathbb{Q}}(7, G) = \{G\}$ except in the case of $G \cong \{\mathcal{O}\}$, where $\Phi_{\mathbb{Q}}(d, \{\mathcal{O}\}) = \{\{\mathcal{O}\}, \mathbb{Z}/7\mathbb{Z}\}$, and that $\Phi_{\mathbb{Q}}(d, G) = \{G\}$ for all number fields of degree $d$, where the smallest prime divisor of $d$ is at least 11.

## 4.6 Torsion Subgroups of Elliptic Curves over Infinite Extensions

Of course, one need not limit oneself to just number fields. Instead, one can examine the possible torsion structures $E(K)_{\text{tors}}$, where $K/\mathbb{Q}$ is an infinite extension of fields. The Mordell-Weil Theorem no longer applies, so one need prove first that the torsion subgroup is finite (while the rank may be infinite). The first progress in this direction came with Laska, Lorenz, [LL85], and Fujita's, [Fuj04, Fuj05], classification of the possibilities for $E(K)_{\text{tors}}$, where $K$ is the maximal 2-abelian extension of $\mathbb{Q}$, i.e. $K = \mathbb{Q}(\{\sqrt{n}\colon n \in \mathbb{Z}\})$. Generally, the maximal 2-abelian extension of a field $F$ is $K = F(\{\sqrt{n}\colon n \in \mathcal{O}_F\})$, where $\mathcal{O}_F$ is the ring of integers of $F$. For ease of notation, we make the following definition:

**Definition.** For each fixed integer $d \geq 1$, let $\mathbb{Q}(d^\infty)$ denote the compositum of all field extensions $K/\mathbb{Q}$ of degree $d$. More precisely, let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$, then define $\mathbb{Q}(d^\infty) := \mathbb{Q}(\{\beta \in \overline{\mathbb{Q}}\colon [\mathbb{Q}(\beta)\colon \mathbb{Q}] = d\})$.

The fields $\mathbb{Q}(d^\infty)$ have been studied by Gal and Grizzard in [GG14], where they prove a number of interesting results. Laska, Lorenz and Fujita show there are exactly 20 possibilities for $E(\mathbb{Q}(2^\infty))_{\text{tors}}$, where $E/\mathbb{Q}$ is a rational elliptic curve.

**Theorem 4.56** ([LL85, Fuj04, Fuj05])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $\mathbb{Q}(2^\infty)$ be the maximal abelian 2-extension of $\mathbb{Q}$. Then $E(K)_{tors}$ is isomorphic to precisely one of*

*the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 3, 5, 7, 9, 15 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6, 8 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, & \text{or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \text{ or} \\ \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 3, 4. \end{cases}$$

*Moreover, each of the possible torsion subgroups list occur.*

Later in [Ejd18], Ejder determined the possibilities for $E(K)_{\text{tors}}$, where $K$ is the maximal abelian 2-extension of $\mathbb{Q}$ and $E$ is an elliptic curve defined over a quadratic cyclotomic field, i.e. $E/\mathbb{Q}(i)$ or $E/\mathbb{Q}(\sqrt{-3})$.

The next progress came with [DLRNS18]. First, they prove a finiteness theorem about torsion subgroups for rational elliptic curves base extended to (possibly infinite) Galois extensions of $\mathbb{Q}$.

**Theorem 4.57** ([DLRNS18, Thm. 4.1])**.** *Let $E/\mathbb{Q}$ be an elliptic curve, and let $F$ be a (possibly infinite) Galois extension of $\mathbb{Q}$ that contains only finitely many roots of unity. Then $E(F)_{tors}$ is finite. Moreover, there is a uniform bound $B$, depending only on $F$, such that $\#E(F)_{tors} \leq B$ for every elliptic curve $E/\mathbb{Q}$.*

Using this, they are able to prove the following general result:

**Proposition 4.58** ([DLRNS18, Prop. 4.7])**.** *For every $d \geq 2$, the cardinality of $E(\mathbb{Q}(d^{\infty}))_{tors}$ is finite and uniformly bounded as $E$ varies over elliptic curves over $\mathbb{Q}$.*

Daniels, Lozano-Robledo, Najman, and Sutherland then classify the possibilities for the torsion subgroups $E(\mathbb{Q}(3^\infty))_{\text{tors}}$, where $E/\mathbb{Q}$ is a rational elliptic curve.

**Theorem 4.59** ([DLRNS18, Thm. 1.8])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then the torsion subgroup $E(\mathbb{Q}(3^\infty))_{tors}$ is finite and is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 4, 5, 7, 8, 13 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2, 4, 7 \text{ or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6n\mathbb{Z}, & \text{with } n = 1, 2, 3, 5, 7 \text{ or} \\ \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 4, 6, 7, 9. \end{cases}$$

*All but four of the torsion subgroups, $T$, listed above occur for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$. For $T \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/42\mathbb{Z}$, and $\mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, there are only 2, 2, 4, and 1 (respectively) $\overline{\mathbb{Q}}$-isomorphism classes of $E/\mathbb{Q}$ for which $E(\mathbb{Q}(3^\infty))_{tors} \cong T$.*

They give examples of each such torsion subgroup in their paper. Daniels continues to extend this work in [Dan18][3] by first observing a (less general) version of a result of Gal and Grizzard.

**Proposition 4.60** ([Dan18, Prop. 1.9])**.** *Let $K/\mathbb{Q}$ be a finite extension. Then $K \subseteq \mathbb{Q}(d^\infty)$ if and only if the following two conditions are met:*

*(i) There exists a group $H$ which is a subdirect product of transitive subgroups of degree*

[3]In examining this paper, it is important that one also see Daniel's errata in [Dan21]. While the main results of the paper are still true, the claim about the compositum of all $D_4$-extensions over $\mathbb{Q}$ and $\mathbb{Q}(D_4^\infty)$ being the same is not necessarily true.

*d with some normal subgroup $N$ such that*

$$1 \longrightarrow N \longrightarrow H \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1$$

*is a short exact sequence.*

*(ii) We can solve the corresponding Galois embedding problem, i.e. we can find a field $L \supseteq K$ such that* $\mathrm{Gal}(L/\mathbb{Q}) \cong H$.

Motivated by Proposition 4.60(i), Daniels makes the following definition:

**Definition.** Let $G$ be a transitive subgroup of $S_n$ for some $n \geq 2$. We say that a finite group $H$ is of generalized $G$-type if it is isomorphic to a quotient of a subdirect product of transitive subgroups of $G$. Given a number field $K/\mathbb{Q}$ and its Galois closure $\widehat{K}$, we say that $K/\mathbb{Q}$ is of generalized $G$-type if $\mathrm{Gal}(\widehat{K}/\mathbb{Q})$ is a group of generalized $G$-type. Let $\mathbb{Q}(G^\infty)$ be the compositum of all fields that are of generalized $G$-type.

**Example 4.1** ([Dan18, Ex. 3.1])**.** Clearly the groups $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ are all of generalized $D_4$-type. More interestingly, the quaternion group $Q_8$ is generalized $D_4$-type since $Q_8 \cong G/H$ with

$$G = \langle (2,4)(5,6,7,8), (1,2,3,4), (1,3)(2,4), (5,7)(6,8) \rangle,$$
$$H = \langle (1,3)(2,4)(5,7)(6,8) \rangle.$$

◁

Again, when considering infinite extensions of $\mathbb{Q}$, the Mordell-Weil Theorem no longer applies. Then one has to worry whether the torsion subgroup of $E(K)_{\mathrm{tors}}$ can be infinite. One might expect the torsion to remain 'small' if the fields in question cannot contain 'many' roots of unity. With this goal in mind, one often examines compositum of fields

with specified Galois group $G$—a compositum of so-called 'horizontal' fields. The group theoretic condition of being of generalized $G$-type is simply a necessary condition for a number field with a given Galois group to be contained in the compositum. In any case, Daniels is then able to classify the possibilities for $E(\mathbb{Q}(D_4^\infty))_{\text{tors}}$, where $E/\mathbb{Q}$ is a rational elliptic curve.

**Theorem 4.61** ([Dan18, Thm 1.10])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then the torsion subgroup $E(\mathbb{Q}(D_4^\infty))_{tors}$ is finite and is isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{with } n = 1, 3, 5, 7, 9, 13, 15 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z} & \text{with } n = 1, 5 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z} & \text{with } n = 1, 2, 3, 4, 5, 6, 8 \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} & \text{or} \\ \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8n\mathbb{Z} & \text{with } n = 1, 2, 3, 4 \text{ or} \\ \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/12n\mathbb{Z} & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}. \end{cases}$$

*All but three of the 24 torsion structures listed above occur for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$. The torsion structures that occur finitely often are $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z}$, and $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$ which occur for 4, 2, and 1 $\overline{\mathbb{Q}}$-isomorphism classes respectively.*

Examples of each torsion subgroup occurring are found in his paper. Daniels, Derickx, and Hatley[4] classified the possibilities for $E(\mathbb{Q}(A_4^\infty))_{\text{tors}}$ in [DDH19].

[4]While unimportant, it is interesting to note that Hatley owns several llamas: Nimbus, Maverick, Gunnar, and Wes, who have their own Instagram account, see https://www.nimbusthellama.com/. Moreover, they are available for rent for parties—they llama meet you! Union College, as Hatley notes, has an archaic policy that faculty are able to allow their livestock to graze on the quad. So perhaps you may one day find the llamas grazing in the quad.

**Theorem 4.62** ([DDH19, Thm. 1.7])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then the torsion subgroup $E(\mathbb{Q}(A_4^\infty))_{tors}$ is finite and isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 3, 5, 7, 9, 13, 15, 21 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 9 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 3 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7 \text{ or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, & \text{or} \\ \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}. & \end{cases}$$

*All but four of the 26 torsion structures listed above occur for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$. The torsion structures which occur finitely often are $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, and $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$, which occur for 2, 4, 2, and 1 $\overline{\mathbb{Q}}$-isomorphism classes, respectively.*

Examples of each torsion subgroup that appears are given in their paper. Now let $\mathbb{Q}^{\text{ab}}$ denote the maximal abelian extension of $\mathbb{Q}$, i.e. the compositum of all abelian extensions of $\mathbb{Q}$. By the Kronecker-Weber Theorem, $\mathbb{Q}^{\text{ab}} = \mathbb{Q}(\{\zeta_n : n \in \mathbb{Z}^+\})$, where $\zeta_n$ is a primitive $n$th root of unity. Again, if one is to consider torsion subgroups of elliptic curves over $\mathbb{Q}^{\text{ab}}$, one first find a replacement for the Mordell-Weil Theorem—or at least show that the torsion subgroup is a finite abelian group. Ribet [Rib81] proved that given an abelian variety $A/\mathbb{Q}$, $A(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ is finite. Of course, one may then wonder if there is a uniform bound for the size of the torsion structures for elliptic curves over $\mathbb{Q}^{\text{ab}}$. Chou classified the possible torsion structures for $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ for rational elliptic curves, i.e. what are the possibilities for the torsion subgroups for rational elliptic curves when base extended to $\mathbb{Q}^{\text{ab}}$. By carefully examining isogeny conditions, among other techniques, Chou then proved the following:

**Theorem 4.63** ([Cho19])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(\mathbb{Q}^{\mathrm{ab}})_{tors}$ is finite, and is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1,3,5,7,9,11,13,15,17,19,21,25,27,37,43,67,163 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1,2,\ldots,9 \text{ or} \\ \mathbb{Z}3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1,3 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1,2,3,4 \text{ or} \\ \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 5,6,8. \end{cases}$$

*Each of the listed groups appears as a torsion subgroup for $E(\mathbb{Q}^{\mathrm{ab}})_{tors}$ for some elliptic curve over $\mathbb{Q}$.*

Now for a prime $p$, define $\mathbb{Q}_{\infty,p}$ to be the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Let $\mathbb{Q}_{n,p}$ be the $n$th layer of $\mathbb{Q}_{\infty,p}$, i.e. the unique subfield of $\mathbb{Q}_{\infty,p}$ such that $\mathrm{Gal}(\mathbb{Q}_{n,p}/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. We know that $\mathrm{Gal}(\mathbb{Q}_{\infty,p}/\mathbb{Q}) \simeq \mathbb{Z}_p$ and $\mathbb{Z}_p$ is the unique Galois extension of $\mathbb{Q}$ with this property. We know also that

$$G := \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

Fixing a prime $p$, define $\Gamma_p = \mathbb{Z}_p$ and

$$\Delta_p := \begin{cases} \mathbb{Z}/2\mathbb{Z}, & p = 2 \\ \mathbb{Z}/(p-1)\mathbb{Z}, & p \geq 3. \end{cases}$$

Then $G \cong \Delta_p \times \Gamma_p$. We can then define $\mathbb{Q}_{\infty,p} := \mathbb{Q}(\zeta_{p^\infty})^{\Delta_p}$, so that every layer $\mathbb{Q}_{n,p}$ is given by $\mathbb{Q}_{n,p} = \mathbb{Q}(\zeta_{p^{n+1}})^{\Delta_p}$. Then for $p \geq 3$, $\mathbb{Q}_{n,p}$ is the unique subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ of degree $p^n$ over $\mathbb{Q}$. Elliptic curves have been extensively studied in $\mathbb{Z}_p$-extensions. Indeed, understanding elliptic curves in these extensions this is one of the main goals of Iwasawa

Theory for elliptic curves—though this mostly focuses on the rank and $n$-Selmer group of $E$. For more on these fields or Iwasawa Theory for elliptic curves, see [Was97] or [Lan90] and [Gre99], respectively.

Chou, Daniels, Krijan, and Najman classify the possibilities for $E(\mathbb{Q}_{\infty,p})_{\text{tors}}$, where $E/\mathbb{Q}$ is a rational elliptic curve, for each prime $p$.

**Theorem 4.64** ([CDKN21, Thm. 1.1])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $p \geq 5$ be a prime. Then $E(\mathbb{Q}_{\infty,p})_{tors} = E(\mathbb{Q})_{tors}$.*

**Theorem 4.65** ([CDKN21, Thm. 1.2])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the group $E(\mathbb{Q}_{\infty,2})_{tors}$ is isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4. \end{cases}$$

*Each such torsion subgroup occurs for some rational elliptic curve.*

**Theorem 4.66** ([CDKN21, Thm. 1.3])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then the group $E(\mathbb{Q}_{\infty,3})_{tors}$ is isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 21, 27 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, \end{cases}$$

*and each such group occurs for some rational elliptic curve.*

Furthermore, they are able to prove several interesting general results about the fields of definitions for torsion points.

**Lemma 4.67** ([CDKN21, Lem. 2.8]). *Let $p$ and $q$ be prime numbers such that $q-1 \nmid p$ and $p \nmid q-1$. Let $K/\mathbb{Q}$ be a cyclic extension of degree $p$, and $P \in E$ a point of degree $q$. If $P \in E(K)$, then $P \in E(\mathbb{Q})$.*

**Lemma 4.68** ([CDKN21, Lem. 2.9]). *Let $E/\mathbb{Q}$ be a rational elliptic curve and $P \in E$ a point of order $n$ such that $\mathbb{Q}(P)/\mathbb{Q}$ is Galois, and let $E(\mathbb{Q}(P))[n] \simeq \mathbb{Z}/n\mathbb{Z}$. Then the group $\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.*

**Proposition 4.69** ([CDKN21, Prop. 2.11]). *Let $E/F$ be an elliptic curve over a number field $F$, $n$ a positive integer, $P \in E$ be a point of order $p^{n+1}$ such that $E(F(pP))$ has no points of order $p^{n+1}$ and such that $F(P)/F(pP)$ is Galois. Then $[F(P)\colon F(pP)]$ divides $p^2$.*

Note that Proposition 4.69 is [GJN20b, Prop. 4.6] with added assumptions. We make the following definition: $\mathcal{K} := \prod_{p \text{ prime}} \mathbb{Q}_{\infty,p}$; that is, $\mathcal{K}$ is the compositum for all $\mathbb{Z}_p$-extensions of $\mathbb{Q}$. Denote by $\mathcal{K}_{\geq q}$ the compositum of all $\mathbb{Z}_p$-extensions with $p \geq q$. Extending the results in [CDKN21], Gužvić and Krijan classify the possibilities for $E/\mathbb{Q}$ when base extended to a compositum of $\mathbb{Z}_p$-extensions.

**Theorem 4.70** ([GK20, Thm. 1.1]). *Let $E/\mathbb{Q}$ be a rational elliptic curve, then $E(\mathcal{K}_{\geq 5})_{tors} = E(\mathbb{Q})_{tors}$.*

**Theorem 4.71** ([GK20, Thm. 1.2]). *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(\mathcal{K})_{tors}$ is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 21, 27 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4. \end{cases}$$

*Each such possibility occurs as the torsion subgroup for some rational elliptic curve $E/\mathbb{Q}$.*

**Theorem 4.72** ([GK20, Thm. 1.3])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then for a prime $p \geq 5$, we have $E(\mathbb{Q}(\mu_{p^\infty}))_{tors} = E(\mathbb{Q}(\mu_p))_{tors}$. Furthermore, $E(\mathbb{Q}(\mu_{3^\infty}))_{tors} = E(\mathbb{Q}(\mu_{3^3}))_{tors}$ and $E(\mathbb{Q}(\mu_{2^\infty}))_{tors} = E(\mathbb{Q}(\mu_{2^4}))_{tors}$.*

Gužvić and Krijan remark that Theorem 4.72 is the best possible in the following sense: if $E$, $E'$ have Cremona label `27a4` and `32a4`, respectively, then

$$E(\mathbb{Q}(\mu_{3^2}))_{\text{tors}} = \mathbb{Z}/9\mathbb{Z} \subsetneq \mathbb{Z}/27\mathbb{Z} = E(\mathbb{Q}(\mu_{3^3}))_{\text{tors}}$$
$$E(\mathbb{Q}(\mu_{2^3}))_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \subsetneq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} = E(\mathbb{Q}(\mu_{2^4}))_{\text{tors}}.$$

## 4.7 Torsion Subgroups for Elliptic Curves with Specified Structure

There are many other questions one can ask that also lead to interesting classifications. For example, rather than simply classifying the sets $\Phi_{\mathbb{Q}}(d)$, one can be more general and instead try to classify the sets $\Phi_{j\in\mathbb{Q}}(d)$. Of course, one has $\Phi_{\mathbb{Q}}(d) \subseteq \Phi_{j\in\mathbb{Q}}(d)$ for all $d$. But a priori, this need not be an equality. Gužvić classifies the sets $\Phi_{j\in\mathbb{Q}}(d)$ when $d$ is a prime.

**Theorem 4.73** ([Guž19, Thm. 1.1–1.4])**.** *Let $K/\mathbb{Q}$ be a number field of degree $p$, where $p$ is a prime. Then if $p \geq 7$, $\Phi_{j\in\mathbb{Q}}(p) = \Phi(1)$. If $p \in \{3, 5\}$, then $\Phi_{j\in\mathbb{Q}}(p) = \Phi_{\mathbb{Q}}(p)$. Finally, if $p = 2$, then $\Phi_{j\in\mathbb{Q}}(p) = \Phi_{\mathbb{Q}}(2) \cup \{\mathbb{Z}/13\mathbb{Z}\}$.*

Gužvić also proves a number of other interesting results, including several specifically about number fields of odd degree.

**Lemma 4.74** ([Guž19, Lem. 3.9]). *Let $K/\mathbb{Q}$ be a number field of odd degree. Then there does not exist an elliptic curve $E/K$ with rational $j$-invariant such that $\mathbb{Z}/16\mathbb{Z} \subseteq E(K)$.*

**Lemma 4.75** ([Guž19, Lem. 3.9]). *Let $K/\mathbb{Q}$ be a number field of odd degree, and let $E/K$ be an elliptic curve with rational $j$-invariant. Then $E(K)$ cannot contain $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.*

Even more general than elliptic curves $E/K$ with $j_E \in \mathbb{Q}$, one can instead work with elliptic curves that are $\mathbb{Q}$-curves.

**Definition.** An elliptic curve is called a $\mathbb{Q}$-curve if it is isogenous (over $\overline{\mathbb{Q}}$) to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates. $\mathbb{Q}$-curves not isogenous to an elliptic curve with rational $j$-variant are called strict $\mathbb{Q}$-curves.

$\mathbb{Q}$-curves can be thought of as generalizations of elliptic curves with rational $j$-invariant. Assuming Serre's conjecture (now a theorem, see [KW09a, KW09b]), Ribet proved that $\mathbb{Q}$-curves are precisely the modular elliptic curves $E/K$, in that they are a quotient of $J_1(N)$ for some $N$. All CM elliptic curves are $\mathbb{Q}$-curves. The study of such curves have a number of interesting applications, as Le Fourn and Najman note in [LFN20]. For instance, Pila used results about isogenies of non-CM elliptic curves with $j_E \in \mathbb{Q}$ in [Pil17] to prove results about Diophantine equations coming from "unlikely intersections." Furthermore, Dieulefait and Urroz [DJ09] solve the equation $x^4 + dy^2 = z^p$ in the cases $d = 2$, 3 and $p$ 'large' using the properties of $\mathbb{Q}$-curves over quadratic fields.

In a recent paper, Najman studied the isogenies of non-CM elliptic curves with rational $j$-invariant over number fields. Cremona and Najman build on this work to prove a number of interesting results about $\mathbb{Q}$-curves over odd degree number fields.

**Theorem 4.76** ([CN21, Thm. 1.1]). *Let $E$ be a $\mathbb{Q}$-curve without complex multiplication defined over an odd degree number field $K$. Then*

*(a) If $E$ has a $K$-rational isogeny of prime degree $\ell$, then $\ell \in \{2, 3, 5, 7, 11, 13, 17, 37\}$.*

*(b) If $d = [K\colon \mathbb{Q}]$ is not divisible by any prime $\ell \in \{2, 3, 5, 7, 11, 13, 17, 37\}$, and $E$ has a cyclic isogeny of degree $n$, then $n \leq 37$.*

**Theorem 4.77** ([CN21, Thm. 1.2]). *For every odd positive integer $d$, there exists a bound $C_d$, depending only on $d$, such that all cyclic isogenies of all $\mathbb{Q}$-curves over all number fields of degree $d$ are of degree at most $C_d$.*

**Theorem 4.78** ([CN21, Thm. 1.3]). *Let $d$ be a prime $> 7$, let $K$ be a number field of degree $d$ and $E/K$ a $\mathbb{Q}$-curve. Then $E(K)_{tors}$ is one of the groups from Mazur's Theorem, i.e. a torsion group of an elliptic curve over $\mathbb{Q}$.*

Le Fourn and Najman study the torsion subgroups of $\mathbb{Q}$-curves defined over quadratic fields.

**Theorem 4.79** ([LFN20, Thm. 1.1]). *Let $E$ be a $\mathbb{Q}$-curve defined over a quadratic field $K$. Then $E(K)_{tors}$ is isomorphic to one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 18,\ n \neq 11, 17 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

*There are infinitely many $\mathbb{Q}$-curves with each of these torsion subgroups, except for $\mathbb{Z}/14\mathbb{Z}$*

*and* $\mathbb{Z}/15\mathbb{Z}$ *of which there are finitely many.*

One can also study sets $\Phi_{j\in\mathcal{O}_K}(d)$. For instance, we have the following results of Fung, Müller, Ströher, Williams, and Zimmer:

**Theorem 4.80** ([ZSM89, Thm. 4])**.** *Let* $E$ *be an elliptic curve with integral absolute invariant* $j$ *over a quadratic field* $K$*. Then up to isomorphism, the torsion subgroup* $E(K)_{tors}$ *is isomorphic to one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 8, 10 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, & \text{with } n = 1, 2, 3 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}. \end{cases}$$

*Moreover, except for* $\mathbb{Z}/2\mathbb{Z}$*,* $\mathbb{Z}/3\mathbb{Z}$*, and* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$*, each such possibility occurs for finitely many curves* $E$*. The curves* $E/K$ *with* $E(K)_{tors} \cong \mathbb{Z}/3\mathbb{Z}$ *or* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ *have* $j$*-invariants belonging to a finite set.*

**Theorem 4.81** ([FSWZ90b, Thm. 10])**.** *Let* $E$ *be an elliptic curve with integral absolute invariant* $j$ *over a pure cubic field* $K$*. Then up to isomorphism, the torsion subgroup* $E(K)_{tors}$ *is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \end{cases}$$

*Moreover, except for* $\mathbb{Z}/2\mathbb{Z}$*,* $\mathbb{Z}/3\mathbb{Z}$*, and* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$*, each such possibility occurs for finitely many curves* $E$ *and pure cubic fields* $K$*. The curves* $E/K$ *with* $E(K)_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ *have* $j$*-invariants belonging to a finite set.*

Of course in each paper, they give examples and have much more specific results, which we will not state here, about the fields and elliptic curves involved. There are further results in this direction, e.g. the following result of Kishi:

**Theorem 4.82** ([Kis97])**.** *Let $K$ be an imaginary cyclic quartic field, and $E/K$ be an elliptic curve. Suppose that*

*(i)* $\mathfrak{f}_2 < 4$ *or* $\mathfrak{f}_3 < 4$*, where* $\mathfrak{f}_p$ *is the residue degree of a prime ideal over* $p$ *in the extension* $K/\mathbb{Q}$*, and*

*(ii) the* $j \in \mathcal{O}_K$*.*

*Then* $E(K)_{tors}$ *is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 6, 8 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3. \end{cases}$$

*All these cases occur as the torsion subgroup for some elliptic curve $E/K$.*

## 4.8 Torsion Subgroups for Elliptic Curves over Function Fields

One need not restrict to extensions of $\mathbb{Q}$ (finite or infinite) when studying torsion subgroups of elliptic curves. After all, the Mordell-Weil Theorem (and the Lang-Néron generalization) equally applies in the case of function fields. Before discussing results in this direction, we will need to make some definitions.

**Definition.** Let $\mathbb{F}$ be a finite field with characteristic $p$, and let $\mathcal{C}/\mathbb{F}$ be be a smooth projec-

tive curve. Let $K = \mathbb{F}(\mathcal{C})$, and let $E/K$ be an elliptic curve. We say that...

(i) $E$ is constant if there is an elliptic curve $E_0/\mathbb{F}$ with $E \cong E_0 \times_{\mathbb{F}} K$. Otherwise, we say that $E$ is non-constant.

(ii) $E$ is isotrivial if there is a finite extension $L/K$ such that $E/L$ is constant. Otherwise, we say that $E$ is non-isotrivial.

Essentially, isotriviality states that the curve $E$ is a base extension of a curve over a finite field. Early progress in the classification of the torsion subgroups $E(K)_{\text{tors}}$ in the case where $K$ is a function field came with the work of Levin and Cox and Parry.

**Corollary 4.83** ([Lev68])**.** *Let $\mathbb{F}$ be a finite field of characteristic $p$, and define $K = \mathbb{F}(T)$. Let $E/K$ be a non-isotrivial elliptic curve. Suppose $\ell^e \mid \#E(K)_{tors}$ for some prime $\ell$. Then if $\ell \neq p$,*

$$\ell \leq 7 \text{ and } e \leq \begin{cases} 4, & \text{if } \ell = 2 \\ 2, & \text{if } \ell = 3, 5 \\ 1, & \text{if } \ell = 7. \end{cases}$$

*If $\ell = p$, then*

$$\ell \leq 11 \text{ and } e \leq \begin{cases} 3, & \text{if } \ell = 2 \\ 2, & \text{if } \ell = 3 \\ 1, & \text{if } \ell = 5, 7, 11. \end{cases}$$

**Theorem 4.84** ([CP80])**.** *Let $\mathbb{F}$ be a finite field of characteristic $p \geq 5$. Let $m, n$ be positive integers. Then the following are equivalent:*

*(i) There is a non-isotrivial elliptic curve $E$ over $\mathbb{F}(T)$ such that $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/nm\mathbb{Z} \cong E(K)_{tors} \setminus E(K)[p^\infty]$.*

*(ii) If $p \nmid n$, the field $\mathbb{F}$ contains a primitive $n$th root of unity and $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/nm\mathbb{Z}$ is one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \text{or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}. & \end{cases}$$

*Furthermore, if $E(K)_{tors} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/nm\mathbb{Z}$ and $\mathbb{F}$ contains a primitive $n$th root of unity, then this torsion group appears for infinitely many non-isomorphic, non-isotrivial elliptic curves.*

Despite these results having been known for many years, no one had used them to classify the possibilities for $E(K)_{\text{tors}}$. Recent work of McDonald has finally classified the possibilities for $E(K)_{\text{tors}}$ in the case where $K$ is a function field of a curve of genus zero or one.

**Theorem 4.85** ([McD18, Thm. 1.13])**.** *Let $k = \mathbb{F}_q$ for $q$ a power of $p$. Define $K = k(T)$, and let $E/K$ be a non-isotrivial elliptic curve. If $p \nmid \#E(K)_{tors}$, then $E(K)_{tors}$ is isomor-*

*phic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}. \end{cases} \tag{4.8}$$

*If $p \leq 11$ and $p \mid \#E(K)_{tors}$, then $E(K)_{tors}$ is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/p\mathbb{Z}, & \text{or} \\ \mathbb{Z}/2p\mathbb{Z}, & \text{if } p = 2, 3, 5, 7 \text{ or} \\ \mathbb{Z}/3p\mathbb{Z}, & \text{if } p = 2, 3, 5 \text{ or} \\ \mathbb{Z}/4p\mathbb{Z}, & \text{if } p = 2, 3 \text{ or} \\ \mathbb{Z}/5p\mathbb{Z} & \text{if } p = 2, 3 \text{ or} \end{cases} \qquad \begin{cases} \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/14\mathbb{Z}, \mathbb{Z}/18\mathbb{Z}, & \text{if } p = 2 \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}, & \text{if } p = 2 \text{ and } \zeta_5 \in k \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}, & \text{if } p = 3 \text{ and } \zeta_4 \in k \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}, & \text{if } p = 5. \end{cases}$$

*If $p \geq 13$, then the complete list of possible torsion subgroups is given in (4.8). Furthermore, every group in this list appears infinitely often as $E(K)_{tors}$ for some elliptic curve.*

**Theorem 4.86** ([McD18, Thm. 3.3])**.** *Let $k$ be a finite field of characteristic 5, and define $K = k(T)$. Let $E/K$ be a non-isotrivial elliptic curve. Then the torsion subgroup $E(K)_{tors}$*

*is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 15 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2 \text{ if } \zeta_3 \in k \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

*Furthermore, each of these groups appears infinitely often as $E(K)_{tors}$ for some elliptic curve.*

**Theorem 4.87** ([McD19a, Thm. 1.4.3; McD19b])**.** *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, where $\mathbb{F}$ is a field of characteristic $p$, and define $K = \mathbb{F}(\mathcal{C})$. Let $E/K$ be a non-isotrivial. If $p \nmid \#E(K)_{tors}$, then $E(K)_{tors}$ is isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 12, 14, 15 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 6 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & \text{with } n = 1, 2, 3 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & \text{with } n = 1, 2 \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, & \text{or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. \end{cases} \tag{4.9}$$

*If* $p \mid \#E(K)_{tors}$*, then* $p \leq 13$ *and* $E(K)_{tors}$ *is one of the following:*

$$\begin{cases} \mathbb{Z}/p\mathbb{Z}, & \text{if } p = 2,3,5,7,11,13 \text{ or} \\ \mathbb{Z}/2p\mathbb{Z}, & \text{if } p = 3,5,7 \text{ or} \\ \mathbb{Z}/3p\mathbb{Z}, & \text{if } p = 2,3,5 \text{ or} \\ \mathbb{Z}/4p\mathbb{Z}, & \text{if } p = 2,3,5 \text{ or} \\ \mathbb{Z}/5p\mathbb{Z}, & \text{if } p = 2,3 \text{ or} \\ \mathbb{Z}/6p\mathbb{Z}, & \text{if } p = 2,3 \text{ or} \\ \mathbb{Z}/7p\mathbb{Z}, & \text{if } p = 2,3 \text{ or} \\ \mathbb{Z}/8p\mathbb{Z}, & \text{if } p = 2,3 \text{ or} \\ \mathbb{Z}/2n\mathbb{Z}, & \text{for } n = 9,10,11,15, \text{ if } p = 2 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2p\mathbb{Z}, & \text{for } n = 3,5,7 \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6n\mathbb{Z}, & \text{for } n = 1,2,3, \text{if } p = 2 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}, & \text{if } p = 3 \text{ or} \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}, & \text{if } p = 2. \end{cases}$$

*If* $p \geq 17$*, then* (4.9) *is the complete list of possible torsion subgroups. Furthermore, if* $E(K)_{tors} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/nm\mathbb{Z}$ *and* $\mathbb{F}$ *contains a primitive* $n$*th root of unity, then this torsion group appears for infinitely many non-isomorphic, non-isotrivial elliptic curves.*

## 4.9 Other Related Results

There are a plethora of other interesting results related to torsion subgroups of elliptic curves. Indeed, many of these results make appearances in the works above. For instance, Kenku [Ken82] has shown that there are at most eight $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class, and has a number of other bounds based on what isogenies

there are.

**Theorem 4.88** ([Ken82, Thm. 2])**.** *There are at most eight $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class.*

Let $C(E)$ denote the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in the $\mathbb{Q}$-isogeny class of $E$. $C(E)$ is also the number of distinct $\mathbb{Q}$-rational cyclic subgroups of $E$ (including the identity subgroup). For a prime $p$, let $C_p(E)$ be the $p$ component of $C(E)$. We have the product formula $C(E) = \prod_p C_p(E)$. By Manin's theorem $C_p(E)$ is bounded for each $p$ as $E$ varies over all the $\mathbb{Q}$-isogeny classes of elliptic curves. We have the following table for bounds $C_p$, of $C_p(E)$

Table 4.3: Bounds for $C_p$

| $p$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 37 | 43 | 67 | 163 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_p$ | 8 | 4 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |

and $C_p = 1$ for all other primes.

As a final few remarks, Harron and Snowden have counted torsion subgroups of rational elliptic curves, see [HS17], and Pizzo, Pomerance, and Voight have recently counted elliptic curves with an isogeny of degree three, see [PPV20]. Bandini and Paladino have studied fields generated by torsion points of elliptic curves, see [BP12, BP16a]. Finally, González-Jiménez and Tornero [GJT10] remark on the ubiquity of trivial torsion on elliptic curves, i.e. the well-known result that "most" rational elliptic curves are such that $E(\mathbb{Q})_{\text{tors}} \cong \{\mathcal{O}\}$. The same is true for elliptic curves over function fields, see [Phi21].

# Chapter 5

# The Nonic Galois Case

In this chapter, we will classify the possibilities for the torsion subgroups $E(K)_{\text{tors}}$, where $K/\mathbb{Q}$ is a nonic Galois field and $E/\mathbb{Q}$ is a rational elliptic curve; that is, we determine the set $\Phi_{\mathbb{Q}}^{\text{Gal}}(9)$. We then determine the possible growths of torsion subgroups when base extending an elliptic curve $E/\mathbb{Q}$ to $K$, i.e. given a fixed torsion subgroup $E(\mathbb{Q})_{\text{tors}}$, we determine the possibilities for the torsion subgroup $E(K)_{\text{tors}}$. Finally, we completely determine the possibilities for $E(K)_{\text{tors}}$ based on the isomorphism type of $\text{Gal}(K/\mathbb{Q})$.

## 5.1 Overview for the Classification

We wish to classify the possible isomorphism classes of torsion subgroups for rational elliptic curves over nonic Galois fields. It will be useful to give a brief overview of the process we will use for the classification. We will begin by finding the possible prime orders for torsion points on these elliptic curves. This determines the possible non-trivial Sylow $p$-subgroups that can occur. Bounding the Sylow $p$-subgroups for each possible prime $p$, we can then produce a finite list of possible torsion subgroups for these elliptic curves.

Of course, many of these torsion subgroups will occur. We can easily find examples for many of these torsion subgroups by 'base extending' rational elliptic curves and elliptic curves $E(K)$, where $K$ is a cubic Galois field, to a nonic Galois field—being sure to avoid adding any additional torsion points. This will give us a much smaller list of possible torsion subgroups whose existence/non-existence we will need to consider. We eliminate many of the remaining possibilities on a case-by-case basis, and we find examples for the rest. Combining all this work, the classification will then immediately follow. Note that in this chapter and the next, as with the previous chapters, we use the Cremona [Cre] labeling system for elliptic curves as well as the LMFDB Database [Col21] (our primary reference). When necessarily, we will label fields by their LMFDB label. Computations were primarily made in Sage [The20], but other test cases, especially ranks, were made in MAGMA [BCP97, BCFS10].

Before beginning the proof, we will make a few general remarks of things that we may implicitly use. We are considering rational elliptic curves, $E/\mathbb{Q}$, over nonic Galois fields. As $|\operatorname{Gal}(K/\mathbb{Q})| = 9$ is the square of a prime, $\operatorname{Gal}(K/\mathbb{Q})$ is necessarily an abelian group. Moreover, we know that $\operatorname{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$ or $\operatorname{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Let $F$ be an intermediate cubic subfield of $K$, i.e. $\mathbb{Q} \subseteq F \subseteq K$ and $[F\colon \mathbb{Q}] = 3$. Because $\operatorname{Gal}(K/\mathbb{Q})$ is abelian, we know that the subgroup $\operatorname{Gal}(F/\mathbb{Q})$ is normal and hence $F/\mathbb{Q}$ is an abelian Galois extension, and we know that $\operatorname{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Furthermore, as the extension $K/\mathbb{Q}$ is Galois, $K$ is totally real or totally imaginary.

Recall that often when we say "isogeny", we will often mean $\mathbb{Q}$-rational cyclic isogeny. As in previous chapters, a "point of order $n$" will often be taken to mean a point whose order divides $n$. Otherwise, we will often say "a point of exact order $n$." Finally, we will make frequent use of the notation established at the start of Chapter 4 and the results contained therein. When convenient, we will simply restate the results.

## 5.2 Points of Prime Order

The first step in any classification of torsion subgroups for elliptic curves naturally begins with a determination of the possible points of prime order for a specified collection of fields. Lozano-Robledo showed, [LR13, Corollary 1.5], that $S_{\mathbb{Q}}(9) = \{2, 3, 5, 7, 11, 13, 17, 19\}$. Further work of González-Jiménez and Najman proved the following result, which we restate for convenience:

**Corollary 4.54** ([GJN20b, Cor. 6.1 (i)–(iv)])**.**

*(i)* $11 \in R_{\mathbb{Q}}(d)$ *if and only if* $5 \mid d$.

*(ii)* $13 \in R_{\mathbb{Q}}(d)$ *if and only if* $3 \mid d$ *or* $4 \mid d$.

*(iii)* $17 \in R_{\mathbb{Q}}(d)$ *if and only if* $8 \mid d$.

*(iv)* $37 \in R_{\mathbb{Q}}(d)$ *if and only if* $12 \mid d$.

Then the following result is immediate.

**Lemma 5.1.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic field. If $P \in E(K)_{tors}$ is a point of order $p$, then $p \in \{2, 3, 5, 7, 13, 19\}$.*

*Proof.* We know from [LR13, Corollary 1.5] that $S_{\mathbb{Q}}(9) = \{2, 3, 5, 7, 11, 13, 17, 19\}$. By definition, we know that $R_{\mathbb{Q}}(9) \subseteq S_{\mathbb{Q}}(9)$. Points of order 2, 3, 5, and 7 already occur for elliptic curves $E(\mathbb{Q})$ and hence for torsion subgroups $E(K)_{\text{tors}}$, c.f. Proposition 5.17 and Corollary 5.18. Therefore, $2, 3, 5, 7 \in R_{\mathbb{Q}}(9)$. We then only need to consider the primes 11, 13, 17, and 19. By Proposition 4.54, we know that $11, 17 \notin R_{\mathbb{Q}}(9)$ and $13, 19 \in R_{\mathbb{Q}}(9)$, c.f. Table 5.3. Therefore, $R_{\mathbb{Q}}(9) = \{2, 3, 5, 7, 13, 19\}$. So if $P \in E(K)$ is a point of order $p$, we must have $p \in \{2, 3, 5, 7, 13, 19\}$. □

## 5.3 Bounding the $p$-Sylow Subgroups

We will now work prime-by-prime to bound the Sylow $p$-subgroups for each of the primes $p \in \{2, 3, 5, 7, 13, 19\}$. Fortunately, it will turn out that the only "real work" involved will be in the case of $p = 2$ because the cases where $p \in \{3, 5, 7, 13, 19\}$ can all be handled essentially in the same way.

### 5.3.1 The Case of $p = 2$

For elliptic curves without CM, Rouse and Zureick-Brown have classified all the possible 2-adic images of $\rho_{E,2} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_2)$.

**Theorem 5.2** ([RZB15]). *Let $E/\mathbb{Q}$ be a rational elliptic curve without CM. Then there are exactly 1,208 possibilities for the 2-adic image $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugacy in $\mathrm{GL}_2(\mathbb{Z}_2)$. Moreover,*

*(i) the index of $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ in $\mathrm{GL}_2(\mathbb{Z}_2)$ divides 64 or 96, and*

*(ii) the image $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the full inverse image of $\rho_{E,32}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ under reduction modulo 32.*

The 1,208 distinct possibilities for the 2-adic images in [RZB15], along with 1-parameter families determining the curves with these images, are given in a searchable database on Rouse's website, https://users.wfu.edu/rouseja/2adic/. Using this result, González-Jiménez and Lozano-Robledo were able to determine the minimal degrees of definition for the subgroup $E[2^n]$.

**Theorem 5.3** ([GJLR17, Theorem 1.4]). *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $1 \leq s \leq N$ be fixed integers, and let $T \subseteq E[2^N]$ be a subgroup isomorphic to $\mathbb{Z}/2^s/Z \oplus \mathbb{Z}/2^N\mathbb{Z}$.*

*Then* $[\mathbb{Q}(T)\colon \mathbb{Q}]$ *is divisible by 2 if* $s = N = 2$*, and otherwise by* $2^{2N+2s-8}$ *if* $N \geq 3$*, unless* $s \geq 4$ *and* $j(E)$ *is one of the two values:*

$$-\frac{3 \cdot 18249920^3}{17^{16}} \text{ or } -\frac{7 \cdot 1723187806080^3}{79^{16}}$$

*in which case* $[\mathbb{Q}(T)\colon \mathbb{Q}]$ *is divisible by* $3 \cdot 2^{2N+2s-9}$*. Moreover, this is best possible in that there are one-parameter families* $E_{s,N}(t)$ *of elliptic curves over* $\mathbb{Q}$ *such that for each* $s, N \geq 0$ *and each* $t \in \mathbb{Q}$*, and subgroups* $T_{s,N} \in E_{s,N}(t)(\overline{\mathbb{Q}})$ *isomorphic to* $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$ *such that* $[\mathbb{Q}(T_{s,N})\colon \mathbb{Q}]$ *is equal to the bound given above.*

In particular, we can create an initial bound for the 2-Sylow subgroup for $E(K)_{\text{tors}}$, where $K$ is *any* odd degree number field, by combining Theorem 4.17 (or generally Theorem 4.18) and Theorem 5.3.

**Lemma 5.4.** *Let* $E/\mathbb{Q}$ *be a rational elliptic curve, and* $K/\mathbb{Q}$ *be an odd degree number field. Then* $E(K)_{tors}$ *does not contain the group* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ *or the group* $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$*.*

*Proof.* Suppose that $E$ had CM. Then $E(K)_{\text{tors}}$ would be a subgroup of the list given in Theorem 4.17 (or more generally, Theorem 4.18), but this is not the case. Suppose then that $E$ does not have CM. Using Theorem 5.3 with $s = 1$, $N = 4$ and $s = N = 2$, we find that $[K\colon \mathbb{Q}]$ is divisible by 4 or 2, respectively, which is impossible. Therefore, $E(K)_{\text{tors}}$ cannot contain $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, respectively. □

Lemma 5.4 serves as an initial partial bound. However, we can create a better bound for the 2-Sylow subgroup as we shall show that for nonic Galois fields $K$, $E(K)_{\text{tors}} \not\supseteq \mathbb{Z}/16\mathbb{Z}$. First, we prove two lemmas that we shall often make tacit use of.

**Lemma 5.5.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(\mathbb{Q})[2] \cong E^d(\mathbb{Q})[2]$ for all twists $E^d$ of $E$.*

*Proof.* Choosing a model $y^2 = x^3 + Ax + B$ for $E$, if $P = (x, y)$ is a nontrivial point of order 2, then $x(P)$ is a root of $x^3 + Ax + B$. But $r$ is a root of $x^3 + Ax + B$ if and only if $dr$ is a root for $x^3 + Ad^2x + Bd^3$, where $d \in \mathbb{Q}$. □

**Lemma 5.6.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Let $E^d$ be a twist of $E$. Choose a model $y^2 = x^3 + Ax + B$ for $E$. If $\Delta_E$ is a square, then $\Delta_{E^d}$ is a square for all twists $E^d$. Similarly, if $\mathrm{disc}(x^3 + Ax + B)$ is a square, then $\mathrm{disc}(x^3 + Ad^2x + Bd^3)$ is a square.*

*Proof.* We know that $\Delta_E = -16(4A^3 + 27B^2)$. Twisting $E$ by $d$ gives $\Delta_{E^d} = -16(4A^3 + 27B^2) \cdot d^6$ and the first claim follows. Similarly, $\mathrm{disc}(x^3 + Ad^2x + Bd^3) = -(4A^3 - 27B^2) \cdot d^6$ and the second claim follows. □

We can now prove the lemma.

**Lemma 5.7.** *Let $E/\mathbb{Q}$ be a rational elliptic curve and $K/\mathbb{Q}$ an odd degree Galois field. Then $E(K)_{tors} \not\supseteq \mathbb{Z}/16\mathbb{Z}$.*

*Proof.* Assume that $E(K)_{\mathrm{tors}} \supseteq \mathbb{Z}/16\mathbb{Z}$. Clearly, either $E(\mathbb{Q})[2^\infty] = \{\mathcal{O}\}$ or $E(\mathbb{Q})[2^\infty] \neq \{\mathcal{O}\}$. If $E(\mathbb{Q})[2^\infty] \neq \{\mathcal{O}\}$, then it follows from Lemma 4.44 that $E(\mathbb{Q})[2^\infty] = E(K)[2^\infty] \supseteq \mathbb{Z}/16\mathbb{Z}$, which contradicts Mazur's classification of $\Phi(1)$, c.f. Theorem 4.2. Therefore, it must be that $E(\mathbb{Q})[2^\infty] = \{\mathcal{O}\}$.

Choose a model $y^2 = x^3 + Ax + B$ for $E$. If $P = (x, y)$ is a point of order 2, then $x(P)$ is a root of $x^3 + Ax + B$. Because $E(\mathbb{Q})[2^\infty] = \{\mathcal{O}\}$, we know that $x^3 + Ax + B$ must

be irreducible. In particular, $\mathbb{Q}(P) \subseteq K$ is a cubic extension. Because $K/\mathbb{Q}$ is an abelian Galois extension, $\mathbb{Q}(P)$ is Galois. But then the irreducible polynomial $x^3 + Ax + B$ then generates a cubic Galois extension. It is well known, for example see [DF04, Conb], that this implies $\operatorname{disc}(x^3 + Ax + B)$ is a square in $\mathbb{Q}$.

Furthermore by Lemma 5.10, $E$ must have a rational cyclic 16-isogeny. Therefore using [LR13, Table 3], c.f. Table 7.3, any elliptic curve with a rational cyclic 16-isogeny must have $j$-invariant

$$j = \frac{(h^8 - 16h^4 + 16)^3}{h^4(h^4 - 16)}$$

for some $h \in \mathbb{Q} \setminus \{0, \pm 2\}$. In particular, $E$ is a twist of the curve

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

Because $E$ is a twist of the curve $E'$, the discriminant of $E$ will only differ from the discriminant of $E'$ by at most a square. In particular, the discriminant of $E'$ must be a square. Therefore, after computing the discriminant of $E'$, there exists $y \in \mathbb{Q}$ such that

$$y^2 = \frac{136048896h^4(h^4 - 16)(h^8 - 16h^4 + 16)^6}{(h^{12} - 24h^8 + 120h^4 + 64)^6}.$$

Absorbing squares into the left hand side, a rational solution $(y, h)$ to the equation above implies the existence of a rational solution $(n, m)$ to the equation $n^2 = m^4 - 16$. But the curve given by $n^2 = m^4 - 16$ is birationally equivalent to the elliptic curve given by $C \colon y^2 = x^3 + 64x$. Using SAGE, we find that this curve has rank 0 and torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ generated by the point $(8, 24)$. Furthermore, $C(\mathbb{Q}) = \{\mathcal{O}, (-4, 0), (0, \pm 8), (8, \pm 24)\}$. The points $(0, \pm 8)$ correspond to cusps for $j$, and it is routine to check that the remaining rational solutions $(n, m)$ do not correspond to rational solutions $(y, h)$. $\square$

With all these results in hand, the following bound for 2-Sylow subgroup $E(K)[2^\infty]$ is immediate:

**Proposition 5.8.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K$ be a nonic Galois field. Then $E(K)[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.*

*Proof.* This follows immediately from Lemma 5.4 and Lemma 5.7. □

### 5.3.2 The Case of $p = 3, 5, 7, 13, 19$

Bounding the $p$-Sylow subgroups for $p > 2$ simply makes use of the isogeny restrictions forced on rational elliptic curves over odd degree Galois number fields. First, we observe the well known result, see [Naj16, Cho16, GJ17, Cho19, Gužv19] for just a few references, that full $n$-torsion cannot be defined over an odd degree number field (not necessarily Galois) for any integer $n > 2$.

**Lemma 5.9.** *Let $E/\mathbb{Q}$ be an elliptic curve and let $K/\mathbb{Q}$ be an odd degree number field. Then $E[n] \not\subseteq E(K)_{tors}$ for all $n > 2$. In particular, $E(K)_{tors}$ does not contain full $p$-torsion for $p > 2$.*

*Proof.* Suppose that $E[n] \subseteq E(K)$ for some $n$. It is well known (see Corollary 3.15) that by the existence of the Weil pairing, full $n$-torsion can be defined over a number field $K$ only if the $n$th roots of unity are defined over $K$, i.e. $\mathbb{Q}(\zeta_n) \subseteq K$. But we know that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, where $\phi$ is the Euler-phi function. Therefore,

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [K : \mathbb{Q}(\zeta_n)]\,\phi(n).$$

Because $\phi(n)$ is even for $n > 2$, it must be that $n = 2$. □

We now recall the classification of the possible rational cyclic isogenies.

**Theorem 3.24.** *Let $N \geq 2$ be such that $X_0(N)$ has a non-cuspidal $\mathbb{Q}$-rational point. Then*

*(i) $N \leq 10$ or $N = 12$, 13, 16, 18, or 25. In this case, $X_0(N)$ is a curve of genus 0, and the $\mathbb{Q}$ rational points on $X_0(N)$ form an infinite 1-parameter family, or*

*(ii) $N = 11$, 14, 15, 17, 19, 21, or 27, i.e. $X_0(N)$ is a rational elliptic curve (in each case $X_0(N)(\mathbb{Q})$) is finite, or*

*(iii) $N = 37$, 43, 67, or 163. In this case, $X_0(N)$ is a curve of genus $\geq 2$ and by Faltings' Theorem has only finitely many $\mathbb{Q}$-rational points.*

*In particular, a rational elliptic curve may only have a rational cyclic $n$-isogeny for $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$. Furthermore, if $E$ does not have CM, then $n \leq 18$ or $n \in \{21, 25, 37\}$.*

This classification of the possible rational cyclic isogenies for elliptic curves $E/\mathbb{Q}$ places great restrictions on the possible torsion subgroups for elliptic curves over (odd) degree Galois fields. We prove the following well known results, c.f. [Naj16, Cho16, GJ17, Cho19].

**Lemma 5.10** ([Cho16, Lem. 3.10])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve and $K/\mathbb{Q}$ be a Galois extension. If $E(K)[n] \cong \mathbb{Z}/n\mathbb{Z}$, then $E$ has a rational $n$-isogeny.*

*Proof.* Let $\{P, Q\}$ be a basis for $E[n]$. Without loss of generality, assume that $P \in E(K)$ and $Q \notin E(K)$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Because $K/\mathbb{Q}$ is Galois and $P \in E(K)$, $P^\sigma \in E(K)[n] = \langle P \rangle$. But then $E(K)[n] = \langle P \rangle$ is Galois stable, which implies that $E$ has an $n$-isogeny over $\mathbb{Q}$. □

**Lemma 5.11** ([Cho19, Lem. 2.7])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a Galois extension. If $E(K)_{tors} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$, then $E$ has a rational $n$-isogeny.*

*Proof.* Choose a basis $\{P, Q\}$ for $E(K)_{\text{tors}}$ with $P, Q$ having exact order $m$ and $mn$, respectively, i.e. $E(K)_{\text{tors}} = \langle P, Q\rangle \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$. We know that $[m]E(K)_{\text{tors}} = \langle mP, mQ\rangle \cong \langle nQ\rangle \cong \mathbb{Z}/n\mathbb{Z}$. Let $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Because $K/\mathbb{Q}$ is Galois and $E/\mathbb{Q}$ is a rational elliptic curve, the action of $\sigma$ commutes with $[m]$ and $[n]$. But then $(mQ)^\sigma \in E(K)[n] \cong \langle mQ\rangle$. But then $\langle mQ\rangle$ is a Galois stable subgroup of order $n$ so that $E$ has an $n$-isogeny over $\mathbb{Q}$. □

We can now combine Lemma 5.9 and Lemma 5.10 to bound the $p$-Sylow subgroups for torsion subgroups of $E/\mathbb{Q}$ over nonic Galois fields.

**Proposition 5.12.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then*

$$E(K)[3] \subseteq \mathbb{Z}/27\mathbb{Z}$$

$$E(K)[5] \subseteq \mathbb{Z}/25\mathbb{Z}$$

$$E(K)[7] \subseteq \mathbb{Z}/7\mathbb{Z}$$

$$E(K)[13] \subseteq \mathbb{Z}/13\mathbb{Z}$$

$$E(K)[19] \subseteq \mathbb{Z}/19\mathbb{Z}$$

*Proof.* Because $[K\colon \mathbb{Q}]$ is odd, it follows from Lemma 5.9 that $E(K)[p] \cong \mathbb{Z}/p^n\mathbb{Z}$ for some $n \geq 0$. Then by Lemma 5.10, $E$ has a cyclic rational $p^n$ isogeny. For each $p \in \{3, 5, 7, 13, 19\}$, the maximal such $n$ can be immediately deduced from Theorem 3.24. □

## 5.4 The List of Possible Torsion Subgroups

It follows from Proposition 5.8 and Proposition 5.12 that if $E/\mathbb{Q}$ is a rational elliptic curve and $K/\mathbb{Q}$ is a nonic Galois field, then

$$E(K)_{\text{tors}} \subseteq (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}) \oplus \mathbb{Z}/27\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z} \oplus \mathbb{Z}/19\mathbb{Z}.$$

In particular, we can use these Sylow $p$-subgroup bounds to create a finite list of possibilities for the torsion subgroups $E(K)_{\text{tors}}$. Using only the fact that $E(K)_{\text{tors}}$ is a subgroup of the bounding group above, we would naïvely have a list of 672 possible torsion subgroups (using the above bound and the fact that $E(K)_{\text{tors}} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/nm\mathbb{Z}$ for some $n, m \in \mathbb{Z}^{\geq 0}$). To create a more manageable list, we will first have to eliminate more possibilities for orders of points $P \in E(K)_{\text{tors}}$.

**Lemma 5.13.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. If $p > 7$ is a prime, then $E(K)_{tors}$ contains no points of order $3^n p^m$ for all $n, m \geq 1$. Furthermore, $E(K)_{tors}$ does not contain points of order $3^2 \cdot 5$, $3 \cdot 5^2$, $3^2 \cdot 7$, or $3 \cdot 7^2$.*

*Proof.* If $P \in E(K)_{\text{tors}}$ is a point of order $3^n p^m$, then by Lemma 5.9 $E(K)[3^n p^m] \cong \mathbb{Z}/3^n p^m \mathbb{Z}$. By Lemma 5.10, $E$ has a cyclic rational $3^n p^m$-isogeny. But examining the possible $\mathbb{Q}$ rational isogenies in Theorem 3.24, we see that no such isogeny can exist for $p > 7$. Mutatis mutandis, $E(K)_{\text{tors}}$ does not contain points of order $3^2 \cdot 5$, $3 \cdot 5^2$, $3^2 \cdot 7$, or $3 \cdot 7^2$. □

**Lemma 5.14.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. If $p, q > 3$ are distinct primes, then $E(K)_{tors}$ contains no points of order $p^n q^m$ for all $n, m \geq 1$.*

*Proof.* If $P \in E(K)_{\text{tors}}$ is a point of order $p^n q^m$, then by Lemma 5.9, $E(K)[p^n q^m] \cong$

$\mathbb{Z}/p^nq^m\mathbb{Z}$. By Lemma 5.10, $E$ has a cyclic rational $p^nq^m$-isogeny. But examining the possible $\mathbb{Q}$ rational isogenies in Theorem 3.24, we see that no such isogeny can exist. □

**Lemma 5.15.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors} \ncong \mathbb{Z}/n\mathbb{Z}$ for any $n > 19$, $n \neq 21, 25, 27$. Furthermore, $E(K)_{tors}$ contains neither points of order $n \geq 56$ nor points of order $n \in \{40, 52\}$.*

*Proof.* Suppose that $E(K)_{\text{tors}} \cong \mathbb{Z}/n\mathbb{Z}$ for some $n > 19$, $n \neq 21, 25, 27$. By Lemma 5.1, we know that $n$ cannot be prime. But by Lemma 5.10 $E$ has a cyclic rational $n$-isogeny. But examining the possible $\mathbb{Q}$ rational isogenies in Theorem 3.24, the only possible isogenies for $n > 27$ are prime, a contradiction.

Now suppose that $E(K)_{\text{tors}}$ contained a point of $n$, where $n \in \{40, 52\}$ or $n \geq 56$. If $n$ is odd, then by Lemma 5.9 $E(K)[n] \cong \mathbb{Z}/n\mathbb{Z}$. By Lemma 5.10, $E$ has a cyclic rational $n$-isogeny. But examining the possible $\mathbb{Q}$ rational isogenies in Theorem 3.24, there can be no such isogeny. If $n$ is even, write $n = 2k$, where by necessity $k \geq 28$ or $k \in \{20, 26\}$. Either $E(K)[n] \cong \mathbb{Z}/2k\mathbb{Z}$ or $E(K)[n] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2k\mathbb{Z}$. But in both cases, $E$ has a point of order $k$ and a rational $k$-isogeny by Lemma 5.11. By examining the possible prime $k$ in Lemma 5.1 or $k$-isogenies in Theorem 3.24, we see that no such $k$ exists. □

We are now in a position to create a much smaller list of possibilities for $E(K)_{\text{tors}}$.

**Proposition 5.16.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ is isomorphic to one of the following groups (although not all cases*

*need occur):*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 14, 15, 18, 19, 21, 25, 27 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 7, 9, 10, 12, 13, 14, 15, 18, 19, 21, 25, 27. \end{cases}$$

*Proof.* By Proposition 5.8 and Proposition 5.12, $E(K)_{\text{tors}}$ must be a subgroup of

$$(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}) \oplus \mathbb{Z}/27\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z} \oplus \mathbb{Z}/19\mathbb{Z}.$$

Equivalently, $E(K)_{\text{tors}} \cong \mathbb{Z}/2^i\mathbb{Z} \oplus (2^j \cdot 3^k \cdot 5^m \cdot 7^n \cdot 13^r \cdot 19^s)\mathbb{Z}$ for some $i, j, k, m, n, r, s$, where $i, n, r, s \in \{0, 1\}$, $j, k \in \{0, 1, 2, 3\}$, and $i \leq j$. It is then routine to enumerate 672 possibilities for $E(K)_{\text{tors}}$. Eliminating any torsion subgroups excluded by Lemma 5.13, Lemma 5.14, and Lemma 5.15, we immediately obtain the given list of possible torsion subgroups. □

## 5.5 Base Extension

Many of the possible torsion subgroups in Proposition 5.16 can be realized by base extending elliptic curves $E(\mathbb{Q})$ or $E(F)$, where $F$ is a Galois cubic field, to a nonic Galois field. We begin by observing that given a torsion subgroup $E(\mathbb{Q})_{\text{tors}}$, there always exists a number field $K$ of specified degree over which, when we base extend $E(\mathbb{Q})_{\text{tors}}$ to $E(K)_{\text{tors}}$, there is no torsion growth. This fact is used implicitly and explicitly in many torsion papers, but we do not know of a complete proof of this fact in the literature, so we include one here.

**Proposition 5.17.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $d > 1$ be an integer. Then there exists a number field of degree $d$, $K$, such that $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

*Proof.* By Theorem 4.1, we know that the sets $\Phi(d) \supseteq \Phi_{\mathbb{Q}}(d)$ are uniformly bounded for all $d \geq 1$. ***By the Mordell-Weil Theorem, Theorem 3.5, we know that $E(F)_{\text{tors}}$ is finite for any number field $F$. Furthermore by the work of Merel [Mer96] and Parent [Par99], c.f. Theorem 4.1, we know that the size of $E(F)_{\text{tors}}$ is uniformly bounded as $F$ varies over all number fields of degree $d$. Let $M$ denote the largest possible order for all $E(F)_{\text{tors}}$, where $F$ is a number field of degree $d$. But then there are at most $M$ possibilities for the order of $E(F)_{\text{tors}}$ for any number field $F$ of degree $d$. Let $N$ be the least common multiple of all these possible orders. Now $E(\mathbb{Q})_{\text{tors}} \subseteq E[N]$ and $\mathbb{Q}(E[N])$ is a finite (Galois) extension of $\mathbb{Q}$. In particular, $\mathbb{Q}(E[N])$ has finitely many subfields. As there exists infinitely many number fields of degree $d$ (for instance, this follows from the fact that there are infinitely many primes and that $x^d + p$ is Eisenstein at $p$), we can choose a field $K$ of degree $d$ such that $K \cap \mathbb{Q}(E[N]) = \mathbb{Q}$. But then $E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$, c.f. Lemma 6.14. □

Of course, we have not shown that we can choose the field $K$ in Proposition 5.17 to be a nonic Galois field. Proving this requires little modification from the proof of Proposition 5.17.

**Corollary 5.18.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then there exists a nonic Galois field $K$ such that $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

*Proof.* If $K_1$ and $K_2$ are distinct cubic Galois fields, then $K_1K_2$ is a nonic Galois field, see [DF04, Ch. 14,Prop. 21] or [Lan02, VI,§1,Thm. 1.14]. From the proof of Proposition 5.17, it suffices to prove that we can find infinitely many distinct cubic Galois fields. For any integer $k$, choose $a := k^2 + k + 7$. From [Conb, Cor. 2.5], we know that the polynomial $x^3 - ax + a$ is irreducible over $\mathbb{Q}$ and $K_a := \mathbb{Q}(x^3 - ax + a)$ is a cubic Galois field. By considering discriminants, for distinct integer $a$ and $a'$, the fields $K_a$ and $K_{a'}$ are distinct. □

Furthermore, we will show that every torsion subgroup over a cubic Galois field occurs over some nonic Galois field.

**Theorem 5.19.** *Let $E/\mathbb{Q}$ be a rational elliptic curve and $K_1/\mathbb{Q}$ be a Galois cubic field. Then there exists a Galois cubic field $K_2/\mathbb{Q}$, distinct from $K_1$, with $E(K_1K_2)_{tors} \cong E(K_1)_{tors}$.*

*Proof.* Fixing an algebraic closure $\overline{\mathbb{Q}}$, we have $E(K_1)_{\text{tors}} \subseteq E(\mathbb{Q}(3^\infty))_{\text{tors}}$, where $\mathbb{Q}(3^\infty)$ denotes the compositum of all cubic fields. It follows from Theorem 4.59 that there are only finitely many points in $E(\mathbb{Q}(3^\infty))_{\text{tors}}$. Let $L$ denote the field of definition of the points in $E(\mathbb{Q}(3^\infty))_{\text{tors}}$, i.e. $L = \mathbb{Q}(\{x_i, y_i \colon \mathcal{O} \neq (x_i, y_i) \in E(\mathbb{Q}(3^\infty))_{\text{tors}}\})$. We know that the extension $L/\mathbb{Q}$ is finite and separable. In particular, $L$ has finitely many subfields. Again for any integer $k$, choose $a := k^2+k+7$. From [Conb, Cor. 2.5], we know that the polynomial $x^3 - ax + a$ is irreducible over $\mathbb{Q}$, $K_a := \mathbb{Q}(x^3 - ax + a)$ is a cubic Galois field, and that distinct $a$ generate distinct cubic Galois fields $K_a$. Because $K_a$ contains no subfields other than $\mathbb{Q}$, we know that $L \cap K_a \subseteq K_a$ is either $\mathbb{Q}$ or $K_a$. But as $L \cap K_a$ is a subfield of $L$ and $L/\mathbb{Q}$ has finitely many subfields, there must be an $a \in \mathbb{Z}$ such that $L \cap K_a = \mathbb{Q}$. Note this also implies $K_1 \cap K_a = \mathbb{Q}$.

Because $E(K_a)_{\text{tors}} \subseteq E(\mathbb{Q}(3^\infty))_{\text{tors}}$ and $L \cap K_a = \mathbb{Q}$, we know that $E(K_a)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$. Because $K_1$ and $K_a$ are distinct cubic Galois fields, $K_1K_a$ is a nonic Galois field, see [DF04, Ch. 14,Prop. 21] or [Lan02, VI,§1,Thm. 1.14]. But then $K_1K_2$ is a nonic Galois field with $E(K_1K_2)_{\text{tors}} \cong E(K_1)_{\text{tors}}$. Taking $K_2 := K_a$ completes the proof. □

For convenience, we restate the classification of the sets $\Phi(1)$ and $\Phi_{\mathbb{Q}}(3)$.

**Theorem 4.2** ([Maz77, Maz78])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then $E(\mathbb{Q})_{tors}$ is*

*isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4. \end{cases}$$

*Moreover, each possibility occurs for infinitely many distinct elliptic curves.*

**Theorem 4.30** ([Naj16, Thm. 2])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a cubic number field. Then $E(K)_{tors}$ is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7. \end{cases}$$

*Moreover, each of these groups, except for $\mathbb{Z}/21\mathbb{Z}$, occurs over some cubic field for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes. The elliptic curve `162b1` over $\mathbb{Q}(\zeta_9)^+$ is the unique rational elliptic curve with torsion $\mathbb{Z}/21\mathbb{Z}$.*

By Corollary 5.18, we know that each torsion subgroup in Theorem 4.2 occurs over some nonic Galois field. However, Theorem 5.19 does not yet tell us that every possible torsion subgroup in $\Phi_{\mathbb{Q}}(3)$ occurs over some nonic Galois field. For this to be the case, we would need every possible torsion subgroup in $\Phi_{\mathbb{Q}}(3)$ to occur over a Galois cubic field. By Corollary 5.18, it suffices to show this for the torsion subgroups in $\Phi_{\mathbb{Q}}(3) \setminus \Phi(1)$. Table 5.1 demonstrates that each torsion subgroup in $\Phi_{\mathbb{Q}}(3) \setminus \Phi(1)$ occurs over some cubic Galois field. Then by combining Corollary 5.18, Table 5.1, and Theorem 5.19, we see that every torsion subgroup in $\Phi_{\mathbb{Q}}(3)$ occurs for some rational elliptic curve over some nonic Galois field.

Corollary 5.18 and Theorem 5.19 prove that $\Phi(1) \subseteq \Phi_{\mathbb{Q}}^{\text{Gal}}(9)$ and $\Phi_{\mathbb{Q}}(3) \subseteq \Phi_{\mathbb{Q}}^{\text{Gal}}(9)$. Furthermore, Table 5.2 shows that the torsion subgroups $\mathbb{Z}/19\mathbb{Z}$ and $\mathbb{Z}/27\mathbb{Z}$ do occur for some

Table 5.1: Examples of torsion subgroups $\Phi_{\mathbb{Q}}(3) \setminus \Phi(1)$ over cubic Galois fields

| Torsion Subgroup | Elliptic Curve | Cubic Galois Field |
|---|---|---|
| $\mathbb{Z}/13\mathbb{Z}$ | 147b1 | $\mathbb{Q}(\zeta_7)^+$ |
| $\mathbb{Z}/14\mathbb{Z}$ | 49a3 | $\mathbb{Q}(\zeta_7)^+$ |
| $\mathbb{Z}/18\mathbb{Z}$ | 14a4 | $\mathbb{Q}(\zeta_7)^+$ |
| $\mathbb{Z}/21\mathbb{Z}$ | 162b1 | $\mathbb{Q}(\zeta_9)^+$ |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ | 1922c1 | $\mathbb{Q}(x^3 - x^2 - 10x + 8)$ |

rational elliptic curve over some nonic Galois field.

Table 5.2: Examples of $E(K)$ with 19 and 27-torsion

| $E(K)_{\text{tors}}$ | $E(\mathbb{Q})_{\text{tors}}$ | $E$ | $K$ |
|---|---|---|---|
| $\mathbb{Z}/19\mathbb{Z}$ | $\{\mathcal{O}\}$ | 361a1 | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/27\mathbb{Z}$ | $\mathbb{Z}/3\mathbb{Z}$ | 27a4 | $\mathbb{Q}(\zeta_{27})^+$ |

Eliminating the torsion subgroups occurring in $\Phi(1) \cup \Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}\}$ from the list of possible torsion subgroups from Proposition 5.16 leaves the following list of torsion subgroups whose existence or non-existence we have yet to prove:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 15, 25 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 5, 6, 9, 10, 12, 13, 14, 15, 18, 19, 21, 25, 27. \end{cases}$$

It will turn out that none of the torsion subgroups listed above actually occur for some rational elliptic curve over some nonic Galois field. But of course, we need to actually prove this.

## 5.6 Eliminating Torsion Subgroups

We now eliminate the remaining possibilities for $E(K)_{\text{tors}}$. There are more benefits to working over Galois fields than just Lemma 5.10. The 'Galoisness' of our field will allow us to restrict when there can be torsion growth when base extending our elliptic curve $E$. For instance, Najman proved the following useful results in the classification of $\Phi_{\mathbb{Q}}(3)$, which we stated earlier but we shall restate for convenience:

**Lemma 4.44** ([Naj12b, Lemma 1]). *If the torsion subgroup of an elliptic curves $E$ over $\mathbb{Q}$ has a nontrivial 2-Sylow subgroup, then over any number field of odd degree the torsion of $E$ will have the same 2-Sylow subgroup as over $\mathbb{Q}$, i.e. $E(K)[2^\infty] = E(\mathbb{Q})[2^\infty]$.*

**Lemma 4.45** ([Naj16, Lemma 21]). *Let $K$ be a cubic field. Then the 5-Sylow groups of $E(\mathbb{Q})$ and $E(K)$ are equal.*

**Lemma 4.46** ([Naj16, Lemma 16]). *Let $p, q$ be distinct odd primes, $F_2/F_1$ a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$ and $E/F_1$ an elliptic curve with no $p$-torsion over $F_1$. Then if $q$ does not divide $p-1$ and $\mathbb{Q}(\zeta_p) \not\subset F_2$, then $E(F_2)[p] = 0$.*

**Lemma 4.47** ([Naj16, Lemma 17]). *Let $p$ be an odd prime number, $q$ a prime not dividing $p$, $F_2/F_1$ a Galois extension of number fields such that $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$, $E/F_1$ an elliptic curve, and suppose $E(F_1) \supset \mathbb{Z}/p\mathbb{Z}$, $E(F_1) \not\supset \mathbb{Z}/p^2\mathbb{Z}$, and $\zeta_p \notin F_2$. Then $E(F_2) \not\supset \mathbb{Z}/p^2\mathbb{Z}$.*

There are many generalizations of these results in [GJN20b]. Using the lemmas above, we prove the following:

**Lemma 5.20.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.*

*Proof.* Choose a model for $E$ of the form $y^2 = x^3 + Ax + B$. Suppose that $E(K)_{\mathrm{tors}}$ contains $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. If $P = (x, y)$ is a nontrivial point of order 2, then $x(P)$ is a root of $x^3+Ax+B$. Because $E$ has full 2-torsion over $K$, $K$ contains a splitting field for $x^3+Ax+B$. Call this splitting field $F$. Because $x^3 + Ax + B$ is a cubic polynomial, the only possible degrees for the splitting field $F$ are 1, 3, or 6. Because $F \subseteq K$ and $K/\mathbb{Q}$ has odd degree,

the degree of $F/\mathbb{Q}$ is either 1 or 3, i.e. $F = \mathbb{Q}$ or $F$ is a cubic Galois field. In either case, possibly making use of Lemma 4.45, we know that $E(F)[5^\infty] = E(\mathbb{Q})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z}$. But then $E(F) \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, which is not a possibility for torsion subgroups of rational elliptic curves by Mazur's classification [Maz77, Maz78] of $\Phi(1)$, c.f. Theorem 4.2, or for rational elliptic curves over cubic fields by Najman's classification [Naj16] of $\Phi_{\mathbb{Q}}(3)$, c.f. Theorem 4.30, a contradiction. □

We now eliminate the possibility that $E(K)_{\text{tors}} \cong \mathbb{Z}/25\mathbb{Z}$, which will turn out to be part of a more general result.

**Lemma 5.21.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/25\mathbb{Z}$.*

*Proof.* Denote by $F$ a subfield of $K$ of degree 3. Then $K/F$ is Galois and $\text{Gal}(K/F) \cong \mathbb{Z}/3\mathbb{Z}$. Because $K$ is an odd degree number field and $[\mathbb{Q}(\zeta_p)\colon \mathbb{Q}] = \phi(p)$ (noting that $\phi(p)$ is even for all odd primes $p$), $\mathbb{Q}(\zeta_p) \not\subseteq K$ for all odd primes $p$. Now the point of order five is either defined over $F$ (with the possibility that the point is rational) or strictly over $K$.

Suppose that the point of order 5 is not defined over $F$, i.e. $E(F)[5] = \{\mathcal{O}\}$. Then the point of order five is defined over $K$. Using Lemma 4.46 with $p = 5$ and $q = 3$, we know that $E(K)[5] = \{\mathcal{O}\}$, a contradiction.

Suppose then that the point of order five is defined over $F$, i.e. $E(F)[5] \neq \{\mathcal{O}\}$. Using Najman's classification of $\Phi_{\mathbb{Q}}(3)$, c.f. Theorem 4.30, we know that $E(F) \not\supseteq \mathbb{Z}/25\mathbb{Z}$, which implies $E(F) \cong \mathbb{Z}/5\mathbb{Z}$. But then by Lemma 4.47, we have that $E(K) \not\supseteq \mathbb{Z}/25\mathbb{Z}$. □

In fact, the 5-Sylow subgroup of $E(K)_{\text{tors}}$ is contained entirely within $E(\mathbb{Q})_{\text{tors}}$.

**Lemma 5.22.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then the 5-Sylow subgroup of $E(\mathbb{Q})_{tors}$ and $E(K)_{tors}$ are equal, i.e. $E(\mathbb{Q})[5^\infty] = E(K)[5^\infty]$.*

*Proof.* Let $F/\mathbb{Q}$ be an intermediate field of $K$ of degree 3. By Lemma 4.45, $E(F)[5^\infty] = E(\mathbb{Q})[5^\infty]$. By Mazur's classification of $\Phi(1)$, c.f. Theorem 4.2, either $E(F)[5^\infty] = E(\mathbb{Q})[5^\infty] = \{\mathcal{O}\}$ or $E(F)[5^\infty] = E(\mathbb{Q})[5^\infty] = \mathbb{Z}/5\mathbb{Z}$.

Suppose that $E(F)[5^\infty] = \{\mathcal{O}\}$. Because $K$ is an odd degree number field and $[\mathbb{Q}(\zeta_p)\colon \mathbb{Q}] = \phi(p)$ (noting that $\phi(p)$ is even for all odd primes $p$), $\mathbb{Q}(\zeta_p) \not\subseteq K$ for all odd primes $p$. We know also that $K/F$ is Galois and $\mathrm{Gal}(K/F) \cong \mathbb{Z}/3\mathbb{Z}$. But then by Lemma 4.46, $E(K)[5^\infty] = E(F)[5^\infty] = E(\mathbb{Q})[5^\infty] = \{\mathcal{O}\}$.

Now assume that $E(F)[5^\infty] \cong \mathbb{Z}/5\mathbb{Z}$. By Najman's classification of $\Phi_{\mathbb{Q}}(3)$ in [Naj16], we know that $E(F) \not\supseteq \mathbb{Z}/25\mathbb{Z}$. But then by Lemma 4.47, $E(K)[5^\infty] = E(F)[5^\infty] = E(\mathbb{Q})[5^\infty] \cong \mathbb{Z}/5\mathbb{Z}$. □

Using Lemma 5.20 and Lemma 5.21, we have reduced our list of remaining possible torsion subgroups to the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 15 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 6, 9, 12, 13, 14, 18, 19, 21, 27. \end{cases}$$

In the previous proofs, we eliminated possible torsion subgroups $E(K)_{\text{tors}}$ by showing that points of certain prime orders or prime powers occur 'early on', i.e. over strict subfields of $K$. That is, certain torsion subgroups $E(K)_{\text{tors}}$ can only be obtained by base extending an elliptic curve $E(\mathbb{Q})$ or $E(F)$, where $F \subseteq K$ is a cubic subfield, to $K$. This is part of a

general phenomenon, which we will prove. The proof will make use of the Galois representation attached to an elliptic curve. Following [Cho16, Prop. 2.8], we prove the following:

**Proposition 5.23.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Suppose $P \in E(K)_{tors}$ is a point of order $p$. Then*

*(i) if $p \in \{3, 5\}$, then $P$ is defined over $\mathbb{Q}$, i.e. $P \in E(\mathbb{Q})[p]$.*

*(ii) if $p = 13$, then there is a cubic field $F \subseteq K$ with $P \in E(F)[p]$.*

*(iii) if $p \in \{2, 7\}$, then $P$ is defined over $\mathbb{Q}$, i.e. $P \in E(\mathbb{Q})[p]$, or there is a cubic field $F \subseteq K$ with $P \in E(F)[p]$.*

*Proof.* First, consider the case where $p = 2$. Choosing a model $y^2 = x^3 + Ax + B$ for $E$, the points of order two correspond to roots of $x^3 + Ax + B$. But any root of $x^3 + Ax + B$ is defined either over $\mathbb{Q}$ or some cubic (Galois) field.

Now suppose that $p > 2$. By Lemma 5.9, $E$ cannot contain full $p$-torsion over $K$. But then we can choose a basis $\{P, Q\}$ for $E[p]$ such that $P \in E(K)$ and $Q \notin E(K)$. Let $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(K)) \cong \mathrm{GL}_2(\mathbb{F}_p)$ be the associated Galois representation with respect to the basis $\{P, Q\}$. Because $P \in E(K)$ and $E(K)$ does not contain full $p$-torsion, we know $P^\sigma \in E(K)[p]$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. But as $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, $P^\sigma \in \langle P \rangle$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore, $\operatorname{im} \rho_{E,p}$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Suppose then that

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

where $\phi, \psi$ are both $\mathbb{F}_p$-valued characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\tau : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p$. Using the Galois representation and the Galois correspondence, the field of definition of $P$, $\mathbb{Q}(P)$, is

given by $\ker \phi = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(P))$.

Denote by $S$ the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ fixing $\mathbb{Q}(P)$. We know that

$$|\operatorname{im}\varphi| = |\{P^\sigma : \sigma \in \mathrm{Gal}(K/\mathbb{Q})\}| = \frac{|\mathrm{Gal}(K/\mathbb{Q})|}{|S|} = [\mathbb{Q}(P) : \mathbb{Q}].$$

Now because $\mathbb{Q}(P) \subseteq K$, $[\mathbb{Q}(P) : \mathbb{Q}]$ divides $[K : \mathbb{Q}] = 9$. But we know also that $\operatorname{im}\varphi \leq \mathbb{F}_p^\times$, so that $|\operatorname{im}\varphi| = [\mathbb{Q}(P) : \mathbb{Q}]$ divides $p - 1$.

If $p$ is 3 or 5, then $[\mathbb{Q}(P) : \mathbb{Q}]$ divides 9 and divides either 2 or 4, respectively. In either case, this implies $[\mathbb{Q}(P) : \mathbb{Q}] = 1$ so that $P$ is defined over $\mathbb{Q}(P) = \mathbb{Q}$. If $p = 7$, then $[\mathbb{Q}(P) : \mathbb{Q}]$ divides 9 and 6 so that $[\mathbb{Q}(P) : \mathbb{Q}]$ is either 1, in which case $P$ is defined over $\mathbb{Q}$, or 3, in which case $P$ is defined over a cubic field. Now if $p$ is 13, then $[\mathbb{Q}(P) : \mathbb{Q}]$ divides 9 and 12. But it is not possible that $[\mathbb{Q}(P) : \mathbb{Q}] = 1$ because there are no rational points of order 13 for torsion subgroups $E(\mathbb{Q})_{\text{tors}}$ by Mazur's classification of $\Phi(1)$. Therefore, $[\mathbb{Q}(P) : \mathbb{Q}] = 3$ so that $P$ is defined over a cubic field $F \subseteq K$. □

We can now begin putting Proposition 5.23 to good use.

**Lemma 5.24.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ is not isomorphic to $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/42\mathbb{Z}$.*

*Proof.* If $P \in E(K)_{\text{tors}}$ is a point of order 15, then $E(K)$ contains points of order 3 and 5. By Proposition 5.23, these points are necessarily defined over $\mathbb{Q}$. But then $E(K)_{\text{tors}} \supseteq E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/15\mathbb{Z}$, which is impossible by Mazur's classification of $\Phi(1)$, c.f. Theorem 4.2.

Now if $E(K)_{\text{tors}}$ were isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/42\mathbb{Z}$, $E$ would obviously

contain full 2-torsion. Choosing a model $y^2 = x^3 + Ax + B$ for $E$ and applying the same argument as in Lemma 5.20, $K$ contains a splitting field for $x^3 + Ax + B$, say $F$. Again by the argument in Lemma 5.20, either $F = \mathbb{Q}$ or $F$ is a cubic Galois field.

Suppose that $F = \mathbb{Q}$. By Proposition 5.23, a point of order 13 is defined over a cubic field. The point of order 7 cannot be defined over $\mathbb{Q}$ because then $E(\mathbb{Q})_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, contradicting Mazur's classification of $\Phi(1)$, c.f. Theorem 4.2. By Proposition 5.23, the point of order 7 is then also defined over a cubic field. If $E(K)_{\text{tors}}$ were isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$. There is a cubic field $F'$ containing the point of order 13. But then $E(F')_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$, contradicting Najman's classification of $\Phi_{\mathbb{Q}}(3)$, c.f. Theorem 4.30. If $E(K)_{\text{tors}}$ were isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/42\mathbb{Z}$, there would be a cubic field $F'$ such that $E(F') \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ and $E(\mathbb{Q})_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. But this contradicts Theorem 4.55.

Then it must be that $F$ is a cubic Galois field. Because the point of order 13 is defined strictly over a cubic field, we cannot have $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$ because Theorem 1.4 in [GJNT16], c.f. Theorem 4.55, shows that there is no elliptic curve that has torsion growth from $E(\mathbb{Q})_{\text{tors}} \cong \{\mathcal{O}\}$ to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/13\mathbb{Z}$ over either one, two, or three distinct cubic fields (and there are at most three cubic fields $\widetilde{F}$ such that $E(\widetilde{F})_{\text{tors}} \neq E(\mathbb{Q})_{\text{tors}}$), a contradiction. Similarly, suppose that $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/42\mathbb{Z}$. By Proposition 5.23, the point of order 3 is defined over $\mathbb{Q}$. Then the point of order 7 cannot be defined over $\mathbb{Q}$ because then $E(\mathbb{Q})_{\text{tors}} \supseteq \mathbb{Z}/21\mathbb{Z}$, contradicting the classification of $\Phi(1)$, c.f. Theorem 4.2. Then the point of order 7 is defined over a cubic field. We know that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/3\mathbb{Z}$. But by Theorem 1.4 in [GJNT16], c.f. Theorem 4.55, there exists no elliptic curve with such torsion growth over cubic fields, a contradiction. □

We can apply isogeny restrictions to eliminate three more remaining possibilities. Note that this result does not assume that $K$ is nonic, merely that it is an odd degree Galois

number field.

**Lemma 5.25.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be an odd degree Galois field. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$.*

*Proof.* Suppose that $E(K)_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$. Clearly, $\mathbb{Z}/9\mathbb{Z} \subseteq E(K)_{\text{tors}}$ so that by Lemma 5.10, $E$ has a rational 9-isogeny. In particular, using [LR13, Table 3], c.f. Table 7.3, we know that $E$ is a twist of an elliptic curve with $j$-invariant given by

$$j = \frac{h^3(h^3 - 24)^3}{h^3 - 27}$$

for $h \in \mathbb{Q} \setminus \{3\}$. By [Kub76, Table 2,Prop. III.2.3], there are no rational elliptic curves with a rational 9-isogeny and full 2-torsion or two independent 3-isogenies and full 2-torsion. Therefore, it must be that $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$. Choose a model $y^2 = x^3 + Ax + B$. As $E$ has full 2-torsion over $K$ and $K$ is odd, there is a cubic field $\mathbb{Q} \subseteq F \subseteq K$ such that $F$ is a splitting field for $x^3 + Ax + B$. But then $F/\mathbb{Q}$ is Galois. In particular, we know that $\text{disc}(x^3 + Ax + B)$ is a square. Because twisting changes the discriminant by a square, this implies that there is a $M \in \mathbb{Q}$ such that

$$M^2 = \frac{2^8 \cdot 3^{12} \cdot (h^3 - 27)(h^3 - 24)^6}{(h^6 - 36h^3 + 216)^6}$$

Absorbing squares into the left hand side, a solution to the equation above implies the existence of a rational point $(m, n)$ on the curve $m^2 = n^3 - 27$. This is an elliptic curve $E$, and using SAGE, we find $E(\mathbb{Q}) = \{\mathcal{O}, (3, 0)\}$. The point $(3, 0)$ corresponds to a cusp. Therefore, $E(K)_{\text{tors}} \not\supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$. □

We can use another result of Najman to eliminate yet another two remaining possibilities.

**Lemma 5.26** ([Naj16, Cor. 12])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a cubic Galois field. If $E(\mathbb{Q})$ has no points of order 4, then $E(K)$ has no 4-torsion.*

*Proof.* This is simply Corollary 12 in [Naj16] applied to the case where $K/\mathbb{Q}$ is a Galois cubic field. □

**Lemma 5.27.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.*

*Proof.* Suppose that $E(K)_{\text{tors}}$ contained $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. If $E(\mathbb{Q})_{\text{tors}} \ncong \{\mathcal{O}\}$, then by Lemma 4.44 $E(\mathbb{Q})[2^\infty] \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. By Proposition 5.23, the point of order 3 is defined over $\mathbb{Q}$. But then $E(\mathbb{Q})_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, contradicting Mazur's classification of $\Phi(1)$, Theorem 4.2. Therefore, it must be that $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$. Let $F$ be a cubic Galois subfield of $K$. By Lemma 5.26, we know that $E(F)$ has no 4-torsion.

Suppose that $P = (x(P), y(P))$ is a point of order 4 on $E$. It must be then that $[\mathbb{Q}(P)\colon \mathbb{Q}] > 3$. Because $y(P)$ is defined at most over a quadratic extension of $\mathbb{Q}(x(P))$, noting that $K$ is odd and $x(P)$ is not defined over $\mathbb{Q}$ or a cubic field, it must be that $K = \mathbb{Q}(x(P))$. Choose a model $y^2 = x^3 + Ax + B$ for $E$. We know that $x(P)$ is a root for

$$\psi_4(x) = 4(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),$$

where $\psi_4$ is the 4-division polynomial for $E$. In particular, $x(P)$ is a root of a polynomial of at most degree 6, contradicting the fact that $K = \mathbb{Q}(x(P))$. □

This leaves only the possibilities of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/38\mathbb{Z}$ for $E(K)_{\text{tors}}$ to eliminate.

**Lemma 5.28.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ does not contain $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/38\mathbb{Z}$.*

*Proof.* If $E(K)_{\text{tors}}$ contained $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/38\mathbb{Z}$, then by Lemma 5.11, $E$ has a rational 19-isogeny. In particular by [LR13, Table 4], c.f. Table 7.4, $E$ is a twist of an elliptic curve with $j$-invariant $j = -2^{15} \cdot 3^3$, e.g. `361a1`. Now $E$ is a twist of `361a1` and this elliptic curve has no rational 2-torsion. By Lemma 5.5, $E(\mathbb{Q})[2] = \{\mathcal{O}\}$. Then $E$ gains full 2-torsion over some cubic field $K$. Choosing a model $y^2 = x^3 + Ax + B$ for $E$, making the same argument as in Lemma 5.20, $K$ contains a splitting field for $x^3 + Ax + B$. In particular, $\text{disc}(x^3 + Ax + B)$ is a square. However, the noting that any twist of $E$ has discriminant differing from $E$ by a rational square and that the discriminant of `361a1` is $-1048576/6859$, we have a contradiction.

Mutatis mutandis, if $E(K)_{\text{tors}}$ contained $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$, then $E$ has a rational 14-isogeny. In particular by [LR13, Table 4], c.f. Table 7.4, $E$ is a twist of an elliptic curve with $j$-invariant $j = -3^3 \cdot 5^3$ or $j = 3^3 \cdot 5^3 \cdot 17^3$. It is routine to verify that in either case $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. But then in either case, $E[2]$ is defined over a quadratic extension of $\mathbb{Q}$, which clearly is not contained in $K$. □

This eliminated the remaining two possibilities for $E(K)_{\text{tors}}$. We are finally in a position to give the classification.

## 5.7 The General Nonic Result

We can now combine all our previous results to classify the possible torsion subgroups for rational elliptic curves base extended to nonic Galois fields.

**Theorem 5.29.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field. Then $E(K)_{tors}$ is isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 14, 18, 19, 21, 27 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7. \end{cases}$$

*Moreover, each such possibility occurs for some rational elliptic curve and some nonic Galois field.*

*Proof.* By Proposition 5.16, the only possibilities for $E(K)_{\text{tors}}$ are the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 14, 15, 18, 19, 21, 25, 27 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 7, 9, 10, 12, 13, 14, 15, 18, 19, 21, 25, 27. \end{cases}$$

Eliminating possibilities for $E(K)_{\text{tors}}$ excluded by Lemmas 5.20, 5.21, 5.24, 5.25, 5.27, and 5.28, the only remaining possibilities for $E(K)_{\text{tors}}$ are those given in the statement of the theorem. Finally, Table 5.3 shows that each of these possibilities actually occurs. □

Of course, Theorem 5.29 only classifies the possibilities for $E(K)_{\text{tors}}$ over a general nonic Galois field $K$. We would like a classification for $E(K)_{\text{tors}}$ when $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ and $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$; that is, we would like to know the possibilities for $E(K)_{\text{tors}}$ based on the isomorphism type of $\text{Gal}(K/\mathbb{Q})$, which will be our next goal. However, we first will classify the classify the possible torsion growth when base extending from $E(\mathbb{Q})_{\text{tors}}$ to a nonic Galois field.

Table 5.3: Examples of each possible $E(K)_{\text{tors}}$ in $\Phi_{\mathbb{Q}}^{\text{Gal}}(9)$

| $E(K)_{\text{tors}}$ | Cremona Label | $E(\mathbb{Q})_{\text{tors}}$ | $K$ |
|---|---|---|---|
| $\{\mathcal{O}\}$ | 11a2 | $\{\mathcal{O}\}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/2\mathbb{Z}$ | 14a5 | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/3\mathbb{Z}$ | 19a1 | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/4\mathbb{Z}$ | 15a7 | $\mathbb{Z}/4\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/5\mathbb{Z}$ | 11a1 | $\mathbb{Z}/5\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/6\mathbb{Z}$ | 14a2 | $\mathbb{Z}/6\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/7\mathbb{Z}$ | 26b1 | $\mathbb{Z}/7\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/8\mathbb{Z}$ | 15a4 | $\mathbb{Z}/8\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/9\mathbb{Z}$ | 54b3 | $\mathbb{Z}/9\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/10\mathbb{Z}$ | 66c1 | $\mathbb{Z}/10\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/12\mathbb{Z}$ | 90c3 | $\mathbb{Z}/12\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/13\mathbb{Z}$ | 147b1 | $\{\mathcal{O}\}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/14\mathbb{Z}$ | 49a4 | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/18\mathbb{Z}$ | 260610o2 | $\mathbb{Z}/6\mathbb{Z}$ | 9.9.806460091894081.1 |
| $\mathbb{Z}/19\mathbb{Z}$ | 361a1 | $\{\mathcal{O}\}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/21\mathbb{Z}$ | 162b1 | $\mathbb{Z}/3\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/27\mathbb{Z}$ | 27a4 | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Q}(\zeta_{27})^+$ |
| $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ | 15a2 | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ | 15a1 | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ | 30a2 | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ | 210e2 | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ | 1922c1 | $\{\mathcal{O}\}$ | 9.9.104413920565969.1 |

## 5.8 Torsion Growth

We will determine how the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ grows when base extending to a nonic Galois field; that is, given $E(\mathbb{Q})_{\text{tors}} \in \Phi(1)$, what are the possibilities for $E(K)_{\text{tors}} \in \Phi_{\mathbb{Q}}^{\text{Gal}}(9)$. Note we denote by $\mathcal{C}_n$ the finite abelian group $\mathbb{Z}/n\mathbb{Z}$.

**Theorem 5.30.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Fixing $E(\mathbb{Q})_{tors} \in \Phi(1)$, the possibilities for $E(K)_{tors}$ are given in Table 5.4, indicated by '✓' in the table. These are the only possibilities for $E(K)_{tors}$ and each such possibility indicated occurs.*

*Proof.* Let $G \in \Phi(1)$ and $H \in \Phi_{\mathbb{Q}}^{\text{Gal}}(9)$. Clearly, if $G \not\leq H$, then there is no rational elliptic curve $E/\mathbb{Q}$ such that there is a nonic Galois field with $E(\mathbb{Q})_{\text{tors}} \cong G$ and $E(K)_{\text{tors}} \cong H$.

Table 5.4: The possibilities for $E(K)_{\text{tors}}$ given $E(\mathbb{Q})_{\text{tors}}$

| $E(K)_{\text{tors}}$ \ $E(\mathbb{Q})_{\text{tors}}$ | $\mathcal{C}_1$ | $\mathcal{C}_2$ | $\mathcal{C}_3$ | $\mathcal{C}_4$ | $\mathcal{C}_5$ | $\mathcal{C}_6$ | $\mathcal{C}_7$ | $\mathcal{C}_8$ | $\mathcal{C}_9$ | $\mathcal{C}_{10}$ | $\mathcal{C}_{12}$ | $\mathcal{C}_2 \times \mathcal{C}_2$ | $\mathcal{C}_2 \times \mathcal{C}_4$ | $\mathcal{C}_2 \times \mathcal{C}_6$ | $\mathcal{C}_2 \times \mathcal{C}_8$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathcal{C}_1$ | ✓ | | | | | | | | | | | | | | |
| $\mathcal{C}_2$ | | ✓ | | | | | | | | | | | | | |
| $\mathcal{C}_3$ | | | ✓ | | | | | | | | | | | | |
| $\mathcal{C}_4$ | | | | ✓ | | | | | | | | | | | |
| $\mathcal{C}_5$ | | | | | ✓ | | | | | | | | | | |
| $\mathcal{C}_6$ | | | | | | ✓ | | | | | | | | | |
| $\mathcal{C}_7$ | ✓ | | | | | | ✓ | | | | | | | | |
| $\mathcal{C}_8$ | | | | | | | | ✓ | | | | | | | |
| $\mathcal{C}_9$ | | | ✓ | | | | | | ✓ | | | | | | |
| $\mathcal{C}_{10}$ | | | | | | | | | | ✓ | | | | | |
| $\mathcal{C}_{12}$ | | | | | | | | | | | ✓ | | | | |
| $\mathcal{C}_{13}$ | ✓ | | | | | | | | | | | | | | |
| $\mathcal{C}_{14}$ | | ✓ | | | | | | | | | | | | | |
| $\mathcal{C}_{18}$ | | | | | | ✓ | | | | | | | | | |
| $\mathcal{C}_{19}$ | ✓ | | | | | | | | | | | | | | |
| $\mathcal{C}_{21}$ | | | ✓ | | | | | | | | | | | | |
| $\mathcal{C}_{27}$ | | | ✓ | | | | | | | | | | | | |
| $\mathcal{C}_2 \times \mathcal{C}_2$ | ✓ | | | | | | | | | | | ✓ | | | |
| $\mathcal{C}_2 \times \mathcal{C}_4$ | | | | | | | | | | | | | ✓ | | |
| $\mathcal{C}_2 \times \mathcal{C}_6$ | | | ✓ | | | | | | | | | | | ✓ | |
| $\mathcal{C}_2 \times \mathcal{C}_8$ | | | | | | | | | | | | | | | ✓ |
| $\mathcal{C}_2 \times \mathcal{C}_{14}$ | ✓ | | | | | | | | | | | | | | |

By Corollary 5.18, given $G \in \Phi(1)$, we know that it is always possible to find a nonic Galois field $K$ such that $E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}} \cong G$. This gives the checkmarks 'along the diagonals' in Table 5.4. It remains to consider the cases where $E(K)_{\text{tors}} \supsetneq E(\mathbb{Q})_{\text{tors}}$. We work case-by-case given $G \in \Phi(1)$.

$G = \{\mathcal{O}\}$: By Proposition 5.23, the points of order 3 and 5 are defined over $\mathbb{Q}$. If $E(K)_{\text{tors}}$ had a point of order 2, then it cannot be defined over $\mathbb{Q}$. But then it must be defined over a cubic Galois subfield of $K$. In particular, choosing a model $y^2 = x^3 + Ax + B$ for $E$, $K$ contains a splitting field for $x^3 + Ax + B$. But then $E(K)_{\text{tors}}$ must contain full 2-torsion. Therefore, the only possibilities for $E(K)_{\text{tors}}$ not found in Table 5.5 are $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Suppose $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. By Proposition 5.23, the point of order 7 is defined over $\mathbb{Q}$ or a cubic field. But in either case is not a possibility for torsion

growth when base extending $E(\mathbb{Q})_{\text{tors}}$ to a cubic field by the work in [GJNT16]. Now if $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, we know by Lemma 6.3 that there is a cubic Galois field $F$ with $E(K)_{\text{tors}} = E(F)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. But again, that contradicts the possible torsion growths in [GJNT16].

$G = \mathbb{Z}/2\mathbb{Z}$: By Proposition 5.23, the points of order 3 and 5 are defined over $\mathbb{Q}$. As $E(\mathbb{Q})[2] \neq \{\mathcal{O}\}$, we know by Lemma 4.44 that $E(\mathbb{Q})[2^\infty] = E(K)[2^\infty]$. But then there are no remaining possibilities for $E(K)_{\text{tors}}$ that are not already found in Table 5.5.

$G = \mathbb{Z}/3\mathbb{Z}$: By Proposition 5.23, the points of order 3 and 5 are defined over $\mathbb{Q}$. Then the only possibilities for $E(K)_{\text{tors}}$ not found in Table 5.5 are $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, and $\mathbb{Z}/18\mathbb{Z}$. But in each case, $E(K)_{\text{tors}}$ would gain a point of order 2 and by the arguments above, we know that $E(K)_{\text{tors}}$ must then necessarily contain full 2-torsion.

$G = \mathbb{Z}/4\mathbb{Z}$: By Proposition 5.23, the points of order 3 and 5 are defined over $\mathbb{Q}$. As $E(\mathbb{Q})[2] \neq \{\mathcal{O}\}$, we know by Lemma 4.44 that $E(\mathbb{Q})[2^\infty] = E(K)[2^\infty]$. But then there are no remaining possibilities for $E(K)_{\text{tors}}$ that are not already found in Table 5.5.

$G = \mathbb{Z}/5\mathbb{Z}$: The only possibility for $E(K)_{\text{tors}}$ is $\mathbb{Z}/10\mathbb{Z}$. However, again by the arguments above, if $E(K)_{\text{tors}}$ were $\mathbb{Z}/10\mathbb{Z}$, $E(K)_{\text{tors}}$ would gain a point of order 2 and hence then necessarily contain full 2-torsion.

$G = \mathbb{Z}/6\mathbb{Z}$: By Proposition 5.23, the points of order 3 and 5 are defined over $\mathbb{Q}$. As $E(\mathbb{Q})[2] \neq \{\mathcal{O}\}$, we know by Lemma 4.44 that $E(\mathbb{Q})[2^\infty] = E(K)[2^\infty]$. But then there are no remaining possibilities for $E(K)_{\text{tors}}$ that are not already found in Table 5.5.

$G = \mathbb{Z}/7\mathbb{Z}$: By Proposition 5.23, the points of order 3 and 5 are defined over $\mathbb{Q}$. The only

possibilities for $E(K)_{\text{tors}}$ are $\mathbb{Z}/14\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. By the same arguments above about having full 2-torsion, we know that $\mathbb{Z}/14\mathbb{Z}$ is not possible. Suppose then that $E(K)_{\text{tors}}$ were $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. We know that the points of order 2 will be defined over a cubic Galois subfield of $K$. But there is no such torsion growth by the work in [GJNT16].

$G = \mathbb{Z}/8\mathbb{Z}$: The only possibility for $E(K)_{\text{tors}}$ is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. However, we know that because $E(\mathbb{Q})[2] \neq \{\mathcal{O}\}$, by Lemma 4.44, $E(\mathbb{Q})[2^\infty] = E(K)[2^\infty]$. But then $E(K)_{\text{tors}} \ncong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

$G = \mathbb{Z}/9\mathbb{Z}$: The only possibilities for $E(K)_{\text{tors}}$ are $\mathbb{Z}/18\mathbb{Z}$ or $\mathbb{Z}/27\mathbb{Z}$. Again by the full 2-torsion arguments we have made above, we know that $\mathbb{Z}/18\mathbb{Z}$ is not possible. By Theorem 5.32, we cannot have $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ and have $E(K)_{\text{tors}} \cong \mathbb{Z}/27\mathbb{Z}$. Therefore, if this growth occurs, we must have $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$. Let $\sigma \in \text{Gal}(K/\mathbb{Q})$ be a generator for $\text{Gal}(K/\mathbb{Q})$, and let $P$ be the point of order 27. We know that $P^\sigma = aP$ for some $a \in (\mathbb{Z}/27\mathbb{Z})^\times$. But as $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/9\mathbb{Z}$, the action of $\text{Gal}(K/\mathbb{Q})$ must fix $3P$. Then we know $3P = (3P)^\sigma = 3aP$ so that $a = 1$, which is impossible because then there would be a point of order 27 defined over $\mathbb{Q}$, contradicting the classification of $\Phi(1)$.

$G = \mathbb{Z}/10\mathbb{Z}$ or $G = \mathbb{Z}/12\mathbb{Z}$: The fact that the only possibility is $E(\mathbb{Q})_{\text{tors}} = E(K)_{\text{tors}}$ is immediate in both cases.

$G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$: Because $E(\mathbb{Q})[2] \neq \{\mathcal{O}\}$, we know by Lemma 4.44 that $E(\mathbb{Q})[2^\infty] = E(K)[2^\infty]$. By Proposition 5.23, the points of order 3 and 5 are defined over $\mathbb{Q}$. But then the only possibility that remains is that $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. But the point of order 7 occurs over a cubic field by the structure of $E(\mathbb{Q})_{\text{tors}}$ and Proposition 5.23. But there is no such torsion growth over cubic fields by the work in Theorem 4.55.

$G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$: The only possibility for $E(K)_{\text{tors}}$ is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. But as $E(\mathbb{Q})[2] \neq \{\mathcal{O}\}$, we know by Lemma 4.44 that $E(\mathbb{Q})[2^\infty] = E(K)[2^\infty]$. But then $E(K)_{\text{tors}}$ cannot be $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

$G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ or $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$: The fact that the only possibility is $E(\mathbb{Q})_{\text{tors}} = E(K)_{\text{tors}}$ is immediate in both cases.

Finally, Table 5.5 shows that the remaining cases of torsion growth do occur for some rational elliptic curve over some nonic Galois field. □

Table 5.5: Examples of torsion growth $E(K)_{\text{tors}} \supsetneq E(\mathbb{Q})_{\text{tors}}$

| Cremona Label | $E(\mathbb{Q})_{\text{tors}}$ | $E(K)_{\text{tors}}$ |
|---|---|---|
| 1369b1 | $\{\mathcal{O}\}$ | $\mathbb{Z}/7\mathbb{Z}$ |
| 147b1 | $\{\mathcal{O}\}$ | $\mathbb{Z}/13\mathbb{Z}$ |
| 361a1 | $\{\mathcal{O}\}$ | $\mathbb{Z}/19\mathbb{Z}$ |
| 784i1 | $\{\mathcal{O}\}$ | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ |
| 1922c1 | $\{\mathcal{O}\}$ | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ |
| 49a4 | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/14\mathbb{Z}$ |
| 19a3 | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/9\mathbb{Z}$ |
| 162b1 | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/21\mathbb{Z}$ |
| 27a4 | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/27\mathbb{Z}$ |
| 196b1 | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ |
| 260610o2 | $\mathbb{Z}/6\mathbb{Z}$ | $\mathbb{Z}/18\mathbb{Z}$ |

## 5.9 The Bicyclic Nonic Galois Case

First, we will classify the possibilities for $E(K)_{\text{tors}}$, where $K/\mathbb{Q}$ is a nonic Galois field with $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, i.e. a 'bicyclic' nonic Galois field. Recall from Theorem 4.59 that in [DLRNS18], Daniels, Lozano-Robledo, Najman, and Sutherland classify the possible torsion subgroups of rational elliptic curves over the composition of all cubic fields. In

particular, they showed

$$E(\mathbb{Q}(3^\infty))_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 4, 5, 7, 8, 13 \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 4, 7 \text{ or} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6n\mathbb{Z}, & \text{with } n = 1, 2, 3, 5, 7 \text{ or} \\ \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 4, 6, 7, 9. \end{cases}$$

Let $K$ be a nonic Galois field with $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, i.e. a nonic bicyclic Galois field. Because $K$ is the compositum of its Galois intermediate subfields, it must be that $E(K)_{\text{tors}}$ is a subgroup of the list of possible torsion subgroups above. This will allow us to eliminate two possible torsion subgroups for $\Phi_{\mathbb{Q}}^{\mathcal{C}_3 \times \mathcal{C}_3}(9)$.[1]

**Lemma 5.31.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic bicyclic Galois field, i.e. a nonic field with $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Then $E(K)_{tors}$ is not isomorphic to $\mathbb{Z}/19\mathbb{Z}$ or $\mathbb{Z}/27\mathbb{Z}$.*

*Proof.* Let $F_1, F_2$ be distinct cubic subfields of $K$. Because $F_1 \cap F_2 = \mathbb{Q}$, $K$ is the compositum of $F_1$ and $F_2$, and $\text{Gal}(K/\mathbb{Q}) \cong \text{Gal}(F_1/\mathbb{Q}) \times \text{Gal}(F_2/\mathbb{Q})$, see [DF04, Ch. 14,Prop. 21] or [Lan02, VI,§1,Thm. 1.14]. Fixing an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, we have $E(K)_{\text{tors}} \subseteq E(\mathbb{Q}(3^\infty))_{\text{tors}}$. But then $E(K)_{\text{tors}}$ is a subgroup of some $E(\mathbb{Q}(3^\infty))_{\text{tors}}$ appearing on the list from Theorem 4.59 and is also one of the possibilities from Theorem 5.29. However, $\mathbb{Z}/19\mathbb{Z}$ and $\mathbb{Z}/27\mathbb{Z}$ are not subgroups of the possible torsion subgroups for $E(\mathbb{Q}(3^\infty))_{\text{tors}}$. □

We now prove that each of the torsion subgroups in $\Phi_{\mathbb{Q}}(3)$ occur over a nonic bicyclic field. Fix a torsion subgroup $G \in \Phi_{\mathbb{Q}}^{\text{Gal}}(3)$, i.e. there is a cubic Galois field $K$ with $E(K)_{\text{tors}} \cong G$. We merely need to find a cubic Galois fields $L$ such that $K \cap L = \mathbb{Q}$. Taking the compositum

[1] Note for typographical reasons, we shall use $\mathcal{C}_n$ to denote $\mathbb{Z}/n\mathbb{Z}$ so that we can typeset $\Phi_{\mathbb{Q}}^{\mathcal{C}_3 \times \mathcal{C}_3}(9)$ rather than the much uglier $\Phi_{\mathbb{Q}}^{\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}}(9)$.

$KL$ will result in a nonic bicyclic Galois field over which there is no torsion growth, i.e. $\mathrm{Gal}(KL) \cong \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $E(KL)_{\mathrm{tors}} \cong E(K)_{\mathrm{tors}} \cong G$. But this is precisely what we proved in Theorem 5.19.

In fact, the proof of Theorem 5.19 was computationally explicit in the sense that given $G \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(3)$ and $E(K)_{\mathrm{tors}} \cong G$, a method was given to find a cubic Galois field $L$ with $E(KL)_{\mathrm{tors}} \cong G$. What was not mentioned was how many fields one would need to examine before finding such an $L$. In practice, such a cubic Galois field is found immediately. But in fact, González-Jiménez, Najman, and Tornero have studied the growth of torsion subgroups of rational elliptic curves over cubic number fields in [GJNT16]. Then by Theorem 4.55, one need examine at most 4 possible fields $L$ before finding a suitable candidate. We can use all of the previous discussion to find examples of a rational elliptic curve $E/\mathbb{Q}$ and a nonic bicyclic Galois field $K$ such that $E(K)_{\mathrm{tors}} \cong G$ for all $G \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(9)$. This combined with Lemma 5.31 will complete the classification of $\Phi_{\mathbb{Q}}^{\mathcal{C}_3 \times \mathcal{C}_3}(9)$.

**Theorem 5.32.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic bicyclic Galois field, i.e. a nonic field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Then $E(K)_{tors}$ is precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7. \end{cases}$$

*Moreover, each such possibility occurs for some rational elliptic curve and some nonic bicyclic field.*

*Proof.* We know that $E(K)_{\mathrm{tors}} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(9)$. Eliminating the cases of $\mathbb{Z}/19\mathbb{Z}$ and $\mathbb{Z}/27\mathbb{Z}$ from the list given in Theorem 5.29, we are left only with the possibilities given in the statement of the theorem. Table 5.6 shows that each such possibility occurs. □

Table 5.6: Examples of torsion subgroups $E(K)_{\text{tors}}$ in $\Phi_{\mathbb{Q}}^{\mathcal{C}_3\times\mathcal{C}_3}(9)$

| $E(K)_{\text{tors}}$ | Cremona Label | $E(\mathbb{Q})_{\text{tors}}$ | $K$ |
|---|---|---|---|
| $\{\mathcal{O}\}$ | 11a2 | $\{\mathcal{O}\}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/2\mathbb{Z}$ | 14a5 | $\mathbb{Z}/2\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/3\mathbb{Z}$ | 19a1 | $\mathbb{Z}/3\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/4\mathbb{Z}$ | 15a7 | $\mathbb{Z}/4\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/5\mathbb{Z}$ | 11a1 | $\mathbb{Z}/5\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/6\mathbb{Z}$ | 14a2 | $\mathbb{Z}/6\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/7\mathbb{Z}$ | 26b1 | $\mathbb{Z}/7\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/8\mathbb{Z}$ | 15a4 | $\mathbb{Z}/8\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/9\mathbb{Z}$ | 54b3 | $\mathbb{Z}/9\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/10\mathbb{Z}$ | 66c1 | $\mathbb{Z}/10\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/12\mathbb{Z}$ | 90c3 | $\mathbb{Z}/12\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/13\mathbb{Z}$ | 147b1 | $\{\mathcal{O}\}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/14\mathbb{Z}$ | 49a4 | $\mathbb{Z}/2\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/18\mathbb{Z}$ | 14a4 | $\mathbb{Z}/6\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/21\mathbb{Z}$ | 162b1 | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Q}(\zeta_{27})^+$ |
| $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ | 15a2 | $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ | 15a1 | $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$ | 30a2 | $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$ | 210e2 | $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$ | 1922c1 | $\{\mathcal{O}\}$ | 9.9.104413920565969.1 |

## 5.10 The Cyclic Nonic Galois Case

Finally, we will classify the possibilities for $E(K)_{\text{tors}}$, where $K/\mathbb{Q}$ is a nonic cyclic Galois field, i.e. $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$ and $E(K)_{\text{tors}} \in \Phi_{\mathbb{Q}}^{\mathcal{C}_9}(9)$. This classification will rely on the action of $\text{Gal}(K/\mathbb{Q})$ and the structure of $E(K)_{\text{tors}}$ when base extended to $\mathbb{Q}^{\text{ab}}$. Before classifying $\Phi_{\mathbb{Q}}^{\mathcal{C}_9}(9)$, we will observe that if $E/\mathbb{Q}$ is a rational elliptic curve and $K/\mathbb{Q}$ is a nonic cyclic Galois field, there is a simpler proof that $E(K)_{\text{tors}} \notin \{\mathbb{Z}/15\mathbb{Z}, \mathbb{Z}/16\mathbb{Z}, \mathbb{Z}/25\mathbb{Z}\}$ than we saw in Lemmas 5.4, 5.7, 5.21, and 5.24.

**Lemma 5.33.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic cyclic Galois field, i.e.* $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$. *Then $E(K)_{tors}$ is not isomorphic to $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, or $\mathbb{Z}/25\mathbb{Z}$.*

*Proof.* Suppose that $E(K)_{\text{tors}} \cong \mathbb{Z}/n\mathbb{Z}$, where $n \in \{15, 16, 25\}$, and let $P$ be a point of order $n$. Let $\sigma \in \text{Gal}(K/\mathbb{Q})$ be a generator for $\text{Gal}(K/\mathbb{Q})$. Because $E(K)[n] = \langle P \rangle$, we know that $P^\sigma = aP$ for some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. But for $n \in \{15, 16, 25\}$, $(\mathbb{Z}/n\mathbb{Z})^\times$ has order 8, 8, and 20, respectively. Then the orbit of $P$ under $\text{Gal}(K/\mathbb{Q})$ has size dividing 8 or 20, which implies that $[\mathbb{Q}(P)\colon \mathbb{Q}]$ divides either 8 or 20. However, $\mathbb{Q}(P) \subseteq K$ so that $[\mathbb{Q}(P)\colon \mathbb{Q}]$ divides 9. This shows that $[\mathbb{Q}(P)\colon \mathbb{Q}] = 1$, implying $E(\mathbb{Q})_{\text{tors}}$ has a point of order $n \in \{15, 16, 25\}$. However by Mazur's classification of $\Phi(1)$, no such elliptic curve exists, c.f. Theorem 4.2. □

We will show that the set $\Phi_{\mathbb{Q}}^{\mathcal{C}_9}(9)$ is $\Phi_{\mathbb{Q}}^{\text{Gal}}(9) \setminus \{\mathbb{Z}/14\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}\}$. So to "complete" the classification, we need only show that these possibilities do not occur over a nonic cyclic Galois field.

**Lemma 5.34.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic cyclic Galois field, i.e. $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$. Then $E(K)_{tors}$ is not isomorphic to $\mathbb{Z}/14\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$*

*Proof.* Fix an algebraic closure of $\mathbb{Q}$. Suppose that $E(K)_{\text{tors}}$ contained a subgroup isomorphic to $\mathbb{Z}/14\mathbb{Z}$. Because $[K\colon \mathbb{Q}] = 9$ is the square of a prime, $\text{Gal}(K/\mathbb{Q})$ is abelian. Then we have $E(K)_{\text{tors}} \subseteq E(\mathbb{Q}^{\text{ab}})$. By Chou's classification of the possibilities for the possible groups $E(\mathbb{Q}^{\text{ab}})_{\text{tors}}$ in [Cho19], c.f. Theorem 4.63, it must be that $E(\mathbb{Q}^{\text{ab}})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. In particular, there are finitely many possibilities $j$-invariant for $E$. Examining the possible structures for $\text{Gal}(\mathbb{Q}(E(\mathbb{Q}^{\text{ab}})_{\text{tors}})/\mathbb{Q})$, in each case, we see that there can be no nonic cyclic Galois field $K$ and rational elliptic curve $E$ with $E(K)_{\text{tors}} \supseteq \mathbb{Z}/14\mathbb{Z}$. □

Lemma 5.34 highlights something interesting. There are no elliptic curves with torsion subgroup $\mathbb{Z}/14\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over nonic cyclic Galois fields. In particular, if $E/\mathbb{Q}$ is a rational elliptic curve, and $F/\mathbb{Q}$ is a Galois cubic extension with $E(F)_{\text{tors}}$ isomorphic to

either of these groups, then there is no tower of number fields $K/F/\mathbb{Q}$ with $K/\mathbb{Q}$ a nonic cyclic Galois field. Something about the structures of torsion subgroups for elliptic curves is giving us arithmetic data about number fields. Of course, it is really only giving us data about one specific Galois field in this case. In fact, we could have proven this directly, which we show in Lemma 5.35 explicitly. For simplicity, we show this only for the $\mathbb{Z}/14\mathbb{Z}$, as the other case reduces to the proof for $\mathbb{Z}/14\mathbb{Z}$ anyway. But this observation does leave open the question whether one can find classes of torsion subgroups of rational elliptic curves over number fields that give information about the arithmetic of the number fields to which they have been base extended.

**Lemma 5.35.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic cyclic Galois field, i.e.* $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$. *Then* $E(K)_{tors} \ncong \mathbb{Z}/14\mathbb{Z}$.

*Proof.* We know by Lemma 5.10 that $E$ has a rational 14-isogeny. From [LR13, Table 4], Table 7.4, the only possible $j$-invariants for a rational elliptic curves with a rational 14-isogeny are $j = -3^3 \cdot 5^3$ or $j = 3^3 \cdot 5^3 \cdot 17^3$. If $j = 3^3 \cdot 5^3 \cdot 17^3$, then $E$ is isomorphic to a twist of the the elliptic curve given by $y^2 = x^3 - \frac{613997}{22743}x + \frac{1227994}{22743}$. We know by Proposition 5.23 that the points of order 2 occurs either over $\mathbb{Q}$ or a cubic field. The polynomial $x^3 - \frac{613997}{22743}x + \frac{1227994}{22743}$ is irreducible over $\mathbb{Q}$ so that the point of order 2 is defined over the cubic field $F := \mathbb{Q}\left(x^3 - \frac{613997}{22743}x + \frac{1227994}{22743}\right)$ (note that twisting does not change this, nor the discriminant except by a rational square). But as $K/\mathbb{Q}$ is an abelian Galois extension, $F/\mathbb{Q}$ is Galois. Then the discriminant of $F$ is a square over $\mathbb{Q}$. But the discriminant of $F$ is $-\frac{2^8 \cdot 43^2 \cdot 109^2 \cdot 131^2}{3^6 \cdot 5^3 \cdot 7^3 \cdot 19^6}$, which is impossible.

Then it must be that $E$ is a twist of the elliptic curve with $j$-invariant $j = -3^3 \cdot 5^3$. Thus, $E$ is isomorphic to a twist of the elliptic curve given by $y^2 = x^3 - \frac{125}{7}x + \frac{250}{7}$. Again by Proposition 5.23, the point of order 7, say $P$, is defined either over $\mathbb{Q}$ or a cubic field.

Using division polynomials, we find that the $x$-coordinate of $P$ satisfies an equation $7(x^3 + x^2 - 2x - 1)g(x) = 0$, where $g(x)$ is a degree 21 polynomial that is irreducible over $\mathbb{Q}$. Then the $x$-coordinate of $P$ is a root of $x^3+x^2-2x-1$. But $\mathbb{Q}(x^3+x^2-2x-1) = \mathbb{Q}(\zeta_7)^+$. So $\mathbb{Q}(\zeta_7)^+$ is the unique cubic subfield of $K/\mathbb{Q}$. We show there is no field $K$ with $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_7)^+ \subseteq K$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$.

Suppose such a field $K$ existed. Because $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$ is abelian, by the Kronecker-Weber Theorem, there exists an $N$ with $F \subseteq K \subseteq \mathbb{Q}(\zeta_N)$. We know that $N = 7^s m$ for some $s \geq 0$, $m \geq 1$ with $\gcd(m, 7) = 1$. Now $|(\mathbb{Z}/7^s\mathbb{Z})^\times| = 7^{s-1}(7-1) = 2 \cdot 3 \cdot 7^{s-1}$. Using the Chinese Remainder Theorem, we choose an integer $n$ with $n \equiv 2 \mod 7$ and $n \equiv 1 \mod m$. Let $\phi : \mathbb{Q}(\zeta_N) \to \mathbb{Q}(\zeta_N)$ be the automorphism given by $\zeta_N \mapsto \zeta_N^n$. We know $\phi(K) = K$, and that $\phi$ has order 3 in $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. By construction, the restriction of $\phi$ to $F$ is nontrivial. But $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$ so that the restriction of $\phi$ to $K$ is equal to $\psi^3$ for some $\psi \in \mathrm{Gal}(K/\mathbb{Q})$. As $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$, it must be that $\psi^3$ fixes $F$, a contradiction. □

In any case, we can now give the classification of $\Phi_{\mathbb{Q}}^{\mathcal{C}_9}(9)$.

**Theorem 5.36.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic cyclic Galois field, i.e. a nonic field with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/9\mathbb{Z}$. Then $E(K)_{tors}$ is precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 18, 21 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4. \end{cases}$$

*Moreover, each such possibility occurs for some rational elliptic curve and some nonic cyclic Galois field.*

*Proof.* We know that $E(K)_{\mathrm{tors}}$ must be one of the torsion subgroups from Theorem 5.29.

Eliminating the torsion subgroups excluded by Lemma 5.34, we are left with the possibilities given in the statement of the theorem. Table 5.7 shows that each such possibility occurs. □

Table 5.7: Examples of torsion subgroups $E(K)_{\text{tors}}$ in $\Phi_{\mathbb{Q}}^{\mathcal{C}_9}(9)$

| $E(K)_{\text{tors}}$ | Cremona Label | $E(\mathbb{Q})_{\text{tors}}$ | $K$ |
|---|---|---|---|
| $\{\mathcal{O}\}$ | 11a2 | $\{\mathcal{O}\}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/2\mathbb{Z}$ | 14a5 | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/3\mathbb{Z}$ | 19a1 | $\mathbb{Z}/3\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/4\mathbb{Z}$ | 15a7 | $\mathbb{Z}/4\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/5\mathbb{Z}$ | 11a1 | $\mathbb{Z}/5\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/6\mathbb{Z}$ | 14a2 | $\mathbb{Z}/6\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/7\mathbb{Z}$ | 26b1 | $\mathbb{Z}/7\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/8\mathbb{Z}$ | 15a4 | $\mathbb{Z}/8\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/9\mathbb{Z}$ | 54b3 | $\mathbb{Z}/9\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/10\mathbb{Z}$ | 66c1 | $\mathbb{Z}/10\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/12\mathbb{Z}$ | 90c3 | $\mathbb{Z}/12\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/13\mathbb{Z}$ | 147b1 | $\{\mathcal{O}\}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/18\mathbb{Z}$ | 260610o2 | $\mathbb{Z}/6\mathbb{Z}$ | 9.9.806460091894081.1 |
| $\mathbb{Z}/21\mathbb{Z}$ | 162b1 | $\mathbb{Z}/3\mathbb{Z}$ | 9.9.62523502209.1 |
| $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ | 15a2 | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ | 15a1 | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ | 30a2 | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ | 210e2 | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ | $\mathbb{Q}(\zeta_{19})^+$ |

As a final remark, it is worth noting that $\mathbb{Z}/18\mathbb{Z}$ is 'rare' as a torsion subgroup over nonic cyclic Galois fields in the following sense: suppose that $E(K)_{\text{tors}} \cong \mathbb{Z}/18\mathbb{Z}$. We know by Proposition 5.23 that the point of order 3 is defined over $\mathbb{Q}$. Then $E(\mathbb{Q})_{\text{tors}} \supseteq \mathbb{Z}/3\mathbb{Z}$. We cannot have $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/9\mathbb{Z}$. If this were the case, then letting $\sigma \in \text{Gal}(K/\mathbb{Q})$ be a generator for $\text{Gal}(K/\mathbb{Q})$, we know that $P^\sigma = aP$ for some $a \in (\mathbb{Z}/9\mathbb{Z})^\times$, where $P$ is the point of order 18. But if $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/9\mathbb{Z}$, then we must have $2P = (2P)^\sigma = 2aP$, which implies that $a = 1$. But then we would have a point of order 18 defined over $\mathbb{Q}$, which is impossible. Because $K/\mathbb{Q}$ is Galois and $E(K)_{\text{tors}}$ contains a point of order 2 but not full 2-torsion, the point of order 2 is defined over $\mathbb{Q}$. But then we know that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z}$. By the work in [GJNT16], there is at most one cubic field over which this torsion subgroup grows. Searching across all 6759 torsion subgroups in the LMFDB across all nonic cyclic

Galois fields in the database (of which there are 284), the first such example we found was the one given—the 4699th such curve.

# Chapter 6

# General Odd Degree Galois Fields

In this chapter, we classify the possibilities for torsion subgroups of rational elliptic curves base extended to an odd degree Galois field, i.e. we determine the set $\bigcup_{k=0}^{\infty} \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(2k+1)$. We give examples of each possibility that occurs. We then determine the sets $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$, where $d$ is an odd integer, based solely on the prime factorization of $d$.

## 6.1 Overview for the Classification

Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be an odd degree Galois field of fixed degree $d$. Recall that the set $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ is the set of possible isomorphism classes of torsion subgroups $E(K)_{\mathrm{tors}}$ as $E$ varies over all rational elliptic curves and $K$ varies over all possible Galois fields of degree $d$. To find the sets $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$, we apply the same approach that we used in the nonic classification. First, we find the possible prime orders for points $P \in E(K)_{\mathrm{tors}}$. We then bound the size of the Sylow $p$-subgroups. We can then create a finite list of possibilities for $E(K)_{\mathrm{tors}}$. We will then the eliminate torsion subgroups which do not occur for any rational elliptic curve over any odd degree Galois field. This will

leave us with a list of torsion subgroups that occur for some rational elliptic curve over some odd degree Galois field, i.e. torsion subgroups $E(K)_{\text{tors}} \in \bigcup_{k=0}^{\infty} \Phi_{\mathbb{Q}}^{\text{Gal}}(2k+1)$. We give examples of torsion subgroups $E(K)_{\text{tors}} \in \Phi_{\mathbb{Q}}^{\text{Gal}}(d)$ for a few critically important $d$. Then we prove that these torsion subgroups can be base extended to any Galois field of degree $D$, where $d \mid D$ without adding additional torsion. After working to restrict the fields of definitions for certain torsion subgroups to select critical degrees $d$, we are then able to classify the possible torsion subgroups $E(K)_{\text{tors}} \in \Phi_{\mathbb{Q}}^{\text{Gal}}(d)$ in the case of odd $d$ based on the factorization of $d$.

## 6.2 Points of Prime Order

We must first find the possible prime orders for points on rational elliptic curves over odd degree Galois number fields. Unlike our result in the nonic case, we do not have a complete classification of the possible prime orders for points on rational elliptic curves over arbitrary (Galois) number fields of degree $d$. However, we can make use of the restrictions on points of prime order that isogeny conditions force upon the elliptic curve. This allows us to prove the following:

**Lemma 6.1.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be an odd degree Galois field. If $P \in E(K)_{tors}$ is a point of prime order $p$, then*

$$p \in \{2, 3, 5, 7, 11, 13, 19, 43, 67, 163\}.$$

*Proof.* Because $\Phi(1) \subseteq \Phi(d)$ for all $d$ and observing that points of prime order 2 occur for elliptic curves $E(\mathbb{Q})$, points of order $p = 2$ are possible. In fact, this shows points of order 2, 3, 5, and 7 are possible. Now let $p$ be an odd prime. By Lemma 5.9, $E(K)_{\text{tors}}$ cannot contain full $p$-torsion so that $E(K)[p] \cong \mathbb{Z}/p\mathbb{Z}$. But by Lemma 5.10, this implies that $E(K)_{\text{tors}}$ has a rational $p$-isogeny. From Theorem 3.24, we know this is only possible for

$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$. Finally by Corollary 4.54, we note that points of prime order 17 and 37 occur if and only if $8 \mid d$ and $12 \mid d$, respectively, which obviously cannot occur if $d$ is odd. □

In fact in [GJN20b], González-Jiménez and Najman prove that if $P$ is a point of order $p$ for an elliptic curve $E/\mathbb{Q}$, the possible degrees for the field of definition of $P$ are the ones in Table 6.1 with the starred degrees occurring only for elliptic curves $E/\mathbb{Q}$ with CM. In the case of $p = 37$, these degrees are the only ones possible. In fact, we are able to say more about the fields of definition for these possible prime orders. For ease of reference, we restate the results of González-Jiménez and Najman.

Table 6.1: Orders for the field of definition for points of order $p = 17, 37$

| $p$ | $[\mathbb{Q}(P)\colon \mathbb{Q}]$ |
|---|---|
| 17 | $8, 16, 32^*, 136, 256^*, 272, 288$ |
| 37 | $12, 36, 72^*, 444, 1296^*, 1332, 1368$ |

**Theorem 4.53** ([GJN20b, Thm. 5.8])**.** *Let $E/\mathbb{Q}$ be an elliptic curve, $p$ a prime and $P$ a point of order $p$ in $E$. Then all of the cases in table 4.1 occur for $p \leq 13$ or $p = 37$, and they are the only ones possible. The degrees in Table 4.1 with an asterisk occur only when $E$ has CM. For all other $p$, the possibilities for $[\mathbb{Q}(P)\colon \mathbb{Q}]$ are as is given below. The degrees in equations 4.3–4.5 occur only for CM elliptic curves $E/\mathbb{Q}$. Furthermore, the degrees in equation 4.5 occur only for elliptic curves with $j$-invariant 0. If a given conjecture is true, c.f.* [GJN20b, Conj. 3.5]*, then the degrees in equations 4.6 also occur only for elliptic*

*curves with $j$-invariant 0.*

$$p^2-1 \qquad \text{for all } p, \tag{4.1}$$

$$8, 16, 32^*, 136, 256^*, 272, 288 \qquad \text{for } p=17, \tag{4.2}$$

$$(p-1)/2, p-1, p(p-1)/2, p(p-1) \qquad \text{if } p \in \{19, 43, 67, 163\} \tag{4.3}$$

$$2(p-1), (p-1)^2 \qquad \text{if } p \equiv 1 \mod 3 \text{ or } \left(\frac{-D}{p}\right)=1 \text{ for any } D \in CM \tag{4.4}$$

$$(p-1)^2/3, 2(p-1)^2/3 \qquad p \equiv 4, 7 \mod 9 \tag{4.5}$$

$$(p^2-1)/3, 2(p^2-1)/3 \qquad p \equiv 2, 5 \mod 9 \tag{4.6}$$

*where* $CM = \{1, 2, 7, 11, 19, 43, 67, 163\}$. *Apart from the cases above that have been proven to appear, the only other options that might be possible are:*

$$(p^2-1)/3, 2(p^2-1)/3 \quad \text{if } p \equiv 8 \mod 9. \tag{4.7}$$

| $p$ | $[\mathbb{Q}(P)\colon \mathbb{Q}]$ |
|---|---|
| 2 | 1, 2, 3 |
| 3 | 1, 2, 3, 4, 6, 8 |
| 5 | 1, 2, 4, 5, 8, 10, 16, 20, 24 |
| 7 | 1, 2, 3, 6, 7, 9, 12, 14, 18, 21, 24*, 36, 42, 48 |
| 11 | 5, 10, 20*, 40*, 55, 80*, 100*, 110, 120 |
| 13 | 3, 4, 6, 12, 24*, 39, 48*, 52, 72, 78, 96, 144*, 156, 168 |
| 37 | 12, 36, 72*, 444, 1296*, 1332, 1368 |

**Theorem 4.51** ([GJN20b, Prop. 4.6])**.** *Let $E/F$ be an elliptic curve over a number field $F$, $n$ a positive integer, $P \in E(\overline{F})$ be a point of order $p^{n+1}$. Then $[F(P)\colon F(pP)]$ divides $p^2$ or $(p-1)p$.*

## 6.3 Bounding the $p$-Sylow Subgroups

We now know the possible prime orders for points $P \in E(K)_{\text{tors}}$, where $E/\mathbb{Q}$ is a rational elliptic curve, and $K/\mathbb{Q}$ is an odd degree Galois field. Now we need to bound the possible Sylow $p$-subgroups. However at this stage, this is almost trivial. We have already bounded the 2-Sylow subgroup in classifying $\Phi_{\mathbb{Q}}^{\text{Gal}}(9)$. The others follow immediately from Lemma 5.9 and Lemma 5.10 along with Theorem 3.24.

**Lemma 6.2.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be an odd degree Galois field. Then $E(K)[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.*

*Proof.* By Lemma 5.9, $E(K)_{\text{tors}}$ cannot contain full $n$-torsion for any $n > 2$. Then we know that $E(K)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^n\mathbb{Z}$ for some nonnegative integer $n$. If $E$ has CM and contains full 2-torsion, then by Theorem 4.19, we know $E(K)[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. If $E$ does not have CM, using $s = 1$ in Theorem 5.3 shows that if $N \geq 4$, then $[K\colon \mathbb{Q}]$ is divisible by 2, which is impossible. Then if $E(K)_{\text{tors}}$ contains full 2-torsion, we know $E(K)_{\text{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. We need now only consider the case where $E(K)_{\text{tors}}$ does not contain full 2-torsion, i.e. the case where $E(K)[2^\infty] \cong \mathbb{Z}/2^n\mathbb{Z}$ for some $n$.

We show that $E(K)_{\text{tors}}$ cannot contain $\mathbb{Z}/16\mathbb{Z}$. We know that points of order 2 in $E(K)_{\text{tors}}$ can only occur over fields of degree 1, 2, or 3. Because $K/\mathbb{Q}$ has odd degree, points of order 2 cannot be defined over a quadratic field. Now if $E(\mathbb{Q})[2] \ncong \{\mathcal{O}\}$, then by Lemma 4.44, we know that $E(\mathbb{Q})[2^\infty] \supseteq \mathbb{Z}/16\mathbb{Z}$, which contradicts Mazur's classification of $\Phi(1)$, c.f. Theorem 4.2. Then it must be that the points of order 2 are defined over a cubic field, say $F$. But as $K/\mathbb{Q}$ is an odd degree Galois field, and $3 = [F\colon \mathbb{Q}] = |\operatorname{Gal}(K/\mathbb{Q})\colon \operatorname{Gal}(K/F)|$ is the smallest prime dividing $|\operatorname{Gal}(K/\mathbb{Q})|$, $\operatorname{Gal}(K/F)$ is a normal subgroup of $\operatorname{Gal}(K/\mathbb{Q})$ so that by the Galois correspondence, $F/\mathbb{Q}$ is a cubic Galois extension. But then choosing a model $E : y^2 = x^3 + Ax + B$, it must be that $x^3 + Ax + B$ splits over $F$, so that $E$ has full

2-torsion over $F \subseteq K$, a contradiction. Then in this case $E(K)[2^\infty] \subseteq \mathbb{Z}/8\mathbb{Z}$. Putting the cases together, we have $E(K)[2^\infty] \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. □

We can also prove a stronger result that the Sylow 2-subgroup is either defined over $\mathbb{Q}$ or a cubic Galois field. A similar result holds for any odd degree number field, but we shall not prove this here.

**Lemma 6.3.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be an odd degree Galois field. Then $E(K)_{tors}[2^\infty] = E(\mathbb{Q})[2^\infty]$ or there is a cubic Galois field, $F$, $\mathbb{Q} \subseteq F \subseteq K$ such that $E(K)[2^\infty] = E(F)[2^\infty]$. In particular, $E(K)_{tors} \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.*

*Proof.* If $E(K)[2^\infty] = \{\mathcal{O}\}$, the result is trivial, so assume there is a point of order 2. If $E(\mathbb{Q})[2] \neq \{\mathcal{O}\}$, then by Lemma 4.44, we know that $E(K)[2^\infty] = E(\mathbb{Q})[2^\infty]$. So assume that $E(\mathbb{Q})[2] = \{\mathcal{O}\}$. Then there is a point of order 2 defined over a cubic field, say $F$. Because $K/\mathbb{Q}$ is Galois, we know that $\widehat{F} \subseteq K$, where $\widehat{F}$ is the Galois closure of $F$. But as $F/\mathbb{Q}$ is a cubic extension and $K/\mathbb{Q}$ has odd degree, it must be that $|\operatorname{Gal}(\widehat{F}/\mathbb{Q})| = 3$. But then $\widehat{F} = F$, and hence $F$ is Galois. Note that choosing a model $y^2 = x^3 + Ax + B$, because $E$ has a point of order 2, $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$, and $F/\mathbb{Q}$ is Galois, it must be that $E(K)[2] = E(F)[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. If $E(K)[2^\infty] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \cong E(F)[2]$, we are done. Otherwise, assume that there is a point of order $2^{n+1}$, say $P$, where $n$ is a positive integer. By Theorem 4.51, the only possible degrees of $[\mathbb{Q}(P)\colon \mathbb{Q}(2P)]$ are 1, 2, or 4. As $K/\mathbb{Q}$ has odd degree and $\mathbb{Q}(P) \subseteq K$, it must then be that $[\mathbb{Q}(P)\colon \mathbb{Q}(2P)] = 1$ for all $n \geq 1$. As the 2-torsion is defined over $F$, we then have $E(K)[2^\infty] = E(F)[2^\infty]$. By Mazur's classification of $\Phi(1)$ and Najman's classification of $\Phi_{\mathbb{Q}}(3)$, we see that then $E(K)_{\text{tors}} \subseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, c.f. Theorem 4.2 and Theorem 4.30. □

If one knows Knapp's criterion [Kna92, Thm. 4.2] for halving a point on an elliptic curve,

Lemma 6.3 is not all that surprising. Furthermore, there is a more general result of Gužvić in [Guž19] that if $K$ is an odd degree number field and $E/K$ is an elliptic curve with rational $j$-invariant, then $E(K)_{\text{tors}}$ cannot contain $\mathbb{Z}/16\mathbb{Z}$, c.f. Lemma 4.74. We now easily bound the Sylow $p$-subgroups for odd $p$.

**Lemma 6.4.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be an odd degree Galois field. Then for $p \in \{3, 5, 7, 11, 13, 19, 43, 67, 163\}$, the Sylow $p$-subgroup, $E(K)[p^\infty]$, is bounded as follows:*

$$E(K)[3^\infty] \subseteq \mathbb{Z}/27\mathbb{Z} \qquad E(K)[11^\infty] \subseteq \mathbb{Z}/11\mathbb{Z} \qquad E(K)[43^\infty] \subseteq \mathbb{Z}/43\mathbb{Z}$$
$$E(K)[5^\infty] \subseteq \mathbb{Z}/25\mathbb{Z} \qquad E(K)[13^\infty] \subseteq \mathbb{Z}/13\mathbb{Z} \qquad E(K)[67^\infty] \subseteq \mathbb{Z}/67\mathbb{Z}$$
$$E(K)[7^\infty] \subseteq \mathbb{Z}/7\mathbb{Z} \qquad E(K)[19^\infty] \subseteq \mathbb{Z}/19\mathbb{Z} \qquad E(K)[163^\infty] \subseteq \mathbb{Z}/163\mathbb{Z}.$$

*Proof.* By Lemma 5.9, $E(K)_{\text{tors}}$ cannot contain full $p$-torsion so that $E(K)[p^\infty] \subseteq \mathbb{Z}/p^n\mathbb{Z}$ for some nonnegative integer $n$. But then by Lemma 5.10, $E(K)_{\text{tors}}$ has a rational $p^n$-isogeny. For each prime $p$, we can use Theorem 3.24 to determine the maximal possible $n$ in each case. This yields the bounds given in the statement of the lemma. □

## 6.4 The List of Possible Torsion Subgroups

We can combine all of the data from Lemma 6.2 and Lemma 6.4 to create a list of possible torsion structures for rational elliptic curves over odd degree Galois fields.

**Lemma 6.5.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be an odd degree Galois number field. Then $E(K)_{tors}$ is isomorphic to one of the following (although not all cases*

*need occur):*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 15, 18, 19, 21, 25, 27, 43, 67, 163 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 7, 9, 10, 11, 12, 13, 14, 15, 18, 19, 21, 25, 27, 43, 67, 163. \end{cases}$$

*Proof.* Let $\mathcal{I} = \{2, 7, 8, 11, 13, 19, 25, 27, 43, 67, 163\}$. By Lemma 6.2 and Lemma 6.4, we know that

$$E(K)_{\text{tors}} \subseteq \bigoplus_{n \in \mathcal{I}} \mathbb{Z}/n\mathbb{Z}.$$

One then simply enumerates all possible subgroups of the group above, up to isomorphism. This gives a list of over 10,000 such subgroups. Of course, not all such possibilities are possible for $E(K)_{\text{tors}}$. We only need examine the subgroups of the form $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$. We know by Lemma 5.10 that if $E(K)_{\text{tors}} \cong \mathbb{Z}/n\mathbb{Z}$, then $E$ has an $n$-isogeny. We know also by Lemma 5.11 that if $E(K)_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$, then $E$ has an $n$-isogeny. Using Theorem 3.24, eliminate any subgroup from this list of the form $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$ where $n$ is not a possible degree of an isogeny for a rational elliptic curve. This leaves the 45 remaining possibilities given in the statement of the lemma.[1] □

## 6.5 Eliminating Torsion Subgroups

As stated in Lemma 6.5, not all these subgroups need actually occur for some rational elliptic curve $E/\mathbb{Q}$ and some odd degree Galois field $K/\mathbb{Q}$. We need then eliminate torsion subgroups which do not occur. It will turn out that each of the possibilities of the form $\mathbb{Z}/n\mathbb{Z}$ given in the statement of Lemma 6.5 do occur. So we need only focus on the 'bicyclic' torsion subgroups. We first eliminate the torsion subgroups for the 'bicyclic' torsion

[1] Note one can do this quickly using a coding language of one's choice. Simply enumerate a list of the form $(2^i, 2^j 3^k 5^l 7^m 11^n 13^p 19^q 43^r 67^s 163^t)$, where $i, m, n, p, q, r, s, t \in \{0, 1\}$, $j \in \{0, 1, 2, 3\}$, $k \in \{0, 1, 2, 3\}$, $l \in \{0, 1, 2\}$, and $i \leq j$, representing the possible torsion subgroups. If $i = 0$, then $E$ has a $(2^j 3^k 5^l 7^m 11^n 13^p 19^q 43^r 67^s 163^t)$-isogeny. Otherwise, $E$ has a $(2^{j-1} 3^k 5^l 7^m 11^n 13^p 19^q 43^r 67^s 163^t)$-isogeny. Simply have the algorithm run through all the possibilities and check against the list of possible rational isogenies, printing only those which are possible. This results in the list given in the statement of the lemma.

subgroups corresponding to elliptic curves with an $n$-isogeny occurring for finitely many $j$-invariants. We will make use of the following theorem.

**Theorem 6.6** (Dedekind, c.f. [DF04, Ch. 14.8])**.** *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree $n$, and let $G_f$ be its Galois group. Let $p$ be a prime that does not divide $\Delta_f$, the discriminant of $f$. Let $\overline{f(x)}_p$ denote the reduction of $f(x)$ modulo $p$. If $\overline{f(x)}_p$ is a product of distinct monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree $n_1, \ldots, n_r$, with $\deg f(x) = \sum_i n_i$, then $G_f$ contains a permutation of the roots with cycle type $(n_1, \ldots, n_r)$.*

**Lemma 6.7.** *Let $E/\mathbb{Q}$ be a rational elliptic curve. Then there does not exist an odd degree Galois field $K/\mathbb{Q}$ such that $E(K)_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ for $n \in \{11, 14, 15, 19, 21, 27, 43, 67, 163\}$ or $E(K)_{tors} \cong \mathbb{Z}/15\mathbb{Z}$.*

*Proof.* Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be an odd degree Galois field. Suppose that $n \in \{11, 14, 15, 19, 21, 27, 43, 67, 163\}$. By Lemma 5.11, if $E(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, then $E(K)_{\text{tors}}$ has a rational $n$-isogeny. However by Theorem 3.24, for $n \in \{11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163\}$, there are only finitely many $j$-invariants for rational elliptic curves such that $E$ has a rational $n$-isogeny. Therefore, $E$ must be a twist of an elliptic curve with $j$-invariant given in [LR13, Table 4], c.f. Table 7.4. Using the method of division polynomials, we check each of the primitive factors $f_i$ for $f_{E,n}$. If $f_i$ is of even degree, we can move on because $\mathbb{Q}(f_i) \not\subseteq K$ because $K$ is odd. So suppose that $f_i$ is odd. If $\mathbb{Q}(f_i) \subseteq K$, then because $K/\mathbb{Q}$ is Galois, we know that $\widehat{\mathbb{Q}(f_i)} \subseteq K$, where $\widehat{\mathbb{Q}(f_i)}$ denotes the Galois closure of $\mathbb{Q}(f_i)$. In each case, we can compute the Galois group of $\mathbb{Q}(f_i)$. If the order of the Galois group is even, then clearly we cannot have $\mathbb{Q}(f_i) \subseteq K$. However in some of these cases, the degrees are restrictively large. For instance in the case of $n = 163$, we see this would involve computing the Galois group of a field with degree 13,203. In the cases where the Galois group is obstructively large, we instead apply The-

orem 6.6. We reduce $f_i$ modulo primes $p \nmid \Delta_{f_i}$. This gives us orders of elements in the Galois group. In each case, we see that the Galois group contains an element of even order so that the Galois group must have even order. But then we cannot have $\mathbb{Q}(f_i) \subseteq K$. For each $n \in \{11, 14, 15, 19, 21, 27, 43, 67, 163\}$, one of contradictions above arises. Therefore, $E(K)_{\text{tors}} \ncong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ for $n \in \{11, 14, 15, 19, 21, 27, 43, 67, 163\}$. Applying these techniques in the case of $E(K)_{\text{tors}} \cong \mathbb{Z}/15\mathbb{Z}$, i.e. $E$ is a twist of an elliptic curve with $j \in \{-5^2/2, -5^2 \cdot 241^3/2^3, -5 \cdot 29^3/2^5, 5 \cdot 211^3/2^{15}\}$, show that the case of $E(K)_{\text{tors}} \cong \mathbb{Z}/15\mathbb{Z}$ occurs over no odd degree Galois field. □

Eliminating the torsion subgroups precluded by Lemma 6.7, we are left with these remaining torsion subgroups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 14, 18, 19, 21, 25, 27, 43, 67, 163 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 7, 9, 10, 12, 13, 18, 25. \end{cases}$$

**Lemma 6.8.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be an odd degree Galois field. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.*

*Proof.* If $E(\mathbb{Q})[2] \neq \{\mathcal{O}\}$, then by Lemma 4.44, we know that $E(\mathbb{Q})[2^\infty] \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. By Theorem 4.53, the only possible odd degrees for the field of definition for a point of order three is 1 or 3. In either case, this implies that there is a rational elliptic curve $E$ and a cubic field $F$ such that $E(F)_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, contradicting the classification of $\Phi_{\mathbb{Q}}(3)$, c.f. Theorem 4.30.

So it must be that $E(\mathbb{Q})[2] = \{\mathcal{O}\}$. Choose a model $y^2 = x^3 + Ax + B$ for $E$. As $E(K)_{\text{tors}}$ contains full 2-torsion and $K/\mathbb{Q}$ has odd degree, it must be that there is a cubic subfield

$\mathbb{Q} \subseteq F \subseteq K$ that is a splitting field for $x^3 + Ax + B$. In particular, we know that $F/\mathbb{Q}$ is Galois. Now let $P \in E(K)_{\text{tors}}$ be a point of order 4. By Proposition 4.51, we know that $[\mathbb{Q}(P)\colon \mathbb{Q}(2P)]$ divides 4 or 2. As $\mathbb{Q}(P) \subseteq K$, it must be that $[\mathbb{Q}(P)\colon \mathbb{Q}(2P)] = 1$. But then the field of definition for the point $P$ must be the same as the field of definition for the point $2P$, which must be $F$. But then the point $P$ is defined over $F$. Then $E(F)_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. But in [GJNT16], if $F$ is a cubic field with $E(F)_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, it must be that $E(\mathbb{Q})_{\text{tors}}$ is nontrivial, a contradiction. □

We could have also used a more general result of Gužvić which proves that no elliptic curve with rational $j$-invariant defined over an odd degree number field can contain a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, see [Guž19, Lem. 3.10]. Eliminating the torsion subgroups precluded by Lemma 6.8, we are left with these remaining torsion subgroups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 14, 18, 19, 21, 25, 27, 43, 67, 163 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 5, 7, 9, 10, 13, 25. \end{cases}$$

**Lemma 6.9.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be an odd degree Galois field. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.*

*Proof.* If $E(\mathbb{Q})[2] \neq \{\mathcal{O}\}$, then by Lemma 4.44, we know that $E(\mathbb{Q})_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Theorem 4.53, the only possible odd degrees for the field of definition for a point of order five is 1 or 5. In either case, this implies there is a rational elliptic curve and a quintic field $F$ such that $E(F)_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, contradicting the classification of $\Phi_{\mathbb{Q}}(5)$, c.f. Theorem 4.37.

Then we must have $E(\mathbb{Q})[2] = \{\mathcal{O}\}$. By Lemma 5.10, we know that $E$ has a 5-isogeny. In

particular, by [LR13, Table 3], c.f. Table 7.3, we know that $E$ is a twist of an elliptic curve with $j$-invariant given by

$$j = \frac{(h^2 + 10h + 5)^3}{h}$$

for some $h \in \mathbb{Q}^\times$. Choose a model $y^2 = x^3 + Ax + B$ for $E$. As $E$ has full 2-torsion, we know that there is a cubic subfield, say $F$, with $\mathbb{Q} \subseteq F \subseteq K$ that is a splitting field for $x^3 + Ax + B$. But then $F/\mathbb{Q}$ is Galois. In particular, we know that $\mathrm{disc}(x^3 + Ax + B)$ is a square. This implies that there is a $q \in \mathbb{Q}$ with

$$q^2 = \frac{136048896h(h^2 + 10h + 5)^6}{(h^2 + 4h - 1)^6(h^2 + 22h + 125)^3}.$$

Absorbing squares into the left side, we see that this implies there is a rational point $(n, m)$ on the curve $n^2 = m^3 + 22h^2 + 125h$. This is the elliptic curve $E$ with Cremona label 20a3. Using SAGE, we find that $E$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. We see that the only solution corresponds to a cusp for $j$. □

We have already eliminated the case that $E(K)_{\mathrm{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$ in Lemma 5.25. Eliminating the torsion subgroups precluded by this observation and Lemma 6.9, we are left with these remaining torsion subgroups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 14, 18, 19, 21, 25, 27, 43, 67, 163 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7, 13. \end{cases}$$

**Lemma 6.10.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be an odd degree Galois field. Then $E(K)_{tors}$ does not contain a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$.*

*Proof.* If $E(K)_{\mathrm{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$, then by Lemma 5.11, we know that $E$ has a rational

13-isogeny. In particular, by [LR13, Table 3], c.f. Table 7.3, we know that $E$ is a twist of an elliptic curve with $j$-invariant given by

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

for some $h \in \mathbb{Q}^\times$. By Theorem 4.88, we know that $E$ cannot have any 2-isogenies. But then $E(\mathbb{Q})[2] = \{\mathcal{O}\}$. Choose a model $y^2 = x^3 + Ax + B$ for $E$. Then there is a cubic subfield $\mathbb{Q} \subseteq F \subseteq K$ that is a splitting field for $x^3+Ax+B$. But then $F/\mathbb{Q}$ is Galois so that $\operatorname{disc} E$ is a square. Again by absorbing squares, this implies there is a rational point on the curve $M^2 = h(h^2+6h+13)$. This is an elliptic curve with Cremona label 52a2. Using SAGE, we find that this elliptic curve is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and all the rational solutions correspond to cusps. □

Then by Lemma 6.10, we are left with these remaining torsion subgroups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1,2,\ldots,14,18,19,21,25,27,43,67,163 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1,2,3,4,7. \end{cases}$$

Each one of these possibilities will occur for some rational elliptic curve over some odd degree Galois field.

## 6.6 Base Extension

We will now prove that if $E(K)_{\text{tors}} \in \Phi_{\mathbb{Q}}^{\text{Gal}}(d')$, then $E(K)_{\text{tors}} \in \Phi_{\mathbb{Q}}^{\text{Gal}}(d)$ for all $d$ with $d' \mid d$. Suppose that $d = nd'$. We will show that we can construct a Galois number field of degree $n$, say $L$, such that $L \cap K = \mathbb{Q}$. Then the compositum $LK$ will be a Galois number field of degree $nd' = d$ and $E(LK)_{\text{tors}} \cong E(K)_{\text{tors}}$. We begin with a theorem of Minkowski, see [Neu99, Thm. 2.17].

**Theorem 6.11** (Minkowski)**.** *For any number field $K \neq \mathbb{Q}$,* $\operatorname{disc} K \neq \pm 1$*. In particular, there is a prime that ramifies in $K$, so that there are no unramified extensions of $\mathbb{Q}$.*

**Corollary 6.12.** *If $K, L$ are number fields with* $\gcd(\operatorname{disc} K, \operatorname{disc} L) = 1$*, then $K \cap L = \mathbb{Q}$.*

*Proof.* Let $p$ be a prime and suppose that $p$ ramifies in $K \cap L$. Then $p$ ramifies in both $K$ and $L$. If $\mathfrak{p}$ is a prime of $K \cap L$ lying over $p$, then the degree of $\mathfrak{p}$ over $p$ must be greater than 1. Then if $\mathfrak{P}$ is a prime of $K$ lying over $\mathfrak{p}$, then

$$e(\mathfrak{P} \mid \mathfrak{p}) = e(\mathfrak{P} \mid \mathfrak{p})\, e(\mathfrak{p} \mid p) > 1.$$

Now $\mathfrak{P}$ ramifies in $K$ so that $p$ divides $\operatorname{disc} K$. Mutatis mutandis, $p$ divides $\operatorname{disc} L$. This contradicts the fact that $\gcd(\operatorname{disc} K, \operatorname{disc} L) = 1$. Therefore by Theorem 6.11, it must be that $K \cap L = \mathbb{Q}$. □

We now state the well-known and amazing result of Dirichlet on primes in arithmetic progression.

**Theorem 6.13** (Dirichlet,[Dir37])**.** *For every natural number $n$, there are infinitely many primes with $p \equiv a \mod n$, where* $\gcd(a, n) = 1$*. In particular, there are infinitely many primes $p$ with $p \equiv 1 \mod n$.*

As groundbreaking as it was, now it has sadly been reduced to an exercise, c.f. [DF04, Ch. 13.6, Ex. 8], which only uses cyclotomic polynomials to prove the theorem, or [Neu99, Ch. 1,§10, Ex. 1] for the case of $a = 1$.

**Lemma 6.14.** *Let $d > 1$ be a positive integer. Then there are infinitely many non-*

*isomorphic Galois fields of degree $d$.*

*Proof.* Suppose that $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ is the prime factorization for $d$. For each $i$, we use Theorem 6.13 to choose distinct primes $q_i$ so that $q_i \equiv 1 \mod p_i^{a_i}$. The field $K_i = \mathbb{Q}(\zeta_{q_i})$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/q_i\mathbb{Z})^\times$. Observe that $\mathrm{Gal}(K/\mathbb{Q})$ is abelian and $p_i^{a_i}$ divides $q_i - 1$ so that there is a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ with index $p_i^{a_i}$. By the Fundamental Theorem of Galois Theory, there is an abelian Galois subfield of $K_i$, say $F_i$, of degree $p_i^{a_i}$.

We know that $\operatorname{disc} K_i = (-1)^{\frac{q_i-1}{2}} q_i^{q_i-2}$ and $\operatorname{disc} F_i$ necessarily divides $\operatorname{disc} K_i$. Therefore, the only prime factor of $\operatorname{disc} F_i$ is $q_i$. But then $\gcd(F_i, F_j) = 1$ for $i \neq j$. By Corollary 6.12, $F_i \cap F_j = \mathbb{Q}$ for $i \neq j$. Let $K = F_1 F_2 \cdots F_r$. Because $K$ is a compositum of Galois fields, $K(q_1, \ldots, q_r)$ is necessarily Galois with

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(F_1/\mathbb{Q}) \times \cdots \mathrm{Gal}(F_r/\mathbb{Q}) = \mathbb{Z}/p_1^{a_1} \times \cdots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z}.$$

Furthermore as $F_i \cap F_j = \mathbb{Q}$ for $i \neq j$, $K$ has degree $|F_1||F_2| \cdots |F_r| = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = d$. There are infinitely many choices for $q_1, \ldots, q_r$, each corresponding to a unique field $K$. Therefore, there are infinitely many non-isomorphic Galois fields of degree $d$. □

We now prove the claim we stated at the beginning of this section.

**Proposition 6.15.** *Let $d', d$ be positive integers with $d' \mid d$. If $E(K)_{tors} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d')$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$.*

*Proof.* By Theorem 4.1, a fortiori, we know that for all $d$, the sets $\Phi_{\mathbb{Q}}(d) \supseteq \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ are uniformly bounded. Let $N$ be the least common multiple of all possible orders for torsion subgroups $E(F)_{\mathrm{tors}} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d')$. We know that $M := \mathbb{Q}(E[N])$ is a finite Galois extension of

$\mathbb{Q}$. In particular, it has finitely many subfields. Suppose that $d = nd'$. By Lemma 6.14, we know that we can choose a Galois number field, say $L$, of degree $n$ with $L \cap M = \mathbb{Q}$. The compositum $LK$ is a Galois number field of degree $nd' = n$. Moreover because $L \cap K = \mathbb{Q}$, $E(K)_{\text{tors}}$ does not gain any torsion when base extending to the compositum. But then $E(K)_{\text{tors}} \in \Phi_{\mathbb{Q}}^{\text{Gal}}(d)$. □

Note that we did not need to invoke Theorem 4.1 if we restricted ourselves to odd degree Galois number fields because our previous work (even using the non-sharp bounds given in Lemma 6.5) has already shown that the possibilities for $\Phi_{\mathbb{Q}}^{\text{Gal}}(d)$ are uniformly bounded for all odd $d \geq 1$. Furthermore, if $E(K)_{\text{tors}} \in \Phi_{\mathbb{Q}}(d')$ (not necessarily in $\Phi_{\mathbb{Q}}^{\text{Gal}}(d)$), we can use the same construction in Proposition 6.15 to show that $E(K)_{\text{tors}} \in \Phi_{\mathbb{Q}}(d)$ (the field we construct has degree $nd' = d$, c.f. [DF04, Ch. 14.4, Cor. 20], but is not necessarily Galois). This recovers the following well-known result.

**Corollary 6.16.** *Let $d', d$ be positive integers with $d' \mid d$. If $E(K)_{tors} \in \Phi_{\mathbb{Q}}(d')$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(d)$.*

## 6.7 Fields of Definition

We will now give some results on what are the possible degrees for number fields over which these various torsion subgroups can occur. Because $\Phi(1) \subseteq \Phi_{\mathbb{Q}}^{\text{Gal}}(d) \subseteq \Phi_{\mathbb{Q}}(d)$ for all $d$, we need only focus our attention on torsion subgroups not already in $\Phi(1)$. We break the cases by their method of proof.

**Lemma 6.17.** *Suppose that $p \in \{11, 13, 19, 43, 67, 163\}$. Then $\mathbb{Z}/p\mathbb{Z} \in \Phi_{\mathbb{Q}}(d)$ if and only if $d_n \mid d$, where $d_n$ is given in the table below. Furthermore, we can find an elliptic curve $E/\mathbb{Q}$ and Galois field $K$ such that $E(K)_{tors} \cong \mathbb{Z}/p\mathbb{Z}$ for each such $d_n$. Hence, $\mathbb{Z}/p\mathbb{Z} \in$*

$\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ *if and only if* $d_n \mid d$.

| $n$ | 11 | 13 | 19 | 43 | 67 | 163 |
|---|---|---|---|---|---|---|
| $d_n$ | 5 | 3 | 9 | 21 | 33 | 81 |

*Proof.* We know that $\mathbb{Z}/p\mathbb{Z} \in \Phi_{\mathbb{Q}}(d)$ if and only if there is a number field of degree $d$ such that the $p$-torsion for $E/\mathbb{Q}$ is defined. Theorem 4.53 gives the possible degrees for the field of definition for each $p \in \{11, 13, 19, 43, 67, 163\}$. For each $p$, we see that the possible degrees are all divisible by the $d_n$ given in the table. Using base extension, it suffices to prove that each torsion subgroup occurs over a (Galois) number field of degree $d_n$.[2] From Table 6.2, we see that each such possibility occurs for a rational elliptic curve defined over a number field of degree $d_n$. In fact, each field in Table 6.2 is Galois. By Proposition 6.15 and Corollary 6.16, we see that $E(K)_{\mathrm{tors}} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d) \subseteq \Phi_{\mathbb{Q}}(d)$. □

Table 6.2: Examples such that $\mathbb{Z}/p\mathbb{Z} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d_n) \subseteq \Phi_{\mathbb{Q}}(d_n)$ for $p \in \{11, 13, 19, 43, 67, 163\}$

| $E(K)_{\mathrm{tors}}$ | Cremona Label | Field |
|---|---|---|
| $\mathbb{Z}/11\mathbb{Z}$ | 121c1 | $\mathbb{Q}(\zeta_{11})^+$ |
| $\mathbb{Z}/13\mathbb{Z}$ | 147b1 | $\mathbb{Q}(\zeta_7)^+$ |
| $\mathbb{Z}/19\mathbb{Z}$ | 361a1 | $\mathbb{Q}(\zeta_{19})^+$ |
| $\mathbb{Z}/43\mathbb{Z}$ | 1849a1 | N/A |
| $\mathbb{Z}/67\mathbb{Z}$ | 4489a1 | N/A |
| $\mathbb{Z}/163\mathbb{Z}$ | 26569a1 | N/A |

**Lemma 6.18.** *Suppose that $d > 1$ is an odd integer, and $n \in \{14, 18, 21, 25, 27\}$. Then $\mathbb{Z}/n\mathbb{Z} \in \Phi_{\mathbb{Q}}(d)$ if and only if $d_n \mid d$, where $d_n$ is given in the table below. Furthermore, we can find an elliptic curve $E/\mathbb{Q}$ and Galois field $K$ such that $E(K)_{tors} \cong \mathbb{Z}/n\mathbb{Z}$ for each such $d_n$. Hence, $\mathbb{Z}/n\mathbb{Z} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ if and only if $d_n \mid d$.*

*Proof.* Suppose that $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/14\mathbb{Z}$. By the proof of Lemma 6.3, we know that the

[2] For the 'larger' $p$, these are defined over number fields not currently contained in the LMFDB and are formed by adjoining a root of a tediously long polynomial, which we shall not give. Instead, we write "N/A." To find the field, simply compute and factor the division polynomial. Search through the factors for the irreducible factor with the given degree $d_n$—there will only be one such factor in each case. One can verify that $E$ has the specified torsion over that field, as well as check that the field is indeed Galois.

| $n$ | 14 | 18 | 21 | 25 | 27 |
|---|---|---|---|---|---|
| $d_n$ | 3 | 3 | 3 | 5 | 9 |

point of order 2 must be defined over $\mathbb{Q}$. From Theorem 4.53, the point of order 7 is defined either defined over $\mathbb{Q}$, a septic field, or a field of degree divisible by 3. If the 7-torsion is defined over $\mathbb{Q}$ or a septic field, in either case, this implies that $\mathbb{Z}/14\mathbb{Z} \in \Phi_{\mathbb{Q}}(7)$, contradicting Theorem 4.40. Then the field of definition of the 7-torsion has degree divisible by 3. Table 6.3 shows that we do have $E(F)_{\text{tors}} \cong \mathbb{Z}/14\mathbb{Z}$ for some rational elliptic curve $E$ and some cubic (Galois) field $F$. Then by Proposition 6.15 and Corollary 6.16, we see that there is a field $F'$ such that $E(F')_{\text{tors}} \cong \mathbb{Z}/14\mathbb{Z} \in \Phi_{\mathbb{Q}}^{\text{Gal}}(d) \subseteq \Phi_{\mathbb{Q}}(d)$.

Suppose that $E(K)_{\text{tors}} \cong \mathbb{Z}/18\mathbb{Z}$. By the proof of Lemma 6.3, we know that the point of order 2 must be defined over $\mathbb{Q}$. Because $K/\mathbb{Q}$ has odd degree, by Theorem 4.53, the point of order 3 is defined over $\mathbb{Q}$ or a cubic field. In the latter case, we are done because this implies that $[K\colon \mathbb{Q}]$ is divisible by 3. Assume then that the point of order 3 is defined over $\mathbb{Q}$. Let $P$ be the point of order 9. By Theorem 4.51 and using the fact that $\mathbb{Q}(3P) = \mathbb{Q}$, we know that $[\mathbb{Q}(P)\colon \mathbb{Q}]$ is in the set $\{1, 2, 3, 6, 9\}$. By Mazur's classification of $\Phi(1)$, we know there are no points of order 18 on elliptic curves $E(\mathbb{Q})$, c.f. Theorem 4.2. Then we know $[\mathbb{Q}(P)\colon \mathbb{Q}] \neq 1$. Because $K/\mathbb{Q}$ has odd degree, this means that we must have $[\mathbb{Q}(P)\colon \mathbb{Q}] \in \{3, 9\}$. But then in either case, $[\mathbb{Q}(P)\colon \mathbb{Q}]$ must then be divisible by 3. Table 6.3 shows that we do have $E(F)_{\text{tors}} \cong \mathbb{Z}/18\mathbb{Z}$ for some rational elliptic curve $E$ and cubic (Galois) field $F$. Then by Proposition 6.15 and Corollary 6.16, we see that there is a field $F'$ such that $E(F')_{\text{tors}} \cong \mathbb{Z}/18\mathbb{Z} \in \Phi_{\mathbb{Q}}^{\text{Gal}}(d) \subseteq \Phi_{\mathbb{Q}}(d)$.

Suppose that $E(K)_{\text{tors}} \cong \mathbb{Z}/21\mathbb{Z}$. Because $K/\mathbb{Q}$ has odd degree, by Theorem 4.53, we know that the point of order of order 3 is defined over $\mathbb{Q}$ or a cubic field, and the point of order 7 is defined over $\mathbb{Q}$, a septic field, or a field of degree divisible by 3. Then the only way $[K\colon \mathbb{Q}]$ is not divisible by 3 is if the 3-torsion is defined over $\mathbb{Q}$ and the 7-torsion

is defined over a septic field. But this would imply that $\mathbb{Z}/21\mathbb{Z} \in \Phi_{\mathbb{Q}}(7)$, contradicting Theorem 4.40. Therefore, $3 \mid [K\colon \mathbb{Q}]$. Table 6.3 shows that we do have $E(F)_{\text{tors}} \cong \mathbb{Z}/21\mathbb{Z}$ for some rational elliptic curve $E$ and cubic (Galois) field $F$. Then by Proposition 6.15 and Corollary 6.16, we see that there is a field $F'$ such that $E(F')_{\text{tors}} \cong \mathbb{Z}/21\mathbb{Z} \in \Phi_{\mathbb{Q}}^{\text{Gal}}(d) \subseteq \Phi_{\mathbb{Q}}(d)$.

Suppose that $E(K)_{\text{tors}} \cong \mathbb{Z}/25\mathbb{Z}$. Let $P$ be a point of order $5^n$ for $n > 1$ on a rational elliptic curve $E'/\mathbb{Q}$. By Theorem 4.51, we know that $[\mathbb{Q}(P)\colon \mathbb{Q}(5P)]$ is in the set $\{1, 2, 4, 5, 10, 20, 25\}$ for all $n \geq 1$. For the case where $n = 1$, because $K/\mathbb{Q}$ has odd degree, Theorem 4.53 says that the point of order 5 is defined over $\mathbb{Q}$ or a quintic field. Because $K/\mathbb{Q}$ has odd degree, if $P$ is a point of order $5^n$ for $n \geq 1$, the only way for $[K\colon \mathbb{Q}]$ to not be divisible by 5 is for $[\mathbb{Q}(P)\colon \mathbb{Q}(5P)] = 1$ for all $n$. But this implies there is a point $P$ of order 25 defined over $\mathbb{Q}$ on $E$, contradicting Mazur's classification of $\Phi(1)$. Therefore, $[K\colon \mathbb{Q}]$ is divisible by 5. Table 6.3 shows that we do have $E(F)_{\text{tors}} \cong \mathbb{Z}/25\mathbb{Z}$ for some rational elliptic curve $E$ and quintic (Galois) field $F$. Then by Proposition 6.15 and Corollary 6.16, we see that there is a field $F'$ such that $E(F')_{\text{tors}} \cong \mathbb{Z}/25\mathbb{Z} \in \Phi_{\mathbb{Q}}^{\text{Gal}}(d) \subseteq \Phi_{\mathbb{Q}}(d)$.

Finally, suppose that $E(K)_{\text{tors}} \cong \mathbb{Z}/27\mathbb{Z}$. By Theorem 4.53 and the fact that $K/\mathbb{Q}$ has odd degree, we know that the point of order 3 is defined over $\mathbb{Q}$ or a cubic field. By Theorem 4.53, we know also that for a point of order $3^{n+1}$, say $P$, where $n$ is a positive integer, that $[\mathbb{Q}(P)\colon \mathbb{Q}(3P)] \in \{1, 2, 3, 6, 9\}$. If $\mathbb{Q}(P)$ is contained in an odd degree field, then $[\mathbb{Q}(P)\colon \mathbb{Q}(3P)] \in \{1, 3, 9\}$. Let $P \in E(K)_{\text{tors}}$ be the point of order 27. We know then that $[\mathbb{Q}(P)\colon \mathbb{Q}] = 3^m$ for some $m \geq 0$. But if $m \in \{0, 1\}$, then $\mathbb{Z}/27\mathbb{Z} \in \Phi_{\mathbb{Q}}(3)$, contradicting Theorem 4.30. Then $m \geq 2$ so that $[\mathbb{Q}(P)\colon \mathbb{Q}]$, and hence $[K\colon \mathbb{Q}]$, is divisible by 9. Table 6.3 shows that we do have $E(F)_{\text{tors}} \cong \mathbb{Z}/27\mathbb{Z}$ for some rational elliptic curve $E$ and nonic (Galois) field $F$. Then by Proposition 6.15 and Corollary 6.16, we see that there is a field $F'$ such that $E(F')_{\text{tors}} \cong \mathbb{Z}/27\mathbb{Z} \in \Phi_{\mathbb{Q}}^{\text{Gal}}(d) \subseteq \Phi_{\mathbb{Q}}(d)$. □

Table 6.3: Examples such that $\mathbb{Z}/n\mathbb{Z} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d_n) \subseteq \Phi_{\mathbb{Q}}(d_n)$ for $n \in \{14, 18, 21, 25, 27\}$

| $E(K)_{\mathrm{tors}}$ | Cremona Label | Field |
|---|---|---|
| $\mathbb{Z}/14\mathbb{Z}$ | 49a4 | $\mathbb{Q}(\zeta_7)^+$ |
| $\mathbb{Z}/18\mathbb{Z}$ | 14a6 | $\mathbb{Q}(\zeta_7)^+$ |
| $\mathbb{Z}/21\mathbb{Z}$ | 162b1 | $\mathbb{Q}(\zeta_9)^+$ |
| $\mathbb{Z}/25\mathbb{Z}$ | 11a3 | $\mathbb{Q}(\zeta_{11})^+$ |
| $\mathbb{Z}/27\mathbb{Z}$ | 27a4 | $\mathbb{Q}(\zeta_{27})^+$ |

For the case of $\mathbb{Z}/27\mathbb{Z}$ in Lemma 6.18, if we restricted ourselves to the case of Galois fields, observe we could have instead used the fact that $E$ would have a rational 21-isogeny (which occurs for finitely many $j$-invariants), and then used the method of division polynomials.

**Lemma 6.19.** *If $d$ is odd, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \in \Phi_{\mathbb{Q}}(d)$ if and only if $3 \mid d$. Furthermore, we can find an elliptic curve $E/\mathbb{Q}$ and Galois field $K$ such that $E(K)_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ for each such $d$. Hence, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ if and only if $3 \mid d$.*

*Proof.* By Theorem 4.53, the only odd field degrees over which a point of order 2 is defined is 1 or 3, and the only odd field degrees over which a point of order 7 is defined is 1, 7, or an odd integer divisible by 3. The only way that 3 does not divide $d$ is if the points of order 2 are defined over $\mathbb{Q}$, and the point of order 7 is defined over either $\mathbb{Q}$ or a field of degree 7. In either case, this implies that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \in \Phi(7)$, contradicting Theorem 4.40. Therefore, 3 divides $d$. The elliptic curve with Cremona label 1922e2 has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over the field $\mathbb{Q}(x^3 - x^2 - 10x + 8)$. By Proposition 6.15 and Corollary 6.16, we see that $E(K)_{\mathrm{tors}} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d) \subseteq \Phi_{\mathbb{Q}}(d)$. □

Table 6.4: An elliptic curve $E/\mathbb{Q}$ with $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ for some odd degree Galois field $K$

| $E(K)_{\mathrm{tors}}$ | Cremona Label | Field |
|---|---|---|
| $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ | 1922e2 | $\mathbb{Q}(x^3 - x^2 - 10x + 8)$ |

## 6.8 Odd Order Galois Fields with Small Degree

### 6.8.1 The Case of Cubic Galois Fields

Recall that Najman classified the torsion subgroups for rational elliptic curves over cubic fields in [Naj16], c.f. Theorem 4.30, which we shall restate here:

**Theorem 4.30** ([Naj16, Thm. 2])**.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a cubic number field. Then $E(K)_{tors}$ is isomorphic to precisely one of the following groups:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7. \end{cases}$$

*Moreover, each of these groups, except for $\mathbb{Z}/21\mathbb{Z}$, occurs over some cubic field for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes. The elliptic curve `162b1` over $\mathbb{Q}(\zeta_9)^+$ is the unique rational elliptic curve with torsion $\mathbb{Z}/21\mathbb{Z}$.*

By Proposition 6.15 for every torsion subgroup in $G \in \Phi(1)$, we can find a cubic Galois field so that $G \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(3)$. It remains to show that every torsion subgroup in $\Phi_{\mathbb{Q}}(3) \setminus \Phi(1)$ occurs for some rational elliptic curve over some cubic Galois field. Table 6.5 completes the demonstration that every torsion subgroup in $\Phi_{\mathbb{Q}}(3)$ occurs for some elliptic curve over some cubic Galois field. That is, we have $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(3) = \Phi_{\mathbb{Q}}(3)$.

Table 6.5: Torsion subgroups in $\Phi_{\mathbb{Q}}(3) \setminus \Phi(1)$ occurring over cubic Galois fields

| Torsion Subgroup | Elliptic Curve | Cubic Galois Field |
|---|---|---|
| $\mathbb{Z}/13\mathbb{Z}$ | `147b1` | $\mathbb{Q}(\zeta_7)^+$ |
| $\mathbb{Z}/14\mathbb{Z}$ | `49a3` | $\mathbb{Q}(\zeta_7)^+$ |
| $\mathbb{Z}/18\mathbb{Z}$ | `14a4` | $\mathbb{Q}(\zeta_7)^+$ |
| $\mathbb{Z}/21\mathbb{Z}$ | `162b1` | $\mathbb{Q}(\zeta_9)^+$ |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ | `1922c1` | $\mathbb{Q}(x^3 - x^2 - 10x + 8)$ |

**Corollary 6.20.** $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(3) = \Phi_{\mathbb{Q}}(3)$

### 6.8.2 The Case of Quintic Galois Fields

Recall that González-Jiménez classified the torsion subgroups of rational elliptic curves over quintic number fields in [GJ17], c.f. Theorem 4.37, which we restate here.

**Theorem 4.37** ([GJ17, Thm. 1, Thm. 2]). *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a quintic number field. Then $E(K)_{tors}$ is isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 12, 25 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4 \end{cases}$$

*Moreover, each of these groups, except for $\mathbb{Z}/11\mathbb{Z}$, occurs over some quintic field for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes. The only elliptic curves $E/\mathbb{Q}$ with $E(K)_{tors} \cong \mathbb{Z}/11\mathbb{Z}$ over some quintic field $K$ have Cremona label `121a2`, `121c2`, `121b1`. For elliptic curves $E/\mathbb{Q}$ with CM, $\Phi_{\mathbb{Q}}^{\mathrm{CM}}(5) = \{\mathcal{O}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/11\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\}$.*

By Proposition 6.15 for every torsion subgroup in $G \in \Phi(1)$, we can find a quintic Galois field so that $G \in \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(5)$. It remains to show that every torsion subgroup in $\Phi_{\mathbb{Q}}(5) \setminus \Phi(1)$ occurs for some rational elliptic curve over some quintic Galois field. Table 6.6 completes the demonstration that every torsion subgroup in $\Phi_{\mathbb{Q}}(5)$ occurs for some elliptic curve over some quintic Galois field. That is, we have $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(5) = \Phi_{\mathbb{Q}}(5)$.

**Corollary 6.21.** $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(5) = \Phi_{\mathbb{Q}}(5)$

Table 6.6: Torsion subgroups in $\Phi_{\mathbb{Q}}(5) \setminus \Phi(1)$ occurring over quintic Galois fields

| Torsion Subgroup | Elliptic Curve | Quintic Galois Field |
|---|---|---|
| $\mathbb{Z}/11\mathbb{Z}$ | `121c2` | $\mathbb{Q}(\zeta_{11})^+$ |
| $\mathbb{Z}/25\mathbb{Z}$ | `11a3` | $\mathbb{Q}(\zeta_{11})^+$ |

### 6.8.3 The Case of Septic Galois Fields

Recall that González-Jiménez and Najman classified the torsion subgroups of rational elliptic curves over septic number fields in [GJN20b], c.f. Theorem 4.40, which we restate here.

**Theorem 4.40** ([[GJN20b, Prop7.7]]). *Let $E/\mathbb{Q}$ be an elliptic curve, and $K$ a number field of degree 7.*

*(i) If $E(\mathbb{Q})_{tors} \not\simeq \{\mathcal{O}\}$, then $E(\mathbb{Q})_{tors} = E(K)_{tors}$.*

*(ii) If $E(\mathbb{Q})_{tors} \simeq \{\mathcal{O}\}$, then $E(K)_{tors} \simeq \{\mathcal{O}\}$ or $\mathbb{Z}/7\mathbb{Z}$. Furthermore, if $E(\mathbb{Q})_{tors} \simeq \{\mathcal{O}\}$ and $E(K)_{tors} \simeq \mathbb{Z}/7\mathbb{Z}$, then $K$ is the unique degree 7 number field with this property and $E$ is isomorphic to the elliptic curve*

$$\begin{aligned} E_t\colon y^2 = x^3 &+ 27(t^2-t+1)(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)x \\ &+ 54(t^{12}-522t^{11}-8955t^{10}+37950t^9-70998t_1^8 31562t^7 \\ &- 253239t^6+316290t^5-218058t^4+80090t^3-14631t^2+510t+1) \end{aligned}$$

*for some $t \in \mathbb{Q}$.*

We trivially have $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(7) = \Phi_{\mathbb{Q}}(7)$.

**Corollary 6.22.** $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(7) = \Phi_{\mathbb{Q}}(7)$

### 6.8.4 The Case of Nonic Galois Fields

For ease of reference, we restate our main result from Chapter 5.

**Theorem 5.29.** *Let $E/\mathbb{Q}$ be a rational elliptic curve, and let $K/\mathbb{Q}$ be a nonic Galois field.*

*Then $E(K)_{tors}$ is isomorphic to precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 10, 12, 13, 14, 18, 19, 21, 27 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7. \end{cases}$$

*Moreover, each such possibility occurs for some rational elliptic curve and some nonic Galois field.*

## 6.9 The Case of Prime Degree Galois Fields, $p > 5$

González-Jiménez and Najman show in [GJN20b] that what occurs, i.e. $E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$, for torsion subgroups of rational elliptic over septic fields is actually fairly common in that this is the case for rational elliptic curves over number fields of degree $d$, where $d$ is free of 'small' divisors. We repeat these results here.

**Theorem 4.41** ([GJN20b, Thm. 7.2])**.** *Let $d$ be a positive integer. Let $E/\mathbb{Q}$ be an elliptic curve, and let $K/\mathbb{Q}$ be a number field of degree $N$, where the smallest prime divisor of $N$ is $\geq d$. Then*

*(i) If $d \geq 11$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p$. In particular, $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

*(ii) If $d \geq 7$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 7$.*

*(iii) If $d \geq 5$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 5, 7, 11$.*

*(iv) If $d > 2$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 2, 3, 5, 7, 11, 13, 19, 43, 67, 163$.*

In particular, this proves the following

**Corollary 4.42** ([GJN20b, Cor 7.3]). *Let $d$ be a positive integer such that the smallest prime factor of $d$ is $\geq 11$. Then $\Phi_{\mathbb{Q}}(d) = \Phi(1)$.*

In particular, this proves that for integers (not necessarily odd) $d$ whose smallest prime divisor is at least 11, $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d) = \Phi(1)$. Furthermore, Theorem 4.41 says that over number fields of degree $d$ without "small" prime divisors, $K$, the only torsion for rational elliptic curves $E(K)_{\mathrm{tors}}$ arises as the result of base changing from an elliptic curve $E(\mathbb{Q})_{\mathrm{tors}}$. This is a remarkable result in terms of the sheer number of fields for which this result is applicable. Suppose that $K$ is a number field of degree $d$ with the smallest prime divisor of $d$ being $\geq 11$. Noting that $2 \cdot 3 \cdot 5 \cdot 7 = 210$, we can write $d = 210k + r$, where $k \in \mathbb{Z}_{\geq 0}$ and $(r, 210) = 1$. In particular, we now know the possible torsion subgroups for Galois number fields of degree $d$ with smallest prime divisor $\geq 7$ because the torsion subgroups in $\Phi(1)$ occur over every Galois number field (infinitely often). Ordering number fields by their degree, González-Jiménez and Najman's result applies to $\frac{\phi(210)}{210} = \frac{8}{35} \approx 22.9\%$ of number fields. Finally, as remarked by González-Jiménez and Najman, Corollary 4.42 is perhaps the best possible result in this direction in the following sense: for primes $p \in \{2, 3, 5, 7\}$, the set

$$\bigcup_{n=1}^{\infty} \Phi_{\mathbb{Q}}(p^n)$$

will contain $\mathbb{Z}/p^k\mathbb{Z}$ for each positive integer $k$.

## 6.10 The Classification over Odd Degree Galois Fields

We have enough to classify the possible torsion subgroups for rational elliptic curves over odd degree number fields. By abuse of notation, we define the following set:

$$\Phi_{\mathbb{Q}}^{\mathrm{Gal,odd}}(d^{\infty}) := \bigcup_{\substack{d \in \mathbb{N} \\ d \text{ odd}}} \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d).$$

Of course, a priori, there is no need for this set to be finite. But all of our previous work not only proves that this set is finite, but identifies the set explicitly.

**Theorem 6.23.** *The set $\Phi_{\mathbb{Q}}^{\mathrm{Gal},odd}(d^\infty)$ is finite, and if $E(K)_{tors} \in \Phi_{\mathbb{Q}}^{\mathrm{Gal},odd}(d^\infty)$, then $E(K)_{tors}$ is precisely one of the following:*

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } n = 1, 2, \ldots, 14, 18, 19, 21, 25, 27, 43, 67, 163 \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & \text{with } n = 1, 2, 3, 4, 7. \end{cases}$$

*Moreover, each such possibility occurs for some rational elliptic cure and some odd degree Galois field.*

*Proof.* If $K$ is an odd degree Galois number field and $E/\mathbb{Q}$ is a rational elliptic curve, we know that $E(K)_{\mathrm{tors}}$ is one of the torsion subgroups given in Lemma 6.5. As this is true for any odd degree Galois number field of degree $d$ and any rational elliptic curve $E$, we know that $\Phi_{\mathbb{Q}}^{\mathrm{Gal,odd}}(d^\infty)$ is a subset of the list given in Lemma 6.5. This proves the set $\Phi_{\mathbb{Q}}^{\mathrm{Gal,odd}}(d^\infty)$ is finite.

Eliminating from the list of possible torsion subgroups given in Lemma 6.5 precluded by Lemma 6.7, Lemma 6.8, Lemma 6.9, and Lemma 6.10, we are left with the list of torsion subgroups given in the statement of the theorem. By Proposition 6.15, we know that $\Phi(1) \subseteq \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ for all $d$. Table 6.2, Table 6.3, and Table 6.4 show that all remaining cases occur for some rational elliptic curve over some odd degree Galois field. □

Theorem 6.23 proves, a fortiori, that the sets $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ are uniformly bounded independently of the work of Merel and Parent. Furthermore, the largest possible order for a point $P \in E(K)_{\mathrm{tors}}$, where $E$ is a rational elliptic curve and $K$ is an odd degree Galois field is 163

and this bound is sharp, as Table 6.2, Table 6.3, and Table 6.4 show. Note this is also the largest possible size for the torsion subgroup $E(K)_{\text{tors}}$. Of course, we are primarily interested in the sets $\Phi_{\mathbb{Q}}^{\text{Gal}}(d)$ for some fixed odd integer $d$. So our next goal will be to classify these sets for all odd $d$. To state this theorem, we make the following definition:

**Definition.** Let $d$ be a positive odd integer. Write $d$ as $d = 3^{n_3} \cdot 5^{n_5} \cdot 7^{n_7} \cdot 11^{n_{11}} N$, where $n_i$ is a nonnegative integer and $N$ is an integer not divisible by 3, 5, 7, or 11. Using this notation, define $F(d) := (n_3, n_5, n_7, n_{11})$. We say that $d$ has has type $F(d)$. If an odd degree number field $K$ has degree $d$, we say also that $K$ has type $F(d)$.

If $F(d) = (n_3, n_5, n_7, n_{11})$, by abuse of notation, we shall write $F(d)^+ = (a^+, b, c, d)$ if $F(d) = (n_3, n_5, n_7, n_{11})$ with $n_3 \geq a$, $n_5 = b$, $n_7 = c$, and $n_{11} = d$. We define $F^+(d) = (a, b^+, c, d)$, $\ldots$, $F^+(d) = (a^+, b^+, c, d)$, $F^+(d) = (a^+, b, c^+, d)$, $\ldots$, and $F^+(d) = (a^+, b^+, c^+, d^+)$ mutatis mutandis. We take $F(d)^+ = (a, b, c, d)$ to mean $F(d) = (a, b, c, d)$.[3] Finally, we also denote by $d_{(a,b,c,d)}$ the set of integers such that $d$ has type $F(d) = (a, b, c, d)$.

**Example 6.1.** A sample of values for $F(d)$ is given in Table 6.7. Some examples of $d_{(a,b,c,d)}$ can be found below.

$$d_{(0,1,0,0)} = \{5N \colon N \in \mathbb{N}, \gcd(3, 5, 7, 11, N) = 1\}$$
$$d_{(2,0,0,0)} = \{9N \colon N \in \mathbb{N}, \gcd(3, 5, 7, 11, N) = 1\}$$
$$d_{(1,0,1,0)} = \{21N \colon N \in \mathbb{N}, \gcd(3, 5, 7, 11, N) = 1\}$$

Observe that $F(3)^+ = (1, 0, 0, 0)$, $F(3)^+ = (1^+, 0, 0, 0)$, and $F(3)^+ = (1, 0, 0, 0^+)$ but $F(3)^+ \neq (2, 0, 0, 0)$, $F(3)^+ \neq (1^+, 1, 0, 0)$, and $F(3)^+ \neq (1, 0, 1^+, 0)$. Similarly, $F(55)^+ =$

[3] We are trying to specify at least (or exactly) how many factors of 3, 5, 7, and 11 an integer $d$ has. Saying $F(d) = (a, b, c, d)$ says that $d$ has exactly $a$ factors of 3, $b$ factors of 5, $c$ factors of 7, and $d$ factors of 11. We create the $F^+(d)$ notation to indicate when $d$ has *at least* a specified number of factors for one or more of the primes 3, 5, 7, or 11. Writing $F^+(d) = (a, b, c, d)$ with no '+' on any factor simply means we want $d$ to have exactly the specified number of factors for each of the primes 3, 5, 7, and 11. Hence, $F^+(d) = (a, b, c, d)$ simply means $F(d) = (a, b, c, d)$.

Table 6.7: A table of $F(d)$ for select $d$ values

| $d$ | $F(d)$ |
|---|---|
| 1 | $(0,0,0,0)$ |
| 3 | $(1,0,0,0)$ |
| 5 | $(0,1,0,0)$ |
| 21 | $(1,0,1,0)$ |
| 26 | $(0,0,0,0)$ |
| 45 | $(2,1,0,0)$ |
| 55 | $(0,1,0,1)$ |

$(0,1,0,1)$, $F(55)^+ = (0,1^+,0,1)$, and $F(3)^+ = (0^+,1,0,1)$ but $F(55)^+ \neq (1,1,0,1)$, $F(55)^+ \neq (0,2,0,1)$, and $F(3)^+ \neq (1^+,1,0,1)$. ◁

We can now state our main theorem.

**Theorem 6.24.** *Let $d$ be a positive odd integer. The set of possible isomorphism classes of torsion subgroups $E(K)_{tors}$, where $E$ is a rational elliptic curve and $K/\mathbb{Q}$ is an odd degree number field of degree $d$, i.e. $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$, is given in Table 6.8.*

*Proof.* We know that any torsion subgroup in $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ must be one among the list in Theorem 6.23. By Corollary 6.16 for all $d$ (not necessarily odd), we know that $\Phi(1) \subseteq \Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$. If $d$ has no prime factors $p$ with $p \leq 11$, then by Corollary 4.42, we know that $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d) = \Phi(1)$. Otherwise, by Lemma 6.17, Lemma 6.18, and Lemma 6.19, the torsion subgroups in $\Phi_{\mathbb{Q}}^{\mathrm{Gal,odd}}(d^\infty) \setminus \Phi(1)$ depend only on the factorization of $d$, i.e. how many factors of 3, 5, 7, and 11 $d$ has. Applying these divisibility conditions and the examples from Table 6.2, Table 6.3, and Table 6.4 combined with Proposition 6.15 gives the exact list of possibilities for $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ that appear in Table 6.8, and these are the only torsion subgroups which can appear. □

As a final remark, the largest possible size for $\#\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$, where $d$ is an odd integer, is 42

and occurs whenever $d$ has type $(4^+, 1^+, 1^+, 1^+)$.

Table 6.8: The set of possible isomorphism classes of torsion subgroups $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$, where $d$ is odd, determined by $F(d)^+$

| $F(d)^+$ | $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ | $F(d)^+$ | $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ |
|---|---|---|---|
| $(0,0,0^+,0^+)$ | $\Phi(1)$ | $(2,0,1^+,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}\}$ |
| $(0,1,0^+,0^+)$ | $\Phi_{\mathbb{Q}}(5)$ | $(2,1^+,0,0)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}\}$ |
| $(1,0,0,0)$ | $\Phi_{\mathbb{Q}}(3)$ | $(2,1^+,0,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}\}$ |
| $(1,0,0,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/11\mathbb{Z}\}$ | $(2,1^+,1^+,0)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}\}$ |
| $(1,0,1^+,0)$ | $\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/43\mathbb{Z}\}$ | $(2,1^+,1^+,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}\}$ |
| $(1,0,1^+,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/11\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}\}$ | $(4^+,0,0,0)$ | $\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$ |
| $(1,1^+,0,0)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5)$ | $(4,0,0,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$ |
| $(1,1^+,0,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/67\mathbb{Z}\}$ | $(4,0,1^+,0)$ | $\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/47\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$ |
| $(1,1^+,1^+,0)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/43\mathbb{Z}\}$ | $(4,0,1^+,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$ |
| $(1,1^+,1^+,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}\}$ | $(4,1^+,0,0)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$ |
| $(2,0,0,0)$ | $\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}\}$ | $(4,1^+,0,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$ |
| $(2,0,0,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}\}$ | $(4,1^+,1^+,0)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$ |
| $(2,0,1^+,0)$ | $\Phi_{\mathbb{Q}}(3) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}\}$ | $(4^+,1^+,1^+,1^+)$ | $\Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}, \mathbb{Z}/43\mathbb{Z}, \mathbb{Z}/67\mathbb{Z}, \mathbb{Z}/163\mathbb{Z}\}$ |

# Chapter 7

# Future Directions

After the classification of torsion subgroups of rational elliptic curves over odd degree Galois number fields, there are a great number of directions one could take. One obvious question would be could one replicate the work for rational elliptic curves over even degree Galois number fields. However at present, this would be appear to be a futile direction. Such a classification would necessarily entail classifying the torsion subgroups $E(\mathbb{Q}(\zeta_n))$, where $\zeta_n$ is a primitive $n$th root of unity. For each $n$, the field $\mathbb{Q}(E[n])$ contains $\mathbb{Q}(\zeta_n)$, c.f. Corollary 3.15, this would very nearly amount to the complete classification of $\Phi_{\mathbb{Q}}(d)$ for all $d$, which is not currently likely. Recall that González-Jiménez and Lozano-Robledo's work in [GJLR18], and González-Jiménez and Najman's work in [GJN20b] extending Chou's classification of $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(4)$ in [Cho16] completely determined the set $\Phi_{\mathbb{Q}}(4)$. A future problem could then be to then use the classification of $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(9)$ to assist in determining the set $\Phi_{\mathbb{Q}}(9)$.

If one instead wanted to focus on the set $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(9)$, another direction would be to determine

the possible torsion growth of torsion subgroups when base extending from $\mathbb{Q}$ or a cubic Galois field, similar to the work of González-Jiménez, Najman, and Tornero in [GJNT16]. In fact, some of the work towards this has been done in this paper as we have classified the growth from $E(\mathbb{Q})_{\text{tors}}$ to $E(K)_{\text{tors}}$, where $K/\mathbb{Q}$ is a general nonic Galois field. However, we did not classify the possible torsion growth based on the isomorphism type of $\text{Gal}(K/\mathbb{Q})$. Nor did we classify the possible growth from an intermediate cubic Galois subfield to a general nonic Galois field. However, all the results needed for such a classification should already be contained within this paper. One could also try to determine the possible torsion growths from $E(\mathbb{Q})_{\text{tors}}$ to $E(K)_{\text{tors}}$, where $K$ is a general odd degree Galois number field. Again, all of the results required for such a classification should be contained herein. Furthermore, one could try to classify the possibilities for $E(K)_{\text{tors}}$ as $E$ varies over all rational elliptic curves base extended to a *fixed* nonic Galois field $K$.

One could also try to classify the possible torsion structures $\Phi_{\mathbb{Q}}^{\text{Gal}}(d)$ if one restricts to number fields $K/\mathbb{Q}$ having Galois groups with a specified structure, such as abelian groups. This could then make use of Chou's result [Cho19]. Furthermore, one could look at the interesting interplay between torsion subgroups and the arithmetic of number fields hinted at in Lemma 5.34. This is similar to work of Hanson Smith, who has interesting results connecting elliptic curves and monogenic number fields, c.f. [Smi18], [GSS19], [Smi20a], [Smi20b], and [SvH21]. Finally, following [Guž19] and [CN21], one could try to extend the classification of $\Phi_{\mathbb{Q}}^{\text{Gal}}(d)$ instead to $\Phi_{j\in\mathbb{Q}}^{\text{Gal}}(d)$.

Another possible future research direction would be to try to 'count' torsion subgroups occurring $\Phi_{\mathbb{Q}}^{\text{Gal}}(9)$. For instance in [HS17], Harron and Snowden asked the following question:

> *"Mazur established that there are only 15 possibilities for the torsion subgroup... With this classification in hand, it is natural to ask a more refined*

*question: how often does each of these groups occur?"*

Of course, one must define what one means by 'count.' For each elliptic curve $E$, choose a model $E_{A,B} : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$ are chosen 'minimally', i.e. $\gcd(A^3, B^2)$ is not divisibly by $p^{12}$ for any prime $p$. Equivalently, for all primes $p$, if $p^4 \mid A$, then $p^6 \nmid B$. Otherwise, $E_{A,B} \cong E_{A/p^4,B/p^6}$ using the map $(x, y) \mapsto (p^2x', p^3y')$. All elliptic curves $E/\mathbb{Q}$ are isomorphic to an elliptic curve of this form. One then defines the (naïve) height of $E$ to be $H(E_{A,B}) := \max(|A|^3 3, |B|^2)$.[1] There are then only finitely many elliptic curves up to fixed height $X \in \mathbb{R}$. Then if $G \in \Phi(1)$, Harron and Snowden define $N_G(X)$ to be the number of (isomorphism classes of) elliptic curves $E/\mathbb{Q}$ of height at most $X$ for which $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to $G$. They then prove the following:

**Theorem 7.1** ([HS17, Thm. 1.1])**.** *For any group $G \in \Phi(1)$, the limit*

$$\frac{1}{d(G)} = \lim_{X \to \infty} \frac{\log N_G(X)}{\log X}$$

*exists. The value of $d(G)$ is as indicated in Table 7.1.*

Table 7.1: The values of $d(G)$ for $G \in \Phi(1)$

| $G$ | $d$ | $G$ | $d$ | $G$ | $d$ |
|---|---|---|---|---|---|
| 0 | 6/5 | $\mathbb{Z}/6\mathbb{Z}$ | 6 | $\mathbb{Z}/12\mathbb{Z}$ | 24 |
| $\mathbb{Z}/2\mathbb{Z}$ | 2 | $\mathbb{Z}/7\mathbb{Z}$ | 12 | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | 3 |
| $\mathbb{Z}/3\mathbb{Z}$ | 3 | $\mathbb{Z}/8\mathbb{Z}$ | 12 | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ | 6 |
| $\mathbb{Z}/4\mathbb{Z}$ | 4 | $\mathbb{Z}/9\mathbb{Z}$ | 18 | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ | 12 |
| $\mathbb{Z}/5\mathbb{Z}$ | 6 | $\mathbb{Z}/10\mathbb{Z}$ | 18 | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ | 24 |

Because $d(0) < d(G)$ for all $G \in \Phi(1)$ with $\#G > 1$, this recovers a result of Duke [Duk97] that 'almost all' rational elliptic curves have trivial torsion. Harron and Snowden prove a

[1] Some would define this to be $\max(4|A|^3 3, 27|B|^2)$ to more closely match the discriminant. But for counting purposes, this gives the same count as $H(E_{A,B})$ in the limit as $H \to \infty$ in that the difference tends to 0.

stronger result: for $G \in \Phi(1)$ there exist positive constants $K_1$ and $K_2$ such that

$$K_1 X^{1/d(G)} \leq N_G(X) \leq K_2 X^{1/d(G)}$$

holds for all $X \geq 1$, suggesting that the following limit exists:

$$c(G) = \lim_{X \to \infty} \frac{N_G(X)}{X^{1/d(G)}}$$

They prove this is the case for $\#G \leq 3$.

**Theorem 7.2** ([HS17, Thm. 1.6])**.** *Let $f, g \in \mathbb{Q}[t]$ be non-zero coprime polynomials of degrees $r$ and $s$, with at least one of $r$ or $s$ positive, and write*

$$\max\left(\frac{r}{4}, \frac{s}{6}\right) = \frac{n}{m},$$

*with $n$ and $m$ coprime. Assume $n = 1$ or $m = 1$. Let $\mathcal{E}$ be the family of elliptic curves defined by*

$$y^2 = x^3 + f(t)x + g(t).$$

*Let $N(X)$ be the number of (isomorphism classes of) elliptic curves $E/\mathbb{Q}$ of height at most $X$ for which $E \cong \mathcal{E}_t$ for some $t \in \mathbb{Q}$. Then there exist positive constants $K_1$ and $K_2$ such that*

$$K_1 X^{(m+1)/12n} \leq N(X) \leq K_2 X^{(m+1)/12n}$$

*for all $X \geq 1$.*

Harron and Snowden also discuss several interesting possible future directions for their work in their paper, the most general being the following:

> *"Let $\mathcal{X}$ and $\mathcal{Y}$ be proper smooth Deligne-Mumford stacks over $\mathbb{Q}$ with course space $\mathbb{P}^1$, and let $f : \mathcal{Y} \to \mathcal{X}$ be a map. Suppose that there is a good notion of height $h_{\mathcal{X}}$ on the set $|\mathcal{X}(\mathbb{Q})|$, where $|\cdot|$ denotes isomorphism classes. Then one would like a formula for*
>
> $$\lim_{T\to\infty} \frac{\#\{x \in f(|\mathcal{Y}(\mathbb{Q})|) \mid h_{\mathcal{X}}(x) \leq T\}}{\log T}$$
>
> *in terms of invariants of $\mathcal{X}, \mathcal{Y}$, and $f$. More generally, one may ask these questions over general global fields. What kind of dependence is there on the base field?"*

Pizzo, Pomerance, and Voight perform similar analyses when counting elliptic curves with a 3-isogeny in [PPV20]. Bruin and Najman extend Harron and Snowden's work by extending their result to number fields and level structure $G$ such that the corresponding modular curve $X_G$ is a weighted projective line $\mathbb{P}(w_0, w_1)$ and the morphism $X_G \to X(1)$ some specified conditions, e.g. modular curves $X_1(m, n)$ with a course moduli space of genus 0.

**Theorem 7.3** ([BN20, Thm. 1.1])**.** *Let $n$ be a positive integer, and let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Let $K_G$ be the fixed field of the action of $G$ on $\mathbb{Q}(\zeta_n)$ given by $(g, \zeta_n) \mapsto \zeta_n^{\det g}$. Assume that the stack $X_G$ over $K_G$ is isomorphic to $\mathbb{P}(w)_{K_G}$, where $w = (w_0, w_1)$ is a pair of positive integers, and let $e$ be as in* [BN20, Lem 4.1]*. Furthermore, assume $e = 1$ or $w = (1, 1)$ holds. Then for every finite extension $K$ of $K_G$, we have*

$$N_{G,K}(X) \asymp X^{1/d(G,K)} \text{ as } X \to \infty,$$

*where* $d(G, K) = \dfrac{12e}{w_0 + w_1}$.

Because 'most' of the torsion in $\Phi_{\mathbb{Q}}^{\mathrm{Gal}}(d)$ occurs over $\mathbb{Q}$ for any odd $d$, and one should be able to track the number of fields over which the torsion can grow, one should be able to apply the results from Theorem 7.2 to count the density of elliptic curves over these fields. One could also try to do this in a simpler case, such as for $\Phi_{\mathbb{Q}}(2)$.

# Appendix

Because we made fair use of Tables 2–4 in [LR13] in this work, we reproduce these tables here. See [LR13] for detailed references for these tables.

Table 7.2: Hauptmoduln for the function field of $X_0(N)$, genus 0 case [LR13, Table 2]

| $N$ | Hauptmodul | $N$ | Hauptmodul |
|---|---|---|---|
| 2 | $h = 2^{12} \cdot \left(\frac{\eta(2\tau)}{\eta(\tau)}\right)^{24}$ | 9 | $h = 3 + 3^3 \cdot \left(\frac{\eta(9\tau)}{\eta(\tau)}\right)^{3}$ |
| 3 | $h = 3^6 \cdot \left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}$ | 10 | $h = 4 + 2^2 5 \cdot \frac{\eta(2\tau)\eta(10\tau)^3}{\eta(\tau)^3\eta(5\tau)}$ |
| 4 | $h = 2^8 \cdot \left(\frac{\eta(4\tau)}{\eta(\tau)}\right)^{8}$ | 12 | $h = 3 + 2^3 3 \cdot \frac{\eta(2\tau)^2\eta(3\tau)\eta(12\tau)^3}{\eta(\tau)^3\eta(4\tau)\eta(6\tau)^2}$ |
| 5 | $h = 5^3 \cdot \left(\frac{\eta(5\tau)}{\eta(\tau)}\right)^{6}$ | 13 | $h = 13 \cdot \left(\frac{\eta(13\tau)}{\eta(\tau)}\right)^{2}$ |
| 6 | $h = 2^3 3^2 \cdot \frac{\eta(2\tau)\eta(6\tau)^5}{\eta(\tau)^5\eta(3\tau)}$ | 16 | $h = 2 + 2^3 \cdot \frac{\eta(2\tau)\eta(16\tau)^2}{\eta(\tau)^2\eta(8\tau)}$ |
| 7 | $h = 7^2 \cdot \left(\frac{\eta(7\tau)}{\eta(\tau)}\right)^{4}$ | 18 | $h = 2 + 2 \cdot 3 \cdot \frac{\eta(2\tau)\eta(3\tau)\eta(18\tau)^2}{\eta(\tau)^2\eta(6\tau)\eta(9\tau)}$ |
| 8 | $h = 4 + 2^5 \cdot \frac{\eta(2\tau)^2\eta(8\tau)^4}{\eta(\tau)^4\eta(4\tau)^2}$ | 25 | $h = 1 + 5 \cdot \frac{\eta(25\tau)}{\eta(\tau)}$ |

Notation: $\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$, and $q = e^{2\pi i\tau}$

Table 7.3: All non-cuspidal rational points on $X_0(N)$, genus 0 case [LR13, Table 3]

| $N$ | $j$ and $j'$-invariants such that $E$ and $E'$ are $N$-isogenous | |
|---|---|---|
| 2 | $j = \frac{(h+16)^3}{h}$ | $j' = \frac{(h+256)^3}{h^2}$ |
| 3 | $j = \frac{(h+27)(h+3)^3}{h}$ | $j' = \frac{(h+27)(h+243)^3}{h^3}$ |
| 4 | $j = \frac{(h^2+16h+16)^3}{h(h+16)}$ | $j' = \frac{(h^2+256h+4096)^3}{h^4(h+16)}$ |
| 5 | $j = \frac{(h^2+10h+5)^3}{h}$ | $j' = \frac{(h^2+250h+5^5)^3}{h^5}$ |
| 6 | $j = \frac{(h+6)^3(h^3+18h^2+84h+24)^3}{h(h+8)^3(h+9)^2}$ | $j' = \frac{(h+12)^3(h^3+252h^2+3888h+15552)^3}{h^6(h+8)^2(h+9)^3}$ |
| 7 | $j = \frac{(h^2+13h+49)(h^2+5h+1)^3}{h}$ | $j' = \frac{(h^2+13h+49)(h^2+245h+2401)^3}{h^7}$ |
| 8 | $j = \frac{(h^4-16h^2+16)^3}{(h^2-16)h^2}$ | $j' = \frac{(h^4+240h^3+2144h^2+3840h+256)^3}{(h-4)^8h(h+4)^2}$ |
| 9 | $j = \frac{h^3(h^3-24)^3}{h^3-27}$ | $j' = \frac{(h+6)^3(h^3+234h^2+756h+2160)^3}{(h-3)^8(h^3-27)}$ |
| 10 | $j = \frac{(h^6-4h^5+16h+16)^3}{(h+1)^2(h-4)h^5}$ | $j' = \frac{(h^6+236h^5+1440h^4+1920h^3+3840h^2+256h+256)^3}{(h-4)^{10}h^2(h+1)^5}$ |
| 12 | $j = \frac{(h^2-3)^3(h^6-9h^4+3h^2-3)^3}{h^4(h^2-9)(h^2-1)^3}$ | $j' = \frac{(h^2+6h-3)^3(h^6+234h^5+747h^4+540h^3-729h^2-486h-243)^3}{(h-3)^{12}(h-1)h^3(h+1)^4(h+3)^3}$ |
| 13 | $j = \frac{(h^2+5h+13)(h^4+7h^3+20h^2+19h+1)^3}{h}$ | $j' = \frac{(h^2+5h+13)(h^4+247h^3+3380h^2+15379h+28561)^3}{h^{13}}$ |
| 16 | $j = \frac{(h^8-16h^4+16)^3}{h^4(h^4-16)}$ | |
| | $j' = \frac{(h^8+240h^7+2160h^6+6720h^5+17504h^4+26880h^3+34560h^2+15360h+256)^3}{(h-2)^{16}h(h+2)^4(h^2+4)}$ | |
| 18 | $j = \frac{(h^3-2)^3(h^9-6h^6-12h^3-8)^3}{h^9(h^3-8)(h^3+1)^2}$ | |
| | $j' = \frac{(h^3+6h^2+4)^3(h^9+234h^8+756h^7+2172h^6+1872h^5+3024h^4+48h^3+3744h^2+64)^3}{(h-2)^{18}h^2(h+1)^9(h^2-h+1)(h^2+2h+4)^2}$ | |
| 25 | $j = \frac{(h^{10}+10h^8+35h^6-12h^5+50h^4-60h^3+25h^2-60h+16)^3}{h^5+5h^3+5h-11}$ | |
| | $j' = \frac{(h^{10}+240h^9+2170h^8+8880h^7+34835h^6+83748h^5+206210h^4+313380h^3+503545h^2+424740h+375376)^3}{(h-1)^{25}(h^4+h^3+6h^2+6h+11)}$ | |

Table 7.4: All non-cuspidal rational points on $X_0(N)$, genus $> 0$ case [LR13, Table 3]

| $N$, **genus**$(X_0(N))$ | $j$-**invariants** | **Cremona Labels** | **Conductors** | **CM** |
|---|---|---|---|---|
| 11, $g = 1$ | $j = -11 \cdot 131^3$ | 121a1, 121c2 | $11^2$ | No |
| | $j = -2^{15}$ | 121b1, 121b2 | $11^2$ | $-11$ |
| | $j = -11^2$ | 121c1, 121a2 | $11^2$ | No |
| 14, $g = 1$ | $j = -3^3 \cdot 5^3$ | 49a1, 49a3 | $7^2$ | $-7$ |
| | $j = 3^3 \cdot 5^3 \cdot 17^3$ | 49a2, 49a4 | $7^2$ | $-28$ |
| 15, $g = 1$ | $j = -5^2/2$ | 50a1, 50b3 | $2 \cdot 5^2$ | No |
| | $j = -5^2 \cdot 241^3/2^3$ | 50a2, 50b4 | $2 \cdot 5^2$ | No |
| | $j = -5 \cdot 29^3/2^5$ | 50a3, 50b1 | $2 \cdot 5^2$ | No |
| | $j = 5 \cdot 211^3/2^{15}$ | 50a4, 50b2 | $2 \cdot 5^2$ | No |
| 17, $g = 1$ | $j = -17^2 \cdot 101^3/2$ | 14450p1 | $2 \cdot 5^2 \cdot 17^2$ | No |
| | $j = -17 \cdot 373^3/2^{17}$ | 14450p2 | $2 \cdot 5^2 \cdot 17^2$ | No |
| 19, $g = 1$ | $j = -2^{15} \cdot 3^3$ | 361a1, 361a2 | $19^2$ | $-19$ |
| 21, $g = 1$ | $j = -3^2 \cdot 5^6/2^3$ | 162b1, 162c2 | $2 \cdot 3^4$ | No |
| | $j = 3^3 \cdot 5^3/2$ | 162b2, 162c1 | $2 \cdot 3^4$ | No |
| | $j = -3^2 \cdot 5^3 \cdot 101^3/2^{21}$ | 162b3, 162c4 | $2 \cdot 3^4$ | No |
| | $j = -3^3 \cdot 5^3 \cdot 383^3/2^7$ | 162b4, 162c3 | $2 \cdot 3^4$ | No |
| 27, $g = 1$ | $j = -2^{15} \cdot 3 \cdot 5^3$ | 27a2, 27a4 | $3^3$ | $-27$ |
| 37, $g = 2$ | $j = -7 \cdot 11^3$ | 1225h1 | $5^2 \cdot 7^2$ | No |
| | $j = -7 \cdot 137^3 \cdot 2083^3$ | 1225h2 | $5^2 \cdot 7^2$ | No |
| 43, $g = 3$ | $j = -2^{18} \cdot 3^3 \cdot 5^3$ | 1849a1, 1849a2 | $43^2$ | $-43$ |
| 67, $g = 5$ | $j = -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$ | 4489a1, 4489a2 | $67^2$ | $-67$ |
| 163, $g = 13$ | $j = -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$ | 26569a1, 26569a2 | $163^2$ | $-163$ |

Remark: The Cremona labels are the representatives in this class of least conductor.

# Bibliography

[Ari20] Arizona Winter School, 2020. https://www.math.arizona.edu/~swc/aws/2020/index.html. ↑12

[Bak90] A. Baker, *Transcendental Number Theory*, Cambridge University Press, Cambridge, 1990. ↑42

[BBDN13a] J. Bosman, P. Bruin, A. Dujella, and F. Najman, *Ranks of Elliptic Curves with Prescribed Torsion over Number Fields*, International Mathematics Research Notices **2014** (2013), no. 11, 2885–2923. ↑

[BBDN13b] J. G. Bosman, P. J. Bruin, A. Dujella, and F. Najman, *Ranks of Elliptic Curves with Prescribed Torsion over Number Fields*, International Mathematics Research Notices **2014** (2013), no. 11, 2885–2923. ↑71, 87

[BC20a] A. Bourdon and P. L. Clark, *Torsion points and galois representations on CM elliptic curves*, Pacific Journal of Mathematics **305** (2020), no. 1, 43–88. ↑84

[BC20b] A. Bourdon and P. L. Clark, *Torsion points and isogenies on CM elliptic*

*curves*, Journal of the London Mathematical Society **102** (2020), 580–622. ↑84, 85

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: Wild 3-adic exercises*, Journal of the American Mathematical Society **14** (2001), no. 4, 843–939. ↑16

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, Vol. 24, 1997. ↑126

[BCS17] A. Bourdon, P. L. Clark, and J. Stankewicz, *Torsion points on CM elliptic curves over real number fields*, Transactions of the American Mathematical Society **369** (2017), 8457–8496. ↑79, 80

[BGRW20] A. Bourdon, D. R. Gill, J. Rouse, and L. D. Watson, *Odd degree isolated points on* $X_1(N)$ *with rational* $j$*-invariant*, 2020. ↑75

[BMSW07] B. Bektemirov, B. C. Mazur, W. Stein, and M. Watkins, *Average ranks of elliptic curves: Tension between data and conjecture*, Bulletin of the American Mathematical Society **44** (2007), no. 2, 233–254. ↑41

[BN17] P. Bruin and F. Najman, *Fields of definition of elliptic curves with prescribed torsion*, Acta Arithmetica **181** (2017), 85–95. ↑74

[BN20] P. Bruin and F. Najman, *Counting elliptic curves with prescribed level structures over number fields*, 2020. ↑199

[Bom90] E. Bombieri, *The Mordell conjecture revisited*, Annali Della Scuola Normale Superiore Di Pisa - Classe Di Scienze **17** (1990), no. 4, 615–640. ↑10

[BP12] A. Bandini and L. Paladino, *Number fields generated by the 3-torsion points of an elliptic curve*, Monatshefte für Mathematik **168** (2012), no. 2, 157–181. ↑123

[BP16a] A. Bandini and L. Paladino, *Fields generated by torsion points of elliptic curves*, Journal of Number Theory **169** (2016), 103–133. ↑123

[BP16b] A. Bourdon and P. Pollack, *Torsion subgroups of CM Elliptic Curves over Odd Degree Number Fields*, International Mathematics Research Notices **2017** (2016), no. 16, 4923–4961, available at https://academic.oup.com/imrn/article-pdf/2017/16/4923/19515350/rnw163.pdf. ↑80, 81

[BS10] N. Bruin and M. Stoll, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS Journal of Computation and Mathematics **13** (2010), 272–306. ↑74

[BS15] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Annals of Mathematics **181** (2015), no. 1, 191–242. ↑40

[BS16] B. Bhatt and A. Snowden, *Faltings' Proof of the Mordell Conjecture*, 2016. ↑10

[CCRS14] P. L. Clark, P. Corn, A. Rice, and J. Stankewicz, *Computation on elliptic*

*curves with complex multiplication*, LMS Journal of Computation and Mathematics **17** (2014), no. 1, 509–535. ↑78, 79

[CCS13] P. L. Clark, B. Cook, and J. Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)*, International Journal of Number Theory **2** (2013), 447–479. ↑78

[CDKN21] M. Chou, H. B. Daniels, I. Krijan, and F. Najman, *Torsion groups of elliptic curves over the $\mathbb{Z}_p$-extensions of $\mathbb{Q}$*, New York Journal of Mathematics **27** (2021), 99–123. ↑111, 112

[CDT99] B. Conrad, F. Diamond, and R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, Journal of the American Mathematical Society **12** (1999), no. 2, 521–567. ↑16

[Cha41] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, Comptes rendus de l'Académie des Sciences Paris **212** (1941), 882–885. ↑12

[Cho16] M. Chou, *Torsion of rational elliptic curves over quartic Galois number fields*, Journal of Number Theory **160** (2016), 603–628. ↑87, 88, 89, 91, 132, 133, 145, 195

[Cho19] M. Chou, *Torsion of rational elliptic curves over the maximal abelian extension of $\mathbb{Q}$*, Pacific Journal of Mathematics **302** (2019), no. 2, 481–509. ↑110, 132, 133, 134, 160, 196

[CLR21] G. Chiloyan and Á. Lozano-Robledo, *A classification of isogeny-torsion graphs of $\mathbb{Q}$-isogeny classes of elliptic curves*, Transactions of the London Mathematical Society **8** (2021), no. 1, 1–34. ↑

[CN21] J. Cremona and F. Najman, *$\mathbb{Q}$-curves over odd degree number fields*, 2021. ↑115, 196

[Col21] T. LMFDB Collaboration, *The L-functions and Modular Forms Database*, 2021. ↑126

[Col85] R. F. Coleman, *Effective Chabauty*, Duke Mathematics Journal **52** (1985), no. 3, 765–770. ↑12

[Cona] B. Conrad, *Chow's $K/k$-Image and $K/k$-Trace, and the Lang-Néron Theorem.* ↑37

[Conb] K. Conrad, *Galois groups of cubics and quartics (not in characteristic 2).* https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf. ↑131, 138, 139

[Conc] K. Conrad, *Selmer's Example.* https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf. ↑5

[CP80] D. A. Cox and W. R. Parry, *Torsion in elliptic curves over $k(t)$*, Compositio Mathematica **41** (1980), no. 3, 337–354. ↑118

[Cre] J. Cremona, *Elliptic curve data.* http://johncremona.github.io/ecdata/. ↑126

[Dan18] H. B. Daniels, *Torsion subgroups of rational elliptic curves over the compositum of all $D_4$ extensions of the rational numbers*, Journal of Algebra **509** (2018), 535–565. ↑106, 107, 108

[Dan21] H. B. Daniels, *An Errata for: Torsion subgroups of rational elliptic curves over the compositum of all $D_4$ extensions of the rational numbers*, 2021. ↑106

[DDH19] H. B. Daniels, M. Derickx, and J. Hatley, *Groups of generalized G-type and applications to torsion subgroups of rational elliptic curves over infinite extensions of $\mathbb{Q}$*, Transactions of the London Mathematical Society **6** (2019), no. 1, 22–52. ↑108, 109

[DEvH+20] M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow, and D. Zureick-Brown, *Sporadic Cubic Torsion*, 2020. ↑75

[DF04] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd edition, John Wiley and Sons, Inc., 2004. ↑131, 138, 139, 157, 173, 178, 180

[DGJ20] H. Daniels and E. González-Jiménez, *On the torsion of rational elliptic curves over sextic fields*, Mathematics of Computation **89** (2020), 411–435. ↑92, 103

[DGJU11] L. Dieulefait, E. González-Jiménez, and J. J. Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, Proceedings of the American Mathematical Society **139** (2011), no. 6, 1961–1969. ↑81, 82

[Dic71] L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Dover Publications, 1971. ↑16

[Dir37] P. G. L. Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin (1837), 45–71. ↑178

[DJ09] L. Dieulefait and J. Jiménez, *Solving Fermat-type equations via modular $\mathbb{Q}$-curves over polyquadratic fields*, Journal für die reine und angewandte Mathematik **633** (2009), 183–195. ↑114

[DKSS17] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, *Torsion points on elliptic curves over number fields of small degree* (2017), available at 1707.00364. ↑67

[DLR15] H. B. Daniels and Á. Lozano-Robledo, *On the number of isomorphism classes of CM elliptic curves defined over a number field*, Journal of Number Theory **157** (2015), 367–396. ↑84

[DLR19] H. B. Daniels and Á. Lozano-Robledo, *Coincidences of division fields*, 2019. ↑

[DLRNS18] H. B. Daniels, Á. Lozano-Robledo, F. Najman, and A. Sutherland, *Torsion subgroups of rational elliptic curves over the compositum of all cubic fields*, Mathematics of Computation **87** (2018), 425–458. ↑105, 106, 156

[DN19] M. Derickx and F. Najman, *Torsion of elliptic curves over cyclic cubic fields*, Mathematics of Computation **88** (2019), no. 319, 2443–2459. ↑72, 73, 87

[DR19] P. K. Dey and B. Roy, *Torsion groups of Mordell curves over cubic and sextic fields*, 2019. ↑77

[DS05] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Springer-Verlag New York, 2005. ↑61

[DS17] M. Derickx and A. V. Sutherland, *Torsion subgroups of elliptic curves over quintic and sextic number fields*, Proceedings of the American Mathematical Society **145** (2017), 4233–4245. ↑77

[Duj] A. Dujella, *History of elliptic curves rank records*. https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html. ↑38

[Duk97] W. Duke, *Elliptic curves with no exceptional primes*, Comptes rendus de l'Académie des Sciences Paris **325** (1997), no. 8, 813–818. English, with English and French summaries. ↑197

[Edi93] B. Edixhoven, *Rational torsion points on elliptic curves over number fields*, Séminaire Nicholas Bourbaki **782** (1993), 209–223. ↑68

[Ejd18] Ö. Ejder, *Torsion subgroups of elliptic curves over quadratic cyclotomic fields in elementary abelian 2-extensions*, Journal of Number Theory **193** (2018), 266–301. ↑105

[EMSW20] K. Eisenträger, R. Miller, C. Springer, and L. Westrick, *A Topological Approach to Undefinability in Algebraic Extensions of* $\mathbb{Q}$, 2020. ↑6

[Fal84] G. Faltings, *Finiteness theorems for abelian varieties over number fields*, Inventiones mathematicae **73** (1984), no. 3, 349–366. ↑10

[Fre86] G. Frey, *Links between stable elliptic curves and certain diophantine equations*, Annales Universitatis Saraviensis **1** (1986), 1–40. ↑15

[FSWZ90a] G. Fung, H. Ströher, H. Williams, and H. Zimmer, *Torsion groups of elliptic curves with integral $j$-invariant over pure cubic fields*, Journal of Number Theory **36** (1990), 12–45. ↑78

[FSWZ90b] G. W. Fung, H Ströher, H. C. Williams, and H. G. Zimmer, *Torsion Groups of Elliptic Curves with Integral $j$-invariant over Pure Cubic Fields*, Journal of Number Theory **36** (1990), no. 1, 12–45. ↑116

[Fuj04] Y. Fujita, *Torsion subgroups of elliptic curves with non-cyclic torsion over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$*, Acta Arithmetica **115** (2004), 29–45. ↑104

[Fuj05] Y. Fujita, *Torsion subgroups of elliptic curves in elementary abelian 2-extensions of $\mathbb{Q}$*, Journal of Number Theory **114** (2005), no. 1, 124–134. ↑104

[GG14] I. Gal and R. Grizzard, *On the compositum of all degree d extensions of a number field*, Journal de Théorie des Nombres de Bordeaux **26** (2014), no. 3, 655–672. MR3320497 ↑104

[GJ17] E. González-Jiménez, *Complete classification of the torsion structures of ratio-*

*nal elliptic curves over quintic number fields*, Journal of Algebra **478** (2017), 484–505. ↑91, 92, 103, 132, 133, 186

[GJ20] E. González-Jiménez, *Torsion growth over cubic fields of rational elliptic curves with complex multiplication*, Publicationes Mathematicae Debrecen **97** (2020), no. 1-2, 63–76. ↑103

[GJ21] E. González-Jiménez, *Explicit characterization of the torsion growth of rational elliptic curves with complex multiplication over quadratic fields* (2021), available at 1909.00637. ↑102

[GJLR16] E. González-Jiménez and Á. Lozano-Robledo, *Elliptic Curves with abelian division fields*, Mathematische Zeitschrift **283** (2016), 835–859. ↑

[GJLR17] E. González-Jiménez and Á. Lozano-Robledo, *On the minimal degree of definition of p-primary torsion subgroups of elliptic curves*, Mathematical Research Letters **24** (2017), no. 4, 1067–1096. ↑128

[GJLR18] E. González-Jiménez and Á. Lozano-Robledo, *On the torsion of rational elliptic curves over quartic fields*, Mathematics of Computation **87** (2018), 1457–1478. ↑87, 89, 103, 195

[GJN20a] E. González-Jiménez and F. Najman, *An Algorithm for Determining Torsion Growth of Elliptic Curves*, Experimental Mathematics **0** (2020), no. 0, 1–12, available at https://doi.org/10.1080/10586458.2020.1771638. ↑74, 101, 102

[GJN20b] E. González-Jiménez and F. Najman, *Growth of torsion subgroups of elliptic*

*curves upon base change*, Mathematics of Computation **89** (2020), 1457–1485. ↑87, 90, 91, 94, 95, 96, 97, 98, 99, 100, 101, 103, 112, 127, 142, 167, 168, 187, 188, 189, 195

[GJNT16] E. González-Jiménez, F. Najman, and J. M. Tornero, *Torsion of rational elliptic curves over cubic fields*, Rocky Mountain Journal of Mathematics **46** (2016), no. 6, 1899–1917. ↑102, 147, 154, 155, 158, 163, 175, 196

[GJT10] E. González-Jiménez and J. M. Tornero, *On the ubiquity of trivial torsion on elliptic curves*, Archiv der Mathematik **95** (2010), no. 2, 135–141. ↑123

[GJT14] E. González-Jiménez and J. M. Tornero, *Torsion of rational elliptic curves over quadratic fields*, Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matematicas **108** (2014), 923–934. ↑102

[GJT16] E. González-Jiménez and J. M. Tornero, *Torsion of rational elliptic curves over quadratic fields II*, Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matematicas **110** (2016), 121–143. ↑102

[GK20] T. Gužvić and I. Krijan, *Torsion groups of elliptic curves over some infinite abelian extensions of* $\mathbb{Q}$, 2020. ↑112, 113

[Gre99] R. Greenberg, *Iwasawa theory for elliptic curves* (1999), 51–144. ↑111

[GSGJT10] I. García-Selfa, E. González-Jiménez, and J. M. Tornero, *Galois theory, discriminants and torsion subgroup of elliptic curves*, Journal of Pure and Applied Algebra **214** (2010), 1340–1346. ↑

[GSS19] T. A. Gassert, H. Smith, and K. E. Stange, *A family of monogenic $S_4$ quartic fields arising from elliptic curves*, Journal of Number Theory **197** (2019), 361–382. ↑196

[Gužv19] T. Gužvić, *Torsion of elliptic curves with rational $j$-invariant defined over number fields of prime degree*, 2019. ↑113, 114, 132, 171, 175, 196

[Gužv21] T. Gužvić, *Torsion growth of rational elliptic curves in sextic number fields*, Journal of Number Theory **220** (2021), 330–345. ↑93

[HM19] Y. Hirakawa and H. Matsumura, *A unique pair of triangles*, Journal of Number Theory **194** (2019), 297–302. ↑21

[HS00] M. Hindry and J. H. Silverman, *Diophantine Geometry: An Introduction*, Springer-Verlag New York, 2000. ↑9, 12

[HS17] R. Harron and A. Snowden, *Counting elliptic curves with prescribed torsion*, Journal für die reine und angewandte Mathematik **729** (2017), 151–170. ↑123, 196, 197, 198

[Hus04] D. Husemöller, *Elliptic Curves*, Second Edition, Springer-Verlag New York, 2004. ↑23, 26

[Jeo16] D. Jeon, *Families of Elliptic Curves over Cyclic Cubic Number Fields with Prescribed Torsion*, Mathematics of Computation **85** (2016), no. 299, 1485–1502. ↑72

[JKL11a] D. Jeon, C. H. Kim, and Y. Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Mathematics of Computation **80** (2011), no. 273, 579–591. ↑72

[JKL11b] D. Jeon, C. H. Kim, and Y. Lee, *Families of elliptic curves over quartic number fields with prescribed torsion subgroups*, Mathematics of Computation **80** (2011), 2395–2410. ↑76

[JKL13] D. Jeon, C. H. Kim, and Y. Lee, *Infinite families of elliptic curves over Dihedral quartic number fields*, Journal of Number Theory **133** (2013), no. 1, 115–122. ↑76

[JKL15] D. Jeon, C. H. Kim, and Y. Lee, *Families of elliptic curves with prescribed torsion subgroups over dihedral quartic fields*, Journal of Number Theory **147** (2015), 342–363. ↑76

[JKP16] D. Jeon, C. H. Kim, and E. Park, *On the Torsion of Elliptic Curves over Quartic Number Fields*, Journal of the London Mathematical Society **74** (2016), 1–12. ↑76

[JKS04] D. Jeon, C. H. Kim, and A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arithmetica **113** (2004), no. 3, 291–301. ↑72

[JS20] D. Jeon and A. Schweizer, *Torsion of rational elliptic curves over different types of cubic fields*, International Journal of Number Theory **16** (2020), no. 6, 1307–1323. ↑74

[Kam92a] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Inventiones Mathematicae **109** (1992), no. 1, 221–229. ↑70

[Kam92b] S. Kamienny, *Torsion points on elliptic curves over fields of higher degree*, International Mathematics Research Notices **6** (1992), 129–133. ↑70

[Kat09] V. J. Katz, *A History of Mathematics: An Introduction*, second edition, Boston: Addison-Wesley, 2009. ↑4

[Ken82] M. A. Kenku, *On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class*, Journal of Number Theory **15** (1982), no. 2, 199–202. ↑122, 123

[Kis97] T. Kishi, *On Torsion Subgroups of Elliptic Curves with Integral j-Invariant over Imaginary Cyclic Quartic Fields*, Tokyo Journal of Mathematics **20** (1997), no. 2, 315–329. ↑117

[KM88] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Mathematics Journal **109** (1988), 125–149. ↑70

[KN11] S. Kamienny and F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta Arithmetica **152** (2011), no. 3, 291–305. ↑71, 87

[Kna92] A. W. Knapp, *Elliptic Curves. (MN-40), Volume 40*, Princeton University Press, 1992. ↑23, 26, 60, 170

[Kob93] N. Koblitz, *Introduction to elliptic curves and modular forms* **97** (1993). ↑17

[KSW19] Z. Klagsbrun, T. Sherman, and J. Weigandt, *The Elkies curve has rank 28 subject only to GRH*, Mathematics of Computation **88** (2019), 837–846. ↑38

[Kub76] D. S. Kubert, *Universal Bounds on the Torsion of Elliptic Curves*, Proceedings of the London Mathematical Society **s3-33** (1976), no. 2, 193–237. ↑148

[KW09a] C. Khare and J.-P. Wintenberger, *JP. Serre's modularity conjecture (I)*, Inventiones mathematicae **178** (2009), 485–504. ↑114

[KW09b] C. Khare and J.-P. Wintenberger, *JP. Serre's modularity conjecture (II)*, Inventiones mathematicae **178** (2009), 505–586. ↑114

[Lan02] S. Lang, *Algebra*, reviewed 3rd edition, Springer-Verlag New York, 2002. ↑138, 139, 157

[Lan90] S. Lang, *Cyclotomic Fields I and II*, 2nd ed., Springer-Verlag New York, 1990. ↑111

[Lev68] M. Levin, *On the group of rational points on elliptic curves over function fields*, American Journal of Mathematics **90** (1968), no. 2, 456–462. ↑118

[LFN20] S. Le Fourn and F. Najman, *Torsion of $\mathbb{Q}$-curves over quadratic fields*, Mathematical Research Letters **27** (2020), no. 1, 209–225. ↑114, 115

[LL85] M. Laska and M. Lorenz, *Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$*, Journal für die reine und angewandte Mathematik **355** (1985), 163–172. ↑104

[LN59] S. Lang and A. Neron, *Rational Points of Abelian Varieties Over Function Fields*, American Journal of Mathematics **81** (1959), no. 1, 95–118. ↑37

[LR06] Á. Lozano-Robledo, *On elliptic units and p-adic Galois representations attached to elliptic curves*, Journal of Number Theory **117** (2006), no. 2, 439–470. ↑

[LR13] Á. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Mathematische Annalen **357** (2013), 279–305. ↑xi, 60, 127, 131, 148, 150, 161, 173, 176, 177, 201, 202, 203

[LR15] Á. Lozano-Robledo, *Division fields of elliptic curves with minimal ramification*, Revista Matematica Iberoamericana **31** (2015), no. 4, 1311–1332. ↑

[LR16] Á. Lozano-Robledo, *Ramification in the division fields of elliptic curves with potential supersingular reduction*, Research in Number Theory **2** (2016), no. 1. ↑

[LR18] Á. Lozano-Robledo, *Uniform boundedness in terms of ramification*, Research in Number Theory **4** (2018), no. 6. ↑

[LR19] Á. Lozano-Robledo, *Galois representations attached to elliptic curves with complex multiplication*, 2019. ↑

[LR21] Á. Lozano-Robledo, *A probabilistic model for the distribution of ranks of elliptic curves over* $\mathbb{Q}$, Journal of Number Theory **221** (2021), 270–338. ↑39

[LRL10] Á. Lozano-Robledo and B. Lundell, *Bounds for the torsion of elliptic curves over extensions with bounded ramification*, International Journal of Number Theory **6** (2010), no. 6, 1293–1309. ↑

[Lut37] É. Lutz, *Sur l'equation $y^2 = x^3 - ax - b$ dans les corps p-adic*, Journal für die reine und angewandte Mathematik **177** (1937), 237–247. ↑43

[LV20] B. Lawrence and A. Venkatesh, *Diophantine problems and p-adic period mappings*, Inventiones mathematicae **221** (2020), 893–999. ↑10

[BCFS10] W. Bosma, J. J. Cannon, C. Fieker, and A. Steel (eds.), *Handbook of Magma functions, Edition 2.16*, 2010. ↑126

[Mat93] Y. V. Matiyasevich, *Hilbert's Tenth Problem* (1993). ↑5

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Publications mathématiques de l'IHÉS **47** (1977), 33–186. ↑69, 139, 143

[Maz78] B. Mazur, *Rational isogenies of prime degree*, Inventiones mathematicae **44** (1978), 129–162. ↑69, 139, 143

[McD18] R. J. S. McDonald, *Torsion subgroups of elliptic curves over function fields of genus 0*, Journal of Number Theory **193** (2018), 395–423. ↑119, 120

[McD19a] R. J. S. McDonald, *Torsion Subgroups of Elliptic Curves over Function Fields* (2019). https://opencommons.uconn.edu/dissertations/2106. ↑121

[McD19b] R. J. S. McDonald, *Torsion subgroups of elliptic curves over function fields of genus 1* (2019). ↑121

[Mer96] L. Merel, *Bornes pour la torsiondes courbes elliptiques sur les corps de nombres*, Inventiones mathematicae **124** (1996), no. 1, 437–449. ↑67, 68, 101, 138

[Mil06] J. S. Milne, *Elliptic Curves*, BookSurge Publishers, 2006. ↑23, 26

[Mor22] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proceedings Cambridge Philosophical Society **21** (1922), 179–192. ↑36

[MP12] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, Panoramas & Synthèses **36** (2012), 99–117. ↑12

[MRUV20] C. Martinez-Ranero, J. Utreras, and C. R. Videla, *Undecidability of* $\mathbb{Q}^{(2)}$, Proceedings of the American Mathematical Society **148** (2020), no. 3, 961–964. ↑6

[MSZ89] H. Müller, H. Ströher, and H. Zimmer, *Torsion groups of elliptic curves with integral $j$-invariant over quadratic fields*, Journal für die reine und angewandte Mathematik **397** (1989), 100–161. ↑78

[Nag35] T. Nagell, *Solution de quelque problèmes dans la théorie arithmétique des cubiques planes du premier genre*, Wid. Akad. Skrifter Oslo **1** (1935). ↑43

[Naj10] F. Najman, *Complete classification of torsion of elliptic curves over quadratic*

*cyclotomic fields*, Journal of Number Theory **130** (2010), no. 9, 1964–1968. ↑71, 87

[Naj11] F. Najman, *Torsion of elliptic curves over quadratic cyclotomic fields*, Mathematical Journal of Okayama University **53** (2011), 75–82. ↑71, 87

[Naj12a] F. Najman, *Exceptional elliptic curves over quartic fields*, International Journal of Number Theory **8** (2012), 1231–1246. ↑76

[Naj12b] F. Najman, *Torsion of elliptic curves over cubic fields*, Journal of Number Theory **132** (2012), 26–36. ↑72, 96, 142

[Naj16] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$, Mathematical Research Letters **23** (2016), no. 1, 245–272. ↑74, 86, 87, 97, 132, 133, 140, 142, 143, 144, 149, 185

[Nat00] M. B. Nathanson, *Elementary Methods in Number Theory*, Spring-Verlag, 2000. ↑7

[Nér52] A. Néron, *Problèmes arithmétique et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*, Bulletin de la Société Mathématique de France **80** (1952), 101–166. ↑37

[Neu99] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg, 1999. Translated by Schappacher, N. ↑177, 178

[Ols74] L. D. Olson, *Points of finite order on elliptic curves with complex multiplication*, Manuscripta Mathematica **14** (1974), 195–205. ↑78

[Par89] J. L. Parish, *Rational Torsion in Complex-Multiplication Elliptic Curves*, Journal of Number Theory **33** (1989), 831–838. ↑78

[Par99] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, Journal für die reine und angewandte Mathematik **506** (1999). ↑67, 68, 138

[Phi21] T. Phillips, *Most Elliptic Curves over Global Function Fields are Torsion Free*, 2021. ↑123

[Pil17] J. Pila, *On a modular Fermat equation*, Commentarii Mathematici Helvetici **92** (2017), 85–103. ↑114

[Poi01] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, Journal de Mathématiques pures et appliquées **7** (1901), no. 3, 161–233. ↑36

[Poo03] B. Poonen, *Hilbert's Tenth Problem over Rings of Number-Theoretic Interest* (2003). https://math.mit.edu/~poonen/papers/aws2003.pdf. ↑x, 6

[Poo15] B. Poonen, *Average rank of elliptic curves*, 2015. ↑41

[Poo17] B. Poonen, *Rational Points on Varieties*, American Mathematical Society, 2017. ↑12

[Poo20] B. Poonen, *p-adic approaches to rational and integral points on curves*, 2020. ↑11

[PPV20] M. Pizzo, C. Pomerance, and J. Voight, *Counting elliptic curves with an isogeny of degree three*, Proceedings of the American Mathematical Society, Series B **7** (2020), 28–42. ↑123, 199

[PPVM19] J. Park, B. Poonen, J. Voight, and M. Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, Journal of the European Mathematical Society (2019). ↑39

[PWZ97] A. Pethö, T. Weis, and H. G. Zimmer, *Torsion Groups of Elliptic Curves with Integral $j$-invariant over General Cubic Number Fields*, International Journal of Algebra and Computation **7** (1997), no. 3, 353–413. ↑78

[PY01] D. Prasad and C. S. Yogananda, *Bounding the torsion in CM elliptic curves*, Comptes Rendus Mathematiques de l'Academie des Sciences. La Societe Royale du Canada **23** (2001), no. 1, 1–5. ↑78

[Rab10] P. F. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arithmetica **144** (2010), no. 1, 17–52. ↑70

[Rib04] K. A. Ribet, *Abelian Varieties over $\mathbb{Q}$ and Modular Forms* (J. E. Cremona, J.-C. Lario, J. Quer, and K. A. Ribet, eds.), Birkhäuser Basel, Basel, 2004. ↑

[Rib81] K. A. Ribet, *Torsion points of abelian varieties in cyclotomic extensions*, L'Enseignement Mathématique **27** (1981), 315–319. ↑109

[Rib90] K. A. Ribet, *On modular representations of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) arising from modular forms*, Inventiones Mathematicae **100** (1990), no. 2, 431–476. ↑15

[Rib95] K. A. Ribet, *Galois representations and modular forms*, Bulletins of the American Mathematical Society **32** (1995), 375–402. ↑15

[RZB15] J. Rouse and D. Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Research in Number Theory **1** (2015), no. 12. ↑128

[Sel51] E. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Mathematica **85** (1951), 203–362. ↑5

[Ser72] J.-P. Serre, *Propriètès galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones mathematicae **15** (1972), 259–331. ↑57

[Sil09] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer-Verlag New York, 2009. ↑23, 26, 28, 32, 33, 35, 36, 42, 43, 44, 45, 46, 47, 49, 50, 51, 52, 78

[Sil88] A. Silverberg, *Torsion points on abelian varieties of CM-type*, Compositio Mathematica **68** (1988), no. 3, 241–249. ↑78

[Sil94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, 1st ed., Springer-Verlag New York, 1994. ↑61, 63

[Sin12] S. Singh, *Fermat's Last Theorem*, Harper Press, 2012. ↑15

[Smi18] H. Smith, *Two families of monogenic $S_4$ quartic number fields*, Acta Arithmetica **186** (2018), 257–271. ↑196

[Smi20a] H. Smith, *Non-monogenic Division Fields of Elliptic Curves*, 2020. ↑196

[Smi20b] H. Smith, *Ramification in Division Fields and Sporadic Points on Modular Curves*, 2020. ↑196

[Sno13] A. Snowden, *Course on Mazur's theorem*, 2013. ↑70

[Spr20] C. Springer, *Undecidability, unit groups, and some totally imaginary infinite extensions of* $\mathbb{Q}$, Proceedings of the American Mathematical Society **148** (2020), 4705–4715. ↑6

[SS96] R. Schoof and N. Schappacher, *Beppo Levi and the arithmetic of elliptic curves* **18** (1996), no. 1, 57–69. ↑68

[ST15] J. H. Silverman and J. T. Tate, *Rational Points on Elliptic Curves*, 2nd ed., Springer International Publishing, 2015. ↑23

[ST67] I. Shafarevich and J. Tate, *The rank of elliptic curves*, Transactions of the American Mathematical Society **8** (1967), 917–920. ↑38

[Sut16] A. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum of Mathematics, Sigma **4** (2016). ↑58

[SvH21] H. Smith and M. van Hoeij, *A Divisor Formula and a Bound on the* $\mathbb{Q}$-

*Gonality of the Modular Curve $X_1(N)$*, Research in Number Theory **7** (2021), no. 22. ↑196

[The20] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 8.8)*, 2020. `https://www.sagemath.org`. ↑126

[Trb18] A. Trbović, *Torsion groups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$, $0 < d < 100$*, 2018. ↑88

[Tun83] J. B. Tunnell, *A Classical Diophantine Problem and Modular Forms of Weight 3/2*, Inventiones mathematicae **72** (1983), 323–334. ↑17

[TW95] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Mathematics **141** (1995), no. 3, 553–572. ↑15

[Vél71] J. Vélu, *Isogénies entre courbes elliptiques*, Comptes-Rendus de l'Académie des Sciences, Série I **273** (1971), 238–241. ↑46

[vH14] M. van Hoeij, *Low degree places on the modular curve $X_1(N)$*, 2014. ↑74

[Vog68] K. Vogel, *Neun Bucher arithmetischer Technik*, Braunschweig: Vieweg, 1968. ↑4

[Voj91] P. Vojta, *Siegel's theorem in the compact case*, Annals of Mathematics **133** (1991), no. 2, 509–548. ↑10

[Was03] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman & Hall/CRC, 2003. ↑13, 23, 26

[Was97] L. C. Washington, *Introduction to Cyclotomic Fields* (1997). ↑111

[Wei29] A. Weil, *L'arithmétique sur les courbes algébriques*, Acta Mathematica **52** (1929), 281–315. ↑37

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics **141** (1995), no. 3, 443–551. ↑15

[Zag90] D. Zagier, *Elliptische Kurven: Fortschritte und Anwendungen*, Jahresbericht der Deutschen Mathematiker-Vereinigung (DMV) **92** (1990), no. 2, 58–76. ↑16

[ZSM89] H. G. Zimmer, H. Ströher, and H. H. Müller, *Torsion groups of elliptic curves with integral $j$-invariant over quadratic fields*, Journal für die reine und angewandte Mathematik **397** (1989), 100–161. ↑116

[Zyw15] D. Zywina, *On the possible images of the mod ell representations associated to elliptic curves over* $\mathbb{Q}$ (2015), available at 1508.07660. ↑58

# Caleb G. McWhorter — CV

Department of Mathematics — Syracuse University
215 Carnegie Building — Syracuse, NY 13244
+1 (315) 443 3849 • cgmcwhor@syr.edu
https://cgmcwhor.expressions.syr.edu • https://coffeeintotheorems.com

## Education

- **Ph.D. Mathematics**, *Expected May 2021*
  *Syracuse University; Syracuse, NY*
  *Thesis Advisor: Dr. Steven Diaz*

- **M.S. Mathematics**, *May 2017*
  *Syracuse University; Syracuse, NY*

- **B.A. Mathematics**, *May 2013*
  **B.A. Physics**, *May 2013*
  *Ithaca College; Ithaca, NY*
  *Mathematics Advisors: Dr. David Brown, Dr. Emilie Wiesner*
  *Physics Advisors: Dr. Dan Briotta, Dr. Matthew Sullivan*

### Research Interests

- **Arithmetic Algebraic Geometry**
  Elliptic Curves (especially torsion), Computational Arithmetic Algebraic Geometry, Modular Curves, Modular Forms

- **Number Theory**
  Algebraic Number Theory, Elementary Number Theory, Coefficients of Cyclotomic Polynomials, Cryptography, Coding Theory

- **Other Interests**
  Mathematics Education, Mathematical Art, Mathematics Outreach

## Grants & Awards

### Grants

- NSF Grant, DMS 1908497, $30,000 – Infrastructure Program (Co.P.I. with Dr. Graham Leuschke), 2019 – 2021 — Support Conference Travel for Underrepresented Groups

### Awards

- Outstanding Teaching Assistant Award 2021, Syracuse University
- Certificate in University Teaching, *Fall 2019*
- National Forensics Association: National Novice Lincoln Douglass Best Speaker 2010

## Publications

- ◇ *Torsion of Rational Elliptic Curves over Nonic Galois Fields*, in preparation
- ◇ *Torsion of Rational Elliptic Curves over Odd Degree Galois Fields*, in preparation

### Work in Progress

- ◇ *Densities of Torsion Subgroups of Rational Elliptic Curves over Quadratic Fields*, in progress
- ◇ *Torsion Subgroups of Rational Elliptic Curves over Nonic Fields*, in progress
- ◇ *Torsion Subgroups of Rational Elliptic Curves over Degree 14 & 15 Fields*, in progress

## Advising & Mentoring

▶ **Directed Reading Program**
- Muhammadzhon Badalbaev, Fall 2020, *Project: Combinatorial Game Theory*
- Samuel Wheeler, Spring 2019, *Project: Elliptic Curves And Their Cryptographic Applications*
- Xinxuan Wang, Fall 2018, *Project: Fermat's Last Theorem and Elliptic Curves*

## Employment

▶ **American Mathematical Society**
Editor-in-Chief, Graduate Student Blog, Fall 2019 – Present

▶ **Syracuse University**
Graduate Instructor, Fall 2014 – Present

▶ **SUNY Adirondack**
Adjunct Instructor, Fall 2013 – Spring 2014

▶ **Cornell University**
Cornell Survey Research Institute, January 2013 – June 2013

▶ **Rose-Hulman Institute of Technology**
Research Undergraduate Experience, June 2012 – July 2012
Project: A Comparison of Breads as Liquid Drops and Foams

▶ **Ithaca College**
Academic Assistant, March 2010 – May 2013
Ithaca College Mathematics Help Room, Fall 2012 – Spring 2013
Research Undergraduate Experience, June 2011 – August 2011
Project: A Comparative Analysis of Gains in the MPEX and FCI

## Teaching Experience

### Instructor of Record

▶ **Syracuse University**
- MAT 121: Probability and Statistics for the Liberal Arts I, *Summer 2018, 2019*
- MAT 194: Precalculus, *Summer 2015*
- MAT 222: Probability and Statistics II, *Fall 2019, Spring 2017, 2019*
- MAT 295: Calculus I, *Fall 2016, 2018, Spring 2021*
- MAT 296: Calculus II, *Fall 2017, Spring 2018, Summer 2016*
- MAT 397: Calculus III, *Summer 2017, Spring 2019, Fall 2020*

### Teaching Assistant

▶ **Syracuse University**
- MAT 221: Probability and Statistics I, *Fall 2014*
- MAT 296: Calculus II, *Fall 2014, 2015*
- MAT 397: Calculus III, *Fall 2015, Spring 2016*

▶ **Ithaca College**
- Mathematics for Business, *Spring 2013*
- Introductory Statistics, *Fall 2012*
- Calculus I, *Fall 2012*
- Calculus for Decision Making, *Spring 2012*

### Mathematics Clinics & Tutoring

▶ **Syracuse University**
- University Mathematics Clinic, *Fall 2016 – May 2021*
- Mathematics Help Room, *Fall 2015 – Spring 2016, Spring 2017, 2019*

▶ **SUNY Adirondack**
- Mathematics & Physics Clinic Instructor, *August 2013 – May 2014 (3 credits each)*

▶ **Ithaca College**
- Ithaca College Mathematics Help Room, *Fall 2012 – Spring 2013*
- Academic Assistant, *March 2010 – May 2013*

## Departmental & University Service

### Departmental Service

▶ **Syracuse University**

◇ Associate Seminar Organizer for Technological Support, Algebra Seminar, Mathematics Department, *August 2020 – May 2021*

◇ Colloquium Organizer, Mathematics Graduate Organization, *August 2020 – May 2021*

- ◇ Directed Reading Program Organizer, *February 2019 – May 2021*
- ◇ Organizer, 44th Annual New York State Regional Graduate Mathematics Conference, *2019*
- ◇ Co-Organizer, Annual NYS Regional Graduate Mathematics Conference, *2017, 2018, 2020, 2021*
- ◇ Directed Reading Program Mentor (DRP), *Fall 2018 – May 2021*
- ◇ Website Coordinator & Social Media Manager, *August 2016 – May 2021*
- ◇ President, Mathematics Graduate Organization, *2018 – 2019*
- ◇ Secretary, Mathematics Graduate Organization, *2017 – 2018*
- ◇ Undergraduate Mathematics Committee Graduate Student Representative, *2017 – 2018*
- ◇ Preliminary Exam Help Session Organizer, *2017 – 2018*

## University Service

### ▶ Syracuse University

- ◇ Excellence in Graduate Education (EGE) Faculty Recognition Awards Selection Committee, *February 2021 – April 2021*
- ◇ Agenda Committee, Graduate Student Organization, *November 2020 – May 2021*
- ◇ Pandemic Committee, Graduate Student Organization, *October 2020 – May 2021*
- ◇ Finance Committee, Graduate Student Organization, *September 2019 – May 2021*
- ◇ Teaching Mentor, The Graduate School, *June 2016 – May 2021*
- ◇ Senator, Graduate Student Organization, *August 2019 – May 2021*
- ◇ GRE Preparatory Workshop (Mathematics Portion Instructor), *Fall 2019 – Spring 2020*
- ◇ Teaching Panel, ENL Panel for International Students, *October 2019*
- ◇ Teaching Mentor Selection Committee, The Graduate School, *Spring 2019, 2021*
- ◇ Teaching Panel, Negotiating Student Preparation & Abilities in STEM, *October 2018*
- ◇ Textbook & Course Typist, Whitman School of Management, *Spring 2017 – 2021*
- ◇ Video Captioning, The Graduate School: TA Program Seminars *2016 – 2021*

### ▶ Ithaca College

- ◇ Sydney Landon Debate Tournament Judge, *February 2019, 2020, 2021*

# Presentations

## Invited Talks

◇ *Mordell-Weil Groups of Elliptic Curves* — *November 2019*
Arithmetic Geometry Seminar, Binghamton University

◇ *Rational Points on Curves* — *November 2019*
Arithmetic Geometry Seminar, Binghamton University

## Research Talks

◇ *Torsion Subgroups of Rational Elliptic Curves over Odd Degree Galois Fields* — *April 2021*
Dissertation Defense

◇ *Torsion Subgroups of Rational Elliptic Curves over Odd Degree Galois Fields* — *April 2021*
46th Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC)

◇ *Torsion Subgroups of Rational Elliptic Curves over Odd Degree Galois Fields* — *November 2020*
Binghamton University Graduate Conference in Algebra & Topology (BUGCAT)

◇ *Torsion Subgroups of Rational Elliptic Curves over Nonic Galois Fields* — *November 2019*
Binghamton University Graduate Conference in Algebra & Topology (BUGCAT)

◇ *Torsion Subgroups of Rational Elliptic Curves over Nonic Galois Fields* — *October 2019*
Maine-Québec Number Theory Conference

◇ *Progress in the Classification of Torsion Subgroups of Elliptic Curves* — *March 2019*
44th Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC)

◇ *Torsion of Elliptic Curves over Number Fields of Small Degree* — *October 2018*
Binghamton University Graduate Conference in Algebra & Topology (BUGCAT)

◇ *Torsion of Elliptic Curves over Nonic Fields* — *March 2018*
43rd Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC)

◇ *A Foam Model for Bread Development* — *April 2013*
16th James J. Whalen Academic Symposium

◇ *A Foam Model for Bread Development* — *February 2013*
Ithaca College Physics Seminar

◇ *A Foam Model for Bread Development* — *July 2012*
Indiana Undergraduate Research Conference, Indiana University

## University & Department Talks

◇ *Teaching Online* — *August 2020*
All-University TA Orientation Program

◇ *Building an Online Teaching Portfolio* — *February 2020*
The Graduate School: TA Program Seminars

◇ *Assessment in the Classroom* — *August 2019*
All-University TA Orientation Program

◇ *Narcissus, An Autobiography: Evaluating Your Teaching* — *October 2018*
The Graduate School: TA Program Seminars

◇ *Supporting Students Across the Spectrum of Academic Preparation* — *October 2018*
The Graduate School: TA Program Seminars

◇ *What they didn't tell me in orientation: a follow-up workshop for TAs* — *September 2018*
The Graduate School: TA Program Seminars

◇ *Effective Assessment in the Classroom* — *September 2018*
All-University TA Orientation Program

◇ *Welcome to the Mathematics Department: A Guide for the Perplexed* — *August 2018*
Syracuse University Mathematics Department

◇ *Effective Assessment in the Classroom* — *August 2018*
The Graduate School: Teaching Assistant Orientation

◇ *Constructing an Online Teaching Portfolio* — *February 2018*
The Graduate School: TA Program Seminars

◇ *Constructing a Teaching Portfolio* — *January 2018*
The Graduate School: TA Program Seminars

◇ *Revisiting Orientation: A Follow-Up Workshop for TAs* — *September 2017*
The Graduate School: TA Program Seminars

◇ *Integrating Technology in the Classroom* — *August 2017*
The Graduate School: Teaching Assistant Orientation

◇ *Underrepresented Groups in Mathematics* — *March 2017*
Syracuse University Graduate Mathematics Colloquium

◇ *Constructing a Teaching Portfolio* — *January 2017*
The Graduate School: TA Program Seminars

◇ *Revisiting Orientation: A Follow-Up Workshop for TAs* — *September 2016*
The Graduate School: TA Program Seminars

◇ *(Self)Assessment in Teaching* — *August 2016*
The Graduate School: Teaching Assistant Orientation

## Expository Talks

◇ *Combinatorial Game Theory: NIM Games and Numbers in the Land of Oz* — *October 2020*
Syracuse University Graduate Mathematics Colloquium

◇ *Non-Abelian Chabauty* *March 2020*
45th Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC)

◇ *Ranks of Elliptic Curves: Why Rank is (Almost Certainly) Bounded* *March 2019*
Syracuse University Algebra Seminar

◇ *To Infinity & Beyond: The Tale of really Big NUMBERS!* *September 2018*
Syracuse University Mathematics Graduate Colloquium

◇ *Introduction to Algebraic Number Theory & Arithmetic Geometry* *April 2018*
Syracuse University Graduate Mathematics Colloquium

◇ *Hungry, Hungry, Homology (Parts I & II)* *September 2017*
Syracuse University Graduate Mathematics Colloquium

◇ *Perfectoid Spaces* *April 2017*
Syracuse University Algebra Seminar

◇ *Adic & Perfectoid Spaces* *March 2017*
42nd Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC)

◇ *Analysis on Surreal Numbers* *April 2016*
41st Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC)

◇ *A Zero Divisor Conjecture for Hopf Algebras* *April 2015*
40th Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC)

◇ *Elliptic Curves, Galois Representations, and their L-functions* *October 2014*
Syracuse University Graduate Mathematics Colloquium

◇ *The Critical Thread: The Symmetric Group in Galois Theory, Representation Theory, Representations of Lie Algebras, Combinatorics, and Topology* *May 2013*
Ithaca College Undergraduate Mathematics Thesis Presentation

## Conferences and Workshops

### Conferences

- Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC) *April 2021*
- Joint Mathematics Meeting (JMM) *January 2021*
- Binghamton University Graduate Conference in Algebra & Topology (BUGCAT) *November 2020*
- Maine-Québec Number Theory Conference *September 2020*
- Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC) *March 2020*
- Binghamton University Graduate Conference in Algebra & Topology (BUGCAT) *November 2019*

- Maine-Québec Number Theory Conference *October 2019*
- Union College Mathematics Conference *September 2019*
- Annual Upstate Number Theory Conference *April 2019*
- Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC) *March 2019*
- Binghamton University Graduate Conference in Algebra & Topology (BUGCAT) *October 2018*
- Québec-Maine Number Theory Conference *October 2018*
- Annual Upstate Number Theory Conference *April 2018*
- Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC) *March 2018*
- Maine-Québec Number Theory Conference *October 2017*
- Annual Upstate Number Theory Conference *April 2017*
- Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC) *March 2017*
- Québec-Maine Number Theory Conference *October 2016*
- Route 81 Conference on Commutative Algebra and Algebraic Geometry *September 2016*
- Super QVNTS - Kummer Classes and Anabelian Geometry *September 2016*
- International Conference on Representations of Algebras (ICRA) *August 2016*
- Annual Upstate Number Theory Conference *April 2016*
- Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC) *March 2016*
- Annual New York State Regional Graduate Mathematics Conference (ANYSRGMC) *March 2015*
- Elliptic Curves@UCONN *May 2014*

**Workshops**

- Arizona Winter School: Nonabelian Chabauty *March 2020*
- 33rd Automorphic Forms Workshop *March 2019*
- Arizona Winter School: Topology & Arithmetic *March 2019*
- Connecticut Summer School in Number Theory *June 2018*
- Arizona Winter School: Iwasawa Theory *March 2018*
- Arizona Winter School: Perfectoid Spaces *March 2017*

## Skills

- **Mathematics Programs:** Sage, MAGMA, Mathematica, MATLAB, Maple, Minitab, SPSS, Geogebra, Surface Evolver, (La)TeX
- **Presentational Programs:** Beamer, Microsoft Word, Microsoft Powerpoint, Microsoft Excel, Pages, Keynote, Inkscape, GoogleDocs, GoogleForms, GoogleSheets, GoogleSlides
- **Programming:** C++, Python, Java, GoogleScript, WordPress
- **Languages:** English, Spanish (Intermediate), German (Beginner), French (Beginner)
- **Debate:** Lincoln-Douglas, Parliamentary, Open/Public Forum, Worlds, Policy
- **Music:** Classically Trained Violinist

## References

**Dr. Steven Diaz**
*Professor (Thesis Advisor)*
*Department of Mathematics*
*Syracuse University*
*Email: spdiaz@syr.edu*
*Phone: 315.443.1583*

**Dr. Graham Leuschke**
*Professor and Department Chair*
*Department of Mathematics*
*Syracuse University*
*Email: gjleusch@syr.edu*
*Phone: 315.443.1500*

**Dr. Duane Graysay**
*Assistant Professor*
*Department of Mathematics*
*Syracuse University*
*Email: dtgraysa@syr.edu*
*Phone: 315.443.1485*

**Shawn Loner**
*TA Program Coordinator*
*The Graduate School*
*Syracuse University*
*Email: scloner@syr.edu*
*Phone: 315.443.3863*

**Glenn Wright**
*Director of Programs*
*The Graduate School*
*Syracuse University*
*Email: glwright@syr.edu*
*Phone: 315.443.3458*

**Dr. Raja Velu**
*Professor*
*Whitman School of Management*
*Syracuse University*
*Email: rpvelu@syr.edu*
*Phone: 315.443.3526*