Research Statement

Robert J.S. McDonald
Department of Mathematics, Yale University;
442 Dunham Lab; 10 Hillhouse Ave; New Haven, CT 06511
1-(860)-608-3329 | robert.j.mcdonald@yale.edu
https://mathrjsm.com

1. Summary

My area of research is number theory, particularly arithmetic geometry. My thesis classifies solutions to a certain type of diophantine equation called an elliptic curve. In particular, given an elliptic curve E whose defining equation has coefficients in the field $\mathbb{Q}$ or $\mathbb{F}_p(T)$, or more generally in a global field K, the set of points on E with coordinates in the field forms a finitely generated abelian group. I am interested in the structure of this group when K is a function field, primarily the structure of the torsion subgroup, which is the points of finite order. My research has culminated in the following two results.

(1) **Torsion subgroups of elliptic curves over function fields of genus 0.** Given any function field $K = \mathbb{F}_q(T)$, of characteristic p, I have determined all possible torsion subgroups of an elliptic curve over K and shown that each appears infinitely often. Moreover, I provide parameterizations of all elliptic curves over K with each torsion subgroup.
(2) **Torsion subgroups of elliptic curves over function fields of genus 1.** Given any genus one function field K, of characteristic p, I have determined all possible torsion subgroups of an elliptic curve over K. Each torsion subgroup appears infinitely often, provided the base curve is isogenous to a specified curve. This time, for each exotic torsion structure, I determine conditions on the base curve necessary for each torsion subgroup to appear.

2. Experience working with undergraduates

In Section 6, I outline a few of the future directions that I would like to take my research, and talk about how I think students could be involved. At the University of Connecticut (UConn), I have had already had some experience mentoring undergraduates in the Directed Reading Program, and in the Connecticut School of Number Theory (CTNT) summer school. Both of these experiences were a unique opportunity to expose myself to undergraduate research as a graduate student.

In the Directed Reading Program, I was able to connect with an undergraduate and read through a graduate-level text in number theory. The student and I met once a week to discuss readings and problems from a section of the book, and work through these together on the board. For the student, this was an exposure to graduate-level mathematics. For me, this was an opportunity to gain experience engaging with undergraduates in a seminar setting, outside the classroom.

The CTNT summer school is aimed at undergraduates with an interest in doing research, some who may even have an interest in pursuing a graduate career. Students spend a week in graduate-level courses, and work through problem sets that may lead to collaboration after the program ends. In this program, I had the responsibility of mentoring students during these problem sets.

The book Elliptic Curves, Modular Forms and Their L-functions, by Álvaro Lozano-Robledo, is a book aimed at undergraduates interested in number theory, and in this context, introduces elliptic curves. I would be very interested reading through a book like this with a student, and

using it as a jumping off point to involvement in my research. Particularly, elliptic curves are used in cryptography and cybersecurity which would interest math or computer science students.

3. Introduction: Elliptic Curves over $\mathbb{Q}$

Many interesting problems in number theory arise from problems which are quite easy to state, but very hard to solve. One such famous result is Fermat's Last Theorem, first written down in the margins of Pierre de Fermat's copy of Diophantus' *Arithmetica* around 1637. Here, Fermat claimed that the following polynomial equation has no non-zero integer solution (x, y, z), for any $n \geq 3$:

$$x^n + y^n = z^n.$$

Although Fermat claimed to have a "truly remarkable proof" of this fact, the margins were "too small to contain it," and the world would have to wait another 350 years before the matter was finally settled by Andrew Wiles in 1994.

Wiles' proof of Fermat's Last Theorem used a special case of certain conjectures about another type of diophantine equation, an elliptic curve, and used a variety of techniques from algebraic geometry and number theory. Elliptic curves are of particular interest to me, and have comprised the bulk of my research. Over the rational numbers, $\mathbb{Q}$, an elliptic curve is a diophantine equation of the form

$$E : y^2 = x^3 + Ax + B, \text{ where } A, B \in \mathbb{Z}.$$

Given such a curve, a natural questions is: can we determine its solutions over $\mathbb{Z}$ or $\mathbb{Q}$? So far, in the general case, this question leads to many unanswered problems.

The $\mathbb{Q}$-rational points will be denoted by $E(\mathbb{Q})$. The most interesting aspect of elliptic curves is the fact that they can be given a group structure, placing them squarely at the crossroads between algebra and geometry. We define elliptic curve addition by "chord and tangent addition:" to add points P and Q, we draw a line ℓ through P and Q and find the third point of intersection with E, which we call R. The point $P+Q$ is then the reflection of R about the x-axis. To add P to itself, we consider the tangent to E at P as intersecting E twice at P. Finally, in the case where ℓ is vertical, we imagine a point of intersection with E "at infinity," and call this point $\mathcal{O}$, which we use as the identity of this operation. See [11, Chapter 3] for a more in-depth description of this group law.

Example 3.1. The curve $E : y^2 = x^3 - x = x(x+1)(x-1)$ has only four integral points $(0, 0)$, $(\pm 1, 0)$, and the point $\mathcal{O}$. Here, if $P = (0, 0)$ and $Q = (1, 0)$, then $2P = 2Q = \mathcal{O}$, and $P+Q = (-1, 0)$. It turns out that E has no other $\mathbb{Q}$-rational points, and hence $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The Mordell-Weil theorem describes the structure of $E(K)$ as a group:

Theorem 3.2 (Mordell-Weil)**.** *Let E be an elliptic curve over K. The group of K-rational points, $E(K)$, is a finitely generated abelian group.*

The fundamental theorem of finitely generated abelian groups and Theorem 3.2 tell us

$$E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^{r_{E/K}},$$

where $E(K)_{\text{tors}}$, the points of finite order, make up what is called the "torsion subgroup" of $E(K)$, and the independent points of infinite order provide $r_{E/K}$ copies of $\mathbb{Z}$. Here $r_{E/K}$ is called the "rank" of $E(K)$. While $r_{E/K}$ is rather difficult to compute, $E(K)_{\text{tors}}$ is very well understood over $\mathbb{Q}$ and low degree number fields. For example, Mazur proved the following result:

Theorem 3.3 (Mazur [11])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups:*

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & \text{with } N = 1, \ldots, 10, 12 \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{with } 1 \leq N \leq 4. \end{array}$$

Moreover, each of these groups appears as $E(\mathbb{Q})_{\text{tors}}$ for infinitely many (non-isomorphic) E.

This is a complete classification of the types of torsion subgroups one should expect to encounter for an elliptic curve over $\mathbb{Q}$. What about over extensions of $\mathbb{Q}$ such as $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$?

Theorem 3.4 (Kamienny–Kenku–Memose, [5, 6])**.** *Let E be an elliptic curve over a quadratic field K. Then the torsion subgroup $E(K)_{\text{tors}}$ is isomorphic to one of the following 26 groups*

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & \text{with } N = 1 \leq N \leq 18, N \neq 17, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{with } 1 \leq N \leq 6, \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, & \text{with } 1 \leq N \leq 2, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \end{array}$$

Moreover, each of these groups appears as $E(\mathbb{Q})_{\text{tors}}$ for infinitely many (non-isomorphic) E.

Note,

Theorem 3.5 (Jeon–Kim–Schweizer, [4])**.** *Let E be an elliptic curve over a cubic field K. Then the following 25 groups appear as $E(K)_{\text{tors}}$ for infinitely many non-isomorphic E.*

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & \text{with } N = 1 \leq N \leq 20, N \neq 17, 19, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{with } 1 \leq N \leq 7. \end{array}$$

Similarly, Jeon, Kim, and Park have determined determined the list of torsion sungroups with infinitely many non-isomorphic examples over cubic fields (see [3]). Again, it is not known whether there are any other sporadic points.

4. Elliptic Curves over Function Fields of Genus 0

Given a smooth curve $\mathcal{C}$ over a finite field $\mathbb{F}$ of characteristic p, we look at the function field $K = \mathbb{F}(\mathcal{C})$. In this section, we are primarily interested in the case where $\mathcal{C}$ has genus 0, so that $K \cong \mathbb{F}(\mathbb{P}^1) = \mathbb{F}(T)$, the field of rational functions in one indeterminate over $\mathbb{F}$.

4.1. **Previously known results.** In this setting, there are strong results for prime-to-p, and p-primary torsion structures, but there seems to be no marriage between the results in the literature. Levin, for example, was able to provide bounds on the size of both components:

Corollary 4.1 (Levin, [7])**.** *Let $\mathbb{F}$ be a finite field of characteristic p, $K = \mathbb{F}(T)$, and E/K an elliptic curve. Suppose $\ell^e \mid \#E(K)_{\text{tors}}$ for some prime ℓ. Then,*

$$\ell \leq 7 \text{ and } e \leq \begin{cases} 4 & \text{if } \ell = 2 \\ 2 & \text{if } \ell = 3, 5 \\ 1 & \text{if } \ell = 7 \end{cases} \quad \text{if } \ell \neq p, \qquad \text{and} \qquad \ell \leq 11 \text{ and } e \leq \begin{cases} 3 & \text{if } \ell = 2 \\ 2 & \text{if } \ell = 3 \\ 1 & \text{if } \ell = 5, 7, 11 \end{cases} \quad \text{if } \ell = p.$$

In [1], for all characteristics $p \neq 2, 3$ (in fact, for characteristic zero as well), Cox and Parry provide the following result for prime-to-p torsion subgroups possible over K.

Theorem 4.2 (Cox, Parry [1])**.** *Let $K = \mathbb{F}(T)$ where $\mathbb{F}$ is a finite field of characteristic $p \neq 2, 3$. Let E/K be non-isotrivial*[1]*. Then, $E(K)'_{\text{tors}}$, the rational points of finite order prime-to-p, is one of the following groups*

$$\begin{gathered} 0,\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \ldots,\ \mathbb{Z}/10\mathbb{Z},\ \mathbb{Z}/12\mathbb{Z}, \\ (\mathbb{Z}/2\mathbb{Z})^2,\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \\ (\mathbb{Z}/3\mathbb{Z})^2,\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\ (\mathbb{Z}/4\mathbb{Z})^2,\ (\mathbb{Z}/5\mathbb{Z})^2. \end{gathered}$$

[1]Non-isotriviality of E will be a common restriction on all of the elliptic curves we encounter in the remaining sections, and in most cases essentially amounts to the coefficients of E being "non-constant." For a more precise description, see [12].

Furthermore, let $G = \mathbb{Z}/m \times \mathbb{Z}/n\mathbb{Z}$ be in this list with $n \mid m$, and $p \nmid m$. Then, if $\mathbb{F}$ contains a primitive nth root of unity, there are infinitely many non-isomorphic, non-isotrivial elliptic curves with $E(K)_{\text{tors}} \cong G$.

All elliptic curves with each of the torsion subgroups in Cox and Parry's theorem can be parameterized using the Tate normal form which looks like

$$E_{a,b} : y^2 + (1-a)xy - by = x^3 - b^2 \text{ for } a, b \in K.$$

Cox and Parry's theorem deals only with prime-to-p torsion. From this, some natural questions arise: which structures from Theorem 4.2 can appear alongside a point of order p? What is the full list of torsion subgroups possible for an elliptic curve E/K? Which appear infinitely often? The following theorem will be paramount in answering these questions.

Theorem 4.3 ([12])**.** *Suppose that E is a non-isotrivial elliptic curve over $K = \mathbb{F}_q(\mathcal{C})$, where q is a power of p. Then, $E(K)$ has a point of order p if and only if $j(E) \in K^p$, and the Hasse invariant is a $(p-1)$st power in $K^\times$.*

The j and Hasse invariants of an elliptic curve over K are quite simple to compute. See [12], for example, for a precise definition of each.

4.2. **My results.** In this section, we summarize my results from [8]. Cox and Parry's theorem above is not stated when $p = 2, 3$, so we begin by developing the analogous statements for these two primes. It can be shown that Cox and Parry's theorem holds even when p is 2 or 3 [8, Theorems 4.2, 4.4]. Then, for each p and each group G from Theorem 4.2, we write a curve in Tate normal form for G. Using Theorem 4.3, or in some cases a division polynomial, we then construct a curve $\mathcal{D}/\mathbb{F}$, parameterizing elliptic curves with torsion subgroup $H = G \times \mathbb{Z}/p^e\mathbb{Z}$. It can be shown that the torsion structure H induces a separable map from $\mathcal{C} = \mathbb{P}^1$ to $\mathcal{D}$. Then, using the Hurwitz formula, if the genus of $\mathcal{D}$ is greater than 0, we obtain a contradiction. We arrive at the following result.

Theorem 4.4 (M)**.** *Let $\mathbb{F}$ be a finite field of characteristic p. Set $K = \mathbb{F}(T)$, and let E/K be a non-isotrivial elliptic curve. If $p \nmid \#E(K)_{\text{tors}}$, then $E(K)_{\text{tors}}$ is as in Theorem 4.2 (even if $p = 2, 3$). If $p \leq 11$, and $p \mid \#E(K)_{\text{tors}}$, then $E(K)_{\text{tors}}$ is isomorphic to one of the following groups:*

$\mathbb{Z}/p\mathbb{Z}$	
$\mathbb{Z}/2p\mathbb{Z}$	*if* $p = 2, 3, 5, 7$,
$\mathbb{Z}/3p\mathbb{Z}$	*if* $p = 2, 3, 5$,
$\mathbb{Z}/4p\mathbb{Z}, \mathbb{Z}/5p\mathbb{Z}$,	*if* $p = 2, 3$,
$\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/14\mathbb{Z}, \mathbb{Z}/18\mathbb{Z}$	*if* $p = 2$,
$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$	*if* $p = 2$, *and* $\zeta_5 \in k$,
$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	*if* $p = 3$, *and* $\zeta_4 \in k$,
$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	*if* $p = 5$.

Furthermore, let $G = \mathbb{Z}/m \times \mathbb{Z}/n\mathbb{Z}$ be in this list with $n \mid m$. Then, if $\mathbb{F}$ contains a primitive nth root of unity, there are infinitely many non-isomorphic, non-isotrivial elliptic curves with $E(K)_{\text{tors}} \cong G$. If $p \geq 13$, then Theorem 4.2 is a complete list of possible subgroups $E(K)_{\text{tors}}$.

For example, when we specialize to the case $p = 5$, the theorem takes the following form:

Corollary 4.5 (M)**.** *Let $\mathbb{F}$ be a finite field of characteristic 5, $K = \mathbb{F}(T)$, and E/K be a non-isotrivial elliptic curve. The torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following*

$\mathbb{Z}/N\mathbb{Z}$	*with* $1 \leq N \leq 10$ *or* $N = 12, 15$,
$\mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	*with* $1 \leq N \leq 5$,
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$,	
$\mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$,	*with* $N = 1, 2$,

Furthermore, let $G = \mathbb{Z}/m\times\mathbb{Z}/n\mathbb{Z}$ be in this list with $n \mid m$. Then, if $\mathbb{F}$ contains a primitive nth root of unity, there are infinitely many non-isomorphic, non-isotrivial elliptic curves with $E(K)_{\text{tors}} \cong G$.

In fact, we can parameterize all of the elliptic curves having each of the indicated torsion subgroups in Theorem 4.4. For example, when $p = 5$, a non-isotrivial E/K has a point of order fifteen if and only if it can be written in Tate normal form with

$$a = \frac{(f+1)(f+2)^2(f+4)^3(f^2+2)}{(f+3)^6(f^2+3)},\ b = a\frac{f(f+4)}{(f+3)^5} \text{ for some } f \in \mathbb{F}(T) \text{ such that } f \notin \mathbb{F}.$$

Here the point $(0, 0)$ is a point of order fifteen. In [8, Table 14] are parameterizations of all elliptic curves over $\mathbb{F}(T)$ with the torsion structures appearing in Theorem 4.4.

5. Elliptic Curves over Function Fields of Genus 1

In this section, we are primarily interested in the case where $\mathcal{C}$ has genus 1, so that $\mathcal{C}$ is an elliptic curve over $\mathbb{F}$. In this setting, [7] provides us with the following corollary.

Corollary 5.1 (Levin, [7])**.** *Let $\mathbb{F}$ be a finite field of characteristic p, $\mathcal{C}/\mathbb{F}$ be a smooth, projective, absolutely irreducible curve, $K = k(\mathcal{C})$, and E/K an elliptic curve. Suppose $\ell^e \mid \#E(K)_{\text{tors}}$ for some prime ℓ. Then,*

$$\ell \le 11 \text{ and } e \le \begin{cases} 4 & \text{if } \ell = 2 \\ 2 & \text{if } \ell = 3, 5 \\ 1 & \text{if } \ell = 7, 11 \end{cases} \text{ if } \ell \ne p, \qquad \text{and} \qquad \ell \le 11 \text{ and } e \le \begin{cases} 4 & \text{if } \ell = 2 \\ 2 & \text{if } \ell = 3 \\ 1 & \text{if } \ell = 5, 7, 11, 13 \end{cases} \text{ if } \ell = p.$$

5.1. **My results.** I have submitted a paper containing a full classification of the possible torsion subgroups for elliptic curves over function fields of genus 1 over finite fields. For the most current draft, please see my website https://mathrjsm.com/#research.

We begin, again, with a result analogous to that of Cox and Parry for the genus 1 case, using modular curves $X_n(m)$ and following their proof in [1] and the proof of [12, Proposition 7.1]:

Theorem 5.2 (M)**.** *Let $\mathcal{C}$ be a curve of genus 1 over a finite field $\mathbb{F}$ of characteristic p, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)'_{\text{tors}}$, the rational points of finite order prime-to-p, is one of the following groups:*

$$\begin{array}{cc} \mathbb{Z}/N\mathbb{Z} & \text{with } N = 1, \dots, 12, 14, 15, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{with } N = 1, \dots, 6, \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{with } N = 1, 2, 3, \\ \mathbb{Z}/4N\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{with } N = 1, 2, \\ (\mathbb{Z}/N\mathbb{Z})^2 & \text{with } N = 5, 6. \end{array}$$

Furthermore, let $G = \mathbb{Z}/m \times \mathbb{Z}/n\mathbb{Z}$ be in this list with $n \mid m$ and $p \nmid m$. Then, if $\mathbb{F}$ contains a primitive nth root of unity, there are infinitely many non-isomorphic, non-isotrivial elliptic curves with $E(K)_{\text{tors}} \cong G$.

We can provide parameterizations for any elliptic curves E with torsion subgroup appearing in this theorem which also appeared in Theorem 4.2, and these torsion subgroups appear infinitely often for some E/K regardless of the base curve $\mathcal{C}$. All the other subgroups, however, are restricted by $\mathcal{C}$. In each case, if a group G from Theorem 5.2 does not appear in Theorem 4.2, then infinitely many elliptic curves E/K can be found with $E(K)'_{\text{tors}} \cong G$ only if $\mathcal{C}$ is in a certain, specified, isogeny class. For example, if $p \ne 11$, E/K has a point of order 11 only if $\mathcal{C}$ is isogenous to $\mathcal{D} : u^2+u = t^3-t^2$.

Next, fixing p, we begin with an elliptic curve in Tate normal form for a torsion subgroup G appearing in Theorem 5.2. Then, using the Hasse invariant and division polynomials of the curve, we again construct a curve $\mathcal{D}/\mathbb{F}$ parameterizing elliptic curves with $G \times \mathbb{Z}/p^e\mathbb{Z}$ torsion. This time, we arrive at a contradiction if the genus of $\mathcal{D}$ is greater than one. We arrive at the following result.

Theorem 5.3 (M). *Let C be a curve of genus 1 over $\mathbb{F}_q$, for $q = p^n$, and let $K = \mathbb{F}_q(C)$. Let E/K be non-isotrivial. If $p \nmid \#E(K)_{\text{tors}}$, then $E(K)_{\text{tors}}$ is as in Theorem 5.2. If $p \mid \#E(K)_{\text{tors}}$, then $p \leq 13$, and $E(K)_{\text{tors}}$ is one of*

$$\begin{array}{cc}
\mathbb{Z}/p\mathbb{Z} & \text{if } p = 2, 3, 5, 7, 11, 13, \\
\mathbb{Z}/2p\mathbb{Z}, \mathbb{Z}/2p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } p = 3, 5, 7, \\
\mathbb{Z}/3p\mathbb{Z}, \mathbb{Z}/4p\mathbb{Z} & \text{if } p = 2, 3, 5 \\
\mathbb{Z}/5p\mathbb{Z}, \mathbb{Z}/6p\mathbb{Z}, \mathbb{Z}/7p\mathbb{Z}, \mathbb{Z}/8p\mathbb{Z} & \text{if } p = 2, 3, \\
\mathbb{Z}/2N\mathbb{Z} & \text{for } N = 9, 10, 11, 15, \text{ if } p = 2, \\
\mathbb{Z}/6N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{for } N = 1, 2, 3, \text{ if } p = 2, \\
\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} & \text{if } p = 2, \\
\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{if } p = 3.
\end{array}$$

Furthermore, let $G = \mathbb{Z}/m\times\mathbb{Z}/n\mathbb{Z}$ be in this list with $n \mid m$. Then, if $\mathbb{F}$ contains a primitive nth root of unity, there are infinitely many non-isomorphic, non-isotrivial elliptic curves with $E(K)_{\text{tors}} \cong G$. If $p \geq 17$, then Theorem 5.2 is a complete list of possible subgroups $E(K)_{\text{tors}}$.

For example, when $p = 5$ we obtain the following result.

Corollary 5.4. *Let $\mathcal{C}$ be a curve of genus 1 over a finite field $\mathbb{F}$ of characteristic 5, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then, $E(K)_{\text{tors}}$ is one of the following groups*

$$\begin{array}{cc}
\mathbb{Z}/N\mathbb{Z} & \text{with } N = 1, \ldots, 12, 14, 15, 20 \\
\mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{with } N = 1, \ldots, 6, \\
\mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{with } N = 1, 2, 3, \\
\mathbb{Z}/4N\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{with } N = 1, 2, \\
(\mathbb{Z}/6\mathbb{Z})^2. &
\end{array}$$

Furthermore, let $G = \mathbb{Z}/m\times\mathbb{Z}/n\mathbb{Z}$ be in this list with $n \mid m$. Then, if $\mathbb{F}$ contains a primitive nth root of unity, there are infinitely many non-isomorphic, non-isotrivial elliptic curves with $E(K)_{\text{tors}} \cong G$.

In Corollary 5.4, if G is already a group that appears in Corollary 4.5, that is, one that already appeared over function fields of genus 0, then we can find infinitely many E/K regardless of the base curve. If G does not appear in Corollary 4.5, however, then infinitely many curves E/K can be found with torsion subgroup G only if the base curve is in a specific isogeny class. For example, $E(K)$ has a point of order 20 only if $\mathcal{C}$ is isogenous to $\mathcal{D} : t^2 + t + 1 = u^4$.

6. Future directions and student involvement

I have already started thinking about future directions to take my research, and the level of student involvement I can see. In all three, there is room for student involvement.

(1) In a short paper *Maximum Difference*, Mizan Khan (Eastern Connecticut State University) has come up with an interesting result about the maximum difference between an element and its inverse modulo n. Currently, I am attempting to prove an analogue of this result for function fields, using degrees instead of absolute value. This project seems readily accessible to any student who has taken an introductory course to number theory.

(2) A *hyper*-elliptic curve is one that has an equation of the form $y^2 = f(x)$, where $f(x)$ is a cubic polynomial. It would be interesting to see what torsion subgroups can appear for elliptic curves over function fields of a hyperelliptic curve. The genus of $\mathcal{C}$ can become arbitrarily large, but there are other invariants of elliptic curves that behave in a similar way. It seems that some of the arguments I've used can be adapted to using these invariants.

This project would likely involve computations using an computer algebra system like Magma, which would be easy to involve a undergraduate in. The level would be appropriate for a student who has been introduced to abstract algebra. The computational aspect may

also be interesting to a student in computer science. The computer algebra systems used to script this type of computation would interest any student with a programming background.

I have already begun to think about taking my work in this direction. For example, a result from [10, Lemma 1.5 b,c] can be adapted to prove the following result

Corollary 6.1 (M)**.** *Let $\mathcal{C}$ be a hyperelliptic curve over a finite field $\mathbb{F}$ of characteristic p. Then, for any elliptic curve E/K, the condition $p^e \mid \#E(K)_{\text{tors}}$ implies*

$$p \leq 17 \qquad \text{and} \qquad e \leq \begin{cases} 4 & \text{if } p = 2, \\ 2 & \text{if } p = 3, \\ 1 & \text{if } p > 3. \end{cases}$$

(3) In [12], Ulmer gives families of elliptic curves with unbounded rank. It would be interesting to use my results and Ulmer's families to construct families with unbounded rank and a fixed point of finite order. The formulas and invariants that Ulmer and my research provide would be accessible to any student who has taken an abstract algebra course and has an interest in learning elementary number theory.

References

[1] David A. Cox and Walter R. Parry. Torsion in elliptic curves over $k(t)$. *Compositio Math.*, 41(3):337–354, 1980. 4.1, 4.2, 5.1

[2] Enrique González-Jiménez and Álvaro Lozano-Robledo. Elliptic curves with abelian division fields. *Math. Z.*, 283(3-4):835–859, 2016.

[3] Daeyeol Jeon, Chang Heon Kim, and Euisung Park. On the torsion of elliptic curves over quartic number fields. *J. London Math. Soc. (2)*, 74(1):1–12, 2006. 3

[4] Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer. On the torsion of elliptic curves over cubic number fields. *Acta Arith.*, 113(3):291–301, 2004. 3.5

[5] Sheldon Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992. 3.4

[6] Monsur Kenku and Fumiyuki Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988. 3.4

[7] Martin Levin. On the group of rational points on elliptic curves over function fields. *Amer. J. Math.*, 90:456–462, 1968. 4.1, 5, 5.1

[8] Robert J. S. McDonald. Torsion subgroups of elliptic curves over function fields of genus 0. *J. Number Theory*, 193:395–423, 2018. 4.2, 4.2

[9] Bjorn Poonen. Gonality of modular curves in characteristic p. *Math. Res. Lett.*, 14(4):691–701, 2007.

[10] Andreas Schweizer. On the p^e-torsion of elliptic curves and elliptic surfaces in characteristic p. *Trans. Amer. Math. Soc.*, 357(3):1047–1059, 2005. 2

[11] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. 3, 3.3

[12] Douglas Ulmer. Elliptic curves over function fields. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 211–280. Amer. Math. Soc., Providence, RI, 2011. 1, 4.3, 4.1, 5.1, 3