Torsion Subgroups of Elliptic Curves over Function Fields

Robert J.S. McDonald, Ph.D.

University of Connecticut, 2019

ABSTRACT

Let $\mathbb{F}$ be a finite field of characteristic p, and $\mathcal{C}/\mathbb{F}$ be a smooth, projective, absolutely irreducible curve. Let $K = \mathbb{F}(\mathcal{C})$ be the function field of $\mathcal{C}$. When the genus of $\mathcal{C}$ is 0, and $p \neq 2, 3$, Cox and Parry provide a minimal list of prime-to-p torsion subgroups that can appear for an elliptic curve E/K. In this thesis, we extend this result by determining the complete list of full torsion subgroups possible for an elliptic curve E/K for any prime p when the genus of $\mathcal{C}$ is 0 or 1.

Torsion Subgroups of Elliptic Curves over Function Fields

Robert J.S. McDonald

M.S. Mathematics, University of Connecticut

B.S. Mathematics, Eastern Connecticut State University

A Dissertation

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

at the

University of Connecticut

2019

APPROVAL PAGE

Doctor of Philosophy Dissertation

Torsion Subgroups of Elliptic Curves over Function Fields

Presented by

Robert J.S. McDonald, B.S. Math., M.S. Math.

Major Advisor ______________________________
Álvaro Lozano-Robledo

Associate Advisor ______________________________
Keith Conrad

Associate Advisor ______________________________
Liang Xiao

University of Connecticut

2019

ACKNOWLEDGMENTS

I would like to thank my advisor, Professor Álvaro Lozano-Robledo, for his support, guidance, and general help in preparing and writing this thesis. I am so happy to have found in him an advisor and friend with whom I worked so well. I would also like to thank the rest of my advising committee, Professors Keith Conrad and Liang Xiao for their continued help and useful suggestions for revision. I especially thank Professor Conrad for taking the time to comb through my application materials and help me practice for interviews on his own time.

A very special thanks goes to Monique Roy, who devotes so much of herself to her graduate students. So many students would not have made it to graduation without her shoulder to lean on, and we all owe her our sincerest gratitude.

I would also like to thank my mother, who began teaching me algebra with chicken nuggets and french fries in a McDonald's when I was four. Watching her put herself through school as a single mother with three jobs and two children was undeniably influential on my decision to pursue mathematics. Thanks, too, to my father, who has always been there for me, and supported my every decision.

Thanks to Professor Stephen Kenton, whose calculus classes I first began attending with my mother when I was nine, and whom I thank, along with Professors Christian Yankov and Mizan Khan, for encouraging me to go to graduate school.

Finally, and most of all, I want thank my wife, Kayla. Without her continued support, financially and emotionally, none of this would have been possible. Neither of us knew of all the sacrifices we would have to make for me to go to graduate school, and I am so thankful to have had her through it all.

Contents

Chapter 1

Introduction

1.1 Introduction: Elliptic Curves over $\mathbb{Q}$

Many interesting problems in number theory arise from questions 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 solution in positive integers x, y, and 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 around 350 years before the matter was finally settled by Andrew Wiles and Richard Taylor in 1995.

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. Over the rational numbers, $\mathbb{Q}$, an elliptic curve is the set of solutions to a diophantine equation of the form

$$E : y^2 = x^3 + Ax + B, \text{ where } A, B \in \mathbb{Z}, \text{ and } 4A^3 - 27B^2 \neq 0.$$

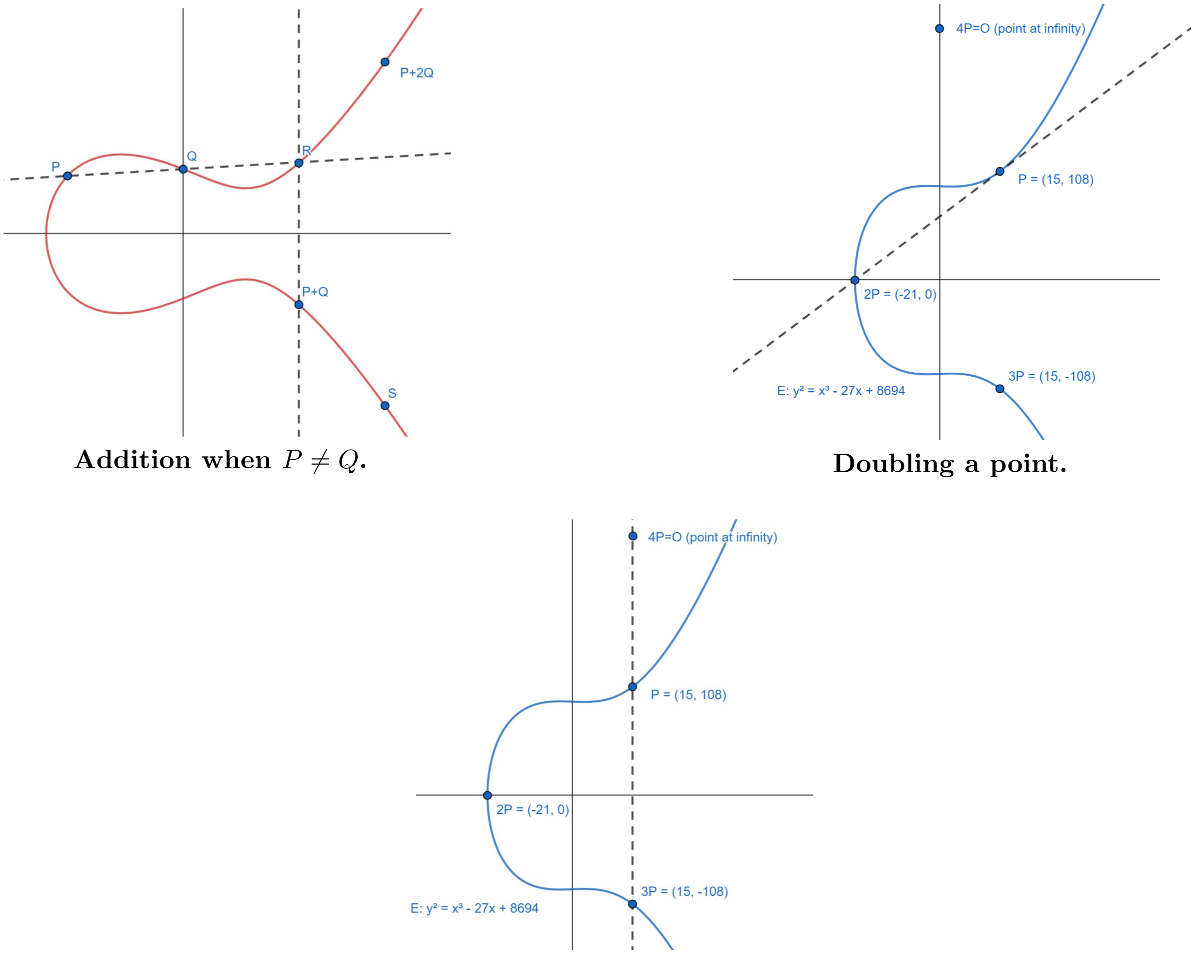
Given such a curve, a natural questions is: can we determine its solutions over $\mathbb{Z}$ or $\mathbb{Q}$? So far, in the general case, this question leads to many unanswered problems.

The $\mathbb{Q}$-rational points on E 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, and reflect the third point of intersection about the x-axis. 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 Figure 1.1 for some examples of this addition.

Remark 1.1.1. More precisely, an elliptic curve $E/\mathbb{Q}$ is a *projective curve*

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3, \text{ where } A, B \in \mathbb{Z}, \text{ and } 4A^3 - 27B^2 \neq 0.$$

Two points are equal if $[X, Y, Z] = [\lambda X, \lambda Y, \lambda Z]$ for some $\lambda \neq 0$. In our model above, we are considering the affine chart corresponding to $Z = 1$. The "missing" point in this affine chart is $\mathcal{O} = [0, 1, 0]$, the "point at infinity" in this projectivization.



Addition when $P \neq Q$.

Doubling a point.

$\mathcal{O}$, the additive identity.

Figure 1.1: Defining addition on $E(\mathbb{Q})$.

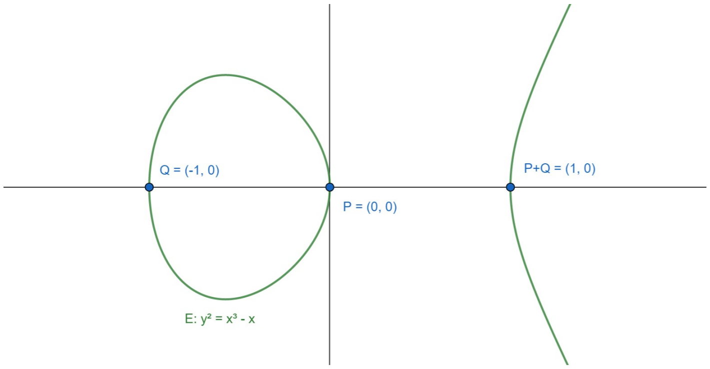


Figure 1.2: The elliptic curve $E : y^2 = x^3 - x = x(x+1)(x-1)$.

Example 1.1.2. The curve $E : y^2 = x^3 - x = x(x+1)(x-1)$, in Figure 1.2, 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 the point $(1,0) = P+Q$ has order two as well. 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 $E(\mathbb{Q})$ as a group:

Theorem 1.1.3 (Mordell–Weil)**.** *Let E be an elliptic curve over $\mathbb{Q}$. The group of $\mathbb{Q}$-rational points, $E(\mathbb{Q})$, is a finitely generated abelian group.*

The fundamental theorem of finitely generated abelian groups and Theorem 1.1.3 tell us

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

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

Theorem 1.1.4 (Mazur [16, p. 242])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to one of the following groups:*

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

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

Remark 1.1.5. We refer the interested reader to [17] for a lecture series on the proof of Mazur's Theorem 1.1.4 for elliptic curves over $\mathbb{Q}$. Shown there, is the general philosophy of turning questions about torsion points on elliptic curves of order N into moduli problems: finding $\mathbb{Q}$-rational points on the modular curve $X_1(N)$. The hard part of Mazur's theorem amounts to showing that the modular curve $X_1(N)(\mathbb{Q})$ is empty for any prime $N > 7$ [17, Lecture 1]. See also [22], for an interesting discussion of moduli spaces with the example of using points on the modular curves $X_1(11)$ and $X_0(11)$ to rule out points of order 11 appearing in $E(\mathbb{Q})$.

Theorem 1.1.4 is a complete classification of the types of torsion subgroups that occur for an elliptic curve over $\mathbb{Q}$. What about over extensions of $\mathbb{Q}$ such as $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$ (c.f. [10])? What about over function fields?

1.2 Elliptic Curves over Global Fields K

For a general field K, an elliptic curve over K is a *non-singular projective curve of genus one with a point defined over K*, and can always be written using the affine model

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ with } a_i \in K.$$

Provided the characteristic of K is not 2 or 3, every elliptic curve over K has a model of the form

$$E : y^2 = x^3 + Ax + B, \text{ with } A, B \in K \text{ such that } 4A^3 - 27B^2 \neq 0.$$

If K is a *global field*, that is, a number field or a function field over a finite field, then we have an analogue of Theorem 1.1.4.

Theorem 1.2.1 (Lang–Néron)**.** *Let E be an elliptic curve over a global field K. The group of K-rational points, $E(K)$, is a finitely generated abelian group.*

Thus, again, we can say

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

In Chapters 2 and 3, we will develop a similar strategy to that in Remark 1.1.5, by using invariants of an elliptic curve over a function field K to construct $X_1(n,m)$ modulo p. We will see that finding the torsion structure $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for an elliptic curve over K essentially amounts to determining whether or not $X_1(n,m)(K)$ has any points.

When K is a number field, $r_{E/K}$ is just as mysterious as when $K = \mathbb{Q}$. Similar classifications to that of Theorem 1.1.4 for $E(K)_{\text{tors}}$ have been determined by Kamienny, Kenku, and Momose (see [9] and [11]) when K is a quadratic number field, and Derickx, Etropolski, Morrow, and Zureick-Brown have announced a similar result when K is a cubic number field (see [4]). What happens when K is a function field? What types of groups can appear as the torsion subgroup of $E(K)$?

1.3 Elliptic Curves over Genus 0 Function Fields

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 $\mathbb{F}$.

1.3.1 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 1.3.1 (Levin [13]). *Let $\mathbb{F}$ be a finite field of characteristic p, $K = \mathbb{F}(T)$, and E/K a non-isotrivial*[1] *elliptic curve. Suppose $\ell^e \mid \#E(K)_{\text{tors}}$ for some prime ℓ. Then*

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

In [2], 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

[1] See Definition 1.3.3 below.

the function field K.

Theorem 1.3.2 (Cox, Parry, [2]). *Let $\mathbb{F}$ be a finite field of characteristic $p \geq 5$. Let m and n be positive integers with $n|m$, and set $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then the following are equivalent:*

(1) *There is a non-isotrivial elliptic curve E over $\mathbb{F}(T)$ such that $G \cong E(K)'_{\text{tors}}$, the rational points of finite order not divisible by p.*

(2) *p does not divide n, the field $\mathbb{F}$ contains a primitive n-th root of unity, and G is one of the following 19 groups:*

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

Non-isotriviality will be a common restriction on the curves that we consider in this thesis, and amounts, essentially, to the curve E not being a base extension of a curve over a finite field.

Definition 1.3.3. Let $\mathcal{C}/\mathbb{F}$ be a smooth curve (of arbitrary genus), $K = \mathbb{F}(\mathcal{C})$ and E/K be an elliptic curve.

1. E is *constant* if there is an elliptic curve $E_0/\mathbb{F}$ such that $E \cong E_0 \times_{\mathbb{F}} K$.
2. E is *isotrivial* if there is a finite extension K' of K such that E/K' is constant.
3. E is *non-isotrivial* if it is not isotrivial, and *non-constant* if it is not constant.

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

$$E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2 \text{ for } a, b \in K, a \neq 1, b \neq 0.$$

Cox and Parry's theorem deals only with prime-to-p torsion. From this, some natural questions arise: which structures from Theorem 1.3.2 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 1.3.4 ([21, p. 17]). *Let $\mathcal{C}/\mathbb{F}$ be a smooth curve (of arbitrary genus) and suppose that E is a non-isotrivial elliptic curve over $K = \mathbb{F}(\mathcal{C})$, where $\mathbb{F}$ has characteristic 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-invariant and Hasse invariant of an elliptic curve over K are quite simple to compute. See [21, p. 14], for example, for a formula for each of them.

1.3.2 Summary of results

In this section, we summarize the results of Chapter 2. Cox and Parry's theorem was not considered in the cases $p = 2, 3$, 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. Then for each p and each group G from Theorem 1.3.2, we write a curve in Tate normal form for G. Using Theorem 1.3.4, or in some cases a division polynomial, we then construct a curve $D/\mathbb{F}$, parameterizing elliptic curves over $\mathbb{F}(T)$ 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 D. Then using the Hurwitz formula, if the genus of D is greater than 0, we obtain a contradiction. We arrive at the following result.

Theorem 1.3.5 (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 2.1.4 (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:*

$$\begin{array}{cl}
\mathbb{Z}/p\mathbb{Z} & \\
\mathbb{Z}/2p\mathbb{Z} & \textit{if } p = 2, 3, 5, 7, \\
\mathbb{Z}/3p\mathbb{Z} & \textit{if } p = 2, 3, 5, \\
\mathbb{Z}/4p\mathbb{Z}, \mathbb{Z}/5p\mathbb{Z}, & \textit{if } p = 2, 3, \\
\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/14\mathbb{Z}, \mathbb{Z}/18\mathbb{Z} & \textit{if } p = 2, \\
\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} & \textit{if } p = 2, \textit{ and } \mathbb{F} \textit{ contains a primitive } 5\textit{th root of unity}, \\
\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{if } p = 3, \textit{ and } \mathbb{F} \textit{ contains a primitive } 4\textit{th root of unity}, \\
\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{if } p = 5.
\end{array}$$

Further, if $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is in this list with $n \mid m$, and $\mathbb{F}$ contains a primitive nth root of unity (or 4th in the case of $G = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), then there are infinitely many non-isomorphic, non-isotrivial elliptic curves with $E(K)_{\text{tors}} \cong G$. If $p \geq 13$, then Theorem 2.1.4 is a complete list of possible subgroups $E(K)_{\text{tors}}$.

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

Corollary 1.3.6 (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 groups:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} && \textit{with } 1 \le N \le 10 \textit{ or } N = 12, 15,\\ &\mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} && \textit{with } 1 \le N \le 5,\\ &\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, && \\ &\mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, && \textit{with } N = 1, 2, \end{aligned}$$

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

In fact, we can parameterize all of the elliptic curves having each of the indicated torsion subgroups in Theorem 1.3.5. 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 the 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 Table 2.14 the reader can find parameterizations of all elliptic curves over $\mathbb{F}(T)$ with the torsion structures appearing in Theorem 1.3.5.

1.4 Elliptic Curves over Genus 1 Function Fields

In this section, we are primarily interested in the case where $\mathcal{C}$ is a smooth curve of genus 1. By the Hasse bound for curves of genus 1 over a finite field we see that $\mathcal{C}$ automatically has a point, and is therefore an elliptic curve over $\mathbb{F}$ (see [7]). In this setting, [13] provides us with the following corollary.

Corollary 1.4.1 (Levin, [13]). *Let $\mathbb{F}$ be a finite field of characteristic p, $\mathcal{C}/\mathbb{F}$ be a smooth, projective, absolutely irreducible curve, $K = \mathbb{F}(\mathcal{C})$, and E/K a non-isotrivial elliptic curve. Suppose $\ell^e \mid \#E(K)_{\text{tors}}$ for some prime ℓ. Then*

$$\ell \leq 11 \textit{ and } e \leq \begin{cases} 4 & \textit{if } \ell = 2 \\ 2 & \textit{if } \ell = 3, 5 \\ 1 & \textit{if } \ell = 7, 11 \end{cases} \textit{ if } \ell \neq p, \quad \textit{and} \quad \ell \leq 11 \textit{ and } e \leq \begin{cases} 4 & \textit{if } \ell = 2 \\ 2 & \textit{if } \ell = 3 \\ 1 & \textit{if } \ell = 5, 7, 11, 13 \end{cases} \textit{ if } \ell = p.$$

1.4.1 Summary of results

We begin by finding an analogue of Cox and Parry's theorem in Section 1.3.1.

Theorem 1.4.2 (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:*

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

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

We can provide parameterizations for all elliptic curves E with torsion subgroup appearing in this theorem which also appeared in Theorem 1.3.2, and these torsion subgroups appear infinitely often as $E(K)_{\mathrm{tors}}$ for some non-isotrivial 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 1.4.2 does not appear in Theorem 1.3.2, then infinitely many elliptic curves E/K can be found with $E(K)'_{\mathrm{tors}} \cong G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ only if $\mathcal{C}$ is isogenous to the modular curve $X_1(n,m)$. For example, if $p \neq 11$, $E(K)$ 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 the Tate normal form over K for a torsion subgroup G appearing in Theorem 1.4.2. Then, using the Hasse invariant and division polynomials of the curve, we again construct a curve $D/\mathbb{F}$ parameterizing elliptic curves with $G \times \mathbb{Z}/p^e\mathbb{Z}$ torsion. This time, we arrive at a contradiction if the genus of D is greater than one. We arrive at the following result.

Theorem 1.4.3 (M). *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, for $\mathbb{F}$ of characteristic p, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. If $p \nmid \#E(K)_{\mathrm{tors}}$, then $E(K)_{\mathrm{tors}}$ is as in Theorem 1.4.2. If $p \mid \#E(K)_{\mathrm{tors}}$, then $p \leq 13$, and $E(K)_{\mathrm{tors}}$ is one of*

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

Further, if $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is in this list with $n \mid m$, and $\mathbb{F}$ contains a primitive

nth root of unity, then there are infinitely many non-isomorphic, non-isotrivial elliptic curves with $E(K)_{\text{tors}} \cong G$. If $p \geq 17$, then Theorem 1.4.2 is a complete list of possible subgroups $E(K)_{\text{tors}}$.

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

Corollary 1.4.4. *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:*

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

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

In Corollary 1.4.4, again, if G is already a group that appears in Corollary 1.3.6, that is, one that already appeared over function fields of genus 0, then we can find infinitely many non-isomorphic, non-isotrivial E/K with torsion subgroup G, regardless of the base curve. If G does not appear in Corollary 1.3.6, 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 $D : t^2 + t + 1 = u^4$.

Chapter 2

Genus 0 Function Fields

2.1 Introduction

In what follows, let p be a prime and $\mathbb{F}$ be a finite field of characteristic p. Let $\mathcal{C}$ be a smooth, projective, absolutely irreducible curve over $\mathbb{F}$, and write $K = \mathbb{F}(\mathcal{C})$ for its function field. In this chapter, we will primarily be interested in the case when $\mathcal{C} = \mathbb{P}^1$, so that $K = \mathbb{F}(\mathbb{P}^1) = \mathbb{F}(T)$ is the rational function field of $\mathbb{F}$. An elliptic curve E/K is a smooth, projective, absolutely irreducible curve of genus 1 over K, with at least one K-rational point. The curve E can always be written as an affine cubic in long Weierstrass form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ for } a_i \in K,$$

and when $p > 3$, we can write $E : y^2 = x^3 + Ax + B$ for $A, B \in K$.

We have the usual definitions for the invariants associated to E (for example in

[16]), including the discriminant, Δ, and the j-invariant, all of which are elements in K. In addition, we will consider the Hasse invariant of E, which we will denote $H(E)$. When $p = 2$, for a curve written in long Weierstrass form, the Hasse invariant is the coefficient a_1. When $p > 2$, we may choose an equation with $a_1 = a_3 = 0$, in which case the Hasse invariant of E is the coefficient of x^{p-1} in the expansion of $(x^3 + a_2x^2 + a_4x + a_6)^{\frac{p-1}{2}}$ (see [21, p. 18]).

The following is a more precise statement of Definition 1.3.3 from Chapter 1.

Definition 2.1.1. Assume that $K = \mathbb{F}(\mathcal{C})$ is the function field of a smooth curve $\mathcal{C}$ over a finite field $\mathbb{F}$, and let E be an elliptic curve over K.

1. E is *constant* if there is an elliptic curve E_0 defined over $\mathbb{F}$ such that $E \cong E_0 \times_{\mathbb{F}} K$, where "$E_0 \times_{\mathbb{F}} K$" is the fiber product of E_0 and K. Equivalently, E is a base extension of $E_0/\mathbb{F}$ to K; it is constant if and only if it can be defined by a Weierstrass cubic with coefficients in $\mathbb{F}$.
2. E is *isotrivial* if there exists a finite extension K' of K such that E becomes constant over K'. Equivalently, $j(E) \in \mathbb{F}$, where $j(E)$ is the j-invariant of E.
3. E is *non-isotrivial* if it is not isotrivial, and *non-constant* if it is not constant.

As in the case of elliptic curves over number fields, we have the following description of the structure of $E(K)$, the set of K-rational points of E.

Theorem 2.1.2 (Mordell–Weil–Lang–Néron [12]). *Assume that $K = \mathbb{F}(\mathcal{C})$ is the function field of a curve over a finite field $\mathbb{F}$, and let E be an elliptic curve over K. Then $E(K)$ is a finitely generated abelian group.*

As an immediate corollary, we have that $E(K)_{\text{tors}}$ is finite. In fact, we have

$$E(K)_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

where n divides m, and p does not divide n, and every such group appears for some K (of some genus) and E (see [21, p. 16]). The following proposition tells us that for any fixed genus g of $\mathcal{C}$ and characteristic p, there are only finitely many possibilities for m and n.

Proposition 2.1.3 (Ulmer, [21, Proposition 7.1])**.** *Let g be the genus of $\mathcal{C}$. Then there is a finite (and effectively calculable) list of groups depending only on g and p, such that for any non-isotrivial elliptic curve E over K, the group $E(K)_{\text{tors}}$ appears on the list.*

Following the proof of Proposition 2.1.3 in [21, Theorem 5.1], if $G = \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ is the prime-to-p torsion subgroup of $E(K)$, a crude list (at least for the prime-to-p part of $E(K)_{\text{tors}}$) can be found by using the Hurwitz formula on the induced morphism from $\mathcal{C}$ to the modular curve $X_1(n, m)$, though one may have to work harder to further refine the list to be minimal for K. For example, when $g = 0$, so that $\mathbb{F}(\mathcal{C}) = \mathbb{F}(T)$, and $p \geq 5$ we have the following restatement of Cox an Parry's minimal list for prime-to-p torsion in Theorem 1.3.2.

Theorem 2.1.4 (Cox, Parry [2])**.** *Let $K = \mathbb{F}(T)$ where $\mathbb{F}$ is a finite field of characteristic $p \neq 2, 3$. 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:*

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

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

Remark 2.1.5. In fact, Cox and Parry's theorem, as stated in [2], is valid for arbitrary fields (i.e. not necessarily finite) of characteristic $p \geq 0$, with $p \neq 2, 3$.

Remark 2.1.6. Throughout the paper, it is essential that E is a *non-isotrivial* elliptic curve. For example, over $K = \mathbb{F}_{11}(T)$, for any non-zero $f \in K$, the curve $E_f : y^2 = x^3 + f^2x^2 + f^4x$ has the point $(0, 0)$ of order sixteen, which does not appear in Cox and Parry's list. However, E is *constant*, because it is isomorphic to the curve $E : y^2 = x^3 + x^2 + x$ under the change of variables $x \mapsto fx$.

As for p-primary torsion, in order for $E(K)$ to have a point of order p, we have the following requirements on the Hasse and j-invariants of E.

Theorem 2.1.7 (Ulmer, [21, p. 17])**.** *Suppose that E is a non-isotrivial elliptic curve over $K = \mathbb{F}(\mathcal{C})$, where $\mathbb{F}$ has characteristic 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 $K^\times$.*

Remark 2.1.8. When $\mathcal{C} = \mathbb{P}^1$, since $\alpha \mapsto \alpha^p$ is an automorphism of $\mathbb{F}$, we have $K^p = \big(\mathbb{F}(T)\big)^p = \mathbb{F}(T^p)$. That is, an element of K is in K^p if and only if it is a rational expression in T^p. With this, it is also not hard to show that if $f, g \in K$, then $f \circ g \in K^p$ if and only if at least one of f or g is in K^p.

Finally, the following result proves very useful in trying to calculate the list referred to in Proposition 2.1.3, though, again, some work is required to minimize it.

Theorem 2.1.9 (Levin, [13])**.** *Let K be a function field in one variable over a finite field of characteristic p, and E/K be an elliptic curve. The order of $E(K)_{\text{tors}}$ is universally bounded, depending only on $g(K)$, the genus of K. In particular if we* *have* $\ell^e \mid \#E(K)_{\text{tors}}$ *for* $e \geq 1$*, then if* $\ell \neq p$*,*

$$\ell \leq 6 + (1 + 24 \cdot g(K))^{\frac{1}{2}},$$

$$e \leq \begin{cases} \log_2(3 + (1 + 8 \cdot g(K))^{\frac{1}{2}}) + 2 & \textit{if } \ell = 2, \\ \log_3(1 + g(K)^{\frac{1}{2}}) + 2 & \textit{if } \ell = 3, \\ \log_5(3 + (4 + 5 \cdot g(K))^{\frac{1}{2}}) + 1 & \textit{if } \ell = 5, \\ \log_p(7(3 + (\frac{1}{2}(11 + 7 \cdot g(K)))^{\frac{1}{2}})) & \textit{if } \ell \geq 7. \end{cases}$$

On the other hand, if $\ell^e \mid \#E(K)_{\text{tors}}$ *for* $e \geq 1$*, and* $\ell = p$*, then we have*

$$\ell \leq 7 + 4(1 + 3 \cdot g(K))^{\frac{1}{2}}$$
$$e \leq \log_\ell(6 + (36 - \ell + 24 \cdot \ell(\ell-1)^{-1}(2 \cdot g(K) - 2 + h_\ell))^{\frac{1}{2}}),$$

where h_ℓ *is found in [13, pp. 460–461].*

Since we are primarily interested in $K = \mathbb{F}(T)$, where we already know the list of possible prime-to-p torsion, and have $g(K) = 0$, we provide the following special case of Theorem 2.1.9.

Corollary 2.1.10. *Let* $\mathbb{F}$ *be a finite field of characteristic* p*,* $K = \mathbb{F}(T)$*, and* E/K *an elliptic curve. Suppose* $p^e \mid \#E(K)_{\text{tors}}$*. Then we have*

$$p \leq 11, \;\; e \leq \begin{cases} 3 & \textit{if } p = 2 \\ 2 & \textit{if } p = 3 \\ 1 & \textit{if } p = 5, 7, 11 \end{cases}.$$

Remark 2.1.11. Note that Corollary 2.1.10 also tells us that for characteristic $p \geq 13$, Cox and Parry's list in Theorem 2.1.4 is a complete list of torsion structures one can expect to encounter.

For convenience, we make the following non-standard definitions.

Definition 2.1.12. Let $\mathcal{C}$ and D be curves over $\mathbb{F}$, with $\mathcal{C}$ smooth, and set $K = \mathbb{F}(\mathcal{C})$. We will call any point in $D(\mathbb{F})$ a *constant point*, and any point in $D(K)$ *non-constant* if it is not a constant point. As in Definition 2.1.1, we will also call the curve D/K *constant*, if it is written in a form with coefficients in $\mathbb{F}$.

Finally, we will make use of the following useful fact, which is stated in more generality for function fields with base curves of higher genus. The proposition will be adapted in this chapter to fit the case when $\mathcal{C} \cong \mathbb{P}^1$ has genus zero, and in Chapter 3 to address the case where $\mathcal{C}$ has genus 1.

Proposition 2.1.13. *Let $\mathbb{F}$ be a finite field of characteristic p, $\mathcal{C}/\mathbb{F}$ and $D/\mathbb{F}$ be projective, absolutely irreducible curves, with $\mathcal{C}$ smooth, and let $K = \mathbb{F}(\mathcal{C})$. If the genus of D is greater than that of $\mathcal{C}$, then every point in $D(K)$ is constant.*

Proof. Let $\pi : \tilde{D} \to D$ be the normalization map associated to D, which is a birational morphism on the irreducible components of D (see [15, p. 128]). D is irreducible, so the map $\pi^{-1} : D \to \tilde{D}$ is a non-constant rational map (if D is smooth, it is the identity map). Suppose that there is a non-constant point $P \in D(K)$. Since $K = \mathbb{F}(\mathcal{C})$, and D is written with coefficients in $\mathbb{F}$, we obtain the rational map

$$\rho : \mathcal{C}/\mathbb{F} \to D/\mathbb{F} \text{ by } t \mapsto P_t.$$

Since $\mathcal{C}$ is smooth, ρ is a morphism, and because P is non-constant, ρ is non-constant, and therefore surjective, hence dominant, so that defining $\tilde{\rho} : \mathcal{C} \to \tilde{D}$ by $\tilde{\rho} = \pi^{-1} \circ \rho$, we obtain a non-constant rational map (see [16, Proposition 2.1 and Theorem 2.3]).

$$\begin{tikzcd}
 & \tilde{D} \arrow[d, "\pi"] \\
\mathcal{C} \arrow[ur, "\tilde{\rho}"] \arrow[r, "\rho"'] & D
\end{tikzcd}$$

Now, $\tilde{\rho} : \mathcal{C} \to \tilde{D}$ is a map of smooth curves, so that by [16, Corollary 2.12] we can factor the map $\tilde{\rho}$ as

$$\begin{tikzcd}
\mathcal{C} \arrow[r, "\alpha"] & \mathcal{C} \arrow[r, "\beta"] & \tilde{D},
\end{tikzcd}$$

where α is the q-th power Frobenius map (q the cardinality of $\mathbb{F}$), and β is separable, and non-constant by assumption. Since α is an automorphism of $\mathcal{C}$, we may assume $\tilde{\rho}$ is separable, and apply the Hurwitz formula:

$$2g(\mathcal{C}) - 2 \geq (\deg \tilde{\rho})(2g(D) - 2) + \sum_{P \in \mathbb{P}^1} (e_{\tilde{\rho}(P)} - 1) \geq 2g(D) - 2.$$

But this means $g(\mathcal{C}) \geq g(D)$, which is a contradiction. Thus $\tilde{\rho}$, and therefore ρ, must be constant, and no such point P can exist. □

When we specialize to the case of $\mathcal{C} = \mathbb{P}^1$, we obtain the following useful corollary.

Corollary 2.1.14. *For $\mathbb{F}$ of characteristic p, and $K = \mathbb{F}(T)$, if $D/\mathbb{F}$ is an irreducible curve of positive genus, then there are no non-constant points in $D(K)$.*

Proof. When $K = \mathbb{F}(T)$, the base curve is isomorphic to $\mathbb{P}^1$. Proposition 2.1.13 shows that if $D(K)$ has a non-constant point, then D must have genus zero. □

Remark 2.1.15. The conclusion of Corollary 2.1.14 is certainly *not* the case if $D/\mathbb{F}$ has genus zero because maps $\mathbb{P}^1 \to D$ exists as long as D has a point.

In the sections to follow, we will prove, and provide parameterizations for, the following result.

Theorem 2.1.16 (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 $p \nmid \#E(K)_{\mathrm{tors}}$, then $E(K)_{\mathrm{tors}}$ is one of the following groups.*

$$\begin{array}{cl}
\mathbb{Z}/N\mathbb{Z} & \textit{with } N = 1, \ldots, 10, 12, \\
\mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{with } N = 1, \ldots, 4, \\
\mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \textit{with } N = 1, 2, \\
(\mathbb{Z}/N\mathbb{Z})^2 & \textit{with } N = 4, 5.
\end{array}$$

Otherwise, if $p \mid \#E(K)_{\mathrm{tors}}$, then $p \leq 13$, and $E(K)_{\mathrm{tors}}$ is one of

$$\begin{array}{cl}
\mathbb{Z}/p\mathbb{Z}, & \\
\mathbb{Z}/2p\mathbb{Z}, & \textit{if } p = 2, 3, 5, 7, \\
\mathbb{Z}/3p\mathbb{Z}, & \textit{if } p = 2, 3, 5, \\
\mathbb{Z}/4p\mathbb{Z}, \mathbb{Z}/5p\mathbb{Z}, & \textit{if } p = 2, 3, \\
\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/14\mathbb{Z}, \mathbb{Z}/18\mathbb{Z}, & \textit{if } p = 2, \\
\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, & \textit{if } p = 2, \textit{ and } \mathbb{F} \textit{ contains a primitive } 5th \textit{ root of unity}, \\
\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \textit{if } p = 3, \textit{ and } \mathbb{F} \textit{ contains a primitive } 4th \textit{ root of unity}, \\
\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \textit{if } p = 5.
\end{array}$$

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

In Section 2.2, we will parameterize all of the torsion subgroups referred to in Cox and Parry's list in Theorem 2.1.4 explicitly, regardless of the characteristic of K. Then, starting with characteristic $p \geq 5$, in Section 2.3, we will use Theorem 2.1.7 and the parameterizations from Section 2.2, to obtain the conditions necessary for a point of order p to appear with a subgroup from Cox and Parry's list. In each case, we will find that such torsion structures correspond to points on certain constant curves, which we will either parameterize, or attempt to apply Corollary 2.1.14. Finally, in Section 2.4, we look at characteristics $p = 2, 3$. After proving a version of Theorem 2.1.4 for each of these characteristics, we will again determine when points of order p can appear. Explicit parameterizations of all exotic torsion, along with generators, for all exotic torsion structures are provided in Section 2.5.

2.2 Explicit Parameterizations of Torsion Structures in Theorem 2.1.4

In this section, having fixed a characteristic $p \geq 2$, we parameterize all elliptic curves with each torsion structure from Cox and Parry's list in Theorem 2.1.4. Let $\mathbb{F}$ be a finite field of characteristic p, let $K = \mathbb{F}(T)$, and let E/K be a non-isotrivial elliptic curve (so that not all of its coefficients are constant). Suppose that there exists a $Q = (x_0, y_0) \in E(K)$ not equal to $\mathcal{O}$. Then with the change of variables $x \mapsto x + x_0$, $y \mapsto y + y_0$, we can move Q to the origin and write

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x, \text{ with } a_i \in K \text{ not all constant.} \tag{2.1}$$

If Q has exact order two, then by [16, Theorem 2.3] we have $(0,0) = -Q = (0, -a_3)$, so that $a_3 = 0$. If, additionally, $p \neq 2$, the change of variables $y \mapsto y - \frac{a_1}{2}$ allows us to write E as an equation with $a_1 = 0$. Thus, for $p \neq 2$, the point $(0,0) \in E(K)$ has exact order two if and only if we can write

$$E_{a,b} : y^2 = x^3 + ax^2 + bx \text{ for some } a, b \in K, \text{with at least one of } a \text{ or } b \text{ non-constant.}$$

By using the group law algorithms in [16, Theorem 2.3], it is easy to show that when $E : y^2 = f(x)$, then *any* point of order two takes the form $(\alpha, 0)$ where α is a root of f. Hence, for $p \neq 2$, any curve with $(\mathbb{Z}/2\mathbb{Z})^2$ torsion may be written in the form

$$E_{a,b} : y^2 = x(x-a)(x-b) \text{ for } a, b \in K, \text{with at least one of } a \text{ or } b \text{ non-constant.}$$

Returning to (2.1), if Q has order greater than two, then $(0,0) \neq -Q = (0, -a_3)$, so that $a_3 \neq 0$. Then, the change of variables $y \mapsto y + (a_4/a_3)x$ (and some renaming of coefficients) allows us to write E as an equation with $a_4 = 0$ as well:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2, \text{ with } a_i \in K \text{ not all constant.} \tag{2.2}$$

If Q has exact order three, then $(0, -a_3) = -Q = 2Q = (-a_2, a_1a_2 - a_3)$ shows that $a_2 = 0$ as well, and thus, *for general* p, the point $(0,0) \in E(K)$ has exact order three if and only if we can write

$$E : y^2 + axy + by = x^3 \text{ for } a, b \in K, \text{with at least one of } a \text{ or } b \text{ non-constant.}$$

In [14, 1.1], for $f \in \mathbb{Q}(\zeta_3)$, we find the family $X^3 + Y^3 + Z^3 = 3fXYZ$ parameterizes all elliptic curves with $(\mathbb{Z}/3\mathbb{Z})^2$ torsion over $\mathbb{Q}(\zeta_3)$. By looking at the affine chart corresponding to $Z = 1$ after the change of variables

$$[X, Y, Z] \mapsto [-3(f^2 + f + 1)(X + Y + Z), 9(f^3 + f^2 + f)(X + Y + Z), X + fY + Z],$$

for the same $f \in \mathbb{Q}(\zeta_3)$, we see that this family is isomorphic to the affine model

$$y^2 + 3(f + 2)xy + 9(f^2 + f + 1)y = x^3.$$

Thus, if $p \neq 3$, and $\mathbb{F}$ contains a primitive 3rd root of unity, for non-constant $f \in K$, we will see $(\mathbb{Z}/3\mathbb{Z})^2$ torsion using this family.

Collecting our results, we have Table 3.6, with two-parameter families for $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^2$ for $n = 2, 3$. Here, with $a, b \in K$ (or $f \in K$), at least one non-constant, as long as $\Delta_{a,b} \neq 0$, we get a non-isotrivial elliptic curve $E_{a,b}$ with $G \subset E_{a,b}(K)_{\text{tors}}$.

Characteristic	$E_{a,b}/K$	G
$p \neq 2$	$y^2 = x^3 + ax^2 + bx$	$\mathbb{Z}/2\mathbb{Z}$
$p \neq 2$	$y^2 = x(x - a)(x - b)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
general p	$y^2 + axy + by = x^3$	$\mathbb{Z}/3\mathbb{Z}$
$p \neq 3,\ \zeta_3 \in \mathbb{F}$	$y^2 + 3(f + 2)xy + (f^2 + f + 1)y = x^3$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Table 2.1: Two-parameter familes of elliptic curves $E_{a,b}/K$ such that $G \subset E_{a,b}(K)_{\text{tors}}$.

On the other hand, if Q has order greater than three, then $(0, -a_3) = -Q \neq 2Q = (-a_2, a_1a_2 - a_3)$ shows that $a_2 \neq 0$, since $-Q \neq 2Q$. The change of variables $x \mapsto (a_3/a_2)^2 x$, $y \mapsto (a_3/a_2)^3 y$ in (2.2) gives

$$E : y^2 + \frac{a_1a_2}{a_3}xy + \frac{a_2^3}{a_3^2}y = x^3 + \frac{a_2^3}{a_3^2}x^2.$$

Setting $b = -a_2^3/a_3^2$ and $a = 1 - (a_1 a_2)/a_3$, we find that *for general* p, the point $(0,0) \in E(K)$ has order greater than three (possibly infinite) if and only if we can write E in Tate normal form:

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

In this form, we can obtain parameterizations for $\mathbb{Z}/n\mathbb{Z}$ for $n = 4, \dots, 10, 12$ and $\mathbb{Z}/2n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, for $n = 2, 3, 4$. For fields of characteristic zero, these parameterizations can be found in the literature, for example in [6, p. 188]. We need only validate these parameterizations for arbitrary characteristic.

By the calculations for a and b in [8, 4.6], the Tate normal form for elliptic curves with torsion structures $\mathbb{Z}/n\mathbb{Z}$ for $n = 4, \dots 9$, can be computed explicitly by starting with $Q = (0,0)$, computing $[\pm m]Q$ for $m = 2, 3, 4$, and comparing coefficients. Husemöller's argument holds regardless of characteristic, using only the order of a point to draw conclusions, so we may use these parameterizations (isomorphic to those in [6]) of $\mathbb{Z}/n\mathbb{Z}$ for $n = 4, \dots 9$, for E over any K.

Recall that for a field K and an elliptic curve E/K with a point $P \in E$, we have

$$x([m]P) = \phi_m(P)/\psi_m(P)^2,$$

where ϕ_m and ψ_m are division polynomials as defined in [16, p. 105]. This relationship, and the fact that ϕ_m and ψ_m^2 are coprime, is valid in any characteristic (see, for example, [5, Section 3.6], or [3]). Thus, we have

$$[m]P = (0,0) \iff x([m]P) = \phi_m(P)/\psi_m(P)^2 = 0 \iff \phi_m(P) = 0.$$

This means that, regardless of the characteristic of K, if $(0,0)$ is a point of order n, we can solve $\phi_m(P) = 0$ to find a and b such that there is a point P with $[mn]P = \mathcal{O}$. Using the characterizations in [6], we can easily calculate the a and b necessary for $\mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$ by solving $\phi_2(P) = 0$ when $(0,0)$ has order five and six respectively. So far, with a change of variables, all of our parameterizations are isomorphic to curves of the desired form in [6, p. 188]. Thus, for general p, we get the families in Table 2.2, parameterizing elliptic curves with torsion structures $\mathbb{Z}/n\mathbb{Z}$ for $n = 4, \ldots 10, 12$.

Characteristic	$E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2$		G
general p	$a = 0$	$b = f$	$\mathbb{Z}/4\mathbb{Z}$
general p	$a = f$	$b = f$	$\mathbb{Z}/5\mathbb{Z}$
general p	$a = f$	$b = f + f^2$	$\mathbb{Z}/6\mathbb{Z}$
general p	$a = f^2 - f$	$b = af$	$\mathbb{Z}/7\mathbb{Z}$
general p	$a = \frac{(2f-1)(f-1)}{f}$	$b = af$	$\mathbb{Z}/8\mathbb{Z}$
general p	$a = f^2(f-1)$	$b = a(f^2 - f + 1)$	$\mathbb{Z}/9\mathbb{Z}$
general p	$a = -\frac{f(f-1)(2f-1)}{f^2-3f+1}$	$b = -a \cdot \frac{f^2}{f^2-3f+1}$	$\mathbb{Z}/10\mathbb{Z}$
general p	$a = \frac{f(1-2f)(3f^2-3f+1)}{(f-1)^3}$	$b = -a \cdot \frac{2f^2-2f+1}{f-1}$	$\mathbb{Z}/12\mathbb{Z}$

Table 2.2: One-parameter familes of elliptic curves $E_{a,b}/K$ such that $G \subset E_{a,b}(K)_{\text{tors}}$.

When $p \neq 2$, we can obtain a parameterization for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by starting with the parameterization of elliptic curves with $\mathbb{Z}/4\mathbb{Z}$ torsion, and rewriting it as $E : y^2 = x^3 + (2f + \frac{1}{4})x^2 + f^2x$. The associated change of variables is valid when $p \neq 2$. In this form, $(0,0)$ is a point of order 2, so there must be $a, b \in K$ such that $a + b = 2f + \frac{1}{4}$, and $ab = f^2$. This is true if and only if $f = g^2 - \frac{1}{16}$ for some $g \in K$. Using our new found parameterization for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, a parameterization of elliptic curves with $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (see Table 3.7, line 3) can then be found by solving $\phi_2(P) = 0$, as above.

In the same way, for $p \neq 2$, we can obtain a parameterization elliptic curves with $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by starting with the parameterization of elliptic curves with $\mathbb{Z}/6\mathbb{Z}$ torsion, and rewriting it in the form $E : y^2 = x^3 + (\frac{3}{4}f^2 - \frac{3}{2}f - \frac{1}{4})x^2 + f^3x$. This time, we need $a + b = \frac{3}{4}f^2 - \frac{3}{2}f - \frac{1}{4}$, and $ab = f^3$, which albeit more complicated, can be parameterized using Magma (see [1]), with $f = (\frac{5}{4}g^2 - 9g + 16)/(g^2 - 3g)$ for some $g \in K$. Changing variables, regardless of characteristic of K, this gives families isomorphic to the remaining curves in [6, p. 188], which we collect in Table 3.7. It remains to find parameterizations for elliptic curves with the torsion subgroups $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^2$ when $n = 4, 5$.

Characteristic	$E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2$		G
$p \neq 2$	$a = 0$	$b = f^2 - \frac{1}{16}$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p \neq 2$	$a = \frac{10-2f}{f^2-9}$	$b = \frac{-2(f-1)^2(f-5)}{(f^2-9)^2}$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p \neq 2$	$a = \frac{(2f+1)(8f^2+4f+1)}{2(4f+1)(8f^2-1)f}$	$b = \frac{(2f+1)(8f^2+4f+1)}{(8f^2-1)^2}$	$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Table 2.3: One-parameter familes of elliptic curves $E_{a,b}/K$ such that $G \subset E_{a,b}(K)_{\text{tors}}$.

2.2.1 $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ torsion

Here, $p \neq 3$ and $\mathbb{F}$ contains a primitive 3rd root of unity. Using our parameterization of elliptic curves with $(\mathbb{Z}/3\mathbb{Z})^2$, if a non-isotrivial elliptic curve E over K has torsion subgroup $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, then without loss of generality, we have a point P such that $2P = (0, 0)$. Looking at $\phi_2(P) = 0$, we can use Magma to find the following genus zero curve over K:

$$C : X^3Z - 27XY^3 - 81XY^2Z - 81XYZ^2 - 54XZ^3 - 162Y^4 - 324Y^3Z - 486Y^2Z^2 - 324YZ^3 - 162Z^4.$$

For a point $[X, Y, Z]$ on C, the following elliptic curve has torsion structure containing $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$:

$$E : y^2 + 3(f+2)xy + 9(f^2+f+1)y = x^3, \text{ with } f = Y/Z \in K.$$

Using Magma to parameterize C about the point $[1, 0, 0]$, we find all points on C are of the form

$$\left[-\tfrac{1}{729}a^4 + \tfrac{1}{9}a^3b - \tfrac{11}{3}a^2b^2 + 54ab^3 - 324b^4,\ \tfrac{1}{243}a^3b - \tfrac{2}{9}a^2b^2 + 4ab^3 - 18b^4,\ ab^3 - 18b^4\right],$$

for $a, b \in K$. If we set $x = X/Z$, $f = Y/Z$, then $[x, f, 1]$ is a point on the curve, and making the substitution $t = a/b$ (the choice $b = 0$ only gives the point $[1, 0, 0]$, which we already knew) we get

$$f = \frac{\frac{1}{243}t^3 - \frac{2}{9}t^2 + 4t - 18}{t - 18}.$$

Finally, making the change of variables $t \mapsto \frac{1}{9}(t^{-1}+2)$, we conclude that if $\mathbb{F}$ contains a primitive 3rd root of unity, and E is a non-isotrivial elliptic curve over K with $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ torsion, then E is isomorphic to the curve

$$E : y^2+3(f+2)xy+9(f^2+f+1)y = x^3, \text{ with } f = \frac{2t^3+1}{3t^2} \text{ for some non-constant } t \in K.$$

2.2.2 $(\mathbb{Z}/4\mathbb{Z})^2$ torsion

Here, $p \neq 2$ and $\mathbb{F}$ contains a primitive 4th root of unity. Starting with our parameterization of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion, we can move the generator of the torsion subgroup with order two to the origin and solve $\phi_2(P) = (0,0)$ to find a new point of order four. Again, using Magma, we find the curve

$$C : X^2Z + Y^3 - \tfrac{1}{2}Y^2Z + \tfrac{1}{16}YZ^2, \text{ with } X, Y, Z \in K.$$

Parameterizing C about the point $[1,0,0]$ and making a change of variables, we find that any non-isotrivial elliptic curve with torsion subgroup $(\mathbb{Z}/4\mathbb{Z})^2$ is isomorphic to

$$E : y^2 + xy - (f^4 - \tfrac{1}{16})y = x^3 - (f^4 - \tfrac{1}{16})x^2, \text{ for some non-constant } f \in K.$$

2.2.3 $(\mathbb{Z}/5\mathbb{Z})^2$ torsion

Here, we assume $p \neq 5$ and $\mathbb{F}$ contains a primitive 5th root of unity. In [6, §6.4], we find a parameterization of all curves with $(\mathbb{Z}/5\mathbb{Z})^2$ torsion structure over $\mathbb{Q}(\zeta_5)$, where ζ_5 is a primitive fifth root of unity. By moving the point of order five defined over $\mathbb{Q}$ to the origin, and changing variables to write the curve in Tate normal form (using the procedure at the beginning of the section), we arrive at a parameterization of $(\mathbb{Z}/5\mathbb{Z})^2$ torsion over $\mathbb{Q}(\zeta_5)$ with a and b given by

$$a = b = \frac{f^4 + 2f^3 + 4f^2 + 3f + 1}{f^5 - 3f^4 + 4f^3 - 2f^2 + f}, \text{ for } f \in F(T).$$

Thus, if $\mathbb{F}$ is of characteristic $p \neq 5$, $\mathbb{F}$ contains a primitive 4th root of unity, and $f \in K$ is non-constant, we will see $(\mathbb{Z}/5\mathbb{Z})^2$ torsion with this parameterization.

Finally, rewriting our parameterization of $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ torsion in Tate normal form, we can collect the remaining parameterizations of torsion structures from Theorem 2.1.4 into Table 2.4.

Characteristic	$E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2$		G
$p \neq 3,\ \zeta_3 \in \mathbb{F}$	$a = -\frac{f(f^2+f+1)}{(f-1)^3}$	$b = -a\frac{4f^2-2f+1}{(f-1)^3}$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$p \neq 4,\ i \in \mathbb{F}$	$a = 0$	$b = f^4 - \frac{1}{16}$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$p \neq 5,\ \zeta_5 \in \mathbb{F}$	$a = \frac{f^4+2f^3+4f^2+3f+1}{f^5-3f^4+4f^3-2f^2+f}$	$b = a$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Table 2.4: One-parameter familes of elliptic curves $E_{a,b}/K$ such that $G \subset E_{a,b}(K)_{\text{tors}}$.

2.3 Torsion Structures with $p \mid E(K)_{\text{tors}}$, for Characteristic $p \geq 5$.

Since Theorem 2.1.4 only refers to function fields of characteristic $p \neq 2, 3$, we will start by assuming that $p \geq 5$. In this section, it will be our goal to determine when the torsion structures appearing in Cox and Parry's list can be combined with a point of order p. When possible, we try to develop a strategy that will work for general p.

2.3.1 Characteristic 5

Let us fix a finite field $\mathbb{F}$ of characteristic 5, and $K = \mathbb{F}(T)$. Let E/K be a non-isotrivial elliptic curve given by $y^2 = x^3 + Ax + B$ for $A, B \in K$. By Theorem 2.1.4, the following prime-to-5 torsion is guaranteed to appear for general q and suitable E:

$$0,\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z},\ \mathbb{Z}/7\mathbb{Z},\ \mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z},\ \mathbb{Z}/12\mathbb{Z}$$
$$(\mathbb{Z}/2\mathbb{Z})^2,\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
$$(\mathbb{Z}/4\mathbb{Z})^2.$$

If, in addition, $\mathbb{F}$ contains a primitive 3rd root of unity (e.g., if $|\mathbb{F}| = 5^2$), we can add the following torsion subgroups to our list:

$$(\mathbb{Z}/3\mathbb{Z})^2,\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

All of these torsion structures can be realized over K as prime-to-5 torsion subgroups by using the families of curves in Section 2.2. It remains to consider points whose order is a power of five. If we use Tate normal form, we see that all non-isotrivial curves with $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z}$ torsion are still parameterized by $E_{a,b}$: $y^2 + (1-a)xy - by = x^3 - bx^2$ with a and b given in Section 2.2. Theorem 2.1.7 gives another way of constructing curves with points of order five by playing with the Hasse and j invariants. When $p = 5$, the Hasse invariant of any curve can be computed by looking at the coefficients of the curve written in short Weierstrass form:

$$(x^3 + Ax + B)^2 = x^6 + 2Ax^4 + 2Bx^3 + A^2x^2 + 2ABx + B^2 \implies H(E) = 2A.$$

Thus, for the hypotheses on the Hasse invariant in Theorem 2.1.7 to be satisfied, we need $2A = u^4$ for some $u \in K^\times$. We use this to see if any of the torsion structures from Cox and Parry's list can appear in combination with a point of order five. Remember that by Corollary 2.1.10 we can have a point of 5-primary order of at most 5, so the possible torsion structures to confirm or rule out are

$$\begin{aligned} &\mathbb{Z}/5N\mathbb{Z} && \text{for } N = 3, 4, 6\ldots, 10, 12, \\ &\mathbb{Z}/10N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} && \text{for } N = 1, \ldots, 4, \\ &\mathbb{Z}/5N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}, && \text{for } N = 3, 4. \end{aligned} \tag{2.3}$$

If, for example, we suppose that E/K is a non-isotrivial elliptic curve with a point of order 4, then E can be written in Tate normal form as $E_{a,b} : y^2+xy-fy = x^3-fx^2$. Since $p = 5$, we can write E in short Weierstrass form:

$$E : y^2 = x^3 + 3(f^2 + f + 1)x + 4(f^3 + 4f + 1).$$

If in addition we assume that E has a point of order five, then by Theorem 2.1.7, we must have

$$H(E) = 2A = f^2 + f + 1 = u^4, \text{ for some } u \in K^\times.$$

Since $f^2+f+1 \in K[f]$ is non-constant and separable, the element $u^4-(f^2+f+1) \in (K[f])[u]$ is irreducible by Eisenstein's criterion[1]. Hence, the equation above gives an absolutely irreducible constant curve $C_{20,1} : f^2 + f + 1 = u^4$ over K. Each point $(f_0, u_0) \in C_{20,1}(K)$, $f_0 \neq 0, -1$, gives an elliptic curve,

$$E_0 : y^2 = x^3 + 3(f_0^2 + f_0 + 1)x + 4(f_0^3 + 4f_0 + 1),$$

whose Hasse invariant is a fourth power in $K^\times$. The curve E_0 is non-isotrivial if and only if its j-invariant,

$$j(E_0) = \frac{f_0^6 + 3f_0^5 + f_0^4 + 2f_0^3 + f_0^2 + 3f_0 + 1}{f_0^5 + f_0^4},$$

is non-constant. Observe that if two rational functions $g(T)$ and $h(T)$ are non-constant, then $g(h(T))$ is non-constant. Conversely, if $h(T)$ is non-constant, then $g(T)$ is non-constant if and only if $h(T)$ is non-constant. In our case, we see that

$$j(T) := \frac{T^6 + 3T^5 + T^4 + 2T^3 + T^2 + 3T + 1}{T^5 + T^4} \notin \mathbb{F}.$$

Thus $j(E_0)$ is non-constant if and only if f_0 is non-constant, and therefore, E_0 is non-isotrivial if and only if (f_0, u_0) is a non-constant point. That is, a point of order

[1] Throughout, absolute irreducibility of curves of the form $u^{p-1} = H(f)$ has been verified using Eisenstein's criterion, using the fact that in each case, $H(f)$ is separable.

20 over K implies the existence of a *non-constant* point on the irreducible constant curve $C_{20,1}$. But $C_{20,1}$ has genus one[2], so by Corollary 2.1.14, all points on $C_{20,1}/K$ are constant. Hence $\mathbb{Z}/20\mathbb{Z}$ torsion is impossible over K.

Remark 2.3.1. Not surprisingly, our curve $C_{20,1}$ is isomorphic over $\mathbb{F}_5(T)$ to the modular curve $X_1(20,1)$ considered over $\mathbb{Q}(T)$ and reduced modulo 5, see, for example [18]. This suggests a different method for finding a curve to parameterize curves with points of order 20. Our method for constructing this curve avoids the subtleties of reducing $X_1(N)$ at the prime p (the characteristic of K) when p divides N.

We can adapt this argument to rule out points of larger order. By using Tate normal form, we may begin by supposing that E is an elliptic curve with a point of order m for $m = 6, 7, 8, 9, 12$. Then, by the above argument, bringing E to short Weierstrass form, E can be written as $y^2 = x^3 + A_m(f)x + B_m(f)$ for non-constant $f \in K$. For each m, an additional point of order five will again imply the existence of a *non-constant* point on the (possibly singular) constant curve

$$C_{5m,1} : H(E) = 2A_m(f) = u^4.$$

In each case, $A_m(f)$ is separable, so that $C_{5m,1}$ is irreducible by Eisenstein's argument above. Thus, if the genus of $C_{5m,1}$ is positive, then by Corollary 2.1.14 this is enough to show that $5m$-torsion is impossible over K.

Example 2.3.2. Over K, a non-isotrivial elliptic curve with a point of order 30 implies a non-constant point on $C_{30,1} : 4f^4 + 2f^3 + 2f + 1 = u^4$, and a point of order 35 gives a non-constant point on the curve $C_{35,1} : f^8 + 3f^7 + 2f^6 + 4f^5 + f^2 + 4f = u^4$.

[2] In this case, C_{20} is hyperelliptic, so that its genus is $g = \frac{4-2}{2} = 1$. Throughout the rest of the paper, however, all genus calculations have been done using Magma [1].

Using Magma, we compute the genera of these curves to be 3 and 9 respectively, and thus, see that $\mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z}/35\mathbb{Z}$ are impossible over K.

By using Corollary 2.1.14, we have already shown that $\mathbb{Z}/20\mathbb{Z}$, $\mathbb{Z}/30\mathbb{Z}$, and $\mathbb{Z}/35\mathbb{Z}$ torsion structures are impossible for elliptic curves defined over K. In Table 2.5, we let $G = \mathbb{Z}/5m\mathbb{Z}$ for $m \geq 4$, and $C_{5m,1} : H(E) = 2A_m(f) = u^4$ be the curve obtained by bringing the Tate normal form to short Weierstrass form. In particular, combining genus calculations with Corollary 2.1.14, the table rules out any torsion structures from (2.3) with a point of order greater than 15.

m	G	Curve $C_{5m,1}$	genus of C_{5m}
4	$\mathbb{Z}/20\mathbb{Z}$	$f^2 + f + 1 = u^4$	1
6	$\mathbb{Z}/30\mathbb{Z}$	$4f^4 + 2f^3 + 2f + 1 = u^4$	3
7	$\mathbb{Z}/35\mathbb{Z}$	$f^8 + 3f^7 + 2f^6 + 4f^5 + f^2 + 4f + 1 = u^4$	9
8	$\mathbb{Z}/40\mathbb{Z}$	(ruled out by C_{20})	n/a
9	$\mathbb{Z}/45\mathbb{Z}$	$f^{12} + 3f^{11} + 4f^{10} + 2f^9 + 4f^8 + 4f^6 + 4f^5 + 2f^4 + 3f^3 + 3f^2 + 1 = u^4$	15
12	$\mathbb{Z}/60\mathbb{Z}$	(ruled out by C_{20})	n/a

Table 2.5: Ruling out $G = \mathbb{Z}/5m\mathbb{Z}$ torsion over K for $m \geq 4$.

Continuing with this strategy, we combine the Tate normal forms parameterizing curves with $\mathbb{Z}/3\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^2$ torsion structures with the hypotheses of Theorem 2.1.7 to look for subgroups $\mathbb{Z}/15\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This time, we have *two-parameter* families with elements $a, b \in K$ (at least one of which is non-constant), that when written in short Weierstrass form and combined with the Hasse invariant give *surfaces* $S_{5m,n} : H(E) = 2A(a, b) = u^4$ with $a, b, u \in K$.

$\mathbb{Z}/5m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$	$S_{5m,n}$	Change of Variables	$C_{5m,n}$	genus of $C_{5m,n}$
$\mathbb{Z}/15\mathbb{Z}$	$a^4 + ab = u^4$	$a \mapsto a/u,\ b \mapsto b/u^3$	$a^4 + ab = 1$	0
$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$a^2 + 4ab + b^2 = u^4$	$a \mapsto a/u^2,\ b \mapsto b/u^2$	$a^2 + 4ab + b^2 = 1$	0

Table 2.6: Curves parameterizing elliptic curves with $G = \mathbb{Z}/15\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion over K.

In Table 2.6, if the torsion subgroup $G = \mathbb{Z}/5m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ exists in a non-isotrivial elliptic curve over K, it implies there is a point (a, b, u) on $S_{5m,n}$ with at least one of a or b non-constant. Note, however, that in the case of $\mathbb{Z}/15\mathbb{Z}$, we are looking at the curve $E : y^2 + axy + by = x^3$. If $H(E) = u^4$, then by the change of variables in [16, p. 45], E is isomorphic to the curve

$$E' : y^2 + au^{-1}xy + bu^{-3}y = x^3,$$

which has Hasse invariant one. Similarly, in the case of $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we are looking at the curve $E : y^2 = x^3 + (a+b)x^2 + abx$, with $H(E) = u^6$, which is in turn isomorphic to the curve $E' : y^2 = x^3 + (a+b)u^{-2}x^2 + abu^{-4}x$, again, with Hasse invariant one. In both cases, $a, b \in K$ are arbitrary parameters, so we can swallow u into them (as in Table 2.6) and fully parameterize elliptic curves with $H(E) = u^6$ (up to isomorphism) by constant *curves*, call them $C_{5m,n}$, which are also given in Table 2.6.

Note, especially, that under our isomorphism, a constant point on $C_{5m,n}$ corresponds, by definition, to a *constant* elliptic curve. Thus, since we are interested in non-isotrivial elliptic curves, we are still looking for non-constant points on $C_{5m,n}$. For example, we can parameterize $C_{15,1}$ by

$$a^4 + ab = 1 \iff b = \frac{1 - a^4}{a},$$

and thus, every non-isotrivial elliptic curve E/K with a point of order three and a fourth-power Hasse invariant is isomorphic to a curve of the form

$$E : y^2 + axy + \frac{1 - a^4}{a}y = x^3, \text{ for some non-constant } a \in K.$$

If, in addition, $j(E) \in K^5$, then we will obtain a curve with a point of order 15. We have

$$j(E) = \frac{3a^4}{a^{16} + 3a^{12} + 2a^4 + 4}.$$

Since $j(E) = j(a)$ is not trivially a fifth power (i.e., $j(a)$ is not a fifth power when we choose $a = T$), then by Remark 2.1.8, we see that $j(a) \in K^5$ if and only if $a \in K^5$, so that setting $a = f^5$, we obtain the following parameterization of all elliptic curves over K with a point of order fifteen:

$$E : y^2 + f^5 xy + \frac{1 - f^{20}}{f^5} y = x^3 \text{ for some non-constant } f \in K.$$

Notice that the equation for $C_{10,2}$ is a conic in the variables a and b, with trivial solution $(a, b) = (1, 0)$. Thus, we can parameterize all solutions over K by

$$a = \frac{g^2 - 1}{g^2 + 4g + 1}, \qquad b = g(a - 1), \qquad \text{for non-constant } g \in K$$

Then, by taking $g \in K$, with g non-constant, we can obtain a non-isotrivial curve whose Hasse invariant is a fourth power in $K^\times$. Again, the j-invariant of E is not trivially a fifth power, so $j(E) \in K^5$ if and only if $g = f^5$ for some non-constant f in K. Thus, if E is a non-isotrivial elliptic curve with torsion subgroup $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, if and only if E can be written in the following form:

$$E : y^2 = x^3 + \frac{2f^{10} + 3f^5 + 4}{f^{10} + 4f^5 + 1} x^2 + \frac{f^{20} + 3f^{15} + 4f^{10} + 2f^5}{f^{20} + 3f^{15} + 3f^{10} + 3f^5 + 1} x \text{ for non-constant } f \in K.$$

It is left to determine whether or not $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ can occur over K when $\mathbb{F}$ contains a primitive 3rd root of unity. For this, we return to Section 2.2 to find curves with $(\mathbb{Z}/3\mathbb{Z})^2$ torsion given by the parameterization

$$y^2 + 3(f+2)xy + 4(f^2+f+1)y = x^3 \text{ for non-constant } f \in K.$$

If a point of order five exists, we must have $H(E) = f^4 + 3f = u^4$ for some $u \in K^\times$. Since $f^4 + 3f = u^4$ defines an absolutely irreducible constant curve over K of genus 3, it can have no non-constant points, and thus $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is impossible over K.

We collect all of our results from this section into the following theorem.

Theorem 2.3.3. *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*

$$\left.\begin{array}{ll} \mathbb{Z}/N\mathbb{Z} & \textit{with } 1 \le N \le 10 \textit{ or } N = 12, 15, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{with } 1 \le N \le 5, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. & \end{array}\right\} \textit{for general } \mathbb{F}.$$

$$\begin{array}{lll} \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, & \textit{with } N = 1, 2, & \textit{if } \zeta_3 \in \mathbb{F}. \end{array}$$

Further, each of these groups occurs infinitely often as $E(K)_{\text{tors}}$ for some elliptic curve E/K.

2.3.2 Characteristic 7

Now we consider a finite field $\mathbb{F}$ with of characteristic 7, and $K = \mathbb{F}(T)$. Let E/K be a non-isotrivial elliptic curve given by $y^2 = x^3 + Ax + B$ for $A, B \in K$. By Theorem 2.1.4, the following prime-to-p torsion groups appear for suitable E:

$$0,\ \mathbb{Z}/2\mathbb{Z},\ \ldots\ ,\ \mathbb{Z}/6\mathbb{Z},\ \mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z},\ \mathbb{Z}/10\mathbb{Z},\ \mathbb{Z}/12\mathbb{Z},$$

$$(\mathbb{Z}/2\mathbb{Z})^2,\ \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},$$
$$(\mathbb{Z}/3\mathbb{Z})^2,\ \mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}.$$

If, in addition, a primitive 4th or 5th root of unity are in $\mathbb{F}$, we may obtain $(\mathbb{Z}/4\mathbb{Z})^2$ or $(\mathbb{Z}/5\mathbb{Z})^2$ respectively, again, both of which will also appear for suitable E. As in the previous section, all of these torsion subgroups, and the subgroup $\mathbb{Z}/7\mathbb{Z}$, can be seen using the parameterizations from Section 2.2.

As before, we will use Theorem 2.1.7 to try and force a point of order seven to appear along with any of the torsion structures from Cox and Parry's list. Again, by Corollary 2.1.10, we can have a point of 7-primary order of at most 7, so the torsion structures to consider are

$$\begin{array}{cl}\mathbb{Z}/7N\mathbb{Z} & \text{for } N=2,\dots,6,8,9,10,12,\\ \mathbb{Z}/14N\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} & \text{for } N=1,\dots,4,\\ \mathbb{Z}/7N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}, & \text{for } N=3,4,5,\\ \mathbb{Z}/42\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}. & \end{array}\tag{2.4}$$

We begin by supposing that E is an elliptic curve with $\mathbb{Z}/m\mathbb{Z}$ torsion for $m=4,5,6,8,9,10,12$. Then E is isomorphic to a curve $E: y^2=x^3+A_m(f)x+B_m(f)$ for some non-constant $f\in K$, where $A(f)$ and $B(f)$ are again non-constant functions of f found by converting Tate normal form into short Weierstrass form. This time, for each m, to discover an additional point of order seven, we will need the Hasse invariant to be a sixth power. Expanding $(x^3+A_m(f)x+B_m(f))^3$ and keeping the coefficient of x^3, we obtain the following revision of our method from Section 2.3.1:

$$H(E)=3B_m(f)=u^6,\ \text{for } u\in K^\times.$$

In Table 2.7, we let $G = \mathbb{Z}/7m\mathbb{Z}$, and $C_{7m,1} : 3B_m(f) = u^6$. As above, in each case, $B_m(f)$ is separable, and we can use Eisenstein's criterion to show that $C_{7m,1}$, therefore, defines an irreducible constant curve over K. Thus, any non-isotrivial elliptic curve with a point of order $7m$ implies the existence of a non-constant point on $C_{7m,1}$, and again, Corollary 2.1.14 shows that G cannot exist for $m \geq 4$.

m	G	$C_{7m,1}$	genus of $C_{7m,1}$
4	$\mathbb{Z}/28\mathbb{Z}$	$6f^3 + f^2 + 3f + 1 = u^6$	4
5	$\mathbb{Z}/35\mathbb{Z}$	$f^6 + 3f^5 + 5f^4 + 5f^2 + 4f + 1 = u^6$	10
6	$\mathbb{Z}/42\mathbb{Z}$	$f^6 + 2f^5 + 2f^4 + 5f^3 + f^2 + 4f + 1 = u^6$	10
8	$\mathbb{Z}/56\mathbb{Z}$	(ruled out by $C_{28,1}$)	n/a
9	$\mathbb{Z}/63\mathbb{Z}$	(to be ruled out by $C_{21,1}$ below)	n/a
10	$\mathbb{Z}/70\mathbb{Z}$	(ruled out by $C_{35,1}$)	n/a
12	$\mathbb{Z}/84\mathbb{Z}$	(ruled out by $C_{28,1}$)	n/a

Table 2.7: Ruling out $G = \mathbb{Z}/7m\mathbb{Z}$ torsion over K for $m \geq 4$.

Next, we suppose that E is an elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, or $(\mathbb{Z}/2\mathbb{Z})^2$, and combine Tate normal forms with the hypotheses of Theorem 2.1.7. Again, torsion structures $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/21\mathbb{Z}$, and $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ give points (a, b, u) with $a, b, u \in K$ and at least one of a or b non-constant on surfaces $S_{7m,n} : 3B(a, b) = u^6$, as in Table 2.8. Again, a change of variables shows that non-constant points on the curves $C_{7m,n}$ in Table 2.8, correspond (up to isomorphism) to non-isotrivial elliptic curves whose Hasse invariant is a sixth power in K. Immediately, we find the existence of torsion structures $\mathbb{Z}/21\mathbb{Z}$ or $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ over K implies non-constant points

G	S_G	change of variables	C_G	genus
$\mathbb{Z}/14\mathbb{Z}$	$a^3 + 6ab = u^6$	$a \mapsto a/u^2,\ b \mapsto b/u^4$	$a^3 + 6ab = 1$	0
$\mathbb{Z}/21\mathbb{Z}$	$a^6 + 6a^3b + 6b^2 = u^6$	$a \mapsto a/u,\ b \mapsto b/u^3$	$a^6 + 6a^3b + 6b^2 = 1$	2
$\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$a^3 + 2a^2b + 2ab^2 + b^3 = u^6$	$a \mapsto a/u^2,\ b \mapsto b/u^2$	$a^3 + 2a^2b + 2ab^2 + b^3 = 1$	1

Table 2.8: Curves parameterizing elliptic curves with $G = \mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/21\mathbb{Z}$ and $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion over K.

on constant curves of positive genus. Using Magma, we find that these curves are absolutely irreducible[3], hence irreducible regardless of the cardinality of $\mathbb{F}$. Thus, using Corollary 2.1.14, we find that these torsion structures are impossible. The curve $C_{14,1}$, however, can be parameterized easily by

$$a^3 + 6ab = 1 \iff b = \frac{1-a^3}{6a}.$$

Again, we can compute $j(E)$ and see that $j(E) \in K^7$ if and only if $a = f^7$ for some non-constant f in K. Thus, if E is a non-isotrivial elliptic curve over K with a point of order 14, it can be written in the following form:

$$E : y^2 = x^3 + f^7x^2 + \frac{1-f^{21}}{6f^7}x \text{ for some non-constant } f \in K.$$

We have, in fact, ruled out any torsion structures from (2.4) with a point of order greater than 14, and the torsion structure $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We can collect all of this into the following theorem.

Theorem 2.3.4. *Let $\mathbb{F}$ be a finite field of characteristic 7, $K = \mathbb{F}(T)$, and E/K be a non-isotrivial elliptic curve. The torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic*

[3] In the cases where $H(E)$ was a function of two parameters, rather than using Eisenstein's criterion, Magma was used to determine irreducibility.

to one of the following

$$\left.\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & \textit{with } 1 \leq N \leq 10 \textit{ or } N = 12, 14, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \textit{with } 1 \leq N \leq 4, \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, & \textit{with } N = 1, 2, \end{array}\right\} \textit{for general } \mathbb{F}.$$

$$(\mathbb{Z}/n\mathbb{Z})^2, \qquad \textit{if } \zeta_n \in \mathbb{F}, \ \textit{where } n = 4, 5.$$

Further, each of these groups occurs infinitely often as $E(K)_{\mathrm{tors}}$ for some elliptic curve E/K.

2.3.3 Characteristic 11

Now we let $\mathbb{F}$ be a finite field of characteristic 11, and $K = \mathbb{F}(T)$. Let E/K be a non-isotrivial elliptic curve given by $y^2 = x^3 + Ax + B$ for $A, B \in K$. By Theorem 2.1.4, the following prime-to-p torsion subgroups appear for suitable E:

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

If, in addition, $\mathbb{F}$ contains a primitive 3rd or 4th root of unity (e.g., if $|\mathbb{F}| = 11^2$), we may obtain $(\mathbb{Z}/3\mathbb{Z})^2$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $(\mathbb{Z}/4\mathbb{Z})^2$ respectively, again, both of which will also appear for suitable E. As in both the cases above, all of these torsion subgroups can be realized using parameterizations from Section 2.2.

It is not immediately clear whether a curve with a point of order eleven even exists, since this is not a torsion structure we have parameterized (since it does not occur over $\mathbb{Q}$). This time, the Hasse invariant of any curve written in short Weierstrass form is $H(E) = 9AB$, and by Theorem 2.1.7, we must have $9AB = u^{10}$ for some

$u \in K^\times$ and $j(E) \in K^{11}$. With this information have the following parameterization.

Theorem 2.3.5. *Let $\mathbb{F}$ be a finite field of characteristic 11, and $K = \mathbb{F}(T)$. The one-parameter family $E_f : y^2 = x^3 + f^{11}x + 5f^{-11}$ for non-constant $f \in K$ is a parameterization of all non-isotrivial curves with a K-rational 11-torsion point.*

Proof. Let $E : y^2 = x^3 + Ax + B$ be a non-isotrivial elliptic curve over K with a K-rational point of order 11. By Theorem 2.1.7, it must be that the Hasse invariant of E is a tenth power in $K^\times$, so that for some $u \in K^\times$, we must have $H(E) = 9AB = u^{10}$. In particular, this means that A and B are both non-zero. Also by Theorem 2.1.7, we have

$$j(E) = \frac{-1728(4A)^3}{-16(4A^3+27B^2)} \in K^{11} \overset{A\neq 0}{\iff} \frac{B^2}{A^3} \in K^{11} \overset{B\neq 0}{\iff} B^2 = A^3 g^{11} \text{ for some non-zero } g \in K.$$

Combining these two restrictions on A and B, we obtain

$$9AB = u^{10} \overset{p=11}{\Longrightarrow} 4A^2B^2 = u^{20} \iff 4A^2A^3g^{11} = u^{20} \iff A^5 = 3g^{-11}u^{20}.$$

Clearly, u^{20} is a fifth power in $K^\times$, so that comparing each side of the equation, $3g^{-11}$ must be a fifth power. In fact, $3g^{-1}$ must be a fifth power, so that setting $h^5 = 3g^{-1}$, we obtain

$$A^5 = 3g^{-11}u^{20} = (3g^{-1})^{11}u^{20} = h^{55}u^{20} \iff A = \zeta_5 h^{11}u^4, \text{ with } \zeta_5 \in \mathbb{F}_{11} \text{ such that } \zeta_5^5 = 1.$$

But $\zeta_5 h^{11} = (\zeta_5 h)^{11}$, so setting $f = \zeta_5 h$, we obtain $A = f^{11}u^4$. We can find B using

$$9AB = u^{10} \iff B = 5A^{-1}u^{10} = 5(f^{-11}u^{-4})u^{10} = 5f^{-11}u^6.$$

Thus, we have

$$E : y^2 = x^3 + f^{11}u^4x + 5f^{-11}u^6,$$

which, after a change of variables, is isomorphic to $E : y^2 = x^3 + f^{11}x + 5f^{-11}$. □

Remark 2.3.6. An identical procedure shows that $E_f : y^2 = x^3 + 3x + f^5$ parameterizes all curves with a point of order 5 over $\mathbb{F}(T)$ of characteristic 5, and $E_f : y^2 = x^3 + f^7x + 5$ parameterizes all curves with a point of order 7 over $\mathbb{F}(T)$ of characteristic 7. In both cases, however, it is not hard to show that these families are equivalent to the ones given by Tate normal form, and no new information is gained.

Now, we will try to combine a point of order eleven with torsion structures from Theorem 2.1.4. This time, Corollary 2.1.10 tells us that we can have a point of 11-primary torsion of at most 11, so the combined torsion structures we would like to consider are

$$\begin{aligned} &\mathbb{Z}/11N\mathbb{Z} && \text{for } N = 2, \ldots, 10, 12, \\ &\mathbb{Z}/11N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} && \text{for } N = 1, \ldots, 4, \\ &\mathbb{Z}/11N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}, && \text{for } N = 3, 4, 5, \\ &\mathbb{Z}/66\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}. \end{aligned} \tag{2.5}$$

This time, we begin by supposing that E has torsion structures $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$. By working with the two-parameter families for these torsion structures and the Hasse invariant, we again arrive at surfaces $S_{11m,n} : 9A(a, b)B(a, b) = u^{10}$. Since $u \in K^\times$, under the same change of variables as in Section 2.3.2, we see that non-isotrivial elliptic curves over K whose Hasse invariant is a tenth power correspond, up to isomorphism, to non-constant points on *curves*, $C_{11m,n} : 9A(a,b)B(a,b) = 1$, given in Table 3.4. Magma again reveals these curves to be absolutely irreducible. In particular, since each of the $C_{11m,n}$ are constant curves of positive genus, we find that all of the torsion subgroups $\mathbb{Z}/22\mathbb{Z}$, $\mathbb{Z}/33\mathbb{Z}$ and $\mathbb{Z}/22\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are impossible over K by Corollary 2.1.14.

G	change of variables	C_G	genus
$\mathbb{Z}/22\mathbb{Z}$	$a \mapsto a/u^2,\ b \mapsto b/u^4$	$a^5 + 9a^3b + 8ab^2 = 1$	2
$\mathbb{Z}/33\mathbb{Z}$	$a \mapsto a/u,\ b \mapsto b/u^3$	$a^{10} + 6a^7b + 2a^4b^2 + 8ab^3 = 1$	9
$\mathbb{Z}/22\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$a \mapsto a/u^2,\ b \mapsto b/u^2$	$a^5 + 3a^4b + a^3b^2 + a^2b^3 + 3ab^4 + b^5 = 1$	6

Table 2.9: Curves parameterizing elliptic curves with $G = \mathbb{Z}/22\mathbb{Z}$, $\mathbb{Z}/33\mathbb{Z}$ and $\mathbb{Z}/22\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion over K.

If we suppose that E has $\mathbb{Z}/m\mathbb{Z}$ torsion for $m = 4, \ldots, 10, 12$, then, E is isomorphic to a curve $E : y^2 = x^3 + A_m(f)x + B_m(f)$, where $A_m(f)$ and $B_m(f)$ are found as above, and

$$C_{11m,1} : H(E) = 9A_m(f)B_m(f) = u^{10}, \text{ for non-constant } f \in K, u \in K^{\times}.$$

This equation is still just an irreducible constant curve over K. In Table 2.10, we let $G = \mathbb{Z}/11m\mathbb{Z}$, and $C_{11m,1}$ be the curve above. Again, we see that such torsion subgroups G cannot exist for $m \geq 4$.

We have ruled out any torsion structures from (2.5) with a point of order greater than 12. In fact, we have ruled out the possibility of combining a point of order eleven with *any* of the torsion structures from Cox and Parry's list. Thus, we have the following theorem.

Theorem 2.3.7. *Let $\mathbb{F}$ be a finite field of characteristic 11, $K = \mathbb{F}(T)$, and E/K be a non-isotrivial elliptic curve. The torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic*

m	G	$C_{11m,1}$	genus of $C_{11m,1}$
4	$\mathbb{Z}/44\mathbb{Z}$	(ruled out by $C_{22,1}$)	n/a
5	$\mathbb{Z}/55\mathbb{Z}$	$f^{10}+3f^9+8f^8+4f^7+8f^6+8f^4+7f^3+8f^2+8f+1=u^{10}$	36
6	$\mathbb{Z}/66\mathbb{Z}$	(ruled out by $C_{22,1}$ and $C_{33,1}$)	n/a
7	$\mathbb{Z}/77\mathbb{Z}$	$f^{20}+3f^{19}+f^{18}+4f^{17}+6f^{16}+5f^{15}+6f^{14}+5f^{13}+9f^{12}+7f^{11}+$ $+5f^{10}+8f^9+8f^8+5f^7+2f^6+7f^5+4f^4+8f^3+6f^2+10f+1=u^{10}$	81
8	$\mathbb{Z}/88\mathbb{Z}$	(ruled out by $C_{22,1}$)	n/a
9	$\mathbb{Z}/99\mathbb{Z}$	(ruled out by $C_{33,1}$)	n/a
10	$\mathbb{Z}/110\mathbb{Z}$	(ruled out by $C_{22,1}$)	n/a
12	$\mathbb{Z}/132\mathbb{Z}$	(ruled out by $C_{33,1}$)	n/a

Table 2.10: Ruling out $G=\mathbb{Z}/11m\mathbb{Z}$ torsion over K for $m\geq 4$.

to one of the following:

$$\left.\begin{array}{ll}\mathbb{Z}/N\mathbb{Z}, & \textit{with } 1\leq N\leq 12,\\ \mathbb{Z}/2N\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}, & \textit{with } 1\leq N\leq 4,\\ \mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z} & \end{array}\right\}\ \textit{for general } \mathbb{F}.$$

$$\begin{array}{lll}\mathbb{Z}/3N\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}, & \textit{with } N=1,2, & \textit{if } \zeta_3\in\mathbb{F}.\\ \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}, & & \textit{if } \zeta_4\in\mathbb{F}.\end{array}$$

Further, each of these groups occurs infinitely often as $E(K)_{\text{tors}}$ for some elliptic curve E/K.

2.4 Torsion Structures for Characteristic $p=2,3$.

Unfortunately, in Theorem 2.1.4, Cox and Parry make the assumption that the characteristic of $\mathbb{F}$ is not 2 or 3. In order to proceed, we need to come up with a similar statement for these characteristics. We will use the following result to extend Cox and Parry's list to one for all primes p.

Proposition 2.4.1 ([2, Proposition 3.7])**.** *The modular curve*[4] $X_1(n, m)$ *has genus* 0 *if and only if* (m, n) *is one of the following* 18 *ordered pairs:*

$$(2,1),\ (3,1),\ \dots,\ (10,1),\ (12,1),$$
$$(2,2),\ (4,2),\ (6,2),\ (8,2),$$
$$(3,3),\ (6,3),\ (4,4),\ (5,5).$$

Cox and Parry use this proposition to provide a list of all possible prime-to-p torsion in Theorem 2.1.4, then show that it is, in fact, minimal. In what remains of this section, for $\mathbb{F}$ a finite field of characteristic $p = 2$ or 3, and $K = \mathbb{F}(T)$, we will show what prime-to-p torsion subgroups can appear, and as in Section 2.3, determine when and in what ways points of order p can be combined with them.

2.4.1 Characteristic 2

We start with $\mathbb{F}$ of characteristic 2, and $K = \mathbb{F}(T)$. Given an elliptic curve E over K, written in long Weierstrass form, E has Hasse invariant $H(E) = a_1$ [21, p. 14]. We have the following theorem about the prime-to-2 torsion structures we should expect over K.

Theorem 2.4.2. *Let* $\mathbb{F}$ *be a finite field of characteristic* 2*,* $K = \mathbb{F}(T)$*, and* E/K *be a non-isotrivial elliptic curve. Let* $G = E(K)'_{\text{tors}}$ *be the group of rational points of finite order not divisible by* 2*. Then* G *is isomorphic to one of the following:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && \textit{with } 1 \le N = 1, 3, 5, 7, 9, \\ &(\mathbb{Z}/N\mathbb{Z})^2, && \textit{with } N = 3, 5. \end{aligned}$$

[4] For $m \mid n$ and $p \nmid m$, $X_1(n, m)$ is a coarse moduli space for elliptic curves with torsion subgroup containing a subgroup isomorphic to $\mathbb{Z}/n \times \mathbb{Z}/m\mathbb{Z}$. See Definition 2.1.1 for a precise definition.

Further, each of these groups appears infinitely often as $E(K)'_{\mathrm{tors}}$ for some elliptic curve E/K.

Proof. Our proof follows that of Proposition 2.1.3 in [21, Proposition 7.1], using the Hurwitz formula to bound the genera of modular curves, a method dating at least back to Levin (see [13]). If $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for $2 \nmid m, n$, then there is a modular curve $X_1(n, m)$ defined over $\mathbb{F}_2(\mu_n)$ that is a coarse moduli space for elliptic curves with torsion structure isomorphic to G. Since E is non-isotrivial, we obtain a non-constant morphism $\mathbb{P}^1 \to X_1(n, m)$ which, by the Hurwitz formula, implies that if $G \subset E(K)_{\mathrm{tors}}$, then the genus of $X_1(n, m)$ must be zero. Thus, G must be given by one of the pairs (m, n) in Proposition 2.4.1 such that $2 \nmid m, n$. Using the parameterizations from Section 2.2, it is easy to show that all of the groups in this list appear infinitely often when $\mathbb{F}$ contains the necessary roots of unity. □

We will have a point of order 2 if and only if $H(E) \in (K^\times)^{2-1} = K^\times$, that is, if $a_1 \neq 0$, and $j(E) \in K^2$. By Levin's bounds, we see that the 2-primary component can have at most order 8. By using parameterizations from Section 2.2, we immediately see infinitely many elliptic curves can have torsion subgroups $\mathbb{Z}/2n\mathbb{Z}$ for $1 \leq n \leq 6$, and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ if $\mathbb{F}$ contains a 3rd root of unity. Thus, for $e = 1, 2, 3$, we only need to confirm or rule out the following torsion structures over K:

$$\begin{aligned} &\mathbb{Z}/2^eN\mathbb{Z} && \text{for } N = 7, 9, 10, 12, \\ &\mathbb{Z}/2^eN\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} && \text{for } N = 3, 5. \end{aligned} \tag{2.6}$$

To see $\mathbb{Z}/14\mathbb{Z}$, recall that Tate normal form with $a = g^2 - g$, $b = ag$, for non-constant $g \in K$ gives a non-isotrivial elliptic curve with $(0, 0)$ a point of order seven. Again we find $j(E) \in K^2$ if and only if $g = f^2$, for some $f \in K$. Hence, any non-isotrivial curve with a point of order 14 is isomorhic to

$$E : y^2+(f^4+f^2+1)xy+(f^6+f^4)y = x^3+(f^6+f^4)x^2 \text{ for some non-constant } f \in K.$$

The same argument shows that any non-isotrivial curve with a point of order 18 is isomorphic to

$$E : y^2+(f^6+f^4+1)xy+(f^{10}+f^4)y = x^3+(f^{10}+f^4)x^2 \text{ for some non-constant } f \in K.$$

Unfortunately, the same type of argument will not work in determining existence of $\mathbb{Z}/20\mathbb{Z}$ or $\mathbb{Z}/24\mathbb{Z}$, since in each of these cases, a point of order two already exists. That is, any curve E with these torsion subgroups has invariants which *already satisfy* the hypotheses of Theorem 2.1.7. Instead, we try a different strategy, using division polynomials. Suppose that E is a non-isotrivial elliptic curve with a point of order ten (respectively twelve), so that E can be written as

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

where the formulas for a and b are as in Section 2.2. Here, $(0, 0)$ is a point of order 10. Thus, without loss of generality, if E has a point of order 20, we must have

$$0 = x([2]P) = \phi_2(P)/\psi_2(P)^2 \iff \phi_2(P) = 0 \iff x^4 + (ab+b)x^2 + b^3 = 0.$$

Combining this with the formulas in Section 2.2 we obtain

$$\phi_2(P) = x^4 + \frac{f^4+f^3}{f^6+f^5+f^3+f+1}x^2 + \frac{f^{12}+f^{11}+f^{10}+f^9}{f^{12}+f^{10}+f^6+f^2+1} = 0 \text{ for } x, f \in K.$$

Finally, we can clear denominators to obtain

$$(f^{12}+f^{10}+f^6+f^2+1)x^4+(f^{10}+f^8+f^7+f^6+f^5+f^3)x^2+f^{12}+f^{11}+f^{10}+f^9=0.$$

Once again, this is a constant curve over K, which Magma reveals is absolutely irreducible, and has genus one. Note that by hypothesis, E is isotrivial if $f\in\mathbb{F}$, so we are looking for solutions (x,f) with f non-constant, and hence (x,f) is non-constant. Thus, by Corollary 2.1.14, no such solution exists. Points of order 20 are therefore impossible over K. In Table 2.11, we use the same strategy to eliminate points of order 24.

To rule out points of order 28, we start with a curve with the point $(0,0)$ of order 7. We have

$$x([4]P)=0 \iff \phi_4(P)=(x+f^3+f^2)^4(x^2+f^3+f)^2\lambda_{28}(x,f)=0,$$

where $\lambda_{28}(x,t)$ is an absolutely irreducible polynomial. The first factor gives the point of order *seven*, $P=(f^3+f^2,0)$. If $f=g^2$ for some $g\in K^\times$, then the second factor gives a point P of order *fourteen* (see above) such that $x(P)=g^3+g$. The equation $\lambda_{28}=0$, however, defines an irreducible curve of genus 3, which by the above argument, shows that a point of order 28 is impossible over K. In Table 2.11, we use an analogous construction for λ_{36}, and rule out points of order 36. Note that we have now ruled out any torsion from (2.6) with a point of order greater than 18.

If $\mathbb{F}$ contains a primitive fifth root of unity, then curves with $(\mathbb{Z}/5\mathbb{Z})^2$ torsion over K are parameterized by $E_{a,b}: y^2+(1-a)xy-by=x^3-bx$ with a and b functions of some non-constant $g\in K$, given in Section 2.2. Here, $H(E)=a_1=1-a\in K^\times$, and

G	$E_{a,b}$	Order of $(0,0)$	C_G	genus of C_G
$\mathbb{Z}/20\mathbb{Z}$	$a=\frac{f(f+1)}{f^2+f+1},\ b=a\frac{f^2}{f^2+f+1}$	10	$\phi_2(P)=0$ (of degree 16)	1
$\mathbb{Z}/24\mathbb{Z}$	$a=\frac{f(f^2+f+1)}{(f-1)^3},\ b=\frac{a}{f-1}$	12	$\phi_2(P)=0$ (of degree 16)	2
$\mathbb{Z}/28\mathbb{Z}$	$a=f^2+f,\ b=af$	7	$\lambda_{28}(P)=0$ (of degree 18)	3
$\mathbb{Z}/36\mathbb{Z}$	$a=f^2(f+1),\ b=a(f+1)^2$	9	$\lambda_{36}(P)=0$ (of degree 30)	5

Table 2.11: Using division polynomials to rule out $\mathbb{Z}/4m\mathbb{Z}$ for $m=5,6,7,9$.

$j(E)\in K^2$ if and only if $g=f^2$ for some $f\in K$. Hence, any curve with $\mathbb{Z}/10\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ torsion is isomorphic to a curve of the form $E_{a,b}$ with

$$a=b=\frac{f^8+f^2+1}{f^{10}+f^8+f^2},\text{ for some non-constant}f\in K.$$

Finally, recall, if $\mathbb{F}$ contains a primitive third root of unity, then any elliptic curve with $(\mathbb{Z}/3\mathbb{Z})^2$ torsion can be written in the form $E_f: y^2+fxy+(f^2+f+1)y=x^3$ for some non-constant $f\in K$, with $(0,0)$ as a point of order three. Without loss of generality if E_f has torsion subgroup $\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, then there is a point P, of order twelve, such that $4P=(0,0)$. Thus, we have $0=\phi_4(P)=x^4(x^2+t^3+t^2+t)^2\lambda(x,f)$. As above, we find that the first two factors correspond to a point of order 3 and 6 (if $f=g^2$ for some $g\in K^\times$) respectively. However, $\lambda=0$ defines an absolutely irreducible curve of genus 1, showing that $\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ is impossible over K.

We can collect all of this into the following theorem.

Theorem 2.4.3. *Let $\mathbb{F}$ be a finite field of characteristic 2, $K=\mathbb{F}(T)$, and E/K be a non-isotrivial elliptic curve. Then the torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following*

$$\begin{array}{lll}\mathbb{Z}/N\mathbb{Z}, & \textit{with } 1\le N\le 10 \textit{ or } N=12,14,18, & \textit{for general } \mathbb{F},\\ (\mathbb{Z}/N\mathbb{Z})^2, \mathbb{Z}/2N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}, & \textit{with } N=3,5, & \textit{if } \zeta_N\in\mathbb{F}.\end{array}$$

Further, each of these groups occurs infinitely often as $E(K)_{\text{tors}}$ for some elliptic curve E/K.

2.4.2 Characteristic 3

Next, we suppose that $\mathbb{F}$ is a finite field of characteristic 3, and again, $K = \mathbb{F}(T)$. Given an elliptic curve E in long Weierstrass form, under the change of variables in [16, p. 42], for $p = 3$, we can write $E : y^2 = f(x)$ for a (monic!) degree three polynomial f, and thus, our normal calculation for the Hasse invariant of E shows $H(E) = a_2$, when written in this form. We can say the following about prime-to-3 torsion structures appearing over K.

Theorem 2.4.4. *Let $\mathbb{F}$ be a finite field of characteristic 3, $K = \mathbb{F}(T)$, and E/K be a non-isotrivial elliptic curve. Let $G = E(K)'_{\text{tors}}$ be the group of rational points of finite order not divisible by 3. Then G is isomorphic to one of the following:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && \text{with } 1 \leq N = 1, 2, 4, 5, 7, 8, 10, \\ &\mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, && \text{with } N = 1, 2, 4, \\ &(\mathbb{Z}/N\mathbb{Z})^2, && \text{with } N = 4, 5. \end{aligned}$$

Further, each of these groups appears infinitely often as $E(K)'_{\text{tors}}$ for some elliptic curve E/K.

Proof. As in the proof of Theorem 2.4.2, if $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subset E(K)_{\text{tors}}$ for $3 \nmid m, n$, then the genus of $X_1(n, m)$ defined over $\mathbb{F}_3(\mu_n)$ must be zero. Therefore, pairs from Proposition 2.4.1 with $3 \nmid m, n$ give a list of possible prime-to-3 torsion subgroups. Again, all of the groups in this list appear infinitely often by using the parameterizations from Section 2.2. □

Remark 2.4.5. Together, Theorems 2.4.2 and 2.4.4 imply that Cox and Parry's list in Theorem 2.1.4 remains valid after we remove the assumption that p is not 2 or 3.

We will have a point of order 3 if and only if $a_2 \in (K^\times)^2$ and $j(E) \in K^3$. This time, by Levin's bounds, we see that the 3-primary component can have at most order 9. Again, using parameterizations from Section 2.2, we see that the torsion subgroups $\mathbb{Z}/3N\mathbb{Z}$ for $N = 1, 2, 3$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ appear infinitely often over K. Thus, for $e = 1, 2$, we need to confirm or rule out the following torsion structures over K:

$$\begin{aligned} &\mathbb{Z}/3^eN\mathbb{Z} && \text{for } N = 5, \ldots, 8, 10, 12, \\ &\mathbb{Z}/3^e2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} && \text{for } N = 1, \ldots, 4, \\ &\mathbb{Z}/3^eN\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} && \text{for } N = 4, 5. \end{aligned} \tag{2.7}$$

Using the change of variables $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ from [16, p. 42], any curve starting in Tate normal form can be written as

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

Thus, over K, any curve written in Tate normal form $E_{a,b}$ has Hasse invariant $a_2 = a^2 + a + 2b + 1$. Note that this change of variables has the effect of moving $(0, 0)$ to $(0, -b)$.

For example, for $\mathbb{Z}/15\mathbb{Z}$ to appear, we may start with Tate normal form for a curve with $\mathbb{Z}/5\mathbb{Z}$ torsion, where $a = b = g$ for some non-constant $g \in K$. Thus, the Hasse invariant of E is

$$H(E) = g^2 + g + 2g + 1 = g^2 + 1.$$

We need $H(E) = u^2$ for some $u \in K^\times$, thus, we are looking for K solutions to the conic

$$g^2 + 1 = u^2.$$

A quick check reveals $(g, u) = (0, 1)$ is a solution, so we can parameterize all solutions by

$$g = \frac{2h}{1-h^2}, \qquad u = hg + 1, \qquad \text{for non-constant } h \in K.$$

Thus, we obtain a family of elliptic curves over K with $H(E) \in K^\times$ equal to a square. Again, $j(E) \in K^3$ if and only if $h = f^3$ for some $f \in K$, so that if E/K is a non-isotrivial elliptic curve with a point of order 15, it can be written as

$$E : y^2 + \frac{f^6 + 2f^3 + 2}{f^6 + 2}xy + \frac{2f^3}{f^6 + 2}y = x^3 + \frac{2f^3}{f^6 + 2}x^2 \text{ for some non-constant } f \in K.$$

Using our strategy in Section 2.3, if E has a point of order $m = 7, 8, 10$, then we can write it in Tate normal form. If in addition, E has a point of order three, then we must have

$$H(E) = a_m(f)^2 + a_m(f) + 2b_m(f) + 1 = u^2 \text{ for some } u \in K^\times, \text{ and non-constant } f \in K.$$

In each case, clearing denominators when necessary, a point of order $3m$ on an elliptic curve E over K implies the existence of a non-constant point on one of the curves in Table 2.12. Again, since each of the $C_{3m,1}$ in this table are irreducible and constant, we know that all of the points in $C_{3m,1}(K)$ are constant. Thus, points of order 21, 24 or 30, and hence 63, 72, and 90, are impossible over K.

m	G	$C_{3m,1}$	genus of $C_{3m,1}$
7	$\mathbb{Z}/21\mathbb{Z}$	$f^4 + 2f + 1 = u^2$	1
8	$\mathbb{Z}/24\mathbb{Z}$	$2f^4 + 2f^3 + f^2 + f + 1 = u^2$	1
10	$\mathbb{Z}/30\mathbb{Z}$	$f^6 + 2f^5 + 2f^4 + 2f^3 + 2f + 1 = u^2$	2

Table 2.12: Ruling out $G = \mathbb{Z}/3m\mathbb{Z}$ torsion over K for $m = 7, 8, 10$.

As in the case when $p = 2$, unfortunately, the same strategy cannot be applied to rule out points of order 18 or 45, since here we need to start with curves which already have invariants satisfying our hypotheses. In the same way we did above, however, we can start with a curve written in Tate normal form to get a point of specified order, then use division polynomials to obtain the necessary conditions. The results are irreducible constant curves, collected in Table 2.13. Here, the polynomial λ_{45} is the irreducible factor of $\phi_5(P) = (x + 2f^5 + 2f^4 + f^3 + f^2)\lambda_{45}$ that corresponds to a point of order 45 (as above). The table shows that points of order 18, 36 and 45 are impossible over K. Note, we have also ruled out any torsion structures from (2.7) with a point of order greater than 15.

G	$E_{a,b}$	order of $(0,0)$	$C_{3m,n}$	genus of $C_{3m,n}$
$\mathbb{Z}/18\mathbb{Z}$	$a = f,\ b = f^2 + f$	6	$\phi_3(P) = 0$ (of degree 13)	1
$\mathbb{Z}/45\mathbb{Z}$	$a = f^2(f-1),\ b = a(f+1)^2$	9	$\lambda_{45}(P) = 0$ (of degree 89)	16

Table 2.13: Using division polynomials to rule out $\mathbb{Z}/9m\mathbb{Z}$ for $m = 2, 5$.

To see $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion, we may start with a curve E/K with torsion structure $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and force the conditions for a point of order three. We can write E in the Tate normal form with $a = 0$ and $b = g^2 - \frac{1}{16} \equiv g^2 - 1$ for some non-constant $g \in K$, and thus, the Hasse invariant of E is

$$H(E) = a^2 + a + 2b + 1 = 2(g^2 - 1) + 1 = 2(g^2 + 1).$$

Thus, we need $2(g^2+1)=u^2$ for some $u \in K^\times$. This shows that $\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ is impossible over K unless $\mathbb{F}$ contains i, where i is a primitive 4th root of unity. If it does, then $H(E)=u^2$ if and only if

$$g = i\frac{h^2+2}{h^2+1}, \qquad\qquad u = h(g-i),$$

for some $h \in K^\times$. Again, $j(E) \in K^3$ if and only if $h = f^3$ for some $f \in K$. Thus, if $\mathbb{F}$ contains a primitive 4th root of unity, and E/K is a non-isotrivial elliptic curve with $\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ torsion, it can be written as

$$y^2 + xy + \frac{2f^{24}+2}{f^{24}+2f^{12}+1}y = x^3 + \frac{2f^{24}+2}{f^{24}+2f^{12}+1}x^2 \text{ for some non-constant } f \in K.$$

We continue supposing $\mathbb{F}$ contains a primitive 4th root of unity, and recall that a non-isotrivial E/K has $(\mathbb{Z}/4\mathbb{Z})^2$ torsion if and only if it can be written in the Tate normal form with $a=0$ and $b = f^4 - \frac{1}{16} \equiv f^4 - 1$. As above, using the Hasse invariant of E, we find $\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ torsion structure implies a non-constant point on the irreducible, constant, genus one curve

$$C : 2(f^4+1) = u^2.$$

Hence, this torsion structure is impossible over K by Corollary 2.1.14.

Finally, if $\mathbb{F}$ contains a primitive fifth root of unity, then any curve with $(\mathbb{Z}/5\mathbb{Z})^2$ torsion can be written as $E(a,b) : y^2 + (1-a)xy - by = x^3 - bx^2$ with

$$a = b = \frac{f^4+2f^3+f^2+1}{f^5+f^3+f^2+f} \text{ for some non-constant } f \in K.$$

Here, if an additional point of order three exists, then the Hasse invariant is

$$H(E) = a^2+a+2b+1 = \frac{f^{10}+1}{(f^5+f^3+f^2+f)^2} \in (K^\times)^2 \iff f^{10}+1 = u^2 \text{ for } u \in K^\times$$

Therefore, if $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ exists over K, it gives a non-constant point on the irreducible constant curve $C : f^{10}+1 = u^2$. But C is hyperelliptic, so its genus is positive ($g = \frac{10-2}{2} = 4$), and therefore C has no non-constant points. Thus, $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ is impossible over K.

We collect this all into the following theorem.

Theorem 2.4.6. *Let $\mathbb{F}$ be a finite field of characteristic 3, $K = \mathbb{F}(T)$, and E/K be a non-isotrivial elliptic curve. Then the torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following*

$$\left.\begin{array}{ll} \mathbb{Z}/N\mathbb{Z}, & \textit{with } 1 \leq N \leq 10, \ \textit{or } N = 12, 15, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \textit{with } 1 \leq N \leq 4, \end{array}\right\} \textit{for general } \mathbb{F}.$$

$$\begin{array}{ll} \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/4\mathbb{Z})^2, & \textit{if } \zeta_4 \in \mathbb{F}. \\ (\mathbb{Z}/5\mathbb{Z})^2, & \textit{if } \zeta_5 \in \mathbb{F}. \end{array}$$

Further, each of these groups occurs infinitely often as $E(K)_{\text{tors}}$ for some elliptic curve E/K.

2.5 Explicit Parameterizations of Exotic Torsion

Let $\mathbb{F}$ be a finite field of characteristic p, and set $K = \mathbb{F}(T)$. In this final section, we give explicit parameterizations of elliptic curves with new torsion structures found possible over K. In Table 2.14, for non-constant $f \in K$, if $\Delta_{a,b} \neq 0$, then $E_{a,b}$ is a non-isotrivial elliptic curve over K such that $E_{a,b}(K)_{\text{tors}}$ has subgroup G. Each family in Table 2.14 comes as a parameterization from Sections 2.3 and 2.4, brought to Tate normal form, so that $(0,0)$ is a point of maximal order in the group.

Characteristic	$E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2$		G
$p = 11$	$a = \frac{(f+3)(f+5)^2(f+9)^2}{3(f+1)(f+4)^4}$	$b = a\frac{(f+1)^2(f+9)}{2(f+4)^3}$	$\mathbb{Z}/11\mathbb{Z}$
$p = 2$	$a = \frac{f(f+1)^3}{f^3+f+1}$	$b = a\frac{1}{f^3+f+1}$	$\mathbb{Z}/14\mathbb{Z}$
$p = 7$	$a = \frac{(f+1)(f+3)^3(f+4)(f+6)}{f(f+2)^2(f+5)}$	$b = a\frac{(f+1)(f+5)^3}{4f(f+2)}$	
$p = 3$	$a = \frac{f^3(f+1)^2}{(f+2)^6}$	$b = a\frac{f(f^4+2f^3+f+1)}{(f+2)^5}$	$\mathbb{Z}/15\mathbb{Z}$
$p = 5$	$a = \frac{(f+1)(f+2)^2(f+4)^3(f^2+2)}{(f+3)^6(f^2+3)}$	$b = a\frac{f(f+4)}{(f+3)^5}$	
$p = 2$	$a = \frac{f(f+1)^2(f^2+f+1)}{f^3+f+1}$	$b = a\frac{(f+1)^2}{f^3+f+1}$	$\mathbb{Z}/18\mathbb{Z}$
$p = 5$	$a = \frac{f(f+1)(f+2)^2(f+3)(f+4)}{(f^2+4f+1)^2}$	$b = a\frac{(f+1)^2(f+3)^2}{4(f^2+4f+1)^2}$	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p = 3,\ i \in \mathbb{F}$	$a = \frac{f(f+1)(f+2)(f^2+2f+2)}{(f^2+f+2)^3}$	$b = a\frac{(f^2+1)^2}{f(f^2+f+2)}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p = 2,\ i \in \mathbb{F}$	$a = \frac{f(f^4+f+1)(f^4+f^3+1)}{(f^2+f+1)^5}$	$b = a\frac{f^2(f^4+f^3+1)^2}{(f^2+f+1)^5}$	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Table 2.14: One-parameter families of elliptic curves $E_{a,b}/K$ such that $E_{a,b}(K)_{\text{tors}}$ has a subgroup G.

Remark 2.5.1. In the table, for $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, a generator of order two has the x-coordinate $x = \frac{f(f+2)^2(f+3)^3}{(f^2+4f+1)^3}$. For $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, a generator of order two has x-coordinate $x = \frac{(1+i)(f+1)(f+i)^2(f+2)(f+2i)^2(f+2i+1)}{(f+i+2)(f+2i+2)^6}$. Finally, for $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, a generator of order five has the x-coordinate

$$x = \frac{f^2(f+\zeta_5^3+\zeta_5+1)(f+\zeta_5^2+\zeta_5+1)(f+\zeta_5^3+\zeta_5)(f+\zeta_5^2+1)^3(f+\zeta_5+1)^3(f+\zeta_5^3+\zeta_5^2+\zeta_5)^2}{(f+\zeta_5^3+\zeta_5^2)^6(f+\zeta_5^3+\zeta_5^2+1)^8}.$$

Chapter 3

Genus 1 Function Fields

3.1 Introduction

Again, let $\mathbb{F}$ be a finite field of characteristic p, let $\mathcal{C}$ be a smooth projective curve of genus 1 over $\mathbb{F}$, and $K = \mathbb{F}(\mathcal{C})$. Less is known about the torsion subgroup in this setting. One useful result is the bounds on the order of a point in $E(K)$, given by Theorem 2.1.9, where Levin gives bounds for arbitrary genus. As for p-primary torsion, when $g(\mathcal{C}) = 1$, Theorem 2.1.9 leads to the the following useful corollary.

Corollary 3.1.1 (Levin, [13])**.** *Let $\mathcal{C}$ be a smooth, projective curve of genus one over $\mathbb{F}$, a finite field of characteristic p. Let $K = \mathbb{F}(\mathcal{C})$. and E/K be an elliptic curve.*

Suppose $p^e \mid \#E(K)_{\text{tors}}$. *Then*

$$p \leq 13,\ \ e \leq \begin{cases} 4 & \textit{if } p = 2, \\ 2 & \textit{if } p = 3, \\ 1 & \textit{if } p = 5, 7, 11, 13. \end{cases}$$

We will also make use of Proposition 2.1.13, and an analogous result to that of Theorem 2.1.4 proven for genus 1. In what follows, we will prove the following result.

Theorem 3.1.2 (M)**.** *Let* $\mathcal{C}$ *be a curve of genus* 1 *over* $\mathbb{F}$, *a finite field of characteristic* p, *and let* $K = \mathbb{F}(\mathcal{C})$. *Let* E/K *be non-isotrivial. If* $p \nmid \#E(K)_{\text{tors}}$, *then* $E(K)_{\text{tors}}$ *is one of the following groups*

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

Otherwise, if $p \mid \#E(K)_{\text{tors}}$, *then* $p \leq 13$, *and* $E(K)_{\text{tors}}$ *is one of*

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

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

In Section 3.2 we will start by proving Theorem 3.2.3, which is an analogue of Cox and Parry's Theorem 2.1.4 when the genus of $\mathcal{C}$ is one. Then as in Chapter 2, starting with characteristic $p \geq 5$, we will use this result and Theorem 2.1.7 to obtain a curve D which parameterizes non-isotrivial elliptic curves which in addition to having a torsion structure G found in Theorem 3.2.3, also have a point of order p. In each case, D will be irreducible with coefficients in $\mathbb{F}$. If D has genus one, then it will turn out that there are elliptic curves with torsion structure $G \times \mathbb{Z}/p\mathbb{Z}$ only if the base curve of K is isogenous to D. If D has genus greater than one, then we will use Proposition 2.1.13 to conclude that this torsion structure is impossible over K. Finally, in Section 3, we include parameterizations of elliptic curves with torsion subgroups that appear over K for any $\mathcal{C}$, and the isogenies required for any torsion subgroups which appear only for specific $\mathcal{C}$.

3.2 Genus one

Let $\mathbb{F}$ be a finite field of characteristic p. By Proposition 2.1.13, given two curves, $D/\mathbb{F}$ and a smooth $\mathcal{C}/\mathbb{F}$, and $K = \mathbb{F}(\mathcal{C})$, we know that $D(K)$ has no non-constant points if $g(D) > g(\mathcal{C})$. What if they are equal? Certainly, in this case, no contradiction comes from the Hurwitz formula. When $g(\mathcal{C}) = g(D) = 1$, in fact, the Hurwitz formula, and the proof of Proposition 2.1.13 yield the following useful corollary.

Corollary 3.2.1. *Let $\mathcal{C}$ and D be irreducible curves over $\mathbb{F}$, a finite field of characteristic p. Suppose $\mathcal{C}$ is smooth of genus 1, and set $K = \mathbb{F}(\mathcal{C})$.*

1. *If $g(D) > 1$, then $D(K)$ has no non-constant points.*

2. *If $g(D) = 1$, and $D(K)$ contains a non-constant point, then $\mathcal{C}$ and $\tilde{D}$, the normalization of D, are isogenous over $\mathbb{F}$.*

Proof. As in the proof of Proposition 2.1.13, a non-constant point P on D induces a non-constant, separable morphism between curves

$$\tilde{\rho} : \mathcal{C} \to \tilde{D}, \text{ defined over } \mathbb{F}$$

where $\tilde{D}$ is the normalization of D, by composing the map $t \mapsto P_t$ on D, with the normalization map. Since $\mathcal{C}$ and $\tilde{D}$ are smooth curves of genus one over a finite field, they have a point, and therefore are elliptic curves. Without loss of generality (by composing with the translation map $P \mapsto P + Q$) we may assume that $\tilde{\rho}(\mathcal{O}) = \mathcal{O}$, and the map $\tilde{\rho}$ is an isogeny. □

3.2.1 Prime-to-p torsion

We start with a statement about modular curves of genus one.

Proposition 3.2.2 (Sutherland, [18] and [19])**.** *For a finite field $\mathbb{F}$ of characteristic $p \nmid n$, the modular curve $X_1(n, m)$ has genus one if and only if (m, n) is one of the following pairs.*

$$(11, 1),\ (14, 1),\ (15, 1),\ (10, 2),\ (12, 2),\ (9, 3),\ (8, 4),\ \textit{or } (6, 6). \tag{3.1}$$

Next, we prove an analogue of Cox and Parry's theorem for genus 1.

Theorem 3.2.3. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field 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*

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

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

$$\begin{cases} \mathcal{C} \textit{ is isogenous to } X_1(n,m) & \textit{if } (m,n) \textit{ is in } (3.1), \\ \mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.} \end{cases}$$

Proof. Following the proof of [21, Proposition 7.1], suppose $E(K)'_{\text{tors}}$ has the form $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ where $n \mid m$ and $p \nmid n$. Then, since the modular curve $X_1(n,m)$, defined over $\mathbb{F}_p(\mu_n)$, is a coarse moduli space for elliptic curves with $G \subset E(K)'_{\text{tors}}$, this induces a non-constant map $\mathcal{C} \to X_1(n,m)$. By the Riemann-Hurwitz formula, since $g(\mathcal{C}) = 1$, we must have $g(X(n,m)) \leq 1$. Thus, by Propositions 2.4.1 and 3.2.2,

(m, n) is one of the pairs

$$\begin{aligned} &(N,1) &&\text{with } N = 1, \dots, 12, 14, 15,\\ &(2N,2) &&\text{with } N = 1, \dots, 6,\\ &(3N,3) &&\text{with } N = 1, 2, 3,\\ &(4N,4) &&\text{with } N = 1, 2,\\ &(N,N) &&\text{with } N = 5, 6.\end{aligned}$$

The torsion subgroups corresponding to Proposition 2.4.1 have already been shown to appear infinitely often in Section 2.2. The only *new* subgroups are those that correspond to a pair in (3.1), namely, $\mathbb{Z}/N\mathbb{Z}$ with $N = 11, 14, 15$, $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and $(\mathbb{Z}/6\mathbb{Z})^2$. We need only show examples of elliptic curves with these new torsion subgroups appearing over $\mathbb{F}(\mathcal{C})$ for some base curve $\mathcal{C}$.

If E has a point of order N, and $X_1(N) := X_1(1, N)$ has genus one, then by Corollary 3.2.1, $\mathcal{C}$ must be *isogenous* to $X_1(N)$. In this case, we can use the optimized equations in [18] to construct examples of elliptic curves with torsion subgroup corresponding to a pair in (3.1). For example, suppose $p \neq 11$, and let $\mathbb{F}$ be a finite field of characteristic p. If E/K has a point of order 11, then there is an isogeny $\mathcal{C} \to X_1(11) : u^2 + (t^2+1)u + t = 0$ over $\mathbb{F}$. If we take the case where $\mathcal{C} = X_1(11)$, for example, then $K = \mathbb{F}(X_1(11)) = \mathbb{F}(t, u)$, and using [18], we can construct the following infinite family of elliptic curves with a point of order 11:

$$E_n : y^2 + (1-a)^{p^n} xy - b^{p^n} y = x^3 - b^{p^n} x^2,$$
$$\text{with } a = -(u+1)t - u^2 - u + 1,\ b = a(ut+1),\ n \geq 0.$$

On the other hand, if $\mathcal{C}$ is only isogenous (but not isomorphic) to $X_1(11)$, and $K = \mathbb{F}(\mathcal{C})$. Then we can use the induced map $\varphi : \mathbb{F}(X_1(11)) \to K$ by $u \mapsto u_\varphi \in K$ and $t \mapsto t_\varphi \in K$ and obtain the following infinite family of elliptic curves with a point of order 11:

$$E_n/K : y^2 + (1-a)^{p^n} xy - b^{p^n} y = x^3 - b^{p^n} x^2,$$
$$\text{with } a = -(u_\varphi + 1)t_\varphi - u_\varphi^2 - u_\varphi + 1,\ b = a(u_\varphi t_\varphi + 1),\ n \geq 0.$$

Similarly, we can use [18] to construct infinite families of elliptic curves with points of order 14 and 15 (as long as $p \neq 2, 7$ or $p \neq 3, 5$ respectively) when $\mathcal{C}$ is isogenous to $X_1(14)$ and $X_1(15)$.

Finally, if $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subset E(K)$, and and $X_1(n,m)$ has genus one, then by Corollary 3.2.1, $\mathcal{C}$ must be *isogenous* to $X_1(n,m)$. This time, we can use [19] to construct examples. For example, suppose $p \neq 2, 5$, and let $\mathbb{F}$ be a finite field of characteristic p. If $G = \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset E(K)$, then $\mathcal{C}$ is isogenous to $X_1(2,10)$: $u^2 = t^3 - t^2 + t$. For example, if $\mathcal{C} = X_1(2,10)$, and $K = \mathbb{F}(X_1(2,10)) = \mathbb{F}(t,u)$, then using [19], for all $n \geq 0$, the following elliptic curve E_n has $G \subset E_n(K)$:

$$E_n : y^2 = x^3 + (s^2 - 2rs)x^2 - (s^2-1)(rs+1)^2 x,$$
$$\text{with } r = (t/u)^{p^n},\ s = (4tu/(tu^2 - t^3 - 3t^2 - u^2))^{p^n}.$$

Again, infinite families of elliptic curves containing the remaining groups from the theorem can be realized when $\mathcal{C}$ is isogenous to $X_1(n,m)$ by using a similar strategy. □

In the rest of this section, we will follow the strategies of Chapter 2 to determine what combinations of p-primary torsion can appear with the subgroups from Theorem 3.2.3. We will start with $p = 5$, then work case-by-case for primes $p = 2, 3, 7, 11, 13$.

3.2.2 Characteristic $p = 5$.

In the spirit of Section 2.3.1, we begin with the prime $p = 5$, to get an idea of how things work when $K = \mathbb{F}(\mathcal{C})$ is a genus one function field. For $p = 5$, Theorem 3.2.3 can be easily restated, giving the full picture of prime-to-5 torsion over $\mathbb{F}(\mathcal{C})$ of characteristic 5.

Corollary 3.2.4. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic 5, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)'_{\text{tors}}$ is one of*

$$\begin{array}{cl} \mathbb{Z}/N\mathbb{Z} & \text{with } N = 1, \ldots, 4, 6, \ldots 9, 11, 12, 14, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{with } N = 1, \ldots, 4, 6, \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{with } N = 1, 2, 3, \\ \mathbb{Z}/4N\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{with } N = 1, 2, \\ (\mathbb{Z}/6\mathbb{Z})^2 & \end{array}$$

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

$$\begin{cases} \mathcal{C} \text{ is isogenous to } X_1(n, m) & \text{if } (m, n) \text{ is in } (3.1), \\ \mathcal{C} \text{ is any smooth curve} & \text{otherwise.} \end{cases}$$

Below, we will follow the strategy used in Section 2.3.1: starting with a group in Corollary 3.2.4, when possible, we write a curve in the Tate normal form E_f parameterizing the torsion structure $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for some $f \in K$ (otherwise we use division polynomials). Then, we write the curve in short Weierstrass form $E_f : y^2 = x^3 + A(f)x + B(f)$. If we assume that $G = \mathbb{Z}/5m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subset E_f(K)$, that is, if it has an additional point of order 5, then we can use Theorem 2.1.7 to say

$$H(E_{A,B}) = 2A(f) = g^4 \text{ for some } g \in K^\times.$$

Now, defining the curve $C_{5m,n} : 2A(t) = u^4$, we see that *non-isotrivial* elliptic curves with G torsion give *non-constant* points on $C_{5m,n}$. We need only compute the genus of $C_{5m,n}$ to determine if torsion subgroup G is possible for $E_f(K)$. By Corollary 3.2.1, if $g(C_{5m,n}) > g(\mathcal{C}) = 1$, G is impossible. Otherwise, if $g(C_{5m,n}) = 1$, then G is possible only when $\mathcal{C}$ is isogenous to $C_{5m,n}$, and if $g(C_{5m,n}) = 0$, then G already occurs over function fields of genus zero, and appears in Theorem 2.3.3.

Theorem 3.2.5. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic 5, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)_{\text{tors}}$ is one of*

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

Further, let $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ be in this list with $n \mid m$, and such that $\mathbb{F}$ contains a primitive nth root of unity. Then there are infinitely many non-isomorphic, non-

isotrivial elliptic curves with $E(K)_{\mathrm{tors}} \cong G$ *only if*

$$\begin{cases} \mathcal{C} \textit{ is isogenous to } X_1(n,m) & \textit{if } (m,n) \textit{ is in } (3.1) \textit{ with } 5 \nmid m, \\ \mathcal{C} \textit{ is isogenous to } C_{20,1} : u^4 = t^2 + t + 1 & \textit{if } (m,n) = (20,1), \\ \mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.} \end{cases}$$

Proof. Using Corollary 3.2.4, and the fact that by Levin, E can have a point of 5-primary order at most 5, we need to rule out or confirm the existence of $\mathbb{Z}/5m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ with $(5m, n)$ coming from

$$\begin{aligned} &(5N,1) && \text{with } N = 3,4,6,7,8,9,11,12,14, \\ &(10N,2) && \text{with } N = 1,2,3,4,6, \\ &(15N,3) && \text{with } N = 1,2,3, \\ &(20N,4) && \text{with } N = 1,2, \\ &(30N,6) && \text{with } N = 1. \end{aligned} \tag{3.2}$$

We have already seen above that the torsion structures $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ can appear infinitely often regardless of the base curve, $\mathcal{C}$. We rule out the rest of the torsion structures by using the strategy outlined above. For example, if $E(K)$ has a point of order 30, then we can write it in the Tate normal form for elliptic curves with a point of order 6:

$$E_t : y^2 + (1-f)xy - (f^2+f)y = x^3 - (f^2+f)x^2, \text{ for some non-constant } f \in K.$$

Since $E_f(K)$ has a point of order 5, by Theorem 2.1.7 we must have

$$g^4 = H(E) = 4f^4 + 2f^3 + 2f + 1, \text{ for some } g \in K^\times.$$

Since g and f are both in K, and f is non-constant, we see that an elliptic curve over K with a point of order 30 would imply the existence of a non-constant point on the curve $C_{30,1} : 4t^4+2t^3+2t+1 = u^4$ over K. The curve C is irreducible, has coefficients in $\mathbb{F}$, and has genus 3. However, by Corollary 3.2.1, we see that a non-constant point on $C_{30,1}$ would induce a map $\mathcal{C} \to C_{30,1}$, which is impossible. Thus, no non-isotrivial elliptic curve E/K can have a point of order 30. Results for other torsion structures are collected in Table 3.1, wherein each curve $C_{5m,n}$ is irreducible by the Eisenstein criterion. With the exception of $\mathbb{Z}/55\mathbb{Z}$, this table rules out any torsion structure G from (3.2) $\#G \geq 40$ or a point of order ≥ 30.

$G = \mathbb{Z}/5m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$	Curve $C_{5m,n}$	genus
$\mathbb{Z}/20\mathbb{Z}$	$t^2 + t + 1 = u^4$	1
$\mathbb{Z}/30\mathbb{Z}$	$4t^4 + 2t^3 + 2t + 1 = u^4$	3
$\mathbb{Z}/35\mathbb{Z}$	$t^8 + 3t^7 + 2t^6 + 4t^5 + t^2 + 4t + 1 = u^4$	9
$\mathbb{Z}/40\mathbb{Z}$	$t^8 + t^7 + 4t^6 + 2t^5 + 2t^3 + t^2 + 4t + 1 = u^4$	9
$\mathbb{Z}/45\mathbb{Z}$	$t^{12} + 3t^{11} + 4t^{10} + 2t^9 + 4t^8 + 4t^6 + 4t^5 + 2t^4 + 3t^3 + 3t^2 + 1 = u^4$	15
$\mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$t^4 + 4t^2 + 1 = u^4$	3
$\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$t^4 + 3t = u^4$	3

Table 3.1: Ruling out $G = \mathbb{Z}/5m\mathbb{Z}$ torsion over K for $m \geq 4$.

As for points of order 55, using a similar strategy, we can start with E/K in the form $E : y^2 + (1 - f)xy - fy = x^3 - fx^3$. Solutions, (x, f), to $\psi_{11}(E) = 0$ give x-coordinates of points, P_x, such that $55P_x = \mathcal{O}$. Unfortunately, however, ψ_{11} defines a degree 72 curve, $C_{55,1}$, whose genus and irreducibility were quite difficult to compute. Magma outputs that $C_{55,1}$ has genus 11 after a 100 hour computation, and after 468 hours[1], that $C_{55,1}$ is absolutely irreducible. Thus, by Corollary 3.2.1, no such points exist, and points of order 55 are impossible for an elliptic curve over K.

With the exception of $\mathbb{Z}/20\mathbb{Z}$, we have already seen from Theorem 3.2.3 and the parameterizations in Section 2.2, that all groups in the theorem appear infinitely often as the torsion subgroup of an elliptic curve E/K (in the case for Theorem 3.2.3 this is as long as $\mathcal{C}$ is in the right isogeny class). We also find that because $g(C_{20,1}) = 1$, in order for an elliptic curve E/K to have a point of order 20, we must have that $\mathcal{C}$ is isogenous to the normalization of $C_{20,1}$ by Corollary 3.2.1. In this case, $C_{20,1}$ is already non-singular. Thus, we may take, for example, the case when $\mathcal{C} = C_{20,1} : t^2 + t + 1 = u^4$, and $\mathbb{F}(\mathcal{C}) = \mathbb{F}(C_{20,1}) = \mathbb{F}(t, u)$. In this case, the following family gives elliptic curves with a point of order 20 for all n:

$$E_n : y^2 + xy - t^{5^n} = x^3 - t^{5^n} x^2 \text{ for } n \geq 1,$$

since $H(E_n) = (u^4)^{5^n} = (u^{5^n})^4 \in K^4$ and $j(E) \in K^5$ for all n. Thus, we find infinitely many curves over K with a point of order 20. If we suppose that $\mathcal{C}$ is isogenous to $C_{20,1}$, then we can use the induced map $\varphi : \mathbb{F}(C_{20,1}) \to K$ with $t \mapsto t_\varphi \in K$ and $u \mapsto u_\varphi \in K$, to construct

$$E_{\varphi,n} : y^2 + xy - t_\varphi^{5n} = x^3 - t_\varphi^{5n} x^2 \text{ for } n \geq 1,$$

which is an infinite family of elliptic curves over $\mathbb{F}(\mathcal{C}) = \mathbb{F}(t, u)$, for $\mathbb{F}$ a finite field of characteristic, with a point of order 20. Here $H(E_{\varphi,n}) = (u_\varphi^{5^n})^4 \in K^4$. See the example below for a deeper discussion. □

[1] Magma V2.20-10 was used for both computations. The irreducibility test was run on a 2013 Mac Pro with a 3.5 GHz 6-Core Intel Xeon E5 processor.

Example 3.2.6. Over $K = \mathbb{F}(\mathcal{C})$, non-isotrivial elliptic curves with points of order 4 can be written in the form $E_f : y^2 + xy - fy = x^3 - fx^2$ for some non-constant $f \in K$. From Section 2.3.1, if in addition, E has a point of order 5, then we must have a point on the curve

$$D : t^2 + t + 1 = u^4.$$

The curve D is a base extension of a curve over $\mathbb{F}_5$. It is already smooth, but to simplify our calculations, we can write it in short Weierstrass form $D_0 : u^2 = t^3 + 3t$, with the isomorphism $\pi : D_0 \to D$ given by

$$[T, U, V] \mapsto [4T^2 + 2UV + 3V^2, YV, TV].$$

Let $t = T/V$ and $u = U/V$, and we have

$$[t, u, 1] \mapsto [4t + 2 + 3t^{-1}, t^{-1}u, 1].$$

If $\mathbb{F} = \mathbb{F}_5$, then since D_0 is the only curve up to isomorphism in its isogeny class over $\mathbb{F}_5$, the base curve $\mathcal{C}$ must be isomorphic to D_0. If $\mathcal{C} = D_0$ for example, then defining $\mathbb{F}(t, u) = \mathbb{F}(D_0)$, the following is an infinite family of elliptic curves with a point of order 20:

$$E_n : y^2 + xy - f^{5^n} y = x^3 - f^{5^n} x^2, \text{ with } f = 4t + 2 + 3t^{-1}, \text{ for all } n \geq 1.$$

For example, E_1 has the following point of order 20:

$$\Big(\frac{u(u+1)^2(t^2 + tu^2 + 2t + 2)}{t^2u^2 + 4t + 2u^2}, \frac{(u+1)^5(u+4)(t^2 + tu^2 + 2u^2 + 3)}{t^2u^2 + 4tu^4 + 2t + u^2}\Big).$$

Over $\mathbb{F}_{25}$, the curve D_0 has three other curves in its isogeny class. For example, D_0 is isogenous to the curve $D_1 : u^2 = t^3 + 3t + \sqrt{3}$ via the isogeny:

$$\varphi : D_0 \to D_1 \text{ by } [t, u, 1] \mapsto \left[\frac{t^2 + \sqrt{3}t + 2}{t + \sqrt{3}}, \frac{t^2 + 2\sqrt{3}t + 1}{t^2 + 2\sqrt{3}t + 3}u, 1\right].$$

Thus, if $\varphi(t) = t_\varphi$, then we can construct an infinite family of elliptic curves over $K = \mathbb{F}(t, u) = \mathbb{F}(D_1)$ with a point of order 20 by using the same family above with $f = 4t_\varphi + 2 + 3t_\varphi^{-1}$. In particular, for all $n \geq 1$, the following is an elliptic curve over $K = \mathbb{F}(D_1)$ with a point of order 20:

$$E_n : y^2 + xy - f^{5^n} y = x^3 - f^{5^n} x^2, \text{ with } f = \frac{4t^4+(3\sqrt{3}+2)t^3+(4\sqrt{3}+1)t^2+2\sqrt{3}t+4\sqrt{3}}{t^3+2\sqrt{3}t^2+2\sqrt{3}}.$$

Note that this is an example of an infinite family of elliptic curves with a point of order 20 over a function field whose base curve is ***not*** isomorphic to D_0.

3.2.3 Characteristic $p = 2$

By specializing to $p = 2$, we may state the following corollary to Theorem 3.2.3, which tells us what prime-to-2 torsion to expect over $\mathbb{F}(\mathcal{C})$, with $\mathbb{F}$ a finite field of characteristic 2.

Corollary 3.2.7. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic 2, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)'_{\text{tors}}$ is one of the following.*

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z} & \textit{with } N = 1, 3, 5, 7, 9, 11, 15, \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \textit{with } N = 1, 3, \\ (\mathbb{Z}/5\mathbb{Z})^2. & \end{array}$$

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

$$\begin{cases} \mathcal{C} \text{ is isogenous to } X_1(n,m) & \text{if } (m,n) \text{ is in } (3.1), \\ \mathcal{C} \text{ is any smooth curve} & \text{otherwise.} \end{cases}$$

Again, we will start with a group in Corollary 3.2.7 and write a curve in the Tate normal form parameterizing the torsion structure $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Recall, our Hasse invariant strategy does not distinguish between points of order p or p^e for $e > 1$. Thus, since in characteristic 2 we may find points of order 2^e for $e = 1, 2, 3, 4$, it may not be possible to use the Hasse invariant. Instead, we use division polynomials to define curves $C_{2^e m,n}$ parameterizing elliptic curves with torsion structure $G \times \mathbb{Z}/2^k\mathbb{Z}$. Recall, if $g(C_{2^e m,n}) = 0$, then G already occurs over function fields of genus zero, and appears in Theorem 2.3.3.

Throughout, we will attempt to provide infinite families of examples when a torsion structure appears for elliptic curves over K.

Theorem 3.2.8. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic 2, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)_{\text{tors}}$ is one of*

$$\begin{array}{rl} \mathbb{Z}/N\mathbb{Z} & \textit{with } N = 1, \ldots, 12, 14, 15, 16, 18, 20, 22, 30 \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \textit{with } N = 1, 2, 3, 4, 6, \\ \mathbb{Z}/5N\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} & \textit{with } N = 1, 2. \end{array}$$

Further, let $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ be in this list with $n \mid m$, and such that $\mathbb{F}$ contains a primitive nth root of unity. Then there are infinitely many non-isomorphic, non-

isotrivial elliptic curves with $E(K)_{\text{tors}} \cong G$ *only if*

$$\begin{cases} \mathcal{C} \text{ is isogenous to } X_1(n,m) & \text{if } (m,n) \text{ is in (3.1) with } 2 \nmid m, \\ \mathcal{C} \text{ is isogenous to a curve in Table 3.9} & \text{if } G \text{ appears in Table 3.9}, \\ \mathcal{C} \text{ is any smooth curve} & \text{otherwise.} \end{cases}$$

Proof. We need to rule or confirm the existence of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with (m,n) coming from

$$\begin{aligned} &(2N,1),(4N,1),(8N,1),(16N,1) && \text{with } N = 1,3,5,7,9,11,15, \\ &(6N,3),(12N,3),(24N,3),(48N,3) && \text{with } N = 1,3, \\ &(10,5),(20,5),(40,5),(80,5). \end{aligned} \tag{3.3}$$

From Chapter 2, we recall $C_{24,1}$, $C_{28,1}$, and $C_{36,1}$ all have genus greater than one, ruling out these torsion structures, and those containing them, from (3.3). To show that no groups appear other than those in the theorem, we need only rule out the pairs $(40,1)$, $(44,1)$, $(60,1)$, $(30,3)$, and $(20,5)$.

We begin with a curve written in the Tate normal form for points of order ten, and look at $\phi_4(x) = 0$. We set λ_{40} to be the numerator of $\phi_4(x)$, and define $C_{40,1} : \lambda_{40} = 0$. The curve $C_{40,1}$ is irreducible of genus 9, and has coefficients in $\mathbb{F}$. By Corollary 3.2.1, this shows that $C_{40,1}$ has no non-constant points, and thus points of order 40 are impossible for non-isotrivial elliptic curves over K.

Starting with a curve written the Tate normal form for a curve with a point of order four, and looking at $\phi_{11}(x) = 0$, we see that $\phi_{11}(E_{a,b}) = x \cdot \lambda_{44}$, where λ_{44} is an irreducible polynomial of degree 120. We define $C_{44,1} : \lambda_{44} = 0$, and after a 5.5 hour calculation find that $C_{44,1}$ is irreducible of genus 11. Again, since $C_{44,1}$ has coefficients in K, this shows that there are no points of order 44 for elliptic curves over K.

Next, beginning with the Tate normal form for points of order 12, and look at $\phi_5(x) = 0$. The numerator factors into a genus 0 curve corresponding to points of order 20, and a degree 96 curve we call λ_{60}. We define $C_{60,1} : \lambda_{60} = 0$, and find that $C_{60,1}$ is irreducible of genus 17, with coefficients in $\mathbb{F}$, again showing that points of order 60 are impossible.

From Section 2.2, we see E/K has $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ torsion if and only if $\zeta_3 \in K$ and E can be written in the Tate normal form for points of order 6 with

$$a = -\frac{f(f^2+f+1)}{(f-1)^3}, \qquad b = -a\frac{4f^2-2f+1}{(f-1)^3}, \qquad f \in K \text{ non-constant},$$

where $(0,0)$ is a point of order 6. Again, we look at $\phi_5(x) = 0$. The numerator factors as $x\lambda_{30,3}$, where $\lambda_{30,3}$ is an irreducible polynomial of degree 132. This time, $C_{30,3} : \lambda_{30,3} = 0$ is absolutely irreducible of genus 9, showing that the torsion subgroup $\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is impossible for a non-isotrivial elliptic curve over K.

Finally, again from Section 2.2, we see that E/K has $(\mathbb{Z}/5\mathbb{Z})^2$ torsion if and only if $\zeta_5 \in K$ and E can be written in the Tate normal form for this torsion structure with

$$a = b = \frac{f^4+2f^3+4f^2+3f+1}{f^5-3f^4+4f^3-2f^2+f}.$$

This time, the numerator of $\phi_5(x) = 0$ factors as $x^4 \cdot g \cdot \lambda_{20,5}$ where g defines a genus 0 curve corresponding to $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. We define $C_{20,5} : \lambda_{20,5} = 0$, and find that $C_{20,5}$ has coefficients in $\mathbb{F}$ and is irreducible of genus 9, showing that this torsion structure is impossible over K.

We have ruled out every torsion structure from (3.3) not appearing in the theorem, and, with the exception of $(16,1)$, $(20,1)$, $(22,1)$, $(30,1)$, $(12,3)$ and $(18,3)$, we have seen that each torsion structure in the theorem appears infinitely often. What is left is to show that each of these pairs appears infinitely often. In what follows, define

$$E_{a,b}^{2^n} : y^2 + (1 - a^{2^n})xy - b^{2^n}y = x^3 - b^{2^n}x^2 \text{ for some } a, b \in K \text{ and } n \in \mathbb{Z}_{\geq 1}.$$

$C_{16,1}$ is isomorphic to $\tilde{C}_{16,1} : u^2 + u = t^3 + t$ with $\pi : \tilde{C}_{16,1} \to C_{16,1}$ sending t to $(t^3 + t^2 + t + 1 + u)/t^4$. Let $K = \mathbb{F}(\tilde{C}_{16,1}) = \mathbb{F}(t, u)$, and set

$$f = \frac{t^3 + t^2 + t + 1 + u}{t^4}, \qquad a = \frac{(2f - 1)(f - 1)}{f}, \qquad b = af.$$

Then, $E_{a,b}^{2^n}$ is an infinite family of curves with a point of order 16. As will be the case in every example bellow, trivially, $H(E_0)$ is a first power in $K^\times$. Thus, we only need $j(E) \in K^2$, which we can ensure by making sure the coefficients of E are all squares.

The normalization of $C_{20,1}$ is $\tilde{C}_{20,1} : u^2 + u = t^3 + t$ with normalization map $\pi : \tilde{C}_{20,1} \to C_{20,1}$ sending

$$t \mapsto \frac{t^4 + t^3 + t + u + 1}{t^4 + 1}.$$

Thus, for example, if $K := \mathbb{F}(\tilde{C}_{20,1}) = \mathbb{F}(t, u)$, and we set

$$f = \frac{t^4 + t^3 + t + u + 1}{t^4 + 1}, \qquad a = -\frac{f(f - 1)(2f - 1)}{f^2 - 3f + 1} \qquad b = -a\frac{f^2}{f^2 - 3f + 1},$$

then $E_{a,b}^{2^n}$ is an infinite family of elliptic curves with a point of order 20 over K.

Recall, E/K has a point of order 11 only if $\mathcal{C}$ is isogenous to the modular curve

$X_1(11) : u^2 + (t^2+1)u + t = 0$. If we consider $K = \mathbb{F}(X_1(11)) = \mathbb{F}(t,u)$ and set

$$a = (u+1)t + u^2 + u, \;\; b = (u^3+u^2)t + u^3 + u^2,$$

then elliptic curve $E^1_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2$ has a point of order 11. Thus, $E^{2^n}_{a,b}$ is an infinite family of elliptic curves with a point of order 22.

The normalization of $C_{30,1}$ is $\tilde{C}_{30,1} : u^2 + tu + u = t^3 + t^2$ with $\pi : \tilde{C}_{30,1} \to C_{30,1}$ by

$$t \mapsto \frac{t^5u + t^4u + t^2 + 1}{t^8 + t^7 + t^5 + t^4 + t^3 + t^2 + 1}.$$

Let $K = \mathbb{F}(\tilde{C}_{30,1}) = \mathbb{F}(t,u)$, and set

$$f = \frac{t^5u + t^4u + t^2 + 1}{t^8 + t^7 + t^5 + t^4 + t^3 + t^2 + 1}, \quad a = -\frac{f(f-1)(2f-1)}{f^2 - 3f + 1}, \quad b = -a\frac{f^2}{f^2 - 3f + 1}.$$

Then $E^{2^n}_{a,b}$ is an infinite family of curves with a point of order 30.

Recall, E/K has torsion structure $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ if and only if $\zeta_3 \in K$ and E can be written in the Tate normal form for this torsion structure with

$$a = -\frac{f(f^2+f+1)}{(f-1)^3}, \qquad\qquad b = -a\frac{4f^2 - 2f + 1}{(f-1)^3}.$$

Here, $E_{a,b}$ has $(0,0)$ as a point of order 6. By looking at the numerator of the division polynomial $\phi_2(E_{a,b})$, we determine that the torsion structure $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ corresponds to points on the curve

$$C_{12,3} : t^{18}u^4 + t^{16}u^4 + t^{12}u^2 + t^9u^2 + t^9 + t^8 + t^6 + t^4u^2 + t^4 + t^3 + t^2u^4 + tu^2 + u^4 = 0.$$

Here, over $\mathbb{F}_2$, the normalization of $C_{12,3}$ is $\tilde{C}_{12,3} : u^2+u = t^3+1$ with $\pi : \tilde{C}_{12,3} \to C_{12,3}$ sending

$$t \mapsto \frac{t^3+t^2+u}{t^4+1}.$$

Thus, E/K has torsion structure $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ only if $\mathcal{C}$ is isogenous to $\tilde{C}_{12,3}$. For example, if $K = \mathbb{F}(\tilde{C}_{16,1}) = \mathbb{F}(t,u)$, then setting

$$f = \frac{t^3+t^2+u}{t^4+1}, \qquad a = -\frac{f(f^2+f+1)}{(f-1)^3}, \qquad b = -a\frac{4f^2-2f+1}{(f-1)^3},$$

makes $E_{a,b}^{2^n}$ an infinite family of elliptic curves with torsion structure $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Similarly, if we begin with a curve written in the Tate normal form for $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ torsion, we can look at the numerator of $\phi_3(E_{a,b})$, to find $C_{18,3}$. It turns out, the normalization of $C_{18,3}$ is again $\tilde{C}_{12,3} : u^2+u = t^3+1$, but we will call it $\tilde{C}_{18,3}$ for consistency. Under the map $\pi : \tilde{C}_{18,3} \to C_{18,3}$ we have

$$t \mapsto \frac{t^2u^2+tu^4+tu^3+tu+t+u^5+u^3+1}{t^2u^4+t^2u^2+u^6+u^5+u^3+u^2+1}.$$

We again have the example where $\mathcal{C} = \tilde{C}_{18,3}$, and $K = \mathbb{F}(\tilde{C}_{18,3}) = \mathbb{F}(t,u)$. Setting

$$f = \tfrac{t^2u^2+tu^4+tu^3+tu+t+u^5+u^3+1}{t^2u^4+t^2u^2+u^6+u^5+u^3+u^2+1}, \quad a = -\frac{f(f^2+f+1)}{(f-1)^3}, \quad b = -a\frac{4f^2-2f+1}{(f-1)^3},$$

$E_{a,b}^{2^n}$ is an infinite family of curves with torsion structure $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ over K.

Again, as above, in each of these examples, we may suppose that $\mathcal{C} \to \tilde{C}_{2m,n}$ is an isogeny of curves with $\varphi : \mathbb{F}(C_{2m,n}) \to K$ such that $t \mapsto t_\varphi$ and $u \mapsto u_\varphi$. Then by replacing t by t_φ and u by u_φ in each equation, we can find $E_{a,b}^{2^n}$, an infinite family of elliptic curves with torsion structure $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ over K. $\square$

3.2.4 Characteristic $p = 3$

Specializing to characteristic $p = 3$, and considering a function field K of genus one, Theorem 3.2.3 provides the following corollary.

Corollary 3.2.9. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic 3, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)'_{\text{tors}}$ is one of*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} && \text{with } N = 1, 2, 4, 5, 7, 8, 10, 11, 14, \\ &\mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} && \text{with } N = 1, 2, 4, 5, \\ &\mathbb{Z}/4N\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} && \text{with } N = 1, 2, \\ &(\mathbb{Z}/5\mathbb{Z})^2. \end{aligned}$$

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

$$\begin{cases} \mathcal{C} \text{ is isogenous to } X_1(n, m) & \text{if } (m, n) \text{ is in } (3.1), \\ \mathcal{C} \text{ is any smooth curve} & \text{otherwise.} \end{cases}$$

Again, as in Section 3.2.3, we may have points of order 3^e with $e = 1, 2$. Thus, we will combine the Tate normal form for $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and division polynomials to define curves $C_{3^e m,n}$ parameterizing elliptic curves with torsion structure $G \times \mathbb{Z}/3^e\mathbb{Z}$.

Theorem 3.2.10. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic*

3, *and let* $K = \mathbb{F}(\mathcal{C})$. *Let* E/K *be non-isotrivial. Then* $E(K)_{\mathrm{tors}}$ *is one of*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} && \textit{with } N = 1, \ldots, 12, 14, 15, 18, 21, 24, \\ &\mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} && \textit{with } N = 1, \ldots, 6, \\ &\mathbb{Z}/4N\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} && \textit{with } N = 1, 2, 3, \\ &(\mathbb{Z}/5\mathbb{Z})^2. \end{aligned}$$

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

$$\begin{cases} \mathcal{C} \textit{ is isogenous to } X_1(n, m) & \textit{if } (m, n) \textit{ is in } (3.1) \textit{ with } 3 \nmid m, \\ \mathcal{C} \textit{ is isogenous to a curve in Table 3.9} & \textit{if } G \textit{ appears in Table 3.9}, \\ \mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.} \end{cases}$$

Proof. This time, by Levin's bounds, E/K can have a point of 3-primary order 3 or 9, so we need to look a subgroups $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with (m, n) coming from

$$\begin{aligned} &(3N, 1), (9N, 1) && \text{with } N = 1, 2, 4, 5, 7, 8, 10, 11, 14, \\ &(6N, 2), (18N, 2) && \text{with } N = 1, 2, 4, 5, \\ &(12N, 4), (26N, 4) && \text{with } N = 1, 2, \\ &(15N, 5), (45N, 5). \end{aligned} \tag{3.4}$$

As we have already seen, the following pairs appear for genus zero function fields:

$$\begin{aligned} &(3N, 1), \quad \text{with } N = 1, \ldots, 5, \\ &(6N, 2), \quad \text{with } N = 1, 2. \end{aligned}$$

We, again, construct curves $C_{3m,n}$ by combining with the Tate normal form, or with division polynomials as in Chapter 2, where we also see that $C_{3m,n}$ has genus ≥ 2 when $(3m, n) = (30, 1),\ (45, 1),$ or $(15, 5)$. This rules out torsion these structures from (3.4), and those containing them.

To rule out points of order 36, we begin with $E_{a,b}$ written in the Tate normal form for points of order 9 and look at the division polynomial $\phi_6(x) = 0$. In this case, $\phi_6 = f \cdot g \cdot \lambda_{36}$, where f, g, and λ are polynomials of degree 5, 10 and 45 respectively. Here, $f = 0$ defines a genus zero curve corresponding to the point P of order 9 such that $[4]P = (0, 0)$, and $g = 0$ defines a genus 1 curve that corresponds to points of order 18 (which we will see below). The irreducible curve defined by $C_{36,1} : \lambda_{36} = 0$ corresponds to points of order 36, but is of genus 7, showing that points of this order are impossible over K.

To rule out points of order 63, we begin with a curve $E_{a,b}$ written in the Tate normal form for points of order 9. By looking at the division polynomial $\psi_7(x) = 0$, we find the conditions for the x-coordinate a point of order 7 to exist. The curve defined by $C_{63,1} : \psi_7(x) = 0$ is irreducible of degree 90 and genus 18.

To rule out $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we begin with the Tate normal form $E_{a,b}$ for $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and look at $\phi_3(x) = 0$. This time, the numerator of ϕ_3, which we denote $\lambda_{18,2}$ defines an irreducible curve $C_{18,2}$ of genus 3, showing that this torsion structure is impossible over K.

To rule out $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we begin with the Tate normal form $E_{a,b}$ for $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and use the Hasse invariant. Recall, for a curve in the Tate normal form over a field of characteristic 3, we have

$$H(E_{a,b}) = a^2 + a + 2b = 1 = \frac{f^8 + 2f^7 + 2f^5 + 2f^4 + f^3 + f + 1}{(f^4 + f^3 + f^2 + 1)^2}.$$

We need $H(E_{a,b}) = g^2$ for some $g \in K^\times$, which amounts to finding non-constant points on the curve

$$C_{24,2} : t^8 + 2t^7 + 2t^5 + 2t^4 + t^3 + t + 1 = u^2.$$

But $C_{24,2}$ is irreducible of genus 3, so no such points exist, and therefore the desired torsion structure is impossible over K.

For points of order 33, we begin with a curve with a point of order 3. Recall, non-isotrivial curves over K with a point of order 3 can be written in the form

$$E_{a,b} : y^2 + axy + by = x^3 \text{ for some } a, b \in K, \text{ not both constant.}$$

If $a = 0$, however, this curve is singular, so we may safely assume $a \neq 0$ and set $f = b/a^3$. This way, we can write $E_{a,b}$ using the single parameter t:

$$E_t : y^2 + xy + fy = x^3 \text{ for some non-constant } f \in K,$$

where $(0, 0)$ is a point of order 3. We find that the division polynomial $\phi_{11}(x) = x \cdot \lambda_{11,1}(x)$, where $\lambda_{11,1}$ is a degree 120 polynomial with coefficients in $\mathbb{F}$. A point of order 33 implies a non-constant point on the curve $C_{33,1} : \lambda_{11,1} = 0$. After a 151 hour calculation, Magma reports that $C_{33,1}$ has genus 6, and is irreducible showing that points of order 33 are impossible over K.

To rule out points of order 36 over K, we start with a curve written in the Tate normal form for curves with a point of order 9. Then looking at the division polynomial $\phi_4(x)$, we see that ϕ_4 factors as $\phi_4 = f \cdot g \cdot \lambda_{36,1}$, where f, g and $\lambda_{36,1}$ are functions in x and t of degrees 5, 10, and 45 respectively, with coefficients in $\mathbb{F}$. The curve $C_f : f = 0$ has genus zero, and corresponds to points of order 9. The curve $C_g : g = 0$ is genus 1, and corresponds to points of order 18 (which we've already seen above). The curve $C_{36,1} : \lambda_{36,1} = 0$, however, gives points of order 36, and is irreducible of genus 7. Thus, we see that points of order 36 are impossible over K.

For points of order 42, we begin with an elliptic curve written in the Tate normal form for curves with a point of order 7 and look at $\phi_6(x)$. Here, ϕ_6 factors as $\phi_6 = f \cdot g \cdot h \cdot \lambda_{42,1}$, where f, g, h and $\lambda_{42,1}$ are functions in x and t of degrees 1, 8, 17, and 37 respectively, with coefficients in $\mathbb{F}$. The curve $C_f : f = 0$ is genus 0, and corresponds to points of order 7. The curve $C_g : g = 0$ is genus 1, and corresponds to points of order 14, which are guaranteed by Theorem 3.2.3. The curve $C_h : h = 0$ is also genus 1, and corresponds to points of order 21 (which we've already seen above). Finally, the curve $C_{42,1} : \lambda_{42,1} = 0$, gives points of order 42, and is irreducible of genus 7. Thus, we see that points of order 42 are impossible over K.

To rule out torsion structure $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we start with a curve written in the Tate the normal form for $\mathbb{Z}/6 \times \mathbb{Z}/2\mathbb{Z}$ torsion. We set $\lambda_{18,2}$ to be the numerator of the division polynomial $\phi_3(x) = 0$, a degree 35 polynomial in the variables x, t with coefficients in $\mathbb{F}$. The curve $C_{18,2} : \lambda_{18,2} = 0$ is irreducible of genus 3, showing that this torsion structure is impossible over K.

Finally, to rule out torsion structure $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we begin with the Tate normal form $E_{a,b}$ for an elliptic curve with torsion structure $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where

$$a = \frac{(2f+1)(8f^2+4f+1)}{2(4f+1)(8f^2-1)t} \qquad \text{and} \qquad b = a\frac{2(4f+1)f}{8f^2-1}.$$

The Hasse invariant for this curve is

$$H(E_t) = a^2 + a + 2b + 1 = \frac{f^8 + 2f^7 + 2f^5 + 2f^4 + f^3 + t + 1}{(f^4 + f^3 + f^2 + f)^2}.$$

Here, since the denominator is a square, we will have $H(E)$ a square in $K^\times$ if and only if the numerator $f^8 + 2f^7 + 2f^5 + 2f^4 + f^3 + f + 1 = g^2$ for some $g \in K^\times$. But this equation corresponds to an irreducible genus 3 curve, so that $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion is impossible over K. Note that we have finally ruled out all pairs from (3.4) which do not appear in the theorem.

In Chapter 2, it was also determined that $C_{3^e m,n}$ has genus 1 when $(3^e m, n) = (18,1)$, $(21,1)$, $(24,1)$, or $(12,4)$, which by the above argument reveals that torsion subgroups corresponding to these pairs can appear over function fields where the base curve is isogenous to the normalizations, $\tilde{C}_{3^e m,n}$. As a reminder, these curves appear in Table 3.2, where we see that, with the exception of $C_{18,1}$, each of these curves is already non-singular. The normalization of $C_{18,1}$ is given, with normalization map

$(3^e m, n)$	$C_{3^e m,n}$	$\tilde{C}_{3^e m,n}$
$(18,1)$	$u^9 + (2t^3+t)u^6 + (t^7+t^4)u^3 + t^{13} + 2t^{10} + t^7 = 0$	$u^2 + 2tu + u = t^3 + 2t^2 + t$
$(21,1)$	$t^4 + 2t + 1 = u^2$	n/a
$(24,1)$	$2t^4 + 2t^3 + t^2 + t + 1 = u^2$	n/a
$(12,4)$	$2(f^4+1) = u^4$	n/a

Table 3.2: Genus one $C_{3m,n}$ for $p = 3$.

$\pi : \tilde{C}_{18,1} \to C_{18,1}$ such that

$$t \mapsto (2t^3 + t + 2)u + 2t^4 + t^3 + t^2 + t + 2.$$

Thus, if $\mathcal{C} = \tilde{C}_{18,1}$, and $K = \mathbb{F}(\tilde{C}_{18,1}) = \mathbb{F}(t, u)$, then the following is an infinite family of elliptic curves with a point of order 18 for all $n \geq 1$:

$$E_n : y^2 + \big((t^3 + 2t + 1)u + (t^4 + 2t^3 + 2t^2 + 2t + 2)\big)^{3^n} xy + (2t^9 + t^3)^{3^n} y = x^3 + (2t^9 + t^3)^{3^n} x^2$$

Furthermore, if $\varphi : D \to \tilde{C}_{18,1}$ is an isogeny, then using the notation above, we have the same family, call it $E_{\varphi,n}$, with t and u replaced by t_φ and u_φ respectively.

If $\varphi : \mathcal{C} \to C_{21,1}$ is an isogeny, then with the above notaion, the following gives an infinite family of curves with a point of order 21 over $\mathbb{F}(\mathcal{C})$:

$$E_{\varphi,n} : y^2 + (t_\varphi^2 - t_\varphi)^{3^n} xy - (t_\varphi^3 - t_\varphi^2)^{3^n} y = x^3 - (t_\varphi^3 - t_\varphi^2)^{3^n} x^2 \text{ for all } n \geq 1.$$

If $\varphi : \mathcal{C} \to C_{24,1}$ is an isogeny, the following gives an infinite family of curves with a point of order 24 over $\mathbb{F}(\mathcal{C}) = \mathbb{F}(t, u)$:

$$E_{\varphi,n} : y^2 + \left(\tfrac{(2t_\varphi-1)(t_\varphi-1)}{t}\right)^{3^n} xy - ((2t_\varphi - 1)(t_\varphi - 1))^{3^n} y = x^3 - ((2t_\varphi - 1)(t_\varphi - 1))^{3^n} x^2 \text{ for all } n \geq 1.$$

Finally, if $\varphi : \mathcal{C} \to C_{12,4}$ is an isogeny, the following gives an infinite family of curves with torsion structure $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ over $\mathbb{F}(\mathcal{C})$:

$$E_{\varphi,n} : y^2 + \left(\tfrac{(2t_\varphi-1)(t_\varphi-1)}{t}\right)^{3^n} xy - ((2t_\varphi - 1)(t_\varphi - 1))^{3^n} y = x^3 - ((2t_\varphi - 1)(t_\varphi - 1))^{3^n} x^2 \text{ for all } n \geq 1.$$

□

3.2.5 Characteristic $p = 7$

When the characteristic of a genus one function field K is 7, Theorem 3.2.3 provides the following corollary about prime-to-7 torsion structures for elliptic curves over K.

Corollary 3.2.11. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic 7, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)'_{\text{tors}}$ is one of*

$$\begin{array}{cl} \mathbb{Z}/N\mathbb{Z} & \text{with } N = 1, \ldots, 6, 8, \ldots, 12, 15, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{with } N = 1, \ldots, 6, \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{with } N = 1, 2, 3, \\ \mathbb{Z}/4N\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{with } N = 1, 2, \\ (\mathbb{Z}/N\mathbb{Z})^2 & \text{with } N = 5, 6. \end{array}$$

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

$$\begin{cases} \mathcal{C} \text{ is isogenous to } X_1(n, m) & \text{if } (m, n) \text{ is in (3.1)}, \\ \mathcal{C} \text{ is any smooth curve} & \text{otherwise.} \end{cases}$$

This time, since we can only have points of order 7^e for at most $e = 1$, we can use the Hasse invariant strategy from Section 3.2.2: Here, we take a curve with torsion structure $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ in Corollary 3.2.11 written in short Weierstrass form $E_f : y^2 = x^3 + A(f)x + B(f)$. If we assume that E_f has a point of order 7, then we can use Theorem 2.1.7 to say

$$H(E_{A,B}) = 3B(f) = g^6 \text{ for some } g \in K^\times.$$

We then define the curve $C_{7m,n} : 3B(t) = u^6$, which parameterizes elliptic curves with torsion structure $G \times \mathbb{Z}/7\mathbb{Z}$, and use the genus arguments above.

Theorem 3.2.12. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic 7, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)_{\text{tors}}$ is one of*

$$\begin{array}{cl} \mathbb{Z}/N\mathbb{Z} & \textit{with } N = 1, \dots, 12, 14, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{with } N = 1, \dots, 6, 7, \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \textit{with } N = 1, 2, 3, \\ \mathbb{Z}/4N\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \textit{with } N = 1, 2, \\ (\mathbb{Z}/N\mathbb{Z})^2 & \textit{with } N = 5, 6. \end{array}$$

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

$$\begin{cases} \mathcal{C} \textit{ is isogenous to } X_1(n, m) & \textit{if } (m, n) \textit{ is in } (3.1) \textit{ with } 7 \nmid m, \\ \mathcal{C} \textit{ is isogenous to } C_{14,2} : t^3 + 2t^2u + 2tu^2 + u^3 = 1 & \textit{if } (m, n) = (14, 2), \\ \mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.} \end{cases}$$

Proof. Using Corollary 3.2.11, and the fact that by Levin, E can have a point of 7-primary order at most 7, we need to rule or confirm the existence of $\mathbb{Z}/7m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

with $(7m,n)$ coming from

$$\begin{aligned}
&(7N,1) && \text{with } N = 3,4,6,8,9,11,12,\\
&(14N,2) && \text{with } N = 1,2,3,4,6,\\
&(21N,3) && \text{with } N = 1,2,3, \qquad (3.5)\\
&(28N,4) && \text{with } N = 1,2\\
&(42,6).
\end{aligned}$$

We have already seen above that the torsion structure $\mathbb{Z}/14\mathbb{Z}$ can appear infinitely often regardless of the base curve $\mathcal{C}$. Again, we can construct curves $C_{7m,n}$ as in Section 3.2.2, by starting with a curve written in the Tate normal form for torsion structure $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, and using the Hasse invariant to force a point of order 7. This time, for $E : y^2 = x^3 + A(f)x + B(f)$, we need

$$H(E_{A,B}) = 3B(f) = g^6 \text{ for some } g \in K^\times.$$

Let $C_{7m,n} : 3B(t) = u^6$ be the curve parameterizing $\mathbb{Z}/7m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, defined by this equation. Again, each $C_{7m,n}$ is a curve defined over $\mathbb{F}$, and we conclude that the torsion structure is impossible for an elliptic curve defined over K if $g(C_{7m,n}) > 1 = g(\mathcal{C})$ by Corollary 3.2.1. Our results are collected in Table 3.3, and with the exception of $\mathbb{Z}/77\mathbb{Z}$, this table rules out any G from (3.5) with a point of order ≥ 28.

For points of order 77, we may again start with E/K in the Tate normal form, parameterized by f, such that $(0,0)$ has order 7. Solutions, (x,f), to $\psi_{11}(E) = 0$ give x-coordinates of points, P_x, such that $77P_x = \mathcal{O}$. This time, $C_{77,1}$ has genus 31 after a Magma 38 hour computation, and is shown to be irreducible after 35. Thus, no such points exist, and therefore $\mathbb{Z}/77\mathbb{Z}$ torsion structure is impossible for an elliptic

$G = \mathbb{Z}/7m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$	Curve $C_{7m,n}$	genus
$\mathbb{Z}/21\mathbb{Z}$	$a^6 + 6a^3b + 6b^2 = 1$	2
$\mathbb{Z}/28\mathbb{Z}$	$6t^3 + t^2 + 3t + 1 = u^6$	4
$\mathbb{Z}/35\mathbb{Z}$	$t^6 + 3t^5 + 5t^4 + 5t^2 + 4t + 1 = u^6$	10
$\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$a^3 + 2a^2b + 2ab^2 + b^3 = 1$	1

Table 3.3: Ruling out G torsion over K for $m \geq 4$.

curve over K.

With the exception of $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we have already seen that all groups in the theorem appear infinitely often as the torsion subgroup of an elliptic curve E/K. Again, we also find that because $g(C_{14,2}) = 1$, in order for an elliptic curve E/K to have a torsion structure $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we must have that $\mathcal{C}$ is isogenous to the normalization of $C_{14,2}$. Again, in this case, $C_{14,2}$ is itself, already non-singular, so we may take as an example the case where $\mathcal{C} = C_{14,2}$, and $\mathbb{F}(\mathcal{C}) = \mathbb{F}(C_{14,2}) = \mathbb{F}(a,b)$. Here, the following family has the desired torsion structure:

$$E_n : y^2 = x(x - a^{7^n})(x - b^{7^n}) \text{ for all } n \geq 1,$$

since, again, $H(E_n) = 1 \in K^6$, and $j(E) \in K^7$. As in the previous example, if $\varphi : C_{14,2} \to \mathcal{C}$ is an isogeny between curves, then

$$E_n^{\varphi} : y^2 = x(x - \varphi(a)^{7^n})(x - \varphi(b)^{7^n}) \text{ for all } n \geq 1,$$

has torsion structure $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for all n.

□

3.2.6 Characteristic $p = 11$

For genus one function fields of characteristic 11, Theorem 3.2.3 yields the following.

Corollary 3.2.13. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic 11, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)'_{\mathrm{tors}}$ is one of*

$$\begin{array}{cl} \mathbb{Z}/N\mathbb{Z} & \textit{with } N = 1, \ldots, 10, 12, 14, 15, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{with } N = 1, \ldots, 6, \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \textit{with } N = 1, 2, 3, \\ \mathbb{Z}/4N\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \textit{with } N = 1, 2, \\ (\mathbb{Z}/N\mathbb{Z})^2 & \textit{with } N = 5, 6. \end{array}$$

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

$$\begin{cases} \mathcal{C} \textit{ is isogenous to } X_1(n, m) & \textit{if } (m, n) \textit{ is in } (3.1), \\ \mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.} \end{cases}$$

Again, we can only have points of order 11^e for at most $e = 1$, and use the Hasse invariant strategy from previous sections. This time, the Hasse invariant is

$$H(E_{A,B}) = 9A(t)B(t) = u^{10}.$$

This time, all of the possible cases have been considered in Section 2.3.3, when we determined the possible torsion subgroups for an elliptic curve over a characteristic 11 function field of genus zero. We summarize and reinterpret the results here.

Theorem 3.2.14. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic 11, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)_{\mathrm{tors}}$ is one of*

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

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

$$\begin{cases} \mathcal{C} \textit{ is isogenous to } X_1(n, m) & \textit{if } (m, n) \textit{ is in } (3.1) \textit{ with } 11 \nmid m, \\ \mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.} \end{cases}$$

Proof. Again, by Theorem 3.2.3, and the fact that E can have a point of 11-primary order at most 11, we need to rule out or confirm the existence of $\mathbb{Z}/11m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $(11m, n)$ coming from

$$\begin{array}{cl} (11N, 1) & \text{with } N = 3, 4, 6, 7, 8, 9, 11, 12, 14, \\ (22N, 2) & \text{with } N = 1, 2, 3, 4, 6 \\ (33N, 3) & \text{with } N = 1, 2, 3, \\ (44N, 4) & \text{with } N = 1, 2 \\ (11N, N) & \text{with } N = 5, 6. \end{array} \tag{3.6}$$

This time, proceeding with our previous strategy, we construct the curves $C_{11m,n}$ in Table 3.4, which rules out every torsion structure with a point of order ≥ 22, thus proving the theorem.

$G = \mathbb{Z}/11m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$	$C_{11m,n}$	genus
$\mathbb{Z}/22\mathbb{Z}$	$a^5 + 9a^3b + 8ab^2 = 1$	2
$\mathbb{Z}/33\mathbb{Z}$	$a^{10} + 6a^7b + 2a^4b^2 + 8ab^3 = 1$	9
$\mathbb{Z}/55\mathbb{Z}$	$f^{10} + 3f^9 + 8f^8 + 4f^7 + 8f^6 + 8f^4 + 7f^3 + 8f^2 + 8f + 1 = u^{10}$	36
$\mathbb{Z}/77\mathbb{Z}$	$f^{20} + 3f^{19} + f^{18} + 4f^{17} + 6f^{16} + 5f^{15} + 6f^{14} + 5f^{13} + 9f^{12} + 7f^{11}+$ $+5f^{10} + 8f^9 + 8f^8 + 5f^7 + 2f^6 + 7f^5 + 4f^4 + 8f^3 + 6f^2 + 10f + 1 = u^{10}$	81

Table 3.4: Curves parameterizing elliptic curves with G torsion over K.

□

Remark 3.2.15. Observe that for $p \neq 11$, elliptic curves over genus one function fields of characteristic p can only have a point of order 11 if the base curve is isogenous to $X_1(11)$. When $p = 11$, however, we can find points of order eleven over function fields of arbitrary curves.

3.2.7 Characteristic $p = 13$

For function genus one function fields K of characteristic 13, we find the following specialization of Theorem 3.2.3.

Corollary 3.2.16. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic*

13, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)'_{\mathrm{tors}}$ is one of

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

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

$$\begin{cases} \mathcal{C} \textit{ is isogenous to } X_1(n, m) & \textit{if } (m, n) \textit{ is in } (3.1), \\ \mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.} \end{cases}$$

In this final case, the Hasse invariant for a curve in short Weierstrass form is

$$H(E_{A,B}) = 7A^3 + 2B^2.$$

Thus, we will check genera of curves written in the form $7A(t)^3+2B(t)^2 = u^{12}$. Again, in some cases we will find it more convenient to work with the division polynomial (and in this setting, the modular polynomial) for points of order 13.

Theorem 3.2.17. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}$, a finite field of characteristic*

13, and let $K = \mathbb{F}(\mathcal{C})$. Let E/K be non-isotrivial. Then $E(K)_{\text{tors}}$ is one of

$$\begin{array}{cl}
\mathbb{Z}/N\mathbb{Z} & \textit{with } N = 1, \ldots, 15, \\
\mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{with } N = 1, \ldots, 6, \\
\mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \textit{with } N = 1, 2, 3, \\
\mathbb{Z}/4N\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \textit{with } N = 1, 2, \\
(\mathbb{Z}/N\mathbb{Z})^2 & \textit{with } N = 5, 6.
\end{array}$$

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

$$\begin{cases}
\mathcal{C} \textit{ is isogenous to } X_1(n, m) & \textit{if } (m, n) \textit{ is in } (3.1) \textit{ with } 13 \nmid m, \\
\mathcal{C} \textit{ is isogenous to } C_{13,1} : u^2 = t^3 + 11 & \textit{if } (m, n) = (13, 1), \\
\mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.}
\end{cases}$$

Proof. Again, by Theorem 3.2.3, and the fact that E can have a point of 13-primary order at most 13, we need to rule out or confirm the existence of $\mathbb{Z}/13m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $(13m, n)$ coming from

$$\begin{array}{cl}
(13N, 1) & \text{with } N = 1, 2, \ldots, 12, 14, 15, \\
(26N, 2) & \text{with } N = 1, \ldots, 6 \\
(39N, 3) & \text{with } N = 1, 2, 3, \\
(52N, 4) & \text{with } N = 1, 2 \\
(13N, N) & \text{with } N = 5, 6.
\end{array} \tag{3.7}$$

This time, proceeding with our previous strategy, we construct the curves $C_{13m,n}$, and record their genera in Table 3.5, which rules out every torsion structure with a point of order ≥ 26, with the exception of $143 = 13 \cdot 11$.

$G = \mathbb{Z}/13m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$	genus of $C_{13m,n}$
$\mathbb{Z}/26\mathbb{Z}$	4
$\mathbb{Z}/39\mathbb{Z}$	15
$\mathbb{Z}/65\mathbb{Z}$	55
$\mathbb{Z}/91\mathbb{Z}$	121

Table 3.5: Curves parameterizing elliptic curves with G torsion over K.

To see a point of order 13, we suppose $E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2$ for $a, b \in K$, and set

$$\lambda_{13} = b^{-56}\psi_{13}\big((0,0)\big) = a^{10} + 12a^9b^2 + 7a^8b^2 + 6a^8b + 5a^7b^3 + 5a^7b^2 + 3a^7b + 11a^6b^3 + \\ + a^6b + 4a^5b^4 + 8a^5b^3 + 7a^5b^2 + 11a^4b^4 + 2a^4b^3 + 4a^3b^5 + 6a^3b^4 + 2a^2b^5 + 7ab^6 + b^7,$$

where ψ_{13} is the 13-division polynomial. If $(0,0)$ has order 13, then we must have that (t,u) is a point on $C_{13,1} : \lambda_{13}(t,u) = 0$. Over $\mathbb{F}_{13}$, the curve $C_{13,1}$ is irreducible of genus 1, and has normalization $\tilde{C}_{13,1} : u^2 = t^3 + 11$ with $\pi : \tilde{C}_{13,1} \to C_{13,1}$ given by Magma as

$$t \mapsto \frac{4t^6 + (9u+5)t^4 + (4u+12)t^3 + (11u+7)t^2 + (9u+11)t + 2u + 5}{(t+4)^5},$$
$$u \mapsto \frac{t^9+(11u+11)t^8+(5u+10)t^7+(11u+9)t^6+(8u+4)t^5+6ut^4+(5u+2)t^3+(4u+8)t^2+(u+10)t+8u+3}{(t+4)^9}$$

By our above argument, if E/K has a point of order 13, then there must be an isogeny from $\mathcal{C}$ to $\tilde{C}_{13,1}$. For example, with $\mathcal{C} = \tilde{C}_{13,1}$, and $K = \mathbb{F}(\tilde{C}_{13,1}) = \mathbb{F}(t,u)$ if we set

$$a = \frac{4t^6 + (9u+5)t^4 + (4u+12)t^3 + (11u+7)t^2 + (9u+11)t + 2u + 5}{(t+4)^5},$$
$$b = \frac{t^9+(11u+11)t^8+(5u+10)t^7+(11u+9)t^6+(8u+4)t^5+6ut^4+(5u+2)t^3+(4u+8)t^2+(u+10)t+8u+3}{(t+4)^9}$$

then the following is an infinite family of elliptic curves with a point of order 13:

$$E_{a,b}^{13^n} : y^2 + (1 - a^{13^n})xy - b^{13^n}y = x^3 - b^{13^n}x^2.$$

If $\varphi : \mathcal{C} \to \tilde{C}_{13,1}$ is an isogeny, then replacing a and b with $\varphi(a)$ and $\varphi(b)$ respectively gives an infinite family of curves with a point of order 13.

Recall, from above, that if E/K has a point of order 11, then $\mathcal{C}$ must be isogenous to $X_1(11) : u^2 + (t^2+1)u + t = 0$, which can be written in short Weierstrass form as

$$D : u^2 = t^3 + 4t + 3.$$

If, in addition, E has a point of order 13, we must have that $\mathcal{C}$ is isogenous to $C_{13,1}$, so that there must be an isogeny, defined over $\mathbb{F}$, from $C_{13,1}$ to D. If we can show that no such isogeny exists in any extension of $\mathbb{F}_{13}$, then points of order 143 are impossible over K. However, if an isogeny between $C_{13,1}$ and D exists, $(j(C_{13,1}), j(D))$ must be a root of the modular polynomial $\Phi_{143}(X, Y)$ defined over $\mathbb{F}_{13}$. We again consult Andrew Sutherland's tables in [20]. Since $j(D) = 0$, we find that

$$\Phi_{143}(X, 0) = \sum_{n=1}^{169} a_n X^{n-1} \text{ where}$$

$$\begin{aligned}[a_1, \ldots, a_n] =[1,\ 11,\ &10,\ 2,\ 5,\ 6,\ 2,\ 9,\ 6,\ 6,\ 1,\ 4,\ 1,\ 11,\ 4,\ 6,\ 9,\\ &3,\ 1,\ 9,\ 8,\ 1,\ 1,\ 11,\ 5,\ 11,\ 10,\ 6,\ 9,\ 7,\ 11,\ 8,\\ &7,\ 12,\ 8,\ 8,\ 10,\ 1,\ 10,\ 2,\ 9,\ 7,\ 4,\ 10,\ 12,\ 4,\ 5,\\ &12,\ 12,\ 2,\ 8,\ 2,\ 5,\ 3,\ 11,\ 10,\ 12,\ 4,\ 10,\ 6,\ 4,\ 4,\\ &5,\ 7,\ 5,\ 6,\ 1,\ 8,\ 12,\ 4,\ 10,\ 12,\ 2,\ 10,\ 10,\ 6,\ 11,\\ &6,\ 2,\ 9,\ 7,\ 4,\ 10,\ 12,\ 4,\ 5,\ 12,\ 12,\ 2,\ 8,\ 2,\ 9,\\ &8,\ 12,\ 5,\ 6,\ 2,\ 5,\ 3,\ 2,\ 2,\ 9,\ 10,\ 9,\ 6,\ 1,\ 8,\\ &12,\ 4,\ 10,\ 12,\ 2,\ 10,\ 10,\ 6,\ 11,\ 6,\ 6,\ 1,\ 8,\ 12,\ 4,\\ &10,\ 12,\ 2,\ 10,\ 10,\ 6,\ 11,\ 6,\ 1,\ 11,\ 10,\ 2,\ 5,\ 6,\ 2,\\ &9,\ 6,\ 6,\ 1,\ 4,\ 1,\ 4,\ 5,\ 1,\ 8,\ 7,\ 11,\ 8,\ 10,\ 11,\\ &11,\ 4,\ 3,\ 4,\ 1,\ 11,\ 10,\ 2,\ 5,\ 6,\ 2,\ 9,\ 6,\ 6,\ 1,\ 4,\ 1]\end{aligned}$$

Thus, we have that $\Phi_{143}(6, 0) = 12$, and an isogeny between $C_{13,1}$ and D cannot exist, that is, there are no points of order 143 over K.

□

3.3 Explicit Parameterizations and Isogenies

Let $\mathbb{F}$ be a finite field of characteristic p, and set $K = \mathbb{F}(\mathcal{C})$ for a smooth, projective, absolutely irreducible curve $\mathcal{C}$. In this final section, we give conditions on the base curve to find torsion structures appearing in this thesis, and parameterizations where possible. Tables 3.6 and 3.7, taken from Chapter 2, give $E_{a,b}$ which parameterize non-isotrivial elliptic curves with torsion subgroup G regardless of the base curve. In each parameterization, $(0, 0)$ is a point of maximal order.

Table 3.8, also taken from Chapter 2, shows the additional torsion subgroups which can appear over K, regardless of $\mathcal{C}$, such that p divides the order of the torsion subgroup. Again, in this table, $E_{a,b}$ parameterizes non-isotrivial elliptic curves with

Characteristic	$E_{a,b}/K$	G
$p \neq 2$	$y^2 = x^3 + ax^2 + bx$	$\mathbb{Z}/2\mathbb{Z}$
$p \neq 2$	$y^2 = x(x-a)(x-b)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
general p	$y^2 + axy + by = x^3$	$\mathbb{Z}/3\mathbb{Z}$
$p \neq 3,\ \zeta_3 \in \mathbb{F}$	$y^2 + 3(f+2)xy + (f^2+f+1)y = x^3$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Table 3.6: Two-parameter familes of elliptic curves $E_{a,b}/K$ such that $G \subset E_{a,b}(K)_{\text{tors}}$.

Characteristic	$E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2$		G
general p	$a = 0$	$b = f$	$\mathbb{Z}/4\mathbb{Z}$
general p	$a = f$	$b = f$	$\mathbb{Z}/5\mathbb{Z}$
general p	$a = f$	$b = f + f^2$	$\mathbb{Z}/6\mathbb{Z}$
general p	$a = f^2 - f$	$b = af$	$\mathbb{Z}/7\mathbb{Z}$
general p	$a = \frac{(2f-1)(f-1)}{f}$	$b = af$	$\mathbb{Z}/8\mathbb{Z}$
general p	$a = f^2(f-1)$	$b = a(f^2 - f + 1)$	$\mathbb{Z}/9\mathbb{Z}$
general p	$a = -\frac{f(f-1)(2f-1)}{f^2-3f+1}$	$b = -a \cdot \frac{f^2}{f^2-3f+1}$	$\mathbb{Z}/10\mathbb{Z}$
general p	$a = \frac{f(1-2f)(3f^2-3f+1)}{(f-1)^3}$	$b = -a \cdot \frac{2f^2-2f+1}{f-1}$	$\mathbb{Z}/12\mathbb{Z}$
$p \neq 2$	$a = 0$	$b = f^2 - \frac{1}{16}$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p \neq 2$	$a = \frac{10-2f}{f^2-9}$	$b = \frac{-2(f-1)^2(f-5)}{(f^2-9)^2}$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p \neq 2$	$a = \frac{(2f+1)(8f^2+4f+1)}{2(4f+1)(8f^2-1)f}$	$b = \frac{(2f+1)(8f^2+4f+1)}{(8f^2-1)^2}$	$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p \neq 3,\ \zeta_3 \in \mathbb{F}$	$a = -\frac{f(f^2+f+1)}{(f-1)^3}$	$b = -a\frac{4f^2-2f+1}{(f-1)^3}$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$p \neq 4,\ i \in \mathbb{F}$	$a = 0$	$b = f^4 - \frac{1}{16}$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$p \neq 5,\ \zeta_5 \in \mathbb{F}$	$a = \frac{f^4+2f^3+4f^2+3f+1}{f^5-3f^4+4f^3-2f^2+f}$	$b = a$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Table 3.7: One-parameter familes of elliptic curves $E_{a,b}/K$ such that $G \subset E_{a,b}(K)_{\text{tors}}$.

torsion subgroup G.

The rest of the torsion structures that were found in this thesis require that $\mathcal{C}$ be isogenous to a specific curve, D. In Table 3.9, we collect all of these curves when p

Characteristic	$E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2$		G
$p = 11$	$a = \frac{(f+3)(f+5)^2(f+9)^2}{3(f+1)(f+4)^4}$	$b = a\frac{(f+1)^2(f+9)}{2(f+4)^3}$	$\mathbb{Z}/11\mathbb{Z}$
$p = 2$	$a = \frac{f(f+1)^3}{f^3+f+1}$	$b = a\frac{1}{f^3+f+1}$	$\mathbb{Z}/14\mathbb{Z}$
$p = 7$	$a = \frac{(f+1)(f+3)^3(f+4)(f+6)}{f(f+2)^2(f+5)}$	$b = a\frac{(f+1)(f+5)^3}{4f(f+2)}$	
$p = 3$	$a = \frac{f^3(f+1)^2}{(f+2)^6}$	$b = a\frac{f(f^4+2f^3+f+1)}{(f+2)^5}$	$\mathbb{Z}/15\mathbb{Z}$
$p = 5$	$a = \frac{(f+1)(f+2)^2(f+4)^3(f^2+2)}{(f+3)^6(f^2+3)}$	$b = a\frac{f(f+4)}{(f+3)^5}$	
$p = 2$	$a = \frac{f(f+1)^2(f^2+f+1)}{f^3+f+1}$	$b = a\frac{(f+1)^2}{f^3+f+1}$	$\mathbb{Z}/18\mathbb{Z}$
$p = 5$	$a = \frac{f(f+1)(f+2)^2(f+3)(f+4)}{(f^2+4f+1)^2}$	$b = a\frac{(f+1)^2(f+3)^2}{4(f^2+4f+1)^2}$	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p = 3,\ i \in \mathbb{F}$	$a = \frac{f(f+1)(f+2)(f^2+2f+2)}{(f^2+f+2)^3}$	$b = a\frac{(f^2+1)^2}{f(f^2+f+2)}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p = 2,\ i \in \mathbb{F}$	$a = \frac{f(f^4+f+1)(f^4+f^3+1)}{(f^2+f+1)^5}$	$b = a\frac{f^2(f^4+f^3+1)^2}{(f^2+f+1)^5}$	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Table 3.8: One-parameter families of elliptic curves $E_{a,b}/K$ such that $E_{a,b}(K)_{\text{tors}}$ has a subgroup G.

divides the order of the torsion subgroup, and in Table 3.10 we provide examples for when $\mathcal{C} = D$ and $K = \mathbb{F}(D) = \mathbb{F}(t, u)$. For prime-to-$p$ torsion, we refer the reader to the tables in [18] and [19].

For other examples where $\mathcal{C}$ is not isomorphic to D, we suppose that $D \to \mathcal{C}$ is an isogeny, and $\varphi : \mathbb{F}(\mathcal{C}) \to \mathbb{F}(D)$ is the induced map on the function fields of D and $\mathcal{C}$. Then writing $\mathbb{F}(\mathcal{C}) = \mathbb{F}(t, u)$, and replacing t with $\varphi(t)$, and u with $\varphi(u)$ in the parameterizations above gives an infinite family of elliptic curves with the desired torsion structure over K.

Characteristic	$\mathcal{C}$	G
$p = 2$	$u^2 + u = t^3 + t$	$\mathbb{Z}/16\mathbb{Z},\ \mathbb{Z}/20\mathbb{Z}$
$p = 2$	$u^2 + (t^2 + 1)u + t = 0$	$\mathbb{Z}/22\mathbb{Z}$
$p = 2$	$u^2 + tu + u = t^3 + t^2$	$\mathbb{Z}/30\mathbb{Z}$
$p = 2$	$u^2 + u = t^3 + 1$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$p = 3$	$u^2 + 2tu + u = t^3 + 2t^2 + t$	$\mathbb{Z}/18\mathbb{Z}$
$p = 3$	$u^2 = t^4 + 2t + 1$	$\mathbb{Z}/21\mathbb{Z}$
$p = 3$	$u^2 = 2t^4 + 2t^3 + t^2 + t + 1$	$\mathbb{Z}/24\mathbb{Z}$
$p = 3$	$u^4 = 2(t^4 + 1)$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$p = 5$	$u^4 = t^2 + t + 1$	$\mathbb{Z}/20\mathbb{Z}$
$p = 7$	$t^3 + 2t^2u + 2tu^2 + u^3 = 1$	$\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p = 13$	$u^2 = t^3 + 11$	$\mathbb{Z}/13\mathbb{Z}$

Table 3.9: Genus one curves that must be isogenous to $\mathcal{C}$ for G to appear for an elliptic curve over K.

Char(K)	$E_{a,b}^{p^n} : y^2 + (1-a)^{p^n}xy - b^{p^n}y = x^3 - b^{p^n}x^2$, $n \geq 1$	G
$p = 2$	$a = \frac{(t+1)^2(t^5+t^2u+t^2+t+u)}{t^{10}}$ $b = a\frac{t^6+t^3+t^2+t+u}{t^6}$	$\mathbb{Z}/16\mathbb{Z}$
$p = 2$	$a = \frac{t^9+t^6u+t^6+t^5+t^4u+t^3+t^2+t+u}{t^2}$ $b = a(t^5 + t^2u + t + u + 1)$	$\mathbb{Z}/20\mathbb{Z}$
$p = 2$	$a = \frac{(u+1)(tu^6+tu^5+tu+u^6+u^5+u^3+u^2+1)}{u^5(u^5+u^3+1)}$ $b = a\frac{tu^2+tu+u^6+u^5+u^2+u+1}{u(u^5+u^3+1)}$	$\mathbb{Z}/22\mathbb{Z}$
$p = 2$	$a = \frac{(t+1)^7(t^2+t+1)^2(t^{12}+t^{10}u+t^9+t^6u+t^5+t^4+t^2+t+u+1)}{t^6(t^4+t^3+1)^2}$ $b = a\frac{t^{13}+t^{12}+t^{11}u+t^{11}+t^{10}u+t^{10}+t^9u+t^8u+t^7+t^6+t^5u+t^4u+t^4+t^3+t^2+tu+u}{(t^4+t^3+1)^2}$	$\mathbb{Z}/30\mathbb{Z}$
$p = 2$	$a = \frac{t^2(t^{31}+t^{30}+t^{28}u+t^{28}+t^{27}+t^{24}u+t^{24}+t^{23}+t^{20}u+t^{20}+t^{17}+t^{16}+t^{15}+t^{14}u+t^{14}+t^{12}u+t^{12}+t^{10}+t^9+t^8+t^6u+t^4+t^3+u)}{(t+1)^6(t^2+t+1)^6(t^3+t+1)^6}$ $b = a\frac{(t^2+t+1)^2(t^{12}+t^{10}+t^8+t^5+t^4+t^2u+1)}{(t^3+t+1)^6}$	$\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$p = 2$	$a = \frac{t^2(t^{15}+t^{14}+t^{13}+t^{12}u+t^{11}+t^{10}u+t^{10}+t^8u+t^5+t^4+t^3+t^2u+t^2+u)}{(t+1)^6(t^2+t+1)^6}$ $b = a\frac{t^6+t^5+t^2u+1}{(t+1)^2(t^2+t+1)^2}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$p = 3$	$a = \frac{(t+1)^3(t+2)^3(t^4+t^3u+t^3+2t^2+2tu+2t+u+2)}{t^9}$ $b = a\frac{(t^7+t^6u+2t^5+2t^4u+2t^3u+2t^3+2t^2+2tu+2t+u+1)}{t^6}$	$\mathbb{Z}/18\mathbb{Z}$
$p = 3$	$a = \frac{t^2(t^{10}+2t^9+t^8u+2t^8+2t^7u+t^7+2t^6u+2t^4u+t^4+2t^2u+t^2+tu+2t+u+1)}{(t+2)^3}$ $b = a(t^3 + t^2 + 2t + 1)(t^5 + 2t^4 + t^3u + t^3 + 2t^2u + t^2 + tu + t + 2)$	$\mathbb{Z}/21\mathbb{Z}$
$p = 3$	$a = \frac{(t+2)(t^{10}+t^8u+t^6u+2t^6+t^5+t^4u+2t^3u+t^3+2t^2u+2tu+t+u+1)}{t^9(t+1)^3}$ $b = a\frac{(t^2+2t+2)(t^6+2t^4+t^3u+2t^2u+t^2+tu+u+1)}{t^7(t+1)}$	$\mathbb{Z}/24\mathbb{Z}$
$p = 3$	$a = \frac{(t^8u+2t^8+2t^4u+2t^4+2u)}{(t+1)^3(t+2)^3(t^2+1)^3}$ $b = a\frac{t^4(t^4+u+1)}{(t+1)(t+2)(t^2+1)(t^2+t+2)(t^2+2t+2)}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$p = 5$	$a = \frac{u(u+2)(tu^4+2tu^3+tu+4t+2u^6+u^5+4u^4+4u^3+3u+1)}{(u+1)(u+3)^7(u+4)}$ $b = a\frac{(tu^4+3tu^3+tu^2+4t+u^6+3u^5+u^4+3u^3+3u+2)}{u(u+3)^5}$	$\mathbb{Z}/20\mathbb{Z}$
$p = 7$	$a = \frac{t^2u^6+t^2u^5+4t^2u^4+2t^2u^3+2t^2u^2+t^2+3tu^7+3tu^3+2tu^2+6tu+t+u^8+5u^7+2u^6+u^5+4u^4+2u^3+3u^2+3u+1}{u(u+4)^4(u+6)}$ $b = a\frac{(t^2u^2+t^2u+t^2+3tu^3+3tu^2+5tu+t+u^4+u^3+4u^2+3u+5)}{(u+4)^2}$	$\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p = 13$	$a = \frac{(t^6+12t^4u+11t^4+t^3u+3t^3+6t^2u+5t^2+12tu+6t+7u+11)}{(t+4)^5}$ $b = a\frac{(t^3+2t^2u+9t^2+9tu+11t+u+1)}{(t+4)^4}$	$\mathbb{Z}/13\mathbb{Z}$

Table 3.10: One-parameter families of elliptic curves $E_{a,b}^{p^n}/K$ such that $E_{a,b}(K)_{\mathrm{tors}}$ has a subgroup G for $n \geq 1$.

Bibliography

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478 2.2, 2

[2] David A. Cox and Walter R. Parry, *Torsion in elliptic curves over $k(t)$*, Compositio Math. **41** (1980), no. 3, 337–354. MR 589086 1.3.1, 1.3.2, 2.1.4, 2.1.5, 2.4.1

[3] Christophe Debry, *Beyond two criteria for supersingularity: coefficients of division polynomials*, J. Théor. Nombres Bordeaux **26** (2014), no. 3, 595–606. MR 3320494 2.2

[4] Maarten Derickx, Anastassia Etropolski, Jim Morrow, Mark van Hoeij, and David Zureick-Brown, *Sporadic torsion on elliptic curves, (in preparation)*. 1.2

[5] Andreas Enge, *Elliptic curves and their applications to cryptography: An introduction*, first ed., Kluwer Academic Publishers,. 2.2

[6] Enrique González-Jiménez and Álvaro Lozano-Robledo, *Elliptic curves with abelian division fields*, Math. Z. **283** (2016), no. 3-4, 835–859. MR 3519984 2.2, 2.2, 2.2.3

[7] Helmut Hasse, *Zur theorie des abstrakten elliptischen funktionenkörper i, ii, iii*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse. Fachgruppe 1, Vandenhoeck & Ruprecht, 1935. 1.4

[8] Dale Husemöller, *Elliptic curves*, Graduate Texts in Mathematics, Springer, 2004. 2.2

[9] Sheldon Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229. MR 1172689 1.2

[10] Sheldon Kamienny and Filip Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta Arithmetica **152** (2011). 1.1

[11] Monsur Kenku and Fumiyuki Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. MR 931956 1.2

[12] Serge Lang and André Néron, *Rational points of abelian varieties over function fields*, Amer. J. Math. **81** (1959), 95–118. MR 0102520 2.1.2

[13] Martin Levin, *On the group of rational points on elliptic curves over function fields*, Amer. J. Math. **90** (1968), 456–462. MR 0230723 1.3.1, 1.4, 1.4.1, 2.1.9, 2.4.1, 3.1.1

[14] Karl Rubin and Alice Silverberg, *Families of elliptic curves with constant mod p representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong

Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 148–161. MR 1363500 2.2

[15] Igor R. Shafarevich, *Basic algebraic geometry*, third ed., Springer-Verlag, 2013. 2.1

[16] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094 1.1.4, 2.1, 2.1, 2.2, 2.2, 2.3.1, 2.4.2, 2.4.2

[17] Andrew Snowden, *Course on Mazur's theorem*, http://www-personal.umich.edu/~asnowden/teaching/2013/679/index.html. 1.1.5

[18] Andrew Sutherland, *Optimized equations for* $X_1(N)$, http://math.mit.edu/~drew/X1_optcurves.html. 2.3.1, 3.2.2, 3.2.1, 3.3

[19] Andrew Sutherland, *Optimized equations for* $X_1(m, mn)$, http://math.mit.edu/~drew/X1mn.html. 3.2.2, 3.2.1, 3.3

[20] Andrew Sutherland, *Modular polynomials*, https://math.mit.edu/~drew/ClassicalModPolys.html. 3.2.7

[21] Douglas Ulmer, *Elliptic curves over function fields*, Arithmetic of L-functions, IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 211–280. MR 2882692 1.3.4, 1.3.1, 2.1, 2.1, 2.1.3, 2.1, 2.1.7, 2.4.1, 2.4.1, 3.2.1

[22] Tom Weston, *The modular curves* $X_0(11)$ *and* $X_1(11)$, 2001. 1.1.5