TORSION SUBGROUPS OF ELLIPTIC CURVES OVER FUNCTION FIELDS OF GENUS 1

ROBERT J.S. MCDONALD

Abstract. Abstract: Let $\mathbb{F}$ be a finite field of characteristic p, and $\mathcal{C}$ be a smooth, projective, absolutely irreducible curve of genus one over $\mathbb{F}$. Let $K = \mathbb{F}(\mathcal{C})$, and E be a non-isotrivial elliptic curve over K. Then, $E(K)$ is a finitely generated abelian group, and there is a finite list of possible torsion subgroups which can appear that depends only on $\mathcal{C}$ and p. In this article, we build on previous work to determine a complete list of possible full torsion subgroups which can appear over K.

1. Introduction: Elliptic curves over number fields

Over a number field K, an elliptic curve is the set of solutions to a diophantine equation of the form

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

The K-rational points will be denoted by $E(K)$. Given such a curve, a natural questions is: can we determine its solutions over K? So far, in the general case, even over $K = \mathbb{Q}$, this question leads to many unanswered problems.

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. For an in depth description of addition of points in this group, see [11, Chapter 3].

Example 1.1. The curve $E : y^2 = x^3 - x = x(x + 1)(x - 1)$, has only four integral points $(0, 0)$, $(\pm 1, 0)$, and the point $\mathcal{O}$. Here, if $P = (0, 0)$ and $Q = (-1, 0)$, then $2P = 2Q = \mathcal{O}$, and $P+Q = (1, 0)$. It turns out that E has no other $\mathbb{Q}$-rational points, and hence $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

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

Theorem 1.2 (Mordell-Weil)**.** *Let E be an elliptic curve over K. The group of K-rational points, $E(K)$, is a finitely generated abelian group.*

The fundamental theorem of finitely generated abelian groups and Theorem 1.2 tell us

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

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

Theorem 1.3 (Mazur [11, p. 242])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups:*

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

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

This is a complete classification of the types of torsion subgroups one should expect to encounter for an elliptic curve over $\mathbb{Q}$. What about over finite extensions of $\mathbb{Q}$? Again, for number fields of degree 2, 3, and 4, a lot is already known.

Theorem 1.4 (Kamienny–Kenku–Memose, [4, 5]). *Let E be an elliptic curve over a quadratic field K. Then the torsion subgroup $E(K)_{\text{tors}}$ is isomorphic to one of the following 26 groups*

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

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

Again, we have a complete classification of all of the torsion subgroups one should expect to encounter for an elliptic curve over a quadratic extension of $\mathbb{Q}$. When K is a cubic number field, we have yet to find the full list of torsion subgroups possible, but rather only those that occur for infinitely many non-isomorphic elliptic curves:

Theorem 1.5 (Jeon–Kim–Schweizer, [3]). *Let E be an elliptic curve over a cubic field K. Then the following 25 groups appear as $E(K)_{\text{tors}}$ for infinitely many non-isomorphic E.*

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

This time, Theorem 1.5 only provides the list of torsion subgroups appearing over a cubic number field *with infinitely many examples.* In [9], Najman shows that the curve

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

has a point of order 21 over the cubic subfield of $\mathbb{Q}(\zeta_9)$. This is our first example of a sporadic torsion structure: one that only appears for finitely many non-isomorphic elliptic curves. Similarly, Jeon, Kim, and Park have determined determined the list of torsion sungroups with infinitely many non-isomorphic examples over quartic fields (see [2]). But in this case, again, it is not known whether there are any other sporadic points.

We refer the interested reader to [12] for a lecture series on the proof of Mazur's Theorem 1.3 for elliptic curves over $\mathbb{Q}$. Shown there, is the general philosophy of turning questions about torsion points on elliptic curves of order N over a number field K into moduli problems: finding K-rational points on the modular curve $X_1(N)(K)$. The hard part of Mazur's theorem amounts to showing that the modular curve $X_1(N)(\mathbb{Q})$ is empty for any prime $N > 7$ [12, Lecture 1]. See also [17], 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 $E(\mathbb{Q})$.

2. Elliptic curves over function fields

In number theory, there is a long history of studying function fields, such as $\mathbb{Q}(T)$, to answer questions about number fields. There are a lot of similarities between function fields and number fields, and so one area of interest is to find analogues to theorems in one setting in the other. Our goal in this paper will be to develop analogues to Theorems 1.3–1.4 in the case where K is a genus one function field. We begin by defining elliptic curves in this setting, and in Section 2.1, state results for elliptic curves over genus zero function fields.

Given a smooth curve $\mathcal{C}$ over a finite field $\mathbb{F}$ of characteristic p, we now turn our attention to the function field $K = \mathbb{F}(\mathcal{C})$. An elliptic curve E is a smooth, irreducible, projective curve of genus one with a point. The curve E can always be written in the form

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

and when $p \neq 2, 3$, we can find a *short Weierstrass* model

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

We have the following

Definition 2.1. Let $K = \mathbb{F}(\mathcal{C})$ (of general genus) and E/K be an elliptic curve.

(1) E is *constant* if there is an elliptic curve E_0/k such that $E \cong E_0 \times_k K$.
(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.

For convenience, we also make the following analogous definition for general curves D over K.

Definition 2.2. 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, we will also call the curve D/K *constant*, if it is written in a form with coefficients in $\mathbb{F}$.

There is no obvious analogue of isotriviality for an elliptic curve over a number field. Therefore, in this paper, we are mostly concerned with non-isotrivial elliptic curves. This essentially amounts to the curve not being a base extension of an elliptic curve over $\mathbb{F}$. It can be shown that E is non-isotrivial if and only if $j(E) \notin \mathbb{F}$, where $j(E)$ is the j-invariant of E (see [16]).

In this setting, we also see that $E(K)$ is has the structure of a group. In fact, we have the following.

Theorem 2.3 (Mordell–Weil–Lang–Néron [6])**.** *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 [16, p. 16]). Moreover, the size of the torsion subgroup is universally bounded, depending only on the genus and characteristic of K, as in the following result.

Theorem 2.4 (Levin, [7])**.** *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 $\ell^e \mid \#E(K)_{\mathrm{tors}}$ for $e \geq 1$, then if $\ell \neq p$,*

$$\ell \leq 6 + (1 + 24 \cdot g(K))^{\frac{1}{2}},$$
$$e \leq \begin{cases} \log_2(3 + (1 + 8 \cdot g(K))^{\frac{1}{2}}) + 2 & \text{if } \ell = 2, \\ \log_3(1 + g(K)^{\frac{1}{2}}) + 2 & \text{if } \ell = 3, \\ \log_5(3 + (4 + 5 \cdot g(K))^{\frac{1}{2}}) + 1 & \text{if } \ell = 5, \\ \log_p(7(3 + (\frac{1}{2}(11 + 7 \cdot g(K)))^{\frac{1}{2}})) & \text{if } \ell \geq 7. \end{cases}$$

On the other hand, if $\ell^e \mid \#E(K)_{\mathrm{tors}}$ 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 [7, pp. 460–461].

In Sections 2.1 and 3, we provide corollaries of Theorem 2.4 in the cases of function fields of genus zero and one. Of particular interest to us is the bounds on p-primary torsion in Levin's theorem (when $\ell = p$). In characteristic p, there are strict requirements on the coefficients of any elliptic curve with a point of order p.

Theorem 2.5 ([16, p. 17])**.** *Suppose that E is a non-isotrivial elliptic curve over $K = \mathbb{F}_q(\mathcal{C})$ (of arbitrary genus), where q is a power of p. Then, $E(K)$ has a point of order p if and only if $j(E) \in K^p$, and the Hasse invariant is a $(p-1)$st power in $K^\times$.*

The j-invariant $j(E)$ and Hasse invariant (which we denote $H(E)$) are quite simple to compute. For example, when $p \geq 5$, we have

$$j(E) = \frac{4A^3}{4A^3 - 27B^2},$$

and when $p \geq 3$, we can write $E : y^2 = f(x)$ for some cubic f, and the Hasse invariant is the coefficient of x^{p-1} in the expansion of $f(x)^{(p-1)/2}$ (see [16, p. 14]).

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 2.6. *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 [10, 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 [11, 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 [11, Corollary 2.12] we can factor the map $\tilde{\rho}$ as

$$\mathcal{C} \xrightarrow{\alpha} \mathcal{C} \xrightarrow{\beta} \tilde{D},$$

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. □

In Section 3, we will provide a corollary to this result when the genus of $\mathcal{C}$ is one. Essentially, the corollary will provide strict restrictions on the isogeny class of the base curve for certain torsion structures to appear.

2.1. **Torsion in genus** 0. 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 $\mathbb{F}$. In this setting, there are strong results for prime-to-p, and p-primary torsion structures. Levin, for example, was able to provide bounds on the size of both components:

Corollary 2.7 (Levin, [7])**.** *Let $\mathbb{F}$ be a finite field of characteristic p, $K = \mathbb{F}(T)$, and E/K a non-isotrivial elliptic curve. Suppose $\ell^e \mid \#E(K)_{\text{tors}}$ for some prime ℓ. Then,*

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

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

Theorem 2.8 (Cox, Parry [1])**.** *Let $K = \mathbb{F}(T)$ where $\mathbb{F}$ is a finite field of characteristic $p \neq 2, 3$. Let E/K be non-isotrivial. Then $E(K)'_{\text{tors}}$, the rational points of finite order prime-to-p, is one of the following groups*

$$\begin{array}{cl} \mathbb{Z}/N\mathbb{Z} & \text{with } 1 \leq N \leq 12, N \neq 11, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{with } 1 \leq N \leq 4, \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{with } N = 1, 2 \\ (\mathbb{Z}/N\mathbb{Z})^2 & \text{with } N = 4, 5. \end{array}$$

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

All elliptic curves with each of the torsion subgroups in Cox and Parry's theorem can be parameterized using the Tate normal form (see [8]) which looks like

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

Acknowledgements. The author thanks Álvaro Lozano-Robledo for his continued support. A special thanks, as well, goes to both Lozano-Robledo and Harris Daniels for lending time and resources on their computers for some very lengthy genus and irreducibility calculations. The author would also like to thank (and is sad to be moving on from) the University of Connecticut Department of Mathematics for several years of financial and research support as a graduate student. Finally, a sincere thank you to the referees for their comments and revisions.

2.2. **Full torsion over genus zero function fields.** We summarize the results of [8]. Cox and Parry's theorem above is not stated when $p = 2, 3$, so we begin by developing the analogous statements for these two primes. It can be shown that Cox and Parry's theorem holds even when p is 2 or 3. Then, for each p and each group G from Theorem 2.8, we write a curve in Tate normal form for G. Using Theorem 2.5, or in some cases a division polynomial, we then construct a curve $\mathcal{D}/\mathbb{F}$, parameterizing elliptic curves with torsion subgroup $H = G \times \mathbb{Z}/p^e\mathbb{Z}$. It can be shown that the torsion structure H induces a separable map from $\mathcal{C} = \mathbb{P}^1$ to $\mathcal{D}$. Then, using the Hurwitz formula, if the genus of $\mathcal{D}$ is greater than 0, we obtain a contradiction. We arrive at the following result.

Theorem 2.9 (M, 2018)**.** *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 2.8 (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:*

$$\begin{array}{ll}
\mathbb{Z}/p\mathbb{Z} & \\
\mathbb{Z}/2p\mathbb{Z} & \textit{if } p = 2, 3, 5, 7, \\
\mathbb{Z}/3p\mathbb{Z} & \textit{if } p = 2, 3, 5, \\
\mathbb{Z}/4p\mathbb{Z}, \mathbb{Z}/5p\mathbb{Z}, & \textit{if } p = 2, 3, \\
\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/14\mathbb{Z}, \mathbb{Z}/18\mathbb{Z} & \textit{if } p = 2, \\
\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} & \textit{if } p = 2, \ \textit{and } \zeta_5 \in k, \\
\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{if } p = 3, \ \textit{and } \zeta_4 \in k, \\
\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{if } p = 5.
\end{array}$$

Furthermore, let $G = \mathbb{Z}/m \times \mathbb{Z}/n\mathbb{Z}$ be in this list with $n \mid m$. Then, if $\mathbb{F}$ contains a primitive nth root of unity, there are infinitely many non-isomorphic, non-isotrivial elliptic curves with $E(K)_{\text{tors}} \cong G$. If $p \geq 13$, then Theorem 2.8 is a complete list of possible subgroups $E(K)_{\text{tors}}$.

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

Corollary 2.10 (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*

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

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

In fact, we can parameterize all of the elliptic curves having each of the indicated torsion subgroups in Theorem 2.9. For example, when $p = 5$, a non-isotrivial E/K has a point of order fifteen if and only if it can be written in Tate normal form with

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

Here the point $(0,0)$ is a point of order fifteen. In Table 8 the reader can find parameterizations of all elliptic curves over $\mathbb{F}(T)$ with the torsion structures appearing in Theorem 2.9.

3. Genus One Function Fields

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 2.4, where Levin gives bounds for arbitrary genus. As for p-primary torsion, when $g(\mathcal{C}) = 1$, Theorem 2.4 leads to the the following useful corollary.

Corollary 3.1 (Levin, [7])**.** *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*

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

We will also make use of Proposition 2.6, and an analogous result to that of Theorem 2.8 proven for genus 1. In what follows, we will prove the following result.

Theorem 3.2 (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 $p \le 13$, 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 4 we will start by proving Theorem 4.4, which is an analogue of Cox and Parry's Theorem 2.8 when the genus of $\mathcal{C}$ is one. Then as in [8], starting with characteristic $p \geq 5$, we will use this result and Theorem 2.5 to obtain a curve D which parameterizes non-isotrivial elliptic curves which in addition to having a torsion structure G found in Theorem 4.4, 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 2.6 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 $\mathcal{C}$.

4. Genus one

Let $\mathbb{F}$ be a finite field of characteristic p. By Proposition 2.6, 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 2.6 yield the following useful corollary.

Corollary 4.1. *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 2.6, 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. □

4.1. Prime-to-p torsion.

A large part of our proofs below will involve genus arguments about modular curves $X_1(n, m)$ over $\mathbb{F}_p(\mu_n)$ (see [16, Proposition 7.1]). We start with two statements about modular curves of genus zero and one.

Proposition 4.2 ([1, Proposition 3.7]). *The modular curve[1] $X_1(n, m)$ has genus 0 if and only if (m, n) is one of the following 18 ordered pairs:*

$$\begin{gathered}(2,1),\ (3,1),\ \ldots,\ (10,1),\ (12,1),\\ (2,2),\ (4,2),\ (6,2),\ (8,2),\\ (3,3),\ (6,3),\ (4,4),\ (5,5).\end{gathered}$$

[1] 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 for a precise definition.

Proposition 4.3 (Sutherland, [13] and [14])**.** *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.*

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

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

Theorem 4.4. *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 $E(K)'_{\mathrm{tors}}$ (the rational points of finite order prime to p) is one of*

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

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 $E(K)_{\mathrm{tors}} \cong G$ only if

$$\begin{cases} \mathcal{C} \text{ is isogenous to } X_1(n,m) & \text{if } (m,n) \text{ is in } (1), \\ \mathcal{C} \text{ is any smooth curve} & \text{otherwise.} \end{cases}$$

Proof. Following the proof of [16, Proposition 7.1], suppose $E(K)'_{\mathrm{tors}}$ 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 $G \subset E(K)'_{\mathrm{tors}}$, 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 $g(X(n,m)) \le 1$. Thus, by Propositions 4.2 and 4.3, (m,n) is one of the pairs

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

The torsion subgroups corresponding to Proposition 4.2 have already been shown to appear infinitely often in [8, Section 2]. The only *new* subgroups are those that correspond to a pair in (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 4.1, $\mathcal{C}$ must be *isogenous* to $X_1(N)$. In this case, we can use the optimized equations in [13] to construct examples of elliptic curves with torsion subgroup corresponding to a pair in (1). For example, suppose $p \ne 11$, 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 [13], we can construct the following infinite family of elliptic curves with a point of order 11:

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

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 [13] 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 4.1, $\mathcal{C}$ must be *isogenous* to $X_1(n,m)$. This time, we can use [14] 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 [14], for all $n \geq 0$, the following elliptic curve E_n has $G \subset E_n(K)$:

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

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. $\square$

In the rest of this section, we will follow the strategies of [8] to determine what combinations of p-primary torsion can appear with the subgroups from Theorem 4.4. We will start with $p = 5$, then work case-by-case for primes $p = 2, 3, 7, 11, 13$.

4.2. **Characteristic** $p = 5$. In the spirit of [8, Section 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 4.4 can be easily restated, giving the full picture of prime-to-5 torsion over $\mathbb{F}(\mathcal{C})$ of characteristic 5.

Corollary 4.5. *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*

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

Further, let $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ be in this list with $n \mid m$ and $p \nmid n$, 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

$$\begin{cases} \mathcal{C} \textit{ is isogenous to } X_1(n,m) & \textit{if } (m,n) \textit{ is in } (1), \\ \mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.} \end{cases}$$

Below, we will follow the strategy used in [8]: starting with a group in Corollary 4.5, 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 2.5 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 4.1, 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 2.9.

Theorem 4.6. *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 $E(K)_{\mathrm{tors}}$ 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

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

Proof. Using Corollary 4.5, 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

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

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 2.5 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 4.1, 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 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 (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 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[2], that $C_{55,1}$ is absolutely irreducible. Thus, by Corollary 4.1, 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 4.4 and the parameterizations in [8, Section 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 4.4 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 4.1. 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

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

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. □

[2]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 4.7. 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 the proof of Theorem 4.6, 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:

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

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.

4.3. **Characteristic $p = 2$.** By specializing to $p = 2$, we may state the following corollary to Theorem 4.4, 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 4.8. *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 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 $E(K)_{\mathrm{tors}} \cong G$ only if

$$\begin{cases} \mathcal{C} \text{ is isogenous to } X_1(n,m) & \text{if } (m,n) \text{ is in (1)}, \\ \mathcal{C} \text{ is any smooth curve} & \text{otherwise.} \end{cases}$$

Again, we will start with a group in Corollary 4.8 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 2.9.

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

Theorem 4.9. *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 $E(K)_{\mathrm{tors}}$ is one of*

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

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 $E(K)_{\mathrm{tors}} \cong G$ only if

$$\begin{cases} \mathcal{C} \text{ is isogenous to } X_1(n,m) & \text{if } (m,n) \text{ is in (1) with } 2 \nmid m, \\ \mathcal{C} \text{ is isogenous to a curve in Table 9} & \text{if } G \text{ appears in Table 9}, \\ \mathcal{C} \text{ is any smooth curve} & \text{otherwise.} \end{cases}$$

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

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

From [8], we see $C_{24,1}$, $C_{28,1}$, and $C_{36,1}$ all have genus greater than one, ruling out these torsion structures, and those containing them, from (3). 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 4.1, 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 [8, Section 2.1], 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 [8, Section 2.3], 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) 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

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

$C_{16,1}$ 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, $E^{2^n}_{a,b}$ 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 $E^{2^n}_{a,b}$ 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

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

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

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

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 $E^{2^n}_{a,b}$ 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

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

$E^{2^n}_{a,b}$ 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 $E^{2^n}_{a,b}$, an infinite family of elliptic curves with torsion structure $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ over K. □

4.4. **Characteristic $p = 3$.** Specializing to characteristic $p = 3$, and considering a function field K of genus one, Theorem 4.4 provides the following corollary.

Corollary 4.10. *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*

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

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 $E(K)_{\mathrm{tors}} \cong G$ only if

$$\begin{cases} \mathcal{C} \textit{ is isogenous to } X_1(n,m) & \textit{if } (m,n) \textit{ is in } (1), \\ \mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.} \end{cases}$$

Again, as in Section 4.3, 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 4.11. *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*

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

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

$$\begin{cases} \mathcal{C} \textit{ is isogenous to } X_1(n,m) & \textit{if } (m,n) \textit{ is in } (1) \textit{ with } 3 \nmid m, \\ \mathcal{C} \textit{ is isogenous to a curve in Table 9} & \textit{if } G \textit{ appears in Table 9}, \\ \mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.} \end{cases}$$

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

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

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 [8], 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 (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 4.4. 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 (4) which do not appear in the theorem.

In [8], we see 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 2, where we see that, with the exception of $C_{18,1}$, each of these curves is

$(3^e m, n)$	$C_{3^e m,n}$	$\tilde{C}_{3^e m,n}$
$(18,1)$	$u^9 + (2t^3+t)u^6 + (t^7+t^4)u^3 + t^{13} + 2t^{10} + t^7 = 0$	$u^2 + 2tu + u = t^3 + 2t^2 + t$
$(21,1)$	$t^4 + 2t + 1 = u^2$	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 2. Genus one $C_{3m,n}$ for $p = 3$.

already non-singular. The normalization of $C_{18,1}$ is given, with normalization map $\pi : \tilde{C}_{18,1} \to C_{18,1}$

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 $n \geq 1$:

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

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 $\mathbb{F}(\mathcal{C})$:

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

$\square$

4.5. **Characteristic $p = 7$.** When the characteristic of a genus one function field K is 7, Theorem 4.4 provides the following corollary about prime-to-7 torsion structures for elliptic curves over K.

Corollary 4.12. *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 $E(K)'_{\mathrm{tors}}$ 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 $E(K)_{\mathrm{tors}} \cong G$ only if

$$\begin{cases} \mathcal{C} \text{ is isogenous to } X_1(n,m) & \text{if } (m,n) \text{ is in } (1), \\ \mathcal{C} \text{ is any smooth curve} & \text{otherwise.} \end{cases}$$

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 4.2: Here, we take a curve with torsion structure $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ in Corollary 4.12 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 2.5 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 4.13. *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

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

Proof. Using Corollary 4.12, 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

$$\begin{array}{cl} (7N, 1) & \text{with } N = 3, 4, 6, 8, 9, 11, 12, \\ (14N, 2) & \text{with } N = 1, 2, 3, 4, 6, \\ (21N, 3) & \text{with } N = 1, 2, 3, \\ (28N, 4) & \text{with } N = 1, 2 \\ (42, 6). & \end{array} \tag{5}$$

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 4.2, 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 4.1. Our results are collected in Table 3, and with the exception of $\mathbb{Z}/77\mathbb{Z}$, this table rules out any G from (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 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

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

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.

□

4.6. **Characteristic** $p = 11$**.** For genus one function fields of characteristic 11, Theorem 4.4 yields the following.

Corollary 4.14. *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 $E(K)'_{\text{tors}}$ is one of*

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

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

$$\begin{cases} \mathcal{C} \text{ is isogenous to } X_1(n, m) & \text{if } (m, n) \text{ is in } (1), \\ \mathcal{C} \text{ is any smooth curve} & \text{otherwise.} \end{cases}$$

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 [8, Section 3.3], where the possible torsion subgroups for an elliptic curve over a characteristic 11 were determined over function fields of genus zero. We summarize and reinterpret the results here.

Theorem 4.15. *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*

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

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

$$\begin{cases} \mathcal{C} \textit{ is isogenous to } X_1(n,m) & \textit{if } (m,n) \textit{ is in } (1) \textit{ with } 11 \nmid m, \\ \mathcal{C} \textit{ is any smooth curve} & \textit{otherwise.} \end{cases}$$

Proof. Again, by Theorem 4.4, 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

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

This time, proceeding with our previous strategy, we construct the curves $C_{11m,n}$ in Table 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 4. Curves parameterizing elliptic curves with G torsion over K.

□

Remark 4.16. 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.

4.7. **Characteristic $p = 13$.** For function genus one function fields K of characteristic 13, we find the following specialization of Theorem 4.4.

Corollary 4.17. *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 $E(K)'_{\mathrm{tors}}$ is one of*

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

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 $E(K)_{\mathrm{tors}} \cong G$ only if

$$\begin{cases} \mathcal{C} \text{ is isogenous to } X_1(n, m) & \text{if } (m, n) \text{ is in (1)}, \\ \mathcal{C} \text{ is any smooth curve} & \text{otherwise.} \end{cases}$$

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 4.18. *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*

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

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 $E(K)_{\mathrm{tors}} \cong G$ only if

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

Proof. Again, by Theorem 4.4, 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

$$\begin{array}{cl} (13N, 1) & \text{with } N = 1, 2, \ldots, 12, 14, 15, \\ (26N, 2) & \text{with } N = 1, \ldots, 6 \\ (39N, 3) & \text{with } N = 1, 2, 3, \\ (52N, 4) & \text{with } N = 1, 2 \\ (13N, N) & \text{with } N = 5, 6. \end{array} \tag{7}$$

This time, proceeding with our previous strategy, we construct the curves $C_{13m,n}$, and record their genera in Table 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 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 [15]. Since $j(D) = 0$, we find that

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

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

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.

$\square$

5. 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 paper, and parameterizations where possible. Tables 6 and 7, taken from [8], 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.

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

Table 8, also taken from [8], 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 torsion subgroup G.

The rest of the torsion structures that were found in this paper require that $\mathcal{C}$ be isogenous to a specific curve, D. In Table 9, we collect all of these curves when p divides the order of the torsion subgroup, and in Table 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 [13] and [14].

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 7. One-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
$p = 11$	$a = \frac{(f+3)(f+5)^2(f+9)^2}{3(f+1)(f+4)^4}$	$b = a\frac{(f+1)^2(f+9)}{2(f+4)^3}$	$\mathbb{Z}/11\mathbb{Z}$
$p = 2$	$a = \frac{f(f+1)^3}{f^3+f+1}$	$b = a\frac{1}{f^3+f+1}$	$\mathbb{Z}/14\mathbb{Z}$
$p = 7$	$a = \frac{(f+1)(f+3)^3(f+4)(f+6)}{f(f+2)^2(f+5)}$	$b = a\frac{(f+1)(f+5)^3}{4f(f+2)}$	
$p = 3$	$a = \frac{f^3(f+1)^2}{(f+2)^6}$	$b = a\frac{f(f^4+2f^3+f+1)}{(f+2)^5}$	$\mathbb{Z}/15\mathbb{Z}$
$p = 5$	$a = \frac{(f+1)(f+2)^2(f+4)^3(f^2+2)}{(f+3)^6(f^2+3)}$	$b = a\frac{f(f+4)}{(f+3)^5}$	
$p = 2$	$a = \frac{f(f+1)^2(f^2+f+1)}{f^3+f+1}$	$b = a\frac{(f+1)^2}{f^3+f+1}$	$\mathbb{Z}/18\mathbb{Z}$
$p = 5$	$a = \frac{f(f+1)(f+2)^2(f+3)(f+4)}{(f^2+4f+1)^2}$	$b = a\frac{(f+1)^2(f+3)^2}{4(f^2+4f+1)^2}$	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p = 3,\ i \in \mathbb{F}$	$a = \frac{f(f+1)(f+2)(f^2+2f+2)}{(f^2+f+2)^3}$	$b = a\frac{(f^2+1)^2}{f(f^2+f+2)}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p = 2,\ i \in \mathbb{F}$	$a = \frac{f(f^4+f+1)(f^4+f^3+1)}{(f^2+f+1)^5}$	$b = a\frac{f^2(f^4+f^3+1)^2}{(f^2+f+1)^5}$	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Table 8. One-parameter families of elliptic curves $E_{a,b}/K$ such that $E_{a,b}(K)_{\text{tors}}$ has a subgroup G.

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

References

[1] David A. Cox and Walter R. Parry. Torsion in elliptic curves over $k(t)$. *Compositio Math.*, 41(3):337–354, 1980. 2.1, 2.8, 4.2

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

[3] Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer. On the torsion of elliptic curves over cubic number fields. *Acta Arith.*, 113(3):291–301, 2004. 1.5

[4] Sheldon Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992. 1.4

[5] Monsur Kenku and Fumiyuki Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988. 1.4

[6] Serge Lang and André Néron. Rational points of abelian varieties over function fields. *Amer. J. Math.*, 81:95–118, 1959. 2.3

[7] Martin Levin. On the group of rational points on elliptic curves over function fields. *Amer. J. Math.*, 90:456–462, 1968. 2.4, 2.7, 3.1

[8] Robert J. S. McDonald. Torsion subgroups of elliptic curves over function fields of genus 0. *J. Number Theory*, 193:395–423, 2018. 2.1, 2.2, 3, 4.1, 4.2, 4.2, 4.2, 4.3, 4.4, 4.6, 5, 5

[9] Filip Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. *Math. Res. Lett.*, 23(1):245–272, 2016. 1

[10] Igor R. Shafarevich. *Basic Algebraic Geometry*. Springer-Verlag, 3 edition, 2013. 2

[11] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. 1, 1.3, 2

[12] Andrew Snowden. *Course on Mazur's theorem*. `http://www-personal.umich.edu/~asnowden/teaching/2013/679/index.html`. 1

[13] Andrew Sutherland. *Optimized equations for $X_1(N)$*. `http://math.mit.edu/~drew/X1_optcurves.html`. 4.3, 4.1, 5

[14] Andrew Sutherland. *Optimized equations for $X_1(m, mn)$*. `http://math.mit.edu/~drew/X1mn.html`. 4.3, 4.1, 5

[15] Andrew Sutherland. *Modular polynomials*. `https://math.mit.edu/~drew/ClassicalModPolys.html`. 4.7

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
$p=2$	$a = \frac{(t+1)^2(t^5+t^2u+t^2+t+u)}{t^{10}}$ $\quad b = a\frac{t^6+t^3+t^2+t+u}{t^6}$	$\mathbb{Z}/16\mathbb{Z}$
$p=2$	$a = \frac{t^9+t^6u+t^6+t^5+t^4u+t^3+t^2+t+u}{t^2}$ $\quad b = a(t^5+t^2u+t+u+1)$	$\mathbb{Z}/20\mathbb{Z}$
$p=2$	$a = \frac{(u+1)(tu^6+tu^5+tu+u^6+u^5+u^3+u^2+1)}{u^5(u^5+u^3+1)}$ $\quad b = a\frac{tu^2+tu+u^6+u^5+u^2+u+1}{u(u^5+u^3+1)}$	$\mathbb{Z}/22\mathbb{Z}$
$p=2$	$a = \frac{(t+1)^7(t^2+t+1)^2(t^{12}+t^{10}u+t^9+t^6u+t^5+t^4+t^2+t+u+1)}{t^6(t^4+t^3+1)^2}$ $b = a\frac{t^{13}+t^{12}+t^{11}u+t^{11}+t^{10}u+t^{10}+t^9u+t^8u+t^7+t^6+t^5u+t^4u+t^4+t^3+t^2+tu+u}{(t^4+t^3+1)^2}$	$\mathbb{Z}/30\mathbb{Z}$
$p=2$	$a = \frac{t^2(t^{31}+t^{30}+t^{28}u+t^{28}+t^{27}+t^{24}u+t^{24}+t^{23}+t^{20}u+t^{20}+t^{17}+t^{16}+t^{15}+t^{14}u+t^{14}+t^{12}u+t^{12}+t^{10}+t^9+t^8+t^6u+t^4+t^3+u)}{(t+1)^6(t^2+t+1)^6(t^3+t+1)^6}$ $b = a\frac{(t^2+t+1)^2(t^{12}+t^{10}+t^8+t^5+t^4+t^2u+1)}{(t^3+t+1)^6}$	$\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$p=2$	$a = \frac{t^2(t^{15}+t^{14}+t^{13}+t^{12}u+t^{11}+t^{10}u+t^{10}+t^8u+t^5+t^4+t^3+t^2u+t^2+u)}{(t+1)^6(t^2+t+1)^6}$ $b = a\frac{t^6+t^5+t^2u+1}{(t+1)^2(t^2+t+1)^2}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$p=3$	$a = \frac{(t+1)^3(t+2)^3(t^4+t^3u+t^3+2t^2+2tu+2t+u+2)}{t^9}$ $b = a\frac{(t^7+t^6u+2t^5+2t^4u+2t^3u+2t^3+2t^2+2tu+2t+u+1)}{t^6}$	$\mathbb{Z}/18\mathbb{Z}$
$p=3$	$a = \frac{t^2(t^{10}+2t^9+t^8u+2t^8+2t^7u+t^7+2t^6u+2t^4u+t^4+2t^2u+t^2+tu+2t+u+1)}{(t+2)^3}$ $b = a(t^3+t^2+2t+1)(t^5+2t^4+t^3u+t^3+2t^2u+t^2+tu+t+2)$	$\mathbb{Z}/21\mathbb{Z}$
$p=3$	$a = \frac{(t+2)(t^{10}+t^8u+t^6u+2t^6+t^5+t^4u+2t^3u+t^3+2t^2u+2tu+t+u+1)}{t^9(t+1)^3}$ $b = a\frac{(t^2+2t+2)(t^6+2t^4+t^3u+2t^2u+t^2+tu+u+1)}{t^7(t+1)}$	$\mathbb{Z}/24\mathbb{Z}$
$p=3$	$a = \frac{(t^8u+2t^8+2t^4u+2t^4+2u)}{(t+1)^3(t+2)^3(t^2+1)^3}$ $\quad b = a\frac{t^4(t^4+u+1)}{(t+1)(t+2)(t^2+1)(t^2+t+2)(t^2+2t+2)}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$p=5$	$a = \frac{u(u+2)(tu^4+2tu^3+tu+4t+2u^6+u^5+4u^4+4u^3+3u+1)}{(u+1)(u+3)^7(u+4)}$ $b = a\frac{(tu^4+3tu^3+tu^2+4t+u^6+3u^5+u^4+3u^3+3u+2)}{u(u+3)^5}$	$\mathbb{Z}/20\mathbb{Z}$
$p=7$	$a = \frac{t^2u^6+t^2u^5+4t^2u^4+2t^2u^3+2t^2u^2+t^2+3tu^7+3tu^3+2tu^2+6tu+t+u^8+5u^7+2u^6+u^5+4u^4+2u^3+3u^2+3u+1}{u(u+4)^4(u+6)}$ $b = a\frac{(t^2u^2+t^2u+t^2+3tu^3+3tu^2+5tu+t+u^4+u^3+4u^2+3u+5)}{(u+4)^2}$	$\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p=13$	$a = \frac{(t^6+12t^4u+11t^4+t^3u+3t^3+6t^2u+5t^2+12tu+6t+7u+11)}{(t+4)^5}$ $b = a\frac{(t^3+2t^2u+9t^2+9tu+11t+u+1)}{(t+4)^4}$	$\mathbb{Z}/13\mathbb{Z}$

Table 10. One-parameter families of elliptic curves $E_{a,b}^{p^n}/K$ such that $E_{a,b}(K)_{\text{tors}}$ has a subgroup G for $n \geq 1$.

[16] Douglas Ulmer. Elliptic curves over function fields. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 211–280. Amer. Math. Soc., Providence, RI, 2011. 2, 2, 2.5, 2, 4.1, 4.1

[17] Tom Weston. The modular curves $X_0(11)$ and $X_1(11)$, 2001. 1

Dept. of Mathematics, University of Connecticut, 341 Mansfield Road U1009, Storrs, CT 06269
Email address: `robert.j.mcdonald@uconn.edu`