TORSION SUBGROUPS OF ELLIPTIC CURVES OVER FUNCTION FIELDS OF GENUS 1

ROBERT J.S. MCDONALD

ABSTRACT. Let $k = \mathbb{F}_q$ be a finite field of characteristic p, and $\mathcal{C}$ be a smooth, projective, absolutely irreducible curve of genus one over k. Let $K = k(\mathcal{C})$, 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 which 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

In what follows, p is a prime and $k = \mathbb{F}_q$ for q a power of p. Let $\mathcal{C}$ be a smooth, projective, absolutely irreducible curve over k, and write $K = k(\mathcal{C})$ for its function field. An elliptic curve E/K is a smooth, projective, irreducible curve of genus one, with at least one K-rational point, and can always be written with the affine model

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

and when $p \geq 3$, we can write $E : y^2 = f(x)$ for some monic cubic function f. In this paper, we will be primarily interested in *non-isotrivial* elliptic curves over K, a property which has no clear analogue for elliptic curves over number fields.

Definition 1.1. Assume that $K = \mathbb{F}_q(\mathcal{C})$ is the function field of a curve over a finite field and let E be an elliptic curve over K.

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

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

Theorem 1.2 (Mordell-Weil-Lang-Néron, [2])**.** *Assume that $K = \mathbb{F}_q(\mathcal{C})$ is the function field of a curve over a finite field and let E be an elliptic curve over K. Then, $E(K)$ is a finitely generated abelian group.*

The discriminant, Δ, and j-invariant are defined in the usual way, but in addition, we have the Hasse invariant of E, which we denote $H(E)$. When $p = 2$, $H(E) = a_1$. When $p \geq 3$, then if we write $E : y^2 = f(x)$, the Hasse invariant is the coefficient of x^{p-1} in the expansion of $f^{(p-1)/2}$. The Hasse invariant will be especially useful to us due to the following theorem.

Theorem 1.3 ([10]). *Suppose that E is a non-isotrivial elliptic curve over $K = \mathbb{F}_q(\mathcal{C})$, where q is a power of p. Then, $E(K)$ has a point of order p if and only if $j(E) \in K^p$, and the Hasse invariant is a $(p-1)$st power in $K^\times$.*

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

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

where m divides n, and p does not divide m, and every such group appears for some K (of some genus) and E [10, p. 16]. The following proposition tells us that for any fixed genus g of $\mathcal{C}$ and characteristic p, there are only finitely many possibilities for m and n.

Proposition 1.4 (Ulmer, [10]). *Let g be the genus of $\mathcal{C}$. Then, there is a finite (and effectively calculable) list of groups depending only on g and p, such that for any non-isotrivial elliptic curve E over K, the group $E(K)_{\text{tors}}$ appears on the list.*

That is, the list of possible torsion subgroups for an elliptic curve E over a function field $\mathbb{F}_q(\mathcal{C})$ depends only on the genus of $\mathcal{C}$, and the characteristic of $\mathbb{F}_q$. A natural question arises: fixing a genus g, what is this list?

1.1. **When $\mathcal{C}$ has genus zero.** In this section, we assume $\mathcal{C}$ is a smooth projective of genus zero over $k = \mathbb{F}^q$, q a power of p. We have $\mathcal{C} \cong \mathbb{P}^1$, so that $K \cong k(\mathbb{P}^1) = k(T)$, the field of rational functions in one variable with coefficients in k. In this setting, the torsion subgroups possible for an elliptic curve E/K have been completely classified. We begin with a result about the prime-to-p torsion of E from 1980.

Theorem 1.5 (Cox, Parry, [1]). *Let $K = \mathbb{F}_q(T)$ for q a power of $p \neq 2, 3$. Let E/K be non-isotrivial. Then, $E(K)'_{\text{tors}}$ (the rational points of finite order prime-to-p) is one of*

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

Further, let $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ such that G is in this list. Then, if $p \nmid m$ and $\zeta_n \in \mathbb{F}_q$, there is a non-isotrivial elliptic curve with $E(K)'_{\text{tors}} \cong G$.

In fact, using Tate normal form for an elliptic curve, for example in [4, Section 2], one can write down explicit parameterizations for all elliptic curves with torsion subgroup appearing in Theorem 1.5. Doing this, one finds that given $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ from Cox and Parry's list, if $p \nmid m$ and $\zeta_n \in \mathbb{F}_q$, there are in fact *infinitely many* non-isotrivial elliptic curves with $E(K)'_{\text{tors}} \cong G$. We will prove a theorem of this type for genus one in a later section.

As for p-primary torsion, we have the following useful fact, due to Levin.

Corollary 1.6 (Levin, [3]). *Let $k = \mathbb{F}_q$ with q a power of p, $K = k(T)$, and E/K an elliptic curve. Suppose $p^e \mid \#E(K)_{\text{tors}}$. Then, Then, we have*

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

The following theorem classifies the full torsion subgroups possible for an elliptic curve over $K = k(T)$. Case by case for each p, the general strategy for its proof involves starting with an

$E(K)'_{\text{tors}}$ from Theorem 1.5 written in Tate normal form, and using the Hasse invariant to attach a point of order p.

Theorem 1.7 (M., [4]). *Let $k = \mathbb{F}_q$ for q a power of p. Set $K = k(T)$, 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 1.5 (which holds valid even when $p = 2, 3$). If $p \leq 11$, and $p \mid \#E(K)_{\text{tors}}$, then $E(K)_{\text{tors}}$ is isomorphic to one of the following groups:*

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

Further, every group in this list appears infinitely often as $E(K)_{\text{tors}}$ for some elliptic curve. On the other hand, if $p \geq 13$, then Theorem 1.5 is a complete list of possible subgroups $E(K)_{\text{tors}}$.

Again, elliptic curves with each of the new subgroups appearing in this list (those not appearing in Cox and Parry's list) can be parameterized using Tate normal form, as in [4, Section 5].

1.2. **When $\mathcal{C}$ has genus greater than zero.** Again, let $k = \mathbb{F}^q$, q a power of p, $\mathcal{C}$ be a smooth projective of arbitrary genus ≥ 1 over k, and $K = k(\mathcal{C})$. Less is known for this setting. One useful result is the bounds on the prime-to-p torsion of E, which in [3], Levin gives for arbitrary genus.

Theorem 1.8 (Levin, [3]). *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 $p^e \mid \#E(K)_{\text{tors}}$ for $e \geq 1$, then*

$$p \leq 7 + 4(1 + 3 \cdot g(K))^{\frac{1}{2}}$$

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

where h_ℓ is found in [3, pp. 460–461].

For example, when $g(\mathcal{C}) = 1$, we obtain the following corollary about the p-primary torsion of an elliptic curve E/K.

Corollary 1.9 (Levin, [3]). *Let $\mathcal{C}$ be a smooth, projective curve of genus one over $k = \mathbb{F}_q$ with q a power of p. Let $K = k(\mathcal{C})$. and E/K be an elliptic curve. Suppose $p^e \mid \#E(K)_{\text{tors}}$. Then,*

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

The following proposition, and it's corollary in Section 2, will also be useful. It was stated for genus $g = 0$ in [4], but can an analogous argument can be adapted to arbitrary genus.

Proposition 1.10. *Let k be a finite field of characteristic p, C/k and D/k be a projective, absolutely irreducible curves, with C smooth, and let $K = k(C)$. If the genus of D is greater than that of C, then every point in $D(K)$ is constant.*

Proof. The proof is identical to that of [4, Proposition 1.1]. Let $\pi : \tilde{D} \to D$ be the normalization map associated to D, which is a birational morphism on irreducible components of D [5, 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 $K = k(C)$, and D is written with coefficients in k, we obtain the rational map

$$\psi : C/k \to D/k \text{ by } t \mapsto P_t.$$

Since C is smooth, ψ is a morphism [6, 2.1], and because P is non-constant, ψ is non-constant, and therefore surjective [6, 2.3], hence dominant. so that defining $\phi : C \to \tilde{D}$ by $\phi = \pi^{-1} \circ \psi$, we obtain a non-constant rational map.

$$\begin{array}{ccc} & & \tilde{D} \\ & \overset{\phi}{\nearrow} & \big\downarrow \pi \\ C & \xrightarrow[\psi]{} & D \end{array}$$

Now, $\phi : C \to \tilde{D}$ is a map of smooth curves, so by [6, 2.12], we can factor ϕ as

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

where α is the q-th power Frobenius map (q the cardinality of k), and β is separable, and non-constant by assumption. Since α is an automorphism of C, we may assume ϕ is separable, and apply the Hurwitz formula:

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

But this means $g(C) \geq g(D)$, which is a contradiction. Thus, ϕ, and therefore ψ, must be constant, and no such point P can exist. □

In the sections to follow, we will prove the following result.

Theorem 1.11 (M)**.** *Let C be a curve of genus 1 over $\mathbb{F}_q$, for $q = p^n$, and let $K = \mathbb{F}_q(C)$. Let E/K be non-isotrivial. If $p \nmid \#E(K)_{\text{tors}}$, then $E(K)_{\text{tors}}$ is as in Theorem* **??***. If $p \mid \#E(K)_{\text{tors}}$, then $p \leq 13$, and $E(K)_{\text{tors}}$ is one of*

$\mathbb{Z}/p\mathbb{Z}$	*if* $p = 2, 3, 5, 7, 11, 13$,
$\mathbb{Z}/2p\mathbb{Z}, \mathbb{Z}/2p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	*if* $p = 3, 5, 7$,
$\mathbb{Z}/3p\mathbb{Z}, \mathbb{Z}/4p\mathbb{Z}$	*if* $p = 2, 3, 5$
$\mathbb{Z}/5p\mathbb{Z}, \mathbb{Z}/6p\mathbb{Z}, \mathbb{Z}/7p\mathbb{Z}, \mathbb{Z}/8p\mathbb{Z}$	*if* $p = 2, 3$,
$\mathbb{Z}/2N\mathbb{Z}$	*for* $N = 9, 10, 11, 15$, *if* $p = 2$,
$\mathbb{Z}/6N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	*for* $N = 1, 2, 3$, *if* $p = 2$,
$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$	*if* $p = 2$,
$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	*if* $p = 3$,

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 Section 2 we will start by proving Theorem 2.2, which is an analogue of Cox and Parry's Theorem 1.5 when the genus of $\mathcal{C}$ is one. Then, as in [4], starting with characteristic $p \geq 5$, we will use this result and Theorem 1.3 to obtain a curve C which parameterizes non-isotrivial elliptic

curves which in addition to having a torsion structure G found in Theorem 2.2, also have a point of order p. In each case, C will be irreducible with coefficients in $\mathbb{F}_q$. If C 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 C. If C has genus greater than one, then we will use Proposition 1.10 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 $\mathcal{C}$.

Acknowledgements. I would like to thank Keith Conrad, Álvaro Lozano-Robledo, and Liang Xiao for their continued support and insight. I would especially like to thank Harris Daniels for the use of his computer to calculate the genus and irreducibility of several of the larger curves (in particular $C_{33,1}$, $C_{55,1}$, and $C_{77,1}$) that appear in this paper, calculations that often took several days. Finally, I would like to thank the referees for their comments and revisions.

2. Genus one

Let $k = \mathbb{F}_q$ for q a power of p. By Proposition 1.10, given two curves D/k and a smooth C/k, and $K = k(C)$ we know that $D(K)$ has no non-constant points if $g(D) > g(C)$, but what if they are equal? Certainly, in this case, no contradiction comes from the Hurwitz formula. When $g(C) = g(D) = 1$, in fact, the Hurwitz fromula, and the proof of Proposition 1.10 yield the following useful corollary.

Corollary 2.1. *Let k be a finite field of characteristic p, C/k and D/k be a projective, absolutely irreducible curves of genus one, with C smooth, and let $K = k(C)$. Then, if $D(K)$ contains a non-constant point, C is isogenous to $\tilde{D}$, where $\tilde{D}$ is the normalization of D.*

Proof. like in the proof of Proposition 1.10, a non-constant point P on D induces a non-constant, separable morphism between curves

$$\phi : C \to \tilde{D}, \text{ defined over } k$$

where $\tilde{D}$ is the normalization of D, by composing the map $t \mapsto P_t$ on D, with the normalization map. Since C and $\tilde{D}$ are genus one curves over a finite field, they are elliptic curves, and without loss of generality (by a change of variables) we may assume that the map ϕ is an isogeny. □

2.1. Prime to p torsion.

We start with an analogue of Cox and Parry's theorem for genus 1.

Theorem 2.2. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}_q$, for q a power of p, and let $K = \mathbb{F}_q(\mathcal{C})$. Let E/K be non-isotrivial. Then, $E(K)'_{\text{tors}}$ (the rational points of finite order prime-to-p) is one of*

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

Further, let $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ such that G is in this list. Then, if $p \nmid m$ and $\zeta_n \in \mathbb{F}_q$, there are infinitely many non-isotrivial elliptic curves with $E(K)'_{\text{tors}} \cong G$ for some $\mathcal{C}$.

Proof. Following the proof of [10, Proposition 7.1] , $E(K)'_{\text{tors}}$ has the form $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ where $n \mid m$ and $p \nmid n$. The modular curve $X_1(n,m)$ defined over $\mathbb{F}_p(\mu_n)$ is a coarse moduli space for elliptic curves with $G \subset E(K)'_{\text{tors}}$. This induces a non-constant map $\mathcal{C} \to X_1(n,m)$. By the Riemann-Hurwitz formula, since $g(\mathcal{C}) = 1$, we must have $g(X(n,m)) \leq 1$. Thus, (m,n) is one of the pairs

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

This shows that $E(K)'_{\text{tors}}$ must be one of the groups listed in the proposition.

The Cox and Parry list has already been shown to appear infinitely often above. The only *new* subgroups are $\mathbb{Z}/N\mathbb{Z}$ with $N = 11,14,15$, (recall, $\mathbb{Z}/11\mathbb{Z}$ appeared before as p-primary torsion when $p = 11$), $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and $(\mathbb{Z}/6\mathbb{Z})^2$. We need only show examples of elliptic curves with these new torsion subgroups appearing over $\mathbb{F}_q(\mathcal{C})$ for some $\mathcal{C}$.

If E has a point of order N, and $X_1(N) := X_1(1,N)$ has genus one, then by Corollary 2.1, $\mathcal{C}$ must be *isogenous* to $X_1(N)$. In this case, we can optimized equations in [7], to construct examples of elliptic curves with torsion subgroup not appearing in Cox and Parry's list. For example, suppose $p \neq 11$, and let $k = \mathbb{F}_q$ for q a power of 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 $\mathbb{F}_q$. If we take the case where $\mathcal{C} = X_1(11)$, for example, then $K = k(X_1(11)) = k(t,u)$, and using [7], we can construct the following infinite family of elliptic curves with a point of order 11:

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

If, on the other hand suppose $\mathcal{C}$ is only isogenous to $X_1(11)$, and $K = k(\mathcal{C})$. Then, we can use the induced map $\phi : k(X_1(11)) \to K$ by $u \mapsto u_\phi \in K$ and $t \mapsto t_\phi \in K$ and obtain the following infinite family of elliptic curves with a point of order 11:

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

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

Finally, if E has torsion structure $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, and and $X_1(n,m)$ has genus one, then $\mathcal{C}$ must be *isogenous* to $X_1(n,m)$. This time, we can use [8] to construct examples. For example, suppose $p \neq 2,5$, and let $k = \mathbb{F}_q$ for q a power of p. If E/K has torsion structure $G = \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 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 $K = k(X_1(2,10)) = k(t,u)$, then using [8], for all $n \geq 0$, the following elliptic curve has torsion structure G:

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

Again, infinite families of elliptic curves containing the remaining groups from the theorem can be realized over the right K by using a similar strategy. □

In the rest of this section, we will follow the strategies of [4] to determine what combinations of p-primary torsion can appear with the subgroups from Theorem 2.2.

2.2. **The case when $p = 5$.** For $p = 5$, Theorem 2.2 can be restated in the following way

Corollary 2.3. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}_q$, for q a power of 5, and let $K = \mathbb{F}_q(\mathcal{C})$. Let E/K be non-isotrivial. Then, $E(K)'_{\text{tors}}$ (the rational points of finite order prime-to-p) is one of*

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

Further, let $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ such that G is in this list with $n \mid m$. Then, if $5 \nmid m$ and $\zeta_n \in \mathbb{F}_q$, there are infinitely many non-isotrivial elliptic curves with $E(K)'_{\text{tors}} \cong G$ for some $\mathcal{C}$.

Below, we will follow the strategy used in [4]: starting with a group in Corollary 2.3, when possible, we write a curve in Tate normal form E_t parameterizing torsion structure $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for some $t \in K$ (otherwise we use division polynomials). If we then write the curve in short Weiertrass form $E_t : y^2 = x^3 + A(t)x + B(t)$. If we assume that E_t has torsion structure $G = \mathbb{Z}/5m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, that is, if it has an additional point of order 5, then we can use Theorem 1.3 to say

$$H(E_{A,B}) = 2A(t) = u^4.$$

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_t/K. By Proposition 1.10, 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 1.7.

Theorem 2.4. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}_q$, for q a power of 5, and let $K = \mathbb{F}_q(\mathcal{C})$. Let E/K be non-isotrivial. Then, $E(K)_{\text{tors}}$ (the rational points of finite order prime-to-p) is one of*

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

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

Proof. Using Theorem 2.2, and the fact that by Levin, E can have a point of 5-primary order at most 5, we need to rule or confirm the existence of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $(5m, n)$ coming from

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

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. We begin ruling 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 Tate normal form for elliptic curves with a point of order 6:

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

Since E_t has a point of order 5, by Theorem 1.3 we must have

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

Since u and t are both in K, and t 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 k, and has genus 3. However, by Proposition 1.10, we see that a non-constant point on $C_{30,1}$ would induce a map $C \to C_{30,1}$, 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. With the exception of

$G = \mathbb{Z}/5m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$	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 $m \geq 4$.

$\mathbb{Z}/55\mathbb{Z}$, this table rules out any torsion structure G from (1) $\#G \geq 40$ or a point of order ≥ 30.

As for points of order 55, using a similar strategy, we can start with E/K in the form $E : y^2 + (1-t)xy - ty = x^3 - tx^3$. Solutions, (x,t), 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, $C_{55,1}$, who's genus and irreducibility were quite difficult to compute. Magma output that $C_{55,1}$ has genus 11 after a 100 hour computation. After showing case-by-case that $C_{55,1}$ was irreducible over $\mathbb{F}_q$, for $q = p^n$, $n = 1, \ldots, 1000$, Magma finally determined (after 468 hours[1]) that $C_{55,1}$ is absolutely irreducible. Thus, by Proposition 1.10, no such points exist, and $\mathbb{Z}/55\mathbb{Z}$ torsion structure is impossible for an elliptic curve over K.

With the exception of $\mathbb{Z}/20\mathbb{Z}$, we have already seen from Theorem 2.2 and the parameterizations in [4], that all groups in the theorem appear infinitely often as the torsion subgroup of an elliptic curve E/K, for the right K. 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 2.1. In this case, $C_{20,1}$ is already non-singular. Thus, we may take, for example, the case when $\mathcal{C} = C_{20,1} : t^2 + t + 1 - u^4$, and $\mathbb{F}_q(\mathcal{C}) = \mathbb{F}_q(C_{20,1}) = \mathbb{F}_q(t,u)$. In this case, the following family gives elliptic curves with a point of order 20 for all n:

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

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

since $H(E_n) = (u^{5^n})^4 \in K^4$ 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 $\phi : k(C_{20,1}) \to K$ with $t \mapsto t_\phi \in K$ and $u \mapsto u_\phi \in K$, to construct

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

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

Example 2.5. Over $K = \mathbb{F}_q(\mathcal{C})$, curves with points of order 4 can be written in the form $E_t : y^2 + xy - ty = x^3 - tx^2$ for some $t \in K$. If, in addition, E has a point of order 5, then we must have a point on the curve

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

D is a base extension of a curve over $\mathbb{F}_5$. It's already a smooth, but we can write it in short Weierstrass form $D_0 : u^2 = t^3 + 3t$, with the isomorphism $\pi : D_0 \to D$ 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 $k = \mathbb{F}_5$, 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 $\mathbb{F}(t, u) = \mathbb{F}_q(D_0)$, the following is an infinite family of elliptic curves with a point of order 20:

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

Over $\mathbb{F}_{25}$, The curve D_0 is isogenous to the curve $D_1 : u^2 = t^3 + 3t + \sqrt{3}$ via the isogeny:

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

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

2.3. **The case when $p = 7$.** For $k = \mathbb{F}_q$, q a power of 7, and $K = k(\mathcal{C})$ for a smooth curve $\mathcal{C}$ over k, we can use the same strategies as above, to conclude the following.

Theorem 2.6. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}_q$, for q a power of 7, and let $K = \mathbb{F}_q(\mathcal{C})$. Let E/K be non-isotrivial. Then, $E(K)_{\text{tors}}$ is one of*

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

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

Proof. Using Theorem 2.2, 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 $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with (n, m) coming from

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

We have already seen above that the torsion structure $\mathbb{Z}/14\mathbb{Z}$ can appear infinitely often, for the right K. Again, we can construct curves $C_{7m,n}$ as in Section 2.2, by starting with a curve in 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 $E : y^2 = x^3 + A(t)x + B(t)$, we need

$$H(E_{A,B}) = 3B(t) = u^6.$$

Let $C_{7m,n}$ 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 $\mathbb{F}_q$, and we conclude that the torsion structure is impossible for an elliptic curve defined over K if $g(C_{7m,n}) > 1 = g(C)$ by Proposition 1.10. Our results are collected in Table 2, and with the exception of $\mathbb{Z}/77\mathbb{Z}$, this table rules out any torsion structure G from (2) with a

$G = \mathbb{Z}/7m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$	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 2. Ruling out G torsion over K for $m \geq 4$.

point of order ≥ 28.

For points of order 77, we may again start with E/K in Tate normal form, parameterized by t, such that $(0, 0)$ has order 7. Solutions, (x, t), 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 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 non-singular, so we may take as an example the case where $\mathcal{C} = C_{14,2}$, and $\mathbb{F}_q(\mathcal{C}) = \mathbb{F}_q(C_{14,2}) = \mathbb{F}_q(a,b)$. 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 $\phi : C_{14,2} \to \mathcal{C}$ is an isogeny between curves, then

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

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

□

2.4. **The case when $p = 11$.**

Theorem 2.7. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}_q$, for q a power of 11, and let $K = \mathbb{F}_q(\mathcal{C})$. Let E/K be non-isotrivial. Then, $E(K)_{\text{tors}}$ is one of*

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

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

Proof. Again, by Theorem 2.2, and the fact that E can have a point of 11-primary order at most 11, we need to rule or confirm the existence of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with (n, m) coming from

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

This time, proceeding with our previous strategy, we construct the curves $C_{11m,n}$ in Table 3, which rules out every torsion structure with a point of order ≥ 22, thus proving the theorem.

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

Table 3. Curves parameterizing elliptic curves with G torsion over K.

□

2.5. **The case when $p = 13$.**

Theorem 2.8. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}_q$, for q a power of 13, and let $K = \mathbb{F}_q(\mathcal{C})$. Let E/K be non-isotrivial. Then, $E(K)_{\text{tors}}$ is one of*

$$\begin{array}{cc} \mathbb{Z}/N\mathbb{Z} & \text{with } N = 1, \dots, 15, \text{ (and possibly 143, see Remark 2.9)} \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{with } N = 1, \dots, 6 \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{with } N = 1, 2, 3, \\ \mathbb{Z}/4N\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{with } N = 1, 2, \\ (\mathbb{Z}/N\mathbb{Z})^2 & \text{with } N = 5, 6. \end{array}$$

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

Proof. Again, by Theorem 2.2, and the fact that E can have a point of 13-primary order at most 13, we need to rule or confirm the existence of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with (n, m) coming from

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

This time, proceeding with our previous strategy, we construct the curves $C_{13m,n}$ in Table 4, which rules out every torsion structure with a point of order ≥ 26, with the exception of $143 = 13 \cdot 11$.

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

Table 4. Curves parameterizing elliptic curves with G torsion over K.

To see a points of order 13, we suppose $E_{t,u} : y^2 + (1-t)xy - uy = x^3 - ux^2$ for $t, u \in K$, and set

$$\begin{aligned} \lambda_{13} = u^{-56}\psi_{13}\big((0,0)\big) = {} & t^{10} + 12t^9u^2 + 7t^8u^2 + 6t^8u + 5t^7u^3 + 5t^7u^2 + 3t^7u + 11t^6u^3 + \\ & + t^6u + 4t^5u^4 + 8t^5u^3 + 7t^5u^2 + 11t^4u^4 + 2t^4u^3 + 4t^3u^5 + 6t^3u^4 + 2t^2u^5 + 7tu^6 + u^7, \end{aligned}$$

where ψ_{13} is the thirteenth division polynomial. If $(0,0)$ has order 13, then we must have that (t, u) is a point on $C_{13,1} : \lambda_{13} = 0$. 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 $\pi : \tilde{C}_{13,1} \to C_{13,1}$ by

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

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 $K = \mathbb{F}_q(\tilde{C}_{13,1}) = \mathbb{F}_q(t,u)$ 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 $\phi : \mathcal{C} \to \tilde{C}_{13,1}$ is an isogeny, then replacing a and b with $\phi(a)$ and $\phi(b)$ respectively gives an infinite family of curves with a point of order 13. □

Remark 2.9. Recall, from above, that if E/K has a point of order 11, then 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 C is isogenous to $C_{13,1}$, so that there must be an isogeny, defined over $\mathbb{F}_q$, from $C_{13,1}$ to D. If we can show that no such isogeny exists, then points of order 143 are impossible over K.

2.6. **The case when $p = 3$.**

Theorem 2.10. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}_q$, for q a power of 3, and let $K = \mathbb{F}_q(\mathcal{C})$. Let E/K be non-isotrivial. Then, $E(K)_{\text{tors}}$ is one of*

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

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

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 $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with (n,m) coming from

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

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

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

We, again, construct curves $C_{3m,n}$ by combining with Tate normal form, or with division polynomials as in [4], 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 (5), and those containing them.

To rule out points of order 36, we begin with $E_{a,b}$ written in Tate normal form for points of order 9 and look at the division polynomial $\phi_7(x) = 0$. In this case, $\phi_7 = fg\lambda_{36}$, 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 42, we begin with $E_{a,b}$ in Tate normal form for points of order 7, and look at $\phi_6(x) = 0$. This time, $\phi_6 = xfg\lambda_{42}$, where f, g and λ_{42} are each irreducible polynomials of degree 8, 17 and 37 respectively. Here, $f = 0$ defines a genus 1 curve that corresponds to points of order 14, and $g = 0$ defines a genus 1 curve that corresponds to points of order 21 (which, again, we will see below). The irreducible curve defined by $C_{42,1} : \lambda_{42} = 0$ corresponds to points of order 42, but is again of genus 7, so these points are impossible.

To rule out points of order 63, we begin with a curve $E_{a,b}$ written in 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 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 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 Tate normal form over a field of characteristic 3, we have

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

We need $H(E_{a,b} = u^2$ for some $u \in K$, 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 $t = b/a^3$. This way, we can write $E_{a,b}$ using the single parameter t:

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

where $(0,0)$ is a point of order 3. We find that the division polynomial $\phi_{11}(x) = x\lambda_{11,1}(x)$, where $\lambda_{11,1}$ is a degree 120 polynomial with coefficients in k. 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 Tate normal form E_t for curves with a point of order 9. Then, looking at the division polynomial $\phi_4(x)$, we see that ϕ_4 factors as $\phi_4 = fg\lambda_{36,1}$, where f, g and $\lambda_{36,1}$ are functions in x and t of degrees 5, 10, and 45 respectively, with coefficients in k. 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 Tate normal form E_t for curves with a point of order 7 and look at $\phi_6(x)$. Here, ϕ_6 factors as $\phi_6 = fgh\lambda_{42,1}$, 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 k. 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 2.2. 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 Tate normal form E_t 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 k. 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 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

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

In characteristic 3, the Hasse invariant for this curve is

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

Here, since the denominator is a square, we will have $H(E)$ a square in $K^\times$ if and only if the numerator $t^8 + 2t^7 + 2t^5 + 2t^4 + t^3 + t + 1 = u^2$ for some $u \in K^\times$. But this equation defines 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 (5) which do not appear in the theorem.

In [4], it was also determined that $C_{3m,n}$ has genus 1 when $(3m, n) = (18, 1)$, $(21, 1)$, $(24, 1)$, 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 of the $\tilde{C}_{3m,n}$. As a reminder, these curves appears in Table 5, where we see that, with the exception of $C_{18,1}$, each of

$(3m, n)$	$C_{3m,n}$	$\tilde{C}_{3m,n}$
$(18, 1)$	$u^9 + (2t^3 + t)u^6 + (t^7 + t^4)u^3 + t^{13} + 2t^{10} + t^7 = 0$	$u^2 + 2tu + u = t^3 + 2t^2 + t$
$(21, 1)$	$t^4 + 2t + 1 = u^2$	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 5. Genus one $C_{3m,n}$ for $p = 3$.

these curves is 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 $K = \mathbb{F}_q(\tilde{C}_{18,1}) = \mathbb{F}_q(t, u)$, then the following is an infinite family of elliptic curves with a point of order 18:

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

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

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

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

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

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

Finally, if $\phi : \mathcal{C} \to C_{12,4}$ 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 $\mathbb{F}_q(\mathcal{C})$:

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

□

2.7. **The case when $p = 2$.**

Theorem 2.11. *Let $\mathcal{C}$ be a curve of genus 1 over $\mathbb{F}_q$, for q a power of 2, and let $K = \mathbb{F}_q(\mathcal{C})$. Let E/K be non-isotrivial. Then, $E(K)_{\text{tors}}$ is one of*

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

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

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

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

From [4], we recall $C_{24,1}$, $C_{28,1}$, and $C_{36,1}$ all have genus greater than one, ruling out these torsion structures, and those containing them, from (6). 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 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 k. By Proposition 1.10, 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 Tate normal form for a curve with a point of order four, and looking at $\phi_{11}(x) = 0$, we see that $\phi_{11}(E_{a,b}) = x\lambda_{44}$, 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 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 k, again showing that points of order 60 are impossible.

From [4], 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 as

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

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, $C_{30,3} : \lambda_{30,3}$ is absolutely irreducible of genus 9, showing that the torsion subgroup $\mathbb{Z}/30 \times \mathbb{Z}/6\mathbb{Z}$ is impossible for a non-isotrivial elliptic curve over K.

Finally, again from [4], 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 Tate normal form 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 $x^4 f \lambda_{20,5}$ where f 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 k and is irreducible of genus 9, showing that this torsion structure is impossible over K.

We have ruled out every torsion structure from 6 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's left is to show that each of these pairs appears infinitely often, as well. 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 $K = \mathbb{F}_q(\tilde{C}_{16,1}) = \mathbb{F}_q(t,u)$, 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.

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 $K := \mathbb{F}_q(\tilde{C}_{20,1}) = \mathbb{F}_q(t,u)$, 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 $X_1(11) : u^2 + (t^2+1)u + t = 0$. If $\mathcal{C} = X_1(11)$, and $K = \mathbb{F}_q(X_1(11)) = \mathbb{F}_q(t,u)$ then if

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

the elliptic curve $E^1_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2$ has a point of order 11. Trivially, $H(E_0) \in K$, so we only need $j(E)$ to be a square. Thus, $E^{2^n}_{a,b}$ is already 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 $K = \mathbb{F}_q(\tilde{C}_{30,1}) = \mathbb{F}_q(t,u)$, 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 Tate normal form with

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

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

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

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 $K = \mathbb{F}_q(\tilde{C}_{16,1}) = \mathbb{F}_q(t,u)$, 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 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

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

Thus, we again have the example where $\mathcal{C} = \tilde{C}_{18,3}$, and $K = \mathbb{F}_q(\tilde{C}_{18,3}) = \mathbb{F}_q(t,u)$: by setting

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

$E^{2^n}_{a,b}$ 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 $\phi : \mathbb{F}_q(C_{2m,n}) \to K$ such that $t \mapsto= t_\phi$ and $u \mapsto u_\phi$. Then, by replacing t by t_ϕ and u

by u_ϕ in each equation, we can find $E_{a,b}^{2^n}$, an infinite family of elliptic curves with torsion structure $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ over K. □

3. Explicit Parameterizations and Isogenies

Let k be a finite field of characteristic p, and set $K = k(\mathcal{C})$ 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 [4], 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	$y^2 + axy + by = x^3$	$\mathbb{Z}/3\mathbb{Z}$
$p \neq 3,\ \zeta_3 \in k$	$y^2 + xy + by = x^3;\ b = \frac{f^2+f+1}{3(f+2)^3}$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

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

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	$a = \frac{f(1-2f)(3f^2-3f+1)}{(f-1)^3}$	$b = -a \cdot \frac{2f^2-2f+1}{f-1}$	$\mathbb{Z}/12\mathbb{Z}$
$p \neq 2$	$a = 0$	$b = f^2 - \frac{1}{16}$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p \neq 2$	$a = \frac{10-2f}{f^2-9}$	$b = \frac{-2(f-1)^2(f-5)}{(f^2-9)^2}$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p \neq 2$	$a = \frac{(2f+1)(8f^2+4f+1)}{2(4f+1)(8f^2-1)f}$	$b = \frac{(2f+1)(8f^2+4f+1)}{(8f^2-1)^2}$	$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p \neq 3,\ \zeta_3 \in k$	$a = -\frac{f(f^2+f+1)}{(f-1)^3}$	$b = -a\frac{4f^2-2f+1}{(f-1)^3}$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$p \neq 4,\ i \in k$	$a = 0$	$b = f^4 - \frac{1}{16}$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$p \neq 5,\ \zeta_5 \in k$	$a = \frac{f^4+2f^3+4f^2+3f+1}{f^5-3f^4+4f^3-2f^2+f}$	$b = a$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Table 7. One-parameter familes of elliptic curves $E_{a,b}/K$ such that $G \subset E_{a,b}(K)_{\text{tors}}$.

Table 8, also taken from [4], 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.

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

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

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 $K = k(D) = k(t,u)$. For prime-to-p torsion, we refer the reader to the tables in [9].

Characteristic	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.

Char(K)	$E^{p^n}_{a,b} : y^2 + (1-a)^{p^n} xy - b^{p^n} y = x^3 - b^{p^n} x^2$, $n \geq 1$			G
$p = 2$	$a = \frac{(2f-1)(f-1)}{f}$,	$b = af$,	$f = \frac{t^3+t^2+t+1+u}{t^4}$,	$\mathbb{Z}/16\mathbb{Z}$
$p = 2$	$a = -\frac{f(f-1)(2f-1)}{f^2-3f+1}$,	$b = -a\frac{f^2}{f^2-3f+1}$,	$f = \frac{t^4+t^3+t+u+1}{t^4+1}$	$\mathbb{Z}/20\mathbb{Z}$
$p = 2$	$a = (u+1)t + u^2 + u$,	$b = (u^3+u^2)t + u^3 + u^2$		$\mathbb{Z}/22\mathbb{Z}$
$p = 2$	$a = -\frac{f(f-1)(2f-1)}{f^2-3f+1}$,	$b = -a\frac{f^2}{f^2-3f+1}$,	$f = \frac{t^5u+t^4u+t^2+1}{t^8+t^7+t^5+t^4+t^3+t^2+1}$	$\mathbb{Z}/30\mathbb{Z}$
$p = 2$	$a = -\frac{f(f^2+f+1)}{(f-1)^3}$,	$b = -a\frac{4f^2-2f+1}{(f-1)^3}$,	$f = \frac{t^3+t^2+u}{t^4+1}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$p = 2$	$a = -\frac{f(f^2+f+1)}{(f-1)^3}$,	$b = -a\frac{4f^2-2f+1}{(f-1)^3}$,	$f = \frac{t^2u^2+tu^4+tu^3+tu+t+u^5+u^3+1}{t^2u^4+t^2u^2+u^6+u^5+u^3+u^2+1}$	$\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$p = 3$	$a = f$	$b = f + f^2$	$f = (2t^3 + t + 2)u + 2t^4 + t^3 + t^2 + t + 2$	$\mathbb{Z}/18\mathbb{Z}$
$p = 3$	$a = t^2 - t$	$b = at$		$\mathbb{Z}/21\mathbb{Z}$
$p = 3$	$a = \frac{(2t-1)(t-1)}{t}$,	$b = at$		$\mathbb{Z}/24\mathbb{Z}$
$p = 3$	$a = 0$,	$b = t^4 - \frac{1}{16}$		$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$p = 5$	$a = 0$	$b = t$		$\mathbb{Z}/20\mathbb{Z}$
$p = 7$	$a = t$	$b = u$		$\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$p = 13$	$a = \frac{4t^6+(9u+5)t^4+(4u+12)t^3+(11u+7)t^2+(9u+11)t+2u+5}{(t+4)^5}$			$\mathbb{Z}/13\mathbb{Z}$
	$b = \frac{t^9+(11u+11)t^8+(5u+10)t^7+(11u+9)t^6+(8u+4)t^5+6ut^4+(5u+2)t^3+(4u+8)t^2+(u+10)t+8u+3}{(t+4)^9}$			

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

For other examples where $\mathcal{C}$ is not isomorphic to D, we suppose that $D \to \mathcal{C}$ is an isogeny, and $\phi : k(\mathcal{C}) \to k(D)$ is the induced map on the function fields of D and $\mathcal{C}$. Then writing $k(\mathcal{C}) = k(t, s)$, and replacing t with $\phi(t)$, and u with $\phi(u)$ in the parameterizations above gives an infinite family of elliptic curves with the desired torsion structure 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] S. Lang and A. Néron. Rational points of abelian varieties over function fields. *Amer. J. Math.*, 81:95–118, 1959.

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

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

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

[6] J. H. Silverman. *The Arithmetic of Elliptic Curves*. 2 edition.

[7] Andrew Sutherland. *Optimized Equations for $X_1(N)$*. http://math.mit.edu/~drew/X1_optcurves.html.

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

[9] Andrew Sutherland. *Optimized Equations for $X_1(N)$*. http://math.mit.edu/~drew/X1_optcurves.html.

[10] 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.

Dept. of Mathematics, University of Connecticut, 341 Mansfield Road U1009, Storrs, CT 06269

Email address: robert.j.mcdonald@uconn.edu