TORSION SUBGROUPS OF ELLIPTIC CURVES OVER FUNCTION FIELDS OF GENUS 0

ROBERT J.S. MCDONALD

Abstract. Let $K = \mathbb{F}_q(T)$ be the function field of a finite field of characteristic p, and E/K be an elliptic curve. It is known that $E(K)$ is a finitely generated abelian group, and that for a given p, there is a finite, effectively calculable, list of possible torsion subgroups which can appear. For $p \neq 2, 3$, a minimal list of prime-to-p torsion subgroups has been determined by Cox and Parry. In this article, we extend this result to the case when $p = 2, 3$, and determine the complete list of possible full torsion subgroups which can appear, and appear infinitely often, for a given p.

1. Introduction

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

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

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

We have the usual definitions for the invariants associated to E (for example in [9]), including the discriminant, Δ, and the j-invariant, all of which are elements in K. In addition, we will consider the Hasse invariant of E, which we will denote $H(E)$. When $p = 2$, for a curve written in long Weierstrass form, the Hasse invariant is the coefficient a_1. When $p > 2$, we may choose an equation with $a_1 = a_3 = 0$, in which case the Hasse invariant of E is the coefficient of x^{p-1} in $(x^3 + a_2x^2 + a_4x + a_6)^{\frac{p-1}{2}}$ [11, p. 18].

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, [5]). *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.*

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 [11, 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 1.3 (Ulmer, [11]). *Let g be the genus of $\mathcal{C}$. Then, there is a finite (and effectively calculable) list of groups depending only on g and p, such that for any non-isotrivial elliptic curve E over K, the group $E(K)_{\text{tors}}$ appears on the list.*

Following the proof of Proposition 1.3 in [11, Theorem 5.1], if $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is the prime-to-p torsion subgroup of $E(K)$, a crude list (at least for the prime-to-p part of $E(K)_{\text{tors}}$) can be found by using the Hurwitz formula on the induced morphism from $\mathcal{C}$ to the modular curve $X_m(n)$, though one may have to work harder to further refine the list to be minimal for K. For example, when $g = 0$, so that $k(\mathcal{C}) = k(T)$, and $p \geq 5$ we have the following minimal list for prime-to-p torsion.

Theorem 1.4 (Cox, Parry, [2]). *Let k be a field of characteristic $p \geq 0$, and assume that $p \neq 2, 3$. Let n and m be positive integers with $m|n$, and set $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Then, the following are equivalent:*

1. *There is a non-isotrivial elliptic curve E over $k(T)$ such that $G \cong E(K)'_{\text{tors}}$, the rational points of finite order not divisible by p.*
2. *p does not divide n, the field k contains a primitive m-th root of unity, and G is one of the following 19 groups:*

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

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

Theorem 1.5 (Ulmer, [11]). *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 $K^\times$.*

Remark 1.6. When $\mathcal{C} = \mathbb{P}^1$, since $\alpha \mapsto \alpha^p$ is an automorphism of k, we have $K^p = \big(k(T)\big)^p = k(T^p)$. That is, an element of K is in K^p if and only if it is a rational expression in T^p. With this, it is also not hard to show that if $f, g \in K$, then $f \circ g \in K^p$ if and only if at least one of f or g is in K^p.

Finally, the following result proves very useful in trying to calculate the list referred to in Proposition 1.3, though, again, some work is required to minimize it.

Theorem 1.7 (Levin, [6]). *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 $\ell^e \mid \#E(K)_{\text{tors}}$ for $e \geq 1$, then if $\ell \neq p$,

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

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

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

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

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

where h_ℓ is found in [6, pp. 460–461].

Since we are primarily interested in $K = \mathbb{F}_q(T)$, where we have $g(K) = 0$, we provide the following special case of Theorem 1.7.

Corollary 1.8. *Let $k = \mathbb{F}_q$ with q a power of p, $K = k(T)$, and E/K an elliptic curve. Suppose $\ell^e | \#E(K)_{\text{tors}}$ for some prime ℓ. Then, we have*

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

Remark 1.9. Note that Corollary 1.8 also tells us that for characteristic $p \geq 13$, Cox and Parry's list in Theorem 1.4 is a complete list of torsion structures one can expect to encounter.

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

Definition 1.10. For a curve $\mathcal{D}/K$, we will call any point in $\mathcal{D}(k)$ a *constant point*, and any point in $\mathcal{D}(K)$ *non-constant* if it is not a constant point. As in Definition 1.1, we will also call a general curve $\mathcal{D}/K$ *constant* if it can be written in a form with coefficients in k.

Finally, we will make use of the following useful fact, which is true in more generality for function fields with base curves of higher genus, but for now, adapted to fit the case when $\mathcal{C} \cong \mathbb{P}^1$.

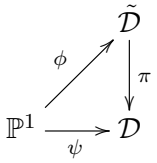
Proposition 1.11. *Let k be a finite field of characteristic p, and $K = k(T)$. If $\mathcal{D}$ is an irreducible constant curve over K (possibly singular) of positive genus, then every point in $\mathcal{D}(K)$ is constant.*

Proof. The genus of $\mathcal{D}$ is the genus of its normalization, $\tilde{\mathcal{D}}$. Let $\pi : \tilde{\mathcal{D}} \to \mathcal{D}$ be the normalization map associated to $\mathcal{D}$. The map π is a birational morphism on irreducible components of $\mathcal{D}$ [8, p. 128]. Since $\mathcal{D}$ is irreducible, the map $\pi^{-1} : \mathcal{D} \to \tilde{\mathcal{D}}$ is either a non-constant rational map, or the identity map if $\mathcal{D}$ is smooth. Suppose that there is a non-constant point $P \in \mathcal{D}(K)$. Since $K = k(\mathbb{P}^1)$, and $\mathcal{D}$ can be written with coefficients in k, we obtain a morphism defined over k:

$$\psi : \mathbb{P}^1_k \to \mathcal{D}/k \text{ by } t \mapsto P_t.$$

The map, ψ, is clearly rational. Since $\mathbb{P}^1$ is smooth, ψ is a morphism [9, 2.1], and because P is non-constant, ψ is non-constant, and therefore surjective [9, 2.3]. Thus, ψ is a dominant rational

map, so that defining $\phi : \mathbb{P}^1 \to \tilde{\mathcal{D}}$ by $\phi = \pi^{-1} \circ \psi$, we obtain a non-constant rational map.



Since $\phi : \mathbb{P}^1 \to \tilde{\mathcal{D}}$ is a map of smooth curves, by [9, 2.12], we can factor ϕ as

$$\mathbb{P}^1 \xrightarrow{\alpha} \mathbb{P}^1 \xrightarrow{\beta} \tilde{\mathcal{D}},$$

where α is the q-th power Frobenius map, and β is separable, and non-constant by assumption. Since α is an automorphism of $\mathbb{P}^1$, we may assume ϕ is separable, and apply the Hurwitz formula:

$$-2 = 2g(\mathbb{P}^1) - 2 \geq (\deg \phi)(2g(\mathcal{D}) - 2) + \sum_{P \in \mathbb{P}^1} (e_{\phi(P)} - 1) \geq 0.$$

This is a contradiction, so that ϕ, and therefore ψ, must be constant, and no such point P should exist. Thus, we conclude that every point in $\mathcal{D}(K)$ is constant. □

Remark 1.12. In other words, if $K = k(T) = k(\mathbb{P}^1)$ for a finite field k, and $\mathcal{D}$ is an irreducible constant curve over K of positive genus, then there are no non-constant points in $\mathcal{D}(K)$. This is certainly *not* the case if $\mathcal{D}/K$ has genus zero because maps $\mathbb{P}^1 \to \mathcal{D}$ exists as long as $\mathcal{D}$ has a point.

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

Theorem 1.13. *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 1.4 (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:*

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

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 1.4 is a complete list of possible subgroups $E(K)_{\text{tors}}$.

Remark 1.14. Throughout the paper, it is essential that E is a *non-isotrivial* elliptic curve. For example, over $K = \mathbb{F}_{11}(T)$, for any non-zero $f \in K$, the curve $E_f : y^2 = x^3 + f^2x^2 + f^4x$ has the point $(0, 0)$ of order sixteen, which does not appear in Cox and Parry's list in Theorem 1.4. However, E is *constant*, because it is isomorphic to the curve $E : y^2 = x^3 + x^2 + x$.

In Section 2, we will parameterize all of the torsion subgroups referred to in Cox and Parry's list in Theorem 1.4 explicitly, regardless of the characteristic of K. Then, starting with characteristic $p \geq 5$, in Section 3, we will use Theorem 1.5 and the parameterizations from Section 2, to obtain the conditions necessary for a point of order p to appear with a subgroup from Cox and Parry's list. In

each case, we will find that such torsion structures correspond to points on certain constant curves, which we will either parameterize, or attempt to apply Proposition 1.11. Finally, in Section 4, we look at characteristics $p = 2, 3$. After proving a version of Theorem 1.4 for each of these characteristics, we will again determine when points of order p can appear. Explicit parameterizations of all exotic torsion, along with generators, for all exotic torsion structures are provided in Section 5.

Acknowledgements. I would like to thank Keith Conrad and Álvaro Lozano-Robledo for their help (special thanks to Álvaro's computer, "R2-D2," which calculated the genus and irreducibility of the genus 16 curve in Table 13 in two hours). I would especially like to thank Liang Xiao for suggesting to use the Hurwitz formula to show constant elliptic curves have only constant points, leading to Proposition 1.11, and Andrew Sutherland, for his encouraging suggestions and showing me his tables in [10]. Finally, I would like to thank the referees for their comments and revisions.

2. Explicit Parameterizations of Torsion Structures in Theorem 1.4

In this section, having fixed a characteristic $p \geq 2$, we parameterize all elliptic curves with each torsion structure from Cox and Parry's list in Theorem 1.4. Let k be a finite field of characteristic p, let $K = k(T)$, and let E/K be a non-isotrivial elliptic curve. Suppose that there exists a $Q = (x_0, y_0) \in E(K)$ not equal to $\mathcal{O}$. Then, with the change of variables $x \mapsto x + x_0$, $y \mapsto y + y_0$, we can move Q to the origin and write

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x \tag{1}$$

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

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

By using the group law algorithms in [9, 2.3], it is easy to show that when $E : y^2 = f(x)$, then *any* point of order two takes the form $(\alpha, 0)$ where α is a root of f. Hence, for $p \neq 2$, any curve with $(\mathbb{Z}/2\mathbb{Z})^2$ torsion may be written in the form

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

Returning to (1), if Q has order greater than two, then $(0,0) \neq -Q = (0, -a_3)$, so that $a_3 \neq 0$. Then, the change of variables $y \mapsto y + \frac{a_4}{a_3}x$ (and some renaming of coefficients) allows us to write E as an equation with $a_4 = 0$ as well:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 \tag{2}$$

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

$$E : y^2 + axy + by = x^3 \text{ for } a, b \in K.$$

In [7, 1.1], for $f \in \mathbb{Q}(\zeta_3)$, we find the family $X^3 + Y^3 + Z^3 = 3fXYZ$ parameterizes all elliptic curves with $(\mathbb{Z}/3\mathbb{Z})^2$ torsion over $\mathbb{Q}(\zeta_3)$. Under a (non-trivial) change of variables, for the same $f \in \mathbb{Q}(\zeta_3)$, this family is isomorphic to the family

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

Thus, for $p \neq 3$, if $\zeta_3 \in k$, and $f \in K$, we will see $(\mathbb{Z}/3\mathbb{Z})^2$ torsion using this family.

Collecting our results, we have Table 1, with two parameter families for $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^2$ for $n = 2, 3$. Here, with $a, b \in K$, at least one non-constant, as long as $\Delta_{a,b} \neq 0$, we get a non-isotrivial elliptic curve $E_{a,b}$ with $G \subset E_{a,b}(K)_{\text{tors}}$.

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

Table 1. Two-parameter familes of elliptic curves $E_{a,b}/K$ such that $G \subset E_{a,b}(K)_{\text{tors}}$.

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

$$E : y^2 + \frac{a_1 a_2}{a_3} xy + \frac{a_2^3}{a_3^2} y = x^3 + \frac{a_2^3}{a_3^2} x^2.$$

Setting $b = -a_2^3/a_3^2$ and $a = 1 - (a_1a_2)/a_3$, we find that *for general* p, the point $(0, 0) \in E(K)$ has order greater than three (possibly infinite) if and only if we can write E in *Tate normal form*:

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

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

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

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

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

where ϕ_m and ψ_m are division polynomials as defined in [9, p. 105]. This relationship, and the fact that ϕ_m and ψ_m^2 are coprime, is valid in any characteristic [9, p. 105]. Thus, we have

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

This means that, regardless of the characteristic of K, if $(0, 0)$ is a point of order n, we can solve $\phi_m(P) = 0$ to find a, and b such that there is a point P with $[mn]P = \mathcal{O}$. Using the characterizations in [3], we can easily calculate the a and b necessary for $\mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$ by solving $\phi_2(P) = 0$ when $(0, 0)$ has order five and six respectively. So far, with a change of variables, all of our parameterizations are isomorphic to curves of the desired form in [3, p. 188]. Thus, for general p, we get the families in Table 2, parameterizing torsion structures $\mathbb{Z}/n\mathbb{Z}$ for $n = 4, \ldots 10, 12$.

When $p \neq 2$, we can obtain a parameterization for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by starting with the parameterization of $\mathbb{Z}/4\mathbb{Z}$ torsion, and rewriting it in the form $E : y^2 = x^3 + (2f + \frac{1}{4})x^2 + f^2x$. The associated

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

Table 2. One-parameter familes of elliptic curves $E_{a,b}/K$ such that $G \subset E_{a,b}(K)_{\text{tors}}$.

change of variables is valid when $p \neq 2$. In this form, $(0,0)$ is a point of order 2, so there must be $a, b \in K$ such that $a + b = 2f + \frac{1}{4}$, and $ab = f^2$. This is true if and only if $f = g^2 - \frac{1}{16}$ for some $g \in K$. Using our new found parameterization for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, a parameterization of $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (given below) can then be found by solving $\phi_2(P) = 0$, as above.

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

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

Table 3. One-parameter familes of elliptic curves $E_{a,b}/K$ such that $G \subset E_{a,b}(K)_{\text{tors}}$.

2.1. $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ **torsion.** Here, $p \neq 3$ and $\zeta_3 \in k$. Using our parameterization of $(\mathbb{Z}/3\mathbb{Z})^2$, if a non-isotrivial elliptic curve E over K has torsion subgroup $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, then without loss of generality, we have a point P such that $2P = (0,0)$. Looking at $\phi_2(P) = 0$, we can use Magma to find the following genus zero curve over K:

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

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

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

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

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

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

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

Finally, making the change of variables $t\mapsto\frac{1}{9}(t^{-1}+2)$, we conclude that if $\zeta_3\in k$, and E is a non-isotrivial elliptic curve over K with $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ torsion, then E is isomorphic to the curve

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

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

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

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

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

2.3. $(\mathbb{Z}/5\mathbb{Z})^2$ **torsion.** Here, $p\neq 5$ and $\zeta_5\in k$. In [3, §6.4], we find a parameterization of all curves with $(\mathbb{Z}/5\mathbb{Z})^2$ torsion structure over $\mathbb{Q}(\zeta_5)$, where ζ_5 is a primitive fifth root of unity. By moving the point of order five defined over $\mathbb{Q}$ to the origin, and changing variables to write the curve in Tate normal form, we arrive at a parameterization of $(\mathbb{Z}/5\mathbb{Z})^2$ torsion over $\mathbb{Q}(\zeta_5)$ with a and b given by

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

Thus, when $\zeta_5\in k$, and $f\in K$, we will see $(\mathbb{Z}/5\mathbb{Z})^2$ torsion with this parameterization.

Finally, rewriting our parameterization of $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ torsion in Tate normal form, we can collect the remaining parameterizations of torsion structures from Theorem 1.4 into Table 4.

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

Table 4. One-parameter familes of elliptic curves $E_{a,b}/K$ such that $G\subset E_{a,b}(K)_{\text{tors}}$.

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

Since Theorem 1.4 only refers to function fields of characteristic $p \neq 2, 3$, we will start by assuming that $p \geq 5$. In this section, it will be our goal to determine when the torsion structures appearing in Cox and Parry's list can be combined with a point of order p. When possible, we try to develop a strategy that will work for general p.

3.1. **Characteristic 5.** Let us fix $k = \mathbb{F}_q$ with q a power of 5, and $K = k(T)$. Let E/K be a non-isotrivial elliptic curve given by $y^2 = x^3 + Ax + B$ for $A, B \in K$. By Theorem 1.4, the following prime-to-5 torsion is guaranteed to appear for general q and suitable E:

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

If, in addition, $\zeta_3 \in K$ (e.g., if $q = 5^2$), we will have a primitive third root of unity in k, and hence for suitable E, we can add the following torsion subgroups to our list:

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

All of these torsion structures can be realized over K as prime-to-5 torsion subgroups by using the families of curves in Section 2. It remains to consider points whose order is a power of five. If we use Tate normal form, we see that all non-isotrivial curves with $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z}$ torsion are still parameterized by $E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2$ with a and b given in Section 2. Theorem 1.5 gives another way of constructing curves with points of order five by playing with the Hasse and j invariants. When $p = 5$, the Hasse invariant of any curve can be computed by looking at the coefficients of the curve written in short Weierstrass form:

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

Thus, for the hypotheses on the Hasse invariant in Theorem 1.5 to be satisfied, we need $2A = u^4$ for some $u \in K^\times$. We use this to see if any of the torsion structures from Cox and Parry's list can appear in combination with a point of order five. Remember that by Corollary 1.8 we can have a point of 5-primary order of at most 5, so the possible torsion structures to confirm or rule out are

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

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

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

If in addition we assume that E has a point of order five, then by Theorem 1.5, we must have

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

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

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

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

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

is non-constant. Clearly, this happens if and only if f_0 is non-constant, and therefore, E_0 is non-isotrivial if and only if (f_0, u_0) is a non-constant point. That is, a point of order 20 over K implies the existence of a *non-constant* point on the irreducible constant curve C. But C has genus one[1], so by Proposition 1.11, all points on C/K are constant. Hence $\mathbb{Z}/20\mathbb{Z}$ torsion is impossible over K.

Remark 3.1. Not surprisingly, our curve C_{20} is isomorphic over $\mathbb{F}_5(T)$ to the modular curve $X_1(20)$ considered over $\mathbb{Q}(T)$ and reduced modulo 5, see, for example [10]. This suggests a different method for finding a curve to parameterize curves with points of order 20. Our method for constructing this curve avoids the subtleties of reducing $X_1(N)$ at the prime p (the characteristic) when p divides N.

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

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

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

Example 3.2. Over K, a non-isotrivial elliptic curve with a point of order 30 implies a non-constant point on $C_{30} : 4f^4 + 2f^3 + 2f + 1 = u^4$, and a point of order 35 gives a non-constant point on the curve $C_{35} : f^8 + 3f^7 + 2f^6 + 4f^5 + f^2 + 4f = u^4$. Using Magma, we compute the genera of these curves to be 3 and 9 respectively, and thus, see that $\mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z}/35\mathbb{Z}$ are impossible over K.

By using Proposition 1.11, we have already shown that $\mathbb{Z}/20\mathbb{Z}$, $\mathbb{Z}/30\mathbb{Z}$, and $\mathbb{Z}/35\mathbb{Z}$ torsion structures are impossible for elliptic curves defined over K. In Table 5, we let $G = \mathbb{Z}/5m\mathbb{Z}$ for $m \geq 4$, and $C_{5m} : H(E) = 2A_m(f) = u^4$ be the curve obtained by bringing the Tate normal form to short Weierstrass form. In particular, combining genus calculations with Proposition 1.11, the table rules out any torsion structures from (3) with a point of order greater than 15.

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

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

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

Continuing with this strategy, we combine the Tate normal forms parameterizing curves with $\mathbb{Z}/3\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^2$ torsion structures with the hypotheses of Theorem 1.5 to look for subgroups $\mathbb{Z}/15\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This time, we have *two*-parameter families with elements $a, b \in K$ (at least one of which is non-constant), that when written in short Weierstrass form and combined with the Hasse invariant give *surfaces* $S_G : H(E) = 2A(a, b) = u^4$ with $a, b, u \in K$.

G	S_G	Change of Variables	C_G	genus of C_G
$\mathbb{Z}/15\mathbb{Z}$	$a^4 + ab = u^4$	$a \mapsto a/u,\ b \mapsto b/u^3$	$a^4 + ab = 1$	0
$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$a^2 + 4ab + b^2 = u^4$	$a \mapsto a/u^2,\ b \mapsto b/u^2$	$a^2 + 4ab + b^2 = 1$	0

Table 6. Curves parameterizing elliptic curves with $G = \mathbb{Z}/15\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion over K.

In Table 6, if the torsion subgroup G exists in a non-isotrivial elliptic curve over K, it implies a point (a, b, u) on S_G with at least one of a or b non-constant. Note, however, that in the case of $\mathbb{Z}/15\mathbb{Z}$, we are looking at the curve $E : y^2 + axy + by = x^3$. If $H(E) = u^4$, then by the change of variables in [9, p. 45], E is isomorphic to the curve $E' : y^2 + au^{-1}xy + bu^{-3}y = x^3$, which has Hasse invariant one. Similarly, in the case of $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we are looking at the curve $E : y^2 = x^3 + (a + b)x^2 + abx$, with $H(E) = u^6$, which is in turn isomorphic to the curve $E' : y^2 = x^3 + (a + b)u^{-2}x^2 + abu^{-4}x$, again, with Hasse invariant one. In both cases, $a, b \in K$ are arbitrary parameters, so we can swallow u into them and fully parameterize elliptic curves with $H(E) = u^6$ (up to isomorphism) by constant *curves*, C_G, which are also given in Table 6.

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

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

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

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

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

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

Since $j(E) = j(a)$ is not trivially a fifth power (i.e., $j(a)$ is not a fifth power when we choose $a = T$), then by Remark 1.6, we see that $j(a) \in K^5$ if and only if $a \in K^5$, so that setting $a = f^5$, we obtain the following parameterization of all elliptic curves over K with a point of order fifteen:

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

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

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

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

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

It is left to determine whether or not $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ can occur over K when $\zeta_3 \in k$. For this, we return to Section 2 to find curves with $(\mathbb{Z}/3\mathbb{Z})^2$ torsion given by the parameterization

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

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

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

Theorem 3.3. *Let k be a finite field of characteristic 5, $K = k(T)$, and E/K be a non-isotrivial elliptic curve. The torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following*

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

$$\mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \quad \text{with } N = 1, 2, \qquad \text{if } \zeta_3 \in k.$$

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

3.2. **Characteristic 7.** Now we consider $k = \mathbb{F}_q$ with q a power of 7, and $K = k(T)$. Let E/K be a non-isotrivial elliptic curve given by $y^2 = x^3 + Ax + B$ for $A, B \in K$. By Theorem 1.4, the following prime-to-p torsion groups appear for general q and suitable E:

$$\begin{gathered} 0,\ \mathbb{Z}/2\mathbb{Z},\ \ldots,\ \mathbb{Z}/6\mathbb{Z},\ \mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z},\ \mathbb{Z}/10\mathbb{Z},\ \mathbb{Z}/12\mathbb{Z}, \\ (\mathbb{Z}/2\mathbb{Z})^2,\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \\ (\mathbb{Z}/3\mathbb{Z})^2,\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}. \end{gathered}$$

If, in addition, ζ_4 or ζ_5 are in k (e.g., $q = 7^2$ or 7^4), we may obtain $(\mathbb{Z}/4\mathbb{Z})^2$ or $(\mathbb{Z}/5\mathbb{Z})^2$ respectively, again, both of which will also appear for suitable E. As in the previous section, all of these torsion subgroups, and the subgroup $\mathbb{Z}/7\mathbb{Z}$, can be seen using the parameterizations from Section 2.

As before, we will use Theorem 1.5 to try and force a point of order seven to appear along with any of the torsion structures from Cox and Parry's list. Again, by Corollary 1.8, we can have a point of 7-primary order of at most 7, so the torsion structures to consider are

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

We begin by supposing that E is an elliptic curve with $\mathbb{Z}/m\mathbb{Z}$ torsion for $m = 4, 5, 6, 8, 9, 10, 12$. Then, E is isomorphic to a curve $E : y^2 = x^3 + A_m(f)x + B_m(f)$ for some non-constant $f \in K$, where $A(f)$ and $B(f)$ are again non-constant functions of f found by converting Tate normal form into short Weierstrass form. This time, for each m, to discover an additional point of order seven,

we will need the Hasse invariant to be a sixth power. Expanding $(x^3 + A_m(f)x + B_m(f))^3$ and keeping the coefficient of x^6, we obtain the following revision of our method from Section 3.1:

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

In Table 7, we let $G = \mathbb{Z}/7m\mathbb{Z}$, and $C_{7m} : 3B_m(f) = u^6$. As above, in each case, $B_m(f)$ is separable, and we can use Eisenstein's criterion to show that C_{7m}, therefore, defines an irreducible constant curve over K. Thus, any non-isotrivial elliptic curve with a point of order $7m$ implies the existence of a non-constant point on C_{7m}, and again, Proposition 1.11 shows that G cannot exist for $m \geq 4$.

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

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

Next, we suppose that E is an elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, or $(\mathbb{Z}/2\mathbb{Z})^2$, and combine Tate normal forms with the hypotheses of Theorem 1.5. Again, torsion structures $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/21\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ give points (a, b, u) with $a, b, u \in K$ and at least one of a or b non-constant on surfaces $S_{7m} : 3B_m(a, b)$, as in Table 8. Again, a change of variables shows that

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

Table 8. Curves parameterizing elliptic curves with $G = \mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/21\mathbb{Z}$ and $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion over K.

non-constant points on the curves C_G in Table 8, correspond (up to isomorphism) to non-isotrivial elliptic curves whose Hasse invariant is a sixth power in K. Immediately, we find the existence of torsion structures $\mathbb{Z}/21\mathbb{Z}$ or $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ over K implies non-constant points on constant curves of positive genus. Using Magma, we find that these curves are absolutely irreducible, hence irreducible regardless of the cardinality of k. Thus, using Proposition 1.11, we find that these torsion structures are impossible. The curve $C_{\mathbb{Z}/14\mathbb{Z}}$, however, can be parameterized easily by

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

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

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

We have, in fact, ruled out any torsion structures from (4) with a point of order greater than 14, and the torsion structure $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We can collect all of this into the following theorem.

Theorem 3.4. *Let k be a finite field of characteristic 7, $K = k(T)$, and E/K be a non-isotrivial elliptic curve. The torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following*

$$\left.\begin{array}{cl} \mathbb{Z}/N\mathbb{Z}, & \text{with } 1 \le N \le 10 \text{ or } N = 12, 14, \\ \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{with } 1 \le N \le 4, \\ \mathbb{Z}/3N\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, & \text{with } N = 1, 2, \end{array}\right\} \text{for general } k.$$

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

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

3.3. **Characteristic 11.** Now we let $k = \mathbb{F}_q$ for q a power of 11, and $K = k(T)$. Let E/K be a non-isotrivial elliptic curve given by $y^2 = x^3 + Ax + B$ for $A, B \in K$. By Theorem 1.4, the following prime-to-p torsion subgroups appear for general q and suitable E:

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

If, in addition, ζ_3 or ζ_4 are in k (e.g., if $q = 11^2$), we may obtain $(\mathbb{Z}/3\mathbb{Z})^2$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $(\mathbb{Z}/4\mathbb{Z})^2$ respectively, again, both of which will also appear for suitable E. As in both the cases above, all of these torsion subgroups can be realized using parameterizations from Section 2.

It is not immediately clear whether a curve with a point of order eleven even exists, since this is not a torsion structure we have parameterized (since it does not occur over $\mathbb{Q}$). This time, the Hasse invariant of any curve written in short Weierstrass form is $H(E) = 9AB$, and by Theorem 1.5, we must have $9AB = u^{10}$ for some $u \in K^\times$ and $j(E) \in K^{11}$. With this information have the following parameterization.

Theorem 3.5. *Let k be a finite field of characteristic 11, and $K = k(T)$. The one-parameter family $E_f : y^2 = x^3 + f^{11}x + 5f^{-11}$ for $f \in K$ is a parameterization of all curves with a K-rational 11-torsion point.*

Proof. Let $E : y^2 = x^3 + Ax + B$ be a non-isotrivial elliptic curve over K with a K-rational point of order 11. By Theorem 1.5, it must be that the Hasse invariant of E is a tenth power in $K^\times$, so that for some $u \in K^\times$, we must have $H(E) = 9AB = u^{10}$. In particular, this means that A and B are both non-zero. Also by Theorem 1.5, we have

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

Combining these two restrictions on A and B, we obtain

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

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

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

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

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

Thus, we have

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

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

Remark 3.6. An identical procedure shows that $E_f : y^2 = x^3 + 3x + f^5$ parameterizes all curves with a point of order 5 over $\mathbb{F}_{5^n}(T)$, and $E_f : y^2 = x^3 + f^7 x + 5$ parameterizes all curves with a point of order 7 over $\mathbb{F}_{7^n}(T)$. In both cases, however, it's not hard to show that these families are equivalent to the ones given by Tate normal form, and no new information is gained.

Now, we will try to combine a point of order eleven with torsion structures from Theorem 1.4. This time, Corollary 1.8 tells us that we can have a point of 11-primary torsion of at most 11, so the combined torsion structures we would like to consider are

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

This time, we begin by supposing that E has torsion structures $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$. By working with the two-parameter families for these torsion structures and the Hasse invariant, we again arrive at surfaces $S_G : 9A(a,b)B(a,b) = u^{10}$. Since $u \in K^\times$, under the same change of variables as in Section 3.2, we see that non-isotrivial elliptic curves over K whose Hasse invariant is a tenth power correspond, up to isomorphism, to non-constant points on *curves*, $C_G : 9A(a,b)B(a,b) = 1$, given in Table 9. Magma again reveals these curves to be absolutely irreducible. In particular, since each of the C_G are constant curves of positive genus, we find that all of the torsion subgroups $\mathbb{Z}/22\mathbb{Z}$, $\mathbb{Z}/33\mathbb{Z}$ and $\mathbb{Z}/22\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are impossible over K by Proposition 1.11.

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

Table 9. Curves parameterizing elliptic curves with $G = \mathbb{Z}/22\mathbb{Z}$, $\mathbb{Z}/33\mathbb{Z}$ and $\mathbb{Z}/22\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion over K.

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

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

This equation is still just an irreducible constant curve over K. In Table 10, we let $G = \mathbb{Z}/11m\mathbb{Z}$, and C_{11m} be the curve above. Again, we see that such torsion subgroups G cannot exist for $m \geq 4$.

We have ruled out any torsion structures from (5) with a point of order greater than 12. In fact, we have ruled out the possibility of combining a point of order eleven with *any* of the torsion structures from Cox and Parry's list. Thus, we have the following theorem.

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

Table 10. Ruling out $G=\mathbb{Z}/11m\mathbb{Z}$ torsion over K for $m\geq 4$.

Theorem 3.7. *Let k be a finite field of characteristic 11, $K=k(T)$, and E/K be a non-isotrivial elliptic curve. The torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following*

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

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

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

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

Unfortunately, in Theorem 1.4, Cox and Parry use the assumption that the characteristic of k is not 2 or 3. In order to proceed, we need to come up with a similar statement for these characteristics. We will use the following result to extend Cox and Parry's list to one for all primes p.

Proposition 4.1 ([2, Proposition 3.7])**.** *The modular curve $X_m(n)$[2] has genus 0 if and only if (n,m) is one of the following 18 ordered pairs:*

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

Cox and Parry use this proposition to provide a list of all possible prime-to-p torsion in Theorem 1.4, then show that it is, in fact, minimal. In what remains of this section, for k, a finite field of characteristic $p=2$ or 3, and $K=k(T)$, we will show what prime-to-p torsion subgroups can appear, and as in Section 3, determine when and in what ways points of order p can be combined with them.

4.1. **Characteristic 2.** We start with $k=\mathbb{F}_q$ for q a power of 2, and $K=k(T)$. Given an elliptic curve E over K, written in long Weierstrass form, E has Hasse invariant $H(E)=a_1$ [11, p. 14]. We have the following theorem about the prime-to-2 torsion structures we should expect over K.

[2]For $m\mid n$ and $p\nmid m$, $X_m(n)$ 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 [2] for a precise definition.

Theorem 4.2. *Let k be a finite field of characteristic 2, $K = k(T)$, and E/K be a non-isotrivial elliptic curve. Let $G = E(K)'_{\text{tors}}$ be the group of rational points of finite order not divisible by 2. Then, G is isomorphic to one of the following:*

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

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

Proof. Our proof follows that of Proposition 1.3 in [11, Prop. 7.1], using the Hurwitz formula to bound the genera of modular curves, a method dating back to Levin. If $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ for $2 \nmid m, n$, then there is a modular curve $X_m(n)$ defined over $\mathbb{F}_2(\mu_m)$ that is a coarse moduli space for elliptic curves with torsion structure isomorphic to G. Since E is non-isotrivial, we obtain a non-constant morphism $\mathbb{P}^1 \to X_m(n)$ which, by the Hurwitz formula, implies that if $G \subset E(K)_{\text{tors}}$, then the genus of $X_m(n)$ must be zero. Thus, G must be given by one of the pairs (n, m) in Proposition 4.1 such that $2 \nmid m, n$. Using the parameterizations from Section 2, it is easy to show that all of the groups in this list appear infinitely often when k contains the necessary roots of unity. □

We will have a point of order 2 if and only if $H(E) \in (K^\times)^{2-1} = K^\times$, that is, if $a_1 \neq 0$, and $j(E) \in K^2$. By Levin's bounds, we see that the 2-primary component can have at most order 8. By using parameterizations from Section 2, we immediately see infinitely many elliptic curves can have torsion subgroups $\mathbb{Z}/2n\mathbb{Z}$ for $1 \leq n \leq 6$, and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ if $\zeta_3 \in k$. Thus, for $j = 1, 2, 3$, we only need to confirm or rule out the following torsion structures over K:

$$\begin{array}{ll} \mathbb{Z}/2^jN\mathbb{Z} & \text{for } N = 7, 9, 10, 12, \\ \mathbb{Z}/2^jN\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} & \text{for } N = 3, 5. \end{array} \tag{6}$$

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

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

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

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

Unfortunately, the same type of argument will not work in determining existence of $\mathbb{Z}/20\mathbb{Z}$ or $\mathbb{Z}/24\mathbb{Z}$, since in each of these cases, a point of order two already exists. That is, any curve E with these torsion subgroups has invariants which *already satisfy* the hypotheses of Theorem 1.5. Instead, we try a "brute-force" strategy using division polynomials. Suppose that E is a non-isotrivial elliptic curve with a point of order ten (respectively twelve), so that E can be written as

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

with $(0, 0)$ a generator of the torsion subgroup. Here, we must have

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

For example, if $(0, 0)$ has order 10, then the formulas for a and b from Section 2 give

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

Finally, we can clear denominators to obtain

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

Once again, this is a constant curve over K, which Magma reveals is absolutely irreducible, and has genus one. Note that by hypothesis, E is isotrivial if $f \in k$, so we are looking for solutions (x, f) with f non-constant, and hence (x, f) is non-constant. Thus, by Proposition 1.11, no such solution exists. Points of order 20 are therefore impossible over K. In the Table 11, we use the same strategy to eliminate points of order 24.

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

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

where $\lambda_{28}(x, t)$ is an absolutely irreducible polynomial. The first factor gives the point of order *seven*, $P = (f^3 + f^2, 0)$. If $f = u^2$ for some $u \in K^\times$, then the second factor gives a point P of order *fourteen* (see above) such that $x(P) = u^3 + u$. The equation $\lambda_{28} = 0$, however, defines an irreducible curve of genus 3, which by the above argument, shows that a point of order 28 is impossible over K. In Table 11, we use an analogous construction for λ_{36}, and rule out points of order 36. Note that we have now ruled out any torsion from (6) with a point of order greater than 18.

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

Table 11. Using division polynomials to rule out $\mathbb{Z}/4m\mathbb{Z}$ for $m = 5, 6, 7, 9$.

If k contains a primitive fifth root of unity, then curves with $(\mathbb{Z}/5\mathbb{Z})^2$ torsion over K are parameterized by $E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx$ with a and b functions of some non-constant $g \in K$, given in Section 2. Here, $H(E) = a_1 = 1 - a \in K^\times$, and $j(E) \in K^2$ if and only if $g = f^2$ for some $f \in K$. Hence, any curve with $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ torsion is isomorphic to a curve of the form $E_{a,b}$ with

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

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

We can collect all of this into the following theorem.

Theorem 4.3. *Let k be a finite field of characteristic 2, $K = k(T)$, and E/K be a non-isotrivial elliptic curve. Then, the torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following*

$\mathbb{Z}/N\mathbb{Z}$,	*with* $1 \le N \le 10$ *or* $N = 12, 14, 18$,	*for general* k,
$(\mathbb{Z}/N\mathbb{Z})^2, \mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$,	*with* $N = 3, 5$,	*if* $\zeta_N \in k$.

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

4.2. **Characteristic 3.** Next, we suppose that $k = \mathbb{F}_q$ with q a power of 3, and again, $K = \mathbb{F}_q(T)$. Given an elliptic curve E in long Weierstrass form, under the change of variables in [9, p. 42], for $p = 3$, we can write $E : y^2 = f(x)$ for a (monic!) degree three polynomial f, and thus, our normal calculation for the Hasse invariant of E shows $H(E) = a_2$, when written in this form. We can say the following about prime-to-3 torsion structures appearing over K.

Theorem 4.4. *Let k be a finite field of characteristic 3, $K = k(T)$, and E/K be a non-isotrivial elliptic curve. Let $G = E(K)'_{\text{tors}}$ be the group of rational points of finite order not divisible by 3. Then, G is isomorphic to one of the following:*

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

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

Proof. As in the proof of Theorem 4.2, if $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \subset E(K)_{\text{tors}}$ for $3 \nmid m, n$, then the genus of $X_m(n)$ defined over $\mathbb{F}_3(\mu_m)$ must be zero. Therefore, pairs from Proposition 4.1 with $3 \nmid m, n$ give a list of possible prime-to-3 torsion subgroups. Again, all of the groups in this list appear infinitely often by using the parameterizations from Section 2. □

Remark 4.5. Together, Theorems 4.2 and 4.4 imply that Cox and Parry's list in Theorem 1.4 remains valid after we remove the assumption that p is not 2 or 3.

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

$$\begin{array}{cc} \mathbb{Z}/3^jN\mathbb{Z} & \text{for } N = 5, \ldots, 8, 10, 12, \\ \mathbb{Z}/3^j2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{for } N = 1, \ldots, 4, \\ \mathbb{Z}/3^jN\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} & \text{for } N = 4, 5. \end{array} \tag{7}$$

Using the change of variables $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ from [9], any curve starting in Tate normal form can be written as

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

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

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

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

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

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

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

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

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

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

Using our strategy in Section 3, if E has a point of order $m=7,8,10$, then we can write it in Tate normal form. If in addition, E has a point of order three, then we must have

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

In each case, clearing denominators when necessary, a point of order $3m$ on an elliptic curve E over K implies the existence of a non-constant point on one of the curves in Table 12. Again, since each

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

Table 12. Ruling out $G=\mathbb{Z}/3m\mathbb{Z}$ torsion over K for $m=7,8,10$.

of the C_{3m} in this table are irreducible and constant, we know that all of the points in $C_{3m}(K)$ are constant. Thus, points of order 21, 24 or 30, and hence 63, 72, and 90, are impossible over K.

As in the case when $p=2$, unfortunately, the same strategy cannot be applied to rule out points of order 18 or 45, since here we need to start with curves which already have invariants satisfying our hypotheses. In the same way we did above, however, we can start with a curve written in Tate normal form to get a point of specified order, then use division polynomials to obtain the necessary conditions. The results are irreducible constant curves, collected in Table 13. Here, the polynomial

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

Table 13. Using division polynomials to rule out $\mathbb{Z}/9m\mathbb{Z}$ for $m=2,5$.

λ_{45} is the irreducible factor of $\phi_4(P)=(x+2f^5+2f^4+f^3+f^2)\lambda_{45}$ that corresponds to a point of order 45 (as above). The table shows that points of order 18, 36 and 45 are impossible over K. Note, we have also ruled out any torsion structures from (7) with a point of order greater than 15.

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

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

Thus, we need $2(g^2+1) = u^2$ for some $u \in K^\times$. Since $i \notin \mathbb{F}_3$, this shows that $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is impossible over K unless $i \in k$. If $i \in k$, then $H(E) = u^2$ if and only if

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

for some $m \in K^\times$. Again, $j(E) \in K^3$ if and only if $m = f^3$ for some $f \in K$. Thus, if $i \in k$, and E/K is a non-isotrivial elliptic curve with $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ torsion, it can be written as

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

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

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

Hence, this torsion structure is impossible over K by Proposition 1.11.

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

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

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

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

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

We collect this all into the following theorem.

Theorem 4.6. *Let k be a finite field of characteristic 3, $K = k(T)$, and E/K be a non-isotrivial elliptic curve. Then, the torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following*

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

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

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

5. Explicit Parameterizations of Exotic Torsion

Let k be a finite field of characteristic p, and set $K = k(T)$. In this final section, we give explicit parameterizations of elliptic curves with new torsion structures found possible over K. In Table 14, for non-constant $f \in K$, if $\Delta_{a,b} \neq 0$, then $E_{a,b}$ is a non-isotrivial elliptic curve over K such that $E_{a,b}(K)_{\text{tors}}$ has subgroup G. Each family in Table 14 comes as a result from Sections 3 and 4, brought to Tate normal form, so that $(0,0)$ is a point of maximal order in the group.

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

Table 14. One-parameter families of elliptic curves $E_{a,b}/K$ such that $E_{a,b}(K)_{\text{tors}}$ has a subgroup G.

Remark 5.1. In the table, for $\mathbb{Z}/10\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, a generator of order two has x-coordinate $\frac{f(f+2)^2(f+3)^3}{(f^2+4f+1)^3}$. For $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, a generator of order two has $x = \frac{(1+i)(f+1)(f+i)^2(f+2)(f+2i)^2(f+2i+1)}{(f+i+2)(f+2i+2)^6}$. Finally, for $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, a generator of order five has

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

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 2, 1

[2] David A. Cox and Walter R. Parry. Torsion in elliptic curves over $k(t)$. *Compositio Math.*, 41(3):337–354, 1980. 1.4, 4.1, 2

[3] Enrique González-Jiménez and Álvaro Lozano-Robledo. Elliptic curves with abelian division fields. *Math. Z.*, 283(3-4):835–859, 2016. 2, 2, 2.3

[4] D. Husemöller. *Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2004. 2

[5] S. Lang and A. Néron. Rational points of abelian varieties over function fields. *Amer. J. Math.*, 81:95–118, 1959. 1.2

[6] Martin Levin. On the group of rational points on elliptic curves over function fields. *Amer. J. Math.*, 90:456–462, 1968. 1.7

[7] K. Rubin and A. Silverberg. Families of elliptic curves with constant mod p representations. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 148–161. Int. Press, Cambridge, MA, 1995. 2

[8] Igor R. Shafarevich. *Basic Algebraic Geometry*. Springer-Verlag, 3 edition, 2013. 1

[9] J. H. Silverman. *The Arithmetic of Elliptic Curves*. 2 edition. 1, 1, 2, 2, 3.1, 4.2, 4.2

[10] Andrew Sutherland. *Optimized Equations for $X_1(N)$*. http://math.mit.edu/~drew/X1_optcurves.html. 1, 3.1

[11] Douglas Ulmer. Elliptic curves over function fields. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 211–280. Amer. Math. Soc., Providence, RI, 2011. 1, 1, 1.3, 1, 1.5, 4.1, 4.1

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