ARTICLE IN PRESS YJNTH:6060

Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

# Torsion subgroups of elliptic curves over function fields of genus 0

Robert J.S. McDonald

*Dept. of Mathematics, University of Connecticut, 341 Mansfield Road U1009, Storrs, CT 06269, United States of America*

ARTICLE INFO

*Article history:*
Received 25 September 2017
Received in revised form 1 March 2018
Accepted 7 May 2018
Available online xxxx
Communicated by A. Pal

*Keywords:*
Elliptic curve
Function field
Torsion subgroup
Torsion
Genus
Genus 0

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

*E-mail address:* robert.j.mcdonald@uconn.edu.

https://doi.org/10.1016/j.jnt.2018.05.017

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, $\Delta$, 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.*

Please cite this article in press as: R.J.S. McDonald, Torsion subgroups of elliptic curves over function fields of genus 0, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.05.017