Rose-Hulman Undergraduate Mathematics Journal

Volume 19
Issue 1

Article 2

On Orders of Elliptic Curves over Finite Fields

Yujin H. Kim
Columbia University, yujin.kim@columbia.edu

Jackson Bahr

Eric Neyman

Gregory Taylor

On Orders of Elliptic Curves over Finite Fields

Cover Page Footnote

We wish to thank our advisor Prof. Liljana Babinkostova for her guidance and support. This research was conducted during the REU Program in Mathematics at Boise State University. Funding for this research was provided by the National Science Foundation under the grant DMS-1062857 and Boise State University.

Rose-
Hulman
Undergraduate
Mathematics
Journal

On Orders of Elliptic Curves over Finite Fields

Jackson Bahr[a] Yujin Kim[b] Eric Neyman[c]
Gregory Taylor[d]

Volume 19, No. 1, Fall 2018

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
mathjournal@rose-hulman.edu
scholar.rose-hulman.edu/rhumj

[a]University of California, Los Angeles
[b]Columbia University
[c]Princeton University
[d]University of Illinois at Chicago

Rose-Hulman Undergraduate Mathematics Journal
Volume 19, No. 1, Fall 2018

On Orders of Elliptic Curves over Finite Fields

Jackson Bahr Yujin Kim Eric Neyman Gregory Taylor

Abstract. In this work, we completely characterize by j-invariant the number of orders of elliptic curves over all finite fields F_{p^r} using combinatorial arguments and elementary number theory. Whenever possible, we state and prove exactly which orders can be realized.

Acknowledgements: We wish to thank our advisor Prof. Liljana Babinkostova for her guidance and support. This research was conducted during the REU Program in Mathematics at Boise State University. Funding for this research was provided by the National Science Foundation under the grant DMS-1062857 and Boise State University.

1 Introduction

The study of elliptic curves is of fundamental importance in the abstract world of arithmetic geometry and Diophantine equations. We focus in particular on counting points on elliptic curves over finite fields, an important topic in both the study of Diophantine equations and elliptic curve cryptography. Many algorithms exist for the efficient computation of the orders of elliptic curve groups and related quantities (see, for instance, [8], [9]).

1.1 Elliptic curves over finite fields.

Given a prime power $q = p^r > 3$, consider the finite field $\mathbb{F}_q$ and a pair (A, B) where $A, B \in \mathbb{F}_q$ such that $4A^3 + 27B^2 \neq 0$. We consider the set of solutions (x, y) to the cubic equation $y^2 = x^3 + Ax + B$ over the finite field $\mathbb{F}_q$. This set of ordered pairs, when augmented by a "point at infinity" $\mathcal{O}$, can be given a natural abelian group structure, where $\mathcal{O}$ serves as the identity element (see [11] for the full details of this complicated group structure). Such groups are called elliptic curves over $\mathbb{F}_q$, and in fact elliptic curve groups can be defined similarly over any field K. We typically write $E(K)$ to denote an elliptic curve group E defined over the field K, and in this paper, we focus exclusively on the case of curves defined over finite fields. In particular, we wish to study the size of these groups.

Note that

$$\left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right) + 1 = \begin{cases} 0 & \text{if } x^3 + Ax + B \text{ is not a square in } \mathbb{F}_q \\ 1 & \text{if } x^3 + Ax + B \equiv 0 \\ 2 & \text{if } x^3 + Ax + B \text{ is a non-zero square in } \mathbb{F}_q, \end{cases}, \tag{1}$$

where $\left(\frac{a}{\mathbb{F}_q}\right)$ denotes the generalized Legendre symbol. It follows that

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} \left(\left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right) + 1 \right) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right), \tag{2}$$

where the $+1$ that precedes the sum above comes from the inclusion of the point at infinity as the group identity. Typically, $a(q) = -\sum_{x \in F_q} \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)$ is called the trace of Frobenius (see [11] for details).

The Hasse-Weil bound tells us

$$|a(q)| \leq 2\sqrt{q}, \tag{3}$$

and therefore the order of every elliptic curve over $\mathbb{F}_q$ lies in the interval

$$[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]. \tag{4}$$

One of the aims of this paper is to exactly determine the possible orders, or at worst, the exact number of possible orders, that an elliptic curve can have over a given finite field.

1.2 Characterization by j-invariant

The j-invariant of an elliptic curve $E(K) : y^2 = x^3+Ax+B$ is an invariant of the isomorphism class of E in an algebraic closure of K defined as

$$j = -1728\frac{4A^3}{4A^3 + 27B^2}. \tag{5}$$

Note that all curves of j-invariant 0 take the form $y^2 = x^3 + B$, and all curves of j-invariant 1728 are of the form $y^2 = x^3 + Ax$. We will find that this invariant is central to results characterizing orders of elliptic curves. For instance, consider the following two theorems of Gauss:

Theorem 1.1 (Gauss)**.** *Let $p \equiv 1 \pmod 3$ be a prime, and let $E(\mathbb{F}_p) : y^2 = x^3 + B$ be an elliptic curve. Then*

$$\#E(\mathbb{F}_p) = \begin{cases} p+1+2a & B \text{ is a sextic residue mod } p \\ p+1-2a & B \text{ is a cubic residue mod } p, \text{ but not a quadratic residue} \\ p+1-a\pm 3b & B \text{ is a quadratic residue mod } p, \text{ but not a cubic residue} \\ p+1+a\pm 3b & B \text{ is neither a quadratic nor cubic residue mod } p \end{cases}$$

where $p = a^2 + 3b^2$, $b > 0$, and $a \equiv 2 \pmod 3$. If $p \equiv 2 \pmod 3$, then

$$\#E(\mathbb{F}_p) = p + 1.$$

A proof of an equivalent statement of this result can be found in [6].

Theorem 1.2 (Gauss)**.** *Let $p \equiv 1 \pmod 4$ be an odd prime, and let $E(\mathbb{F}_p) : y^2 = x^3+Ax$ be an elliptic curve. If a, b are integers such that $p = a^2 + b^2$, b is even, and $a + b \equiv 1 \pmod 4$, then*

$$\#E(\mathbb{F}_p) = \begin{cases} p+1-2a & \text{if } A \text{ is a biquadratic residue in } \mathbb{F}_p \\ p+1+2a & \text{if } A \text{ is a quadratic residue, but not a biquadratic residue in } \mathbb{F}_p \\ p+1\pm 2b & \text{if } A \text{ is not a quadratic residue in } \mathbb{F}_p \end{cases}$$

If $p \equiv 2 \pmod 3$, then

$$\#E(\mathbb{F}_p) = p + 1.$$

This is proven in [6] and [11]. Note that a is determined uniquely while b is determined up to sign. Note that Theorem 1.1 allows one to exactly determine the order of an elliptic curve of j-invariant equal to 0 over a prime field $\mathbb{F}_p$ in terms of p and the coefficients of the curve, while Theorem 1.2 allows one to do the same for an elliptic curve of j-invariant equal to 1728. In section 2, we extend Theorem 1.1 to elliptic curves defined over all finite fields with $j = 0$, and in section 3, we similarly extend Theorem 1.2 to elliptic curves defined over all finite fields with $j = 1728$. Finally, in section 4, we prove that all elliptic curves of given $j \neq 0, 1728$ take on one of two possible orders over a fixed finite field. Moreover, the methods we employ are all elementary ones, and do not require more than a basic understanding of group and field theory.

1.3 Preliminaries

Our goal in the next three sections is to extend results on elliptic curves over prime fields $\mathbb{F}_p$ to arbitrary finite fields F_{p^r}. We begin with a theorem of Weil that will allow us to determine the order of an elliptic curves over a finite field $\mathbb{F}_{q^n}$ given its order over $\mathbb{F}_q$.

Theorem 1.3 (Weil)**.** *Suppose $\#E(\mathbb{F}_q) = q + 1 - a$, where q need not be prime. Then, for any $n \geq 1$,*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n),$$

where $X^2 - aX + q = (X - \alpha)(X - \beta)$.

The proof mostly follows from algebraic manipulation and the definition of the trace of Frobenius, and can be found in [11].

We say that an elliptic curve $E(K)$ has a (quadratic) *twist* if there exists an elliptic curve isomorphic to E over an algebraic closure $\bar{K}$. In particular, two different curves are *twists* of one another if and only if they have the same j-invariant (see [11], p.43). The following lemma completely characterizes elliptic curves of a fixed j-invariant.

Lemma 1.4. *Let K be a field whose characteristic is neither 2 nor 3, and let $j \neq 0, 1728$ be an element of K. Then j_0 is the j-invariant of an elliptic curve $E(K) : y^2 = x^3 + Ax + B$ if and only if $(A, B) = (k^2 A_0, k^3 B_0)$ for some $k \in K^\times$, where*

$$(A_0, B_0) = (3j(1728 - j_0), 2j(1728 - j_0)^2).$$

Proof. Suppose $E(K) : y^2 = x^3 + Ax + B$ satisfies $(A, B) = (k^2 A_0, k^3 B_0)$ for some $k \in K^\times$. Then we have

$$\begin{aligned} j(E) &= 1728\frac{4A^3}{4A^3 + 27B^2} \\ &= 1728\frac{4(k^2 \cdot 3j_0(1728 - j_0))^3}{4(k^2 \cdot 3j_0(1728 - j_0))^3 + 27(k^3 \cdot 2j_0(1728 - j_0)^2)^2} \\ &= 1728\frac{4 \cdot 27 j_0^3 (1728 - j_0)^3}{4 \cdot 27 j_0^3 (1728 - j_0)^3 + 4 \cdot 27 j_0^2 (1728 - j_0)^4} \\ &= 1728\frac{j_0}{j_0 + 1728 - j_0} \\ &= j_0. \end{aligned}$$

Conversely, suppose that $j_0 \neq 0, 1728$ is the j-invariant of $E(K) : y^2 = x^3 + Ax + B$. We have

$$\begin{aligned} 1728 \cdot \frac{4A^3}{4A^3 + 27B^2} &= j_0 \\ j_0(4A^3 + 27B^2) &= 1728 \cdot 4A^3 \\ 27 j_0 B^2 &= 4(1728 - j_0)A^3 \\ \frac{B^2}{A^3} &= \frac{4(1728 - j_0)}{27 j_0}. \end{aligned}$$

Thus, we have

$$\frac{B_0^2}{A_0^3} = \frac{4j_0^2(1728-j_0)^4}{27j_0^3(1728-j_0)^3} = \frac{4(1728-j_0)}{27j_0} = \frac{B^2}{A^3}.$$

This means that $A^3B_0^2 = A_0^3B^2$. Note that since $j \neq 0, 1728$, none of A, B, A_0, and B_0 are zero. Let $k = \frac{A_0B}{AB_0}$. We have

$$(k^2A_0, k^3B_0) = \left(\frac{A_0^3B^2}{A^2B_0^2}, \frac{A_0^3B^3}{A^3B_0^2}\right) = \left(\frac{A^3B_0^2}{A^2B_0^2}, \frac{A_0^3B^3}{A_0^3B^2}\right) = (A, B).$$

□

Twist techniques are often used in computing orders of elliptic curves (see [2]). We give a standard combinatorial proof to the following result regarding the sum of the orders of $E(\mathbb{F}_q)$ and its twist.

Lemma 1.5. *Consider an elliptic curve $E(\mathbb{F}_q) : y^2 = x^3 + Ax + B$ and its twist $\tilde{E}(\mathbb{F}_q) : y^2 = x^3 + g^2Ax + g^3B$ where g is a generator of $\mathbb{F}_q^\times$. Then $\#E(\mathbb{F}_q) + \#\tilde{E}(\mathbb{F}_q) = 2(q+1)$.*

Proof. Let $\mathrm{QR}(q)$ denote the set of all quadratic residues in $\mathbb{F}_q$. Define the following sets

- $S = \{x \in \mathbb{F}_q \mid x^3 + Ax + B \in \mathrm{QR}(q)\}$;
- $T = gS = \{x \in \mathbb{F}_q \mid (g^{-1}x)^3 + A(g^{-1}x) + B \in \mathrm{QR}(q)\}$; and
- $U = \{x \in \mathbb{F}_q \mid x^3 + g^2Ax + g^3B \in \mathrm{QR}(q)\}$.

We will show that $T \cup U = \mathbb{F}_q$. Suppose for sake of contradiction that there is $x \in \mathbb{F}_q$ that is in neither T nor U. Then neither $(g^{-1}x)^3 + A(g^{-1}x) + B$ nor $x^3 + g^2Ax + g^3B$ is a quadratic residue. Note that g^3 is a quadratic non-residue and so the product

$$g^3((g^{-1}x)^3 + A(g^{-1}x) + B) = x^3 + g^2Ax + g^3B$$

is a quadratic residue, which is a contradiction. Thus, $T \cup U = \mathbb{F}_q$.

Next, we will show that $T \cap U$ is the set of roots of $x^3 + g^2Ax + g^3B = 0$ in $\mathbb{F}_q$. Let $x \in T \cap U$. Then $(g^{-1}x)^3 + A(g^{-1}x) + B$ and $x^3 + g^2Ax + g^3B$ are both quadratic residues. Since these differ by a factor of g^3, $x^3 + g^2Ax + g^3B = 0$.

Now, let n be the number of roots of $x^3 + Ax + B$ over $\mathbb{F}_q$. Note that n is also the number of roots of $x^3 + g^2Ax + g^3B$ over $\mathbb{F}_q$, because each root r of the first polynomial corresponds to the root gr of the second polynomial. It is easy to see that the order of $\#E(\mathbb{F}_q) = 1 + 2|S| - n$ and that $|S| = |T|$. Thus, $\#E(\mathbb{F}_q) = 2|T| - n + 1$. Similarly, $\#\tilde{E}(\mathbb{F}_q) = 2|U| - n + 1$. Thus,

$$\#E(\mathbb{F}_q) + \#\tilde{E}(\mathbb{F}_q) = 2(|T| + |U|) - 2n + 2.$$

Note that $|T| + |U| = q + n$, since every element of $\mathbb{F}_q$ is in at least one set, and the n roots of $x^3 + g^2Ax + g^3B$ are in both sets. Thus,

$$\#E(\mathbb{F}_q) + \#\tilde{E}(\mathbb{F}_q) = 2(q+n) - 2n + 2 = 2(q+1).$$

□

2 Determining the orders of $E(\mathbb{F}_{p^r}) : y^2 = x^3 + B$

Recall that the elliptic curves $E(\mathbb{F}_{p^r}) : y^2 = x^3 + B$ are exactly the curves with j-invariant $j(E) = 0$. We will show that for a fixed finite field $\mathbb{F}_{p^r}$, there are at most six possible orders of curves E with $j(E) = 0$.

Proposition 2.1. *Let $a, B \in \mathbb{F}_{p^r}^\times$. Then $E_1(\mathbb{F}_{p^r}) : y^2 = x^3 + B$ and $E_2(\mathbb{F}_{p^r}) : y^2 = x^3 + a^6 B$ have the same order.*

Proof. Consider the transformation $\mu : E_1 \to E_2$ defined by

$$\mu(x, y) = (a^2 x, a^3 y).$$

Since $a \neq 0$, μ is invertible. Note that

$$(a^3 y)^2 = (a^2 x)^3 + a^6 B \iff a^6 y^2 = a^6 x^3 + a^6 B \iff y^2 = x^3 + B.$$

So, $\mu(x, y) \in E_2$ if and only if $(x, y) \in E_1$. That is, there is a bijection between the points of E_1 and E_2. □

Let H be the image of the map on $\mathbb{F}_q$ given by $x \mapsto x^6$. The proposition above shows that the order of $E : y^2 = x^3 + B$ depends only on which coset of H contains B. We refer to these cosets as *sextic residue classes*. Similarly, we refer to the cosets of the cubes (resp. squares) in $\mathbb{F}_q^\times$ as *cubic* (resp. *quadratic*) *residues*. Hence, the collection of elliptic curves $E(\mathbb{F}_q)$ with $j(E) = 0$ have at most six distinct orders. The following lemma gives the relationship between the orders of the elliptic curves $E(\mathbb{F}_q) : y^2 = x^3 + B$ that are twists of one another.

Lemma 2.2. *Let $g \in \mathbb{F}_q$ be a generator of $\mathbb{F}_q$ and $[g^k]$, $[g^{k+2}]$ and $[g^{k+4}]$ be cosets of the image of the sixth power map. Let $E_i(\mathbb{F}_q) : y^2 = x^3 + B_i$ be elliptic curves where B_1, B_2, and B_3 are taken from $[g^k]$, $[g^{k+2}]$ and $[g^{k+4}]$ respectively. Then,*

$$\#E_1(\mathbb{F}_q) + \#E_2(\mathbb{F}_q) + \#E_3(\mathbb{F}_q) = 3(q + 1).$$

Proof. Let $\mathrm{CR}(q)$ denote the set of all cubic residues in $\mathbb{F}_q$. Define the following sets

$$\begin{aligned}
S_0 &:= \{y \in \mathbb{F}_q \mid y^2 - B \in \mathrm{CR}(q)\} \\
T_0 &:= g^2 S_0 = \{y \in \mathbb{F}_q \mid (g^{-2} y)^2 - B \in \mathrm{CR}(q)\} \\
S_1 &:= \{y \in \mathbb{F}_q \mid y^2 - g^2 B \in \mathrm{CR}(q)\} \\
T_1 &:= g S_1 = \{y \in \mathbb{F}_q \mid (g^{-1} y)^2 - g^2 B \in \mathrm{CR}(q)\} \\
S_2 &:= \{y \in \mathbb{F}_q \mid y^2 - g^4 B \in \mathrm{CR}(q)\}
\end{aligned}$$

We will show that $T_0 \cup T_1 \cup S_2 = \mathbb{F}_q$. Suppose to the contrary that there is $y \in \mathbb{F}_q$ such that $y \notin T_0 \cup T_1 \cup S_2$. Then $(g^{-2}y)^2 - B$, $(g^{-1}y)^2 - g^2B$, and $y^2 - g^4B$ are not cubic residues. Note that g^2 is a cubic non-residue and that

$$y^2 - g^4B = g^4((g^{-2}y)^2 - B) = g^2((g^{-1}y)^2 - g^2B).$$

This means that $y^2 - g^4B$, $(g^{-2}y)^2 - B$, and $(g^{-1}y)^2 - g^2B$ are either all zero or they are in distinct cubic residue classes. Since there are three cubic residue classes, one of which contains the cubic residues, this is a contradiction. Thus, $T_0 \cup T_1 \cup S_2 = \mathbb{F}_q$.

Next, we will show that T_0, T_1, and S_2 are pairwise disjoint, except for the elements $y \in \mathbb{F}_q$ satisfying $y^2 - g^4B = 0$. Suppose that $y \in T_0 \cap T_1$. Then $(g^{-2}y)^2 - B$ and $(g^{-1}y)^2 - g^2B$ are both quadratic residues. Since these differ by a factor of g^2, this can only be the case if $(g^{-1}y)^2 - g^2B = 0$, i.e. $y^2 - g^4B = 0$.

The cases of $y \in T_0 \cap S_2$ and $y \in T_1 \cap S_2$ are analogous.

To conclude the proof, consider the elliptic curves $E_1(\mathbb{F}_q) : y^2 = x^3 + B$, $E_2(\mathbb{F}_q) : y^2 = x^3 + g^3B$, and $E_3(\mathbb{F}_q) : y^2 = x^3 + g^4B$. Let n be the number of roots of $y^2 - B$ over $\mathbb{F}_q$. Note that n is also the number of roots of $y^2 - g^2B$ and $y^2 - g^4B$ over $\mathbb{F}_q$, because each root r of the first polynomial corresponds to the roots g^r and g^2r of the second and third polynomial.

It is easy to see that the $\#E_1(\mathbb{F}_q) = 1 + 3\,|S_0| - 2n$ and $|S_0| = |T_0|$. Thus,

$$\#E_1(\mathbb{F}_q) = 3\,|T_0| - 2n + 1$$

Similarly, $\#E_2(\mathbb{F}_q) = 3\,|T_1| - 2n + 1$ and $\#E_3(\mathbb{F}_q) = 3\,|S_2| - 2n + 1$. Thus,

$$\#E_1(\mathbb{F}_q) + \#E_2(\mathbb{F}_q) + \#E_3(\mathbb{F}_q) = 3(|T_0| + |T_1| + |S_2|) - 6n + 3.$$

Note that $|T_0| + |T_1| + |S_2| = q + 2n$, since every element of $\mathbb{F}_q$ is in at least one of the sets T_0, T_1, S_2, and the roots of $y^2 + g^4B$ are in all three sets. Thus,

$$\#E_1(\mathbb{F}_q) + \#E_2(\mathbb{F}_q) + \#E_3(\mathbb{F}_q) = 3(q - 2n) - 6n + 3 = 3q + 3 = 3(q + 1).$$

□

2.1 The order of $E(\mathbb{F}_q) : y^2 = x^3 + B$ for $q \equiv 1 \pmod 3$

In this section we correct the technique used in [7] that determines the order of $E(\mathbb{F}_q) : y^2 = x^3 + B$ when $q \equiv 1 \pmod 3$.

In [7], the authors construct a polynomial with the property that every possible trace (up to a sign) of a curve $E(\mathbb{F}_q) : y^2 = x^3 + B$ appears as a root of this polynomial. However, the authors use without justification the fact that every root of this polynomial is indeed a possible trace of $E(\mathbb{F}_q)$. In this section, we present their argument with proper justification for this step.

Let B be a generator of $\mathbb{F}_q^\times$, so $B^1, B^2, \ldots, B^6$ are in distinct sextic residue classes in $\mathbb{F}_q$. For $i \in \{1, 2, \ldots, 6\}$ define the following elliptic curves

$$E_i(\mathbb{F}_q) \colon y^2 = x^3 + B^i.$$

On E_i, denote the trace of Frobenius by $a_i(q) = q + 1 - \#E_i(\mathbb{F}_q)$. We know these curves represent all possible orders of curves $E(\mathbb{F}_q)$ with $j = 0$ since curves of the form $E(\mathbb{F}_q) : y^2 = x^3 + B$ have the same order if the corresponding B's are in the same sextic residue class.

Note that B^2, B^4, and B^6 are squares in $\mathbb{F}_q$, so they are squares in $\mathbb{F}_{q^3}$. If one of $\{B, B^3, B^5\}$ is a square in $\mathbb{F}_{q^3}$, then the remaining elements in the set are also squares. Thus B^2, B^4, and B^6 are in the same sextic residue class in $\mathbb{F}_{q^3}$, as are B^1, B^3, and B^5. Using Proposition 2.1, we see that

$$\#E_2(\mathbb{F}_{q^3}) = \#E_4(\mathbb{F}_{q^3}) = \#E_6(\mathbb{F}_{q^3}) \tag{6}$$

$$\#E_1(\mathbb{F}_{q^3}) = \#E_3(\mathbb{F}_{q^3}) = \#E_5(\mathbb{F}_{q^3}) \tag{7}$$

Applying Theorem 1.3 with $n = 3$, we have for $i \in \{1, \ldots, 6\}$,

$$\alpha^3 + \beta^3 = (\alpha + \beta)^3 - 3\alpha\beta(\alpha + \beta) = a_i(q)^3 - 3qa_i(q).$$

Then using Eq. (7) we have

$$a_1(q)^3 - 3qa_1(q) = a_3(q)^3 - 3qa_3(q) = a_5(q)^3 - 3qa_5(q).$$

This means that $a_1(q)$, $a_3(q)$, and $a_5(q)$ are roots of the cubic equation

$$x^3 - 3qx - a_1(q)^3 + 3qa_1(q) = 0.$$

The analogous statement holds for $a_2(q)$, $a_4(q)$, and $a_6(q)$.

Lemma 2.3. *The roots of the polynomial $x^3 - 3qx - a_1(q)^3 + 3qa_1(q)$ are exactly the traces $a_1(q)$, $a_3(q)$, and $a_5(q)$.*

Proof. By Vieta's relations, the sum of the roots of $x^3 - 3qx - a_1(q)^3 + 3qa_1(q)$ is zero. Note also that from Lemma 2.2 we have $a_1(q) + a_3(q) + a_5(q) = 0$. Thus, to show that $a_1(q), a_3(q)$ and $a_5(q)$ are distinct it is enough to show then that two of them are distinct. We will show that the trace $a_3(q)$ is even and the trace $a_5(q)$ is odd.

The point $(x, 0)$ is on the elliptic curve $E_3(\mathbb{F}_q) : y^2 = x^3 + B^3$ if and only if x is a root of the equation $x^3 + B^3 = 0$. It is clear that $x^3 + B^3 = 0$ has at least one root. In fact, there must be an odd number of roots, since if we have two roots r_1 and r_2, then $(x^3 + B^3)/((x - r_1)(x - r_2))$ is a linear term which gives a third root. Therefore there are an odd number of points of the form $(x, 0)$ on the elliptic curve $E_3(\mathbb{F}_q) : y^2 = x^3 + B^3$.

Counting all the points on E_3 (including (x, y) for $y \neq 0$ and the "point at infinity"), we have that E_3 has an even order. Since this paper deals with powers of primes $p > 2$, we have that $a_3(q)$ is even.

The curve $E_5(\mathbb{F}_q) : y^2 = x^3 + B^5$ has an odd number of total points, since $x^3 + B^5 = 0$ has no roots. To see this, assume that r is a root of $x^3 + B^5 = 0$. Then

$$B = \frac{-B^6}{-B^5} = \left(\frac{-B^2}{r}\right)^3$$

However this contradicts the fact that B is not a cubic residue, and so $E_5(\mathbb{F}_q)$ has an odd order.

Thus $a_3(q)$ is even and $a_5(q)$ is odd, so they are distinct. This concludes the claim that $a_1(q)$, $a_3(q)$, and $a_5(q)$ are exactly the roots of $x^3 - 3qx - a_1(q)^3 + 3qa_1(q)$. □

2.2 The order of $E(\mathbb{F}_{p^r}) : y^2 = x^3 + B$ for $p^r \equiv 2 \pmod 3$.

We proceed by considering the cases r is odd and r is even separately.

2.2.1 Order of $E(\mathbb{F}_{p^r}) : y^2 = x^3 + B$ when r is odd.

Note that in this case every element of $\mathbb{F}_q$ is a cubic residue. The map $x \mapsto x^3$ is a homomorphism, and the kernel is the set of solutions to $x^3 - 1 = 0$ which has either 1 or 3 roots. The size of the kernel must divide the order $|\mathbb{F}_{p^r}^\times| = p^r - 1$, and so it must be trivial.

Theorem 2.4. *Let $E(\mathbb{F}_{p^r}) : y^2 = x^3 + B$ be an elliptic curve where $p \equiv 2 \pmod 3$, and r is odd. Then $\#E(\mathbb{F}_{p^r}) = p^r + 1$.*

Proof. For each value of y there is a unique choice of x that satisfy the equation $x^3 = y^2 - B$ since every element in $\mathbb{F}_{p^r}$ is a cubic residue. Including the point at infinity yields a group of order $p^r + 1$. □

2.2.2 The order of $E(\mathbb{F}_{p^r}) : y^2 = x^3 + B$ when r is even.

We use Theorem 1.3 to compute the order of $E(\mathbb{F}_{p^r})$ with r even.

Theorem 2.5. *Let $E(\mathbb{F}_{p^r}) : y^2 = x^3 + B$ be an elliptic curve where $p \equiv 2 \pmod 3$ and r is even. Then*

$$\#E(\mathbb{F}_{p^r}) \in \{p^r \pm 2p^{r/2} + 1, p^r \pm p^{r/2} + 1\}.$$

Proof. Let B be a non-cubic, non-quadratic residue in $\mathbb{F}_{p^r}$ and define $E_i : y^2 = x^3 + B^i$ for $1 \le i \le 4$. Also, let $a_i(p^r)$ be the trace of E_i over $\mathbb{F}_{p^r}$. As in the last section, it follows that $a_1(p^r), a_3(p^r)$, and $a_5(p^r)$ are roots of the polynomial

$$f(x) = x^3 - 3p^r x - a(p^{3r})$$

where $a(p^{2r})$ is the trace of E_1 (equivalently E_3 and E_5) over $\mathbb{F}_{p^{3r}}$. We compute $a(p^{2r})$ explicitly by noting that if $A \in \mathbb{F}_p$, then $E' : y^2 = x^3 + A$ taken as an elliptic curve over $\mathbb{F}_p$ has trace 0 by Theorem 2.4. Hence, the trace of Frobenius of $E'(\mathbb{F}_{p^{3r}})$ is

$$\sum_{i=0}^{\lfloor 3r/2 \rfloor} \frac{3r}{3r-i}\binom{3r-i}{i}(-p)^i(a(p))^{3r-2i},$$

where $a(p) = 0$, so we may assume that $a(p^{3r}) = 2(-p)^{3r/2}$.

Now, $a_1(p^r), a_3(p^r)$, and $a_5(p^r)$ are the roots of

$$f(x) = x^3 - 3p^r x - 2p^{3r/2} = (x - 2p^{r/2})(x + p^{r/2})^2.$$

from which the result follows since $a_1(p^r) = -a_4(p^r)$, $a_2(p^r) = -a_5(p^r)$, and $a_3(p^r) = -a_6(p^r)$. □

3 Determining the orders of $E(\mathbb{F}_{p^r}) : y^2 = x^3 + Ax$

Using the following proposition we see that the elliptic curves curves $E_1(\mathbb{F}_q) : y^2 = x^3 + Ax$ and $E_2(\mathbb{F}_q) : y^2 = x^3 + A'x$ have the same order when A and A' are in the same biquadratic residue class. As in the last section, by biquadratic residue class, we mean cosets of the subgroup of fourth powers in $\mathbb{F}_q^\times$. This implies that curves $E : y^2 = x^3 + Ax$ have at most four distinct orders.

Proposition 3.1. *Let $a \in \mathbb{F}_q^\times$. Then the elliptic curves $E_1(\mathbb{F}_q) : y^2 = x^3 + Ax$ and $E_2(\mathbb{F}_q) : y^2 = x^3 + a^4Ax$ have the same order .*

Proof. Let $\mu : E_1 \to E_2$ be as defined in Proposition 2.1. Then we have

$$(a^3y)^2 = (a^2x)^3 + a^4A(a^2x) \quad \Longleftrightarrow \quad a^6y^2 = a^6x^3 + a^6Ax \quad \Longleftrightarrow \quad y^2 = x^3 + Ax.$$

This shows that μ is a bijection. □

3.1 The order of $E(\mathbb{F}_{p^r}) : y^2 = x^3 + Ax$ for $p \equiv 1 \pmod 4$

We extend the techniques of [7] to prove that in the case when $p \equiv 1 \pmod 4$ the elliptic curve $E(\mathbb{F}_{p^r}) : y^2 = x^3 + Ax$ has four possible orders.

Proposition 3.2. *Suppose A is a non-quadratic residue in $\mathbb{F}_{p^r}^\times$ and define the following curves.*

$$E_1 : y^2 = x^3 + Ax$$
$$E_2 : y^2 = x^3 + A^2x$$
$$E_3 : y^2 = x^3 + A^3x$$
$$E_4 : y^2 = x^3 + A^4x$$

Let $a_i(p^r)$ be the trace of $E_i(\mathbb{F}_{p^r}^\times)$. Then each $a_i(p^r)$ is a root to the quartic polynomial.

$$f(x) = x^4 - 4p^rx^2 + 2p^{2r} - a_1(p^{4r})$$

Note that $a_1(p^{4r})$ may be replaced by $a_j(p^{4r})$ for $j = 2, 3, 4$.

Proof. By Lemma 1.5, $a_1(p^r) = -a_3(p^r)$ and $a_2(p^r) = -a_4(p^r)$. As a general fact, every element of $\mathbb{F}_{p^r}$ is a biquadratic residue in $\mathbb{F}_{p^{4r}}$. Hence, A, A^2, A^3, and A^4 are in the same biquadratic residue class of $\mathbb{F}_{p^{4r}}$. Thus,

$$\#E_1(\mathbb{F}_{p^{4r}}) = \#E_2(\mathbb{F}_{p^{4r}}) = \#E_3(\mathbb{F}_{p^{4r}}) = \#E_4(\mathbb{F}_{p^{4r}}).$$

By Weil's theorem, knowing the trace $a_j(p^r) = p^r + 1 - \#E_j(\mathbb{F}_{p^r})$, the trace $a_j(p^{4r})$ of $E_j(\mathbb{F}_{p^{4r}})$ is given by

$$a_j(p^{4r}) = \sum_{i=0}^{2r} \frac{4r}{4r-i} \binom{4r-i}{i} (-p)^i a_j(p^r)^{4r-2i}.$$

Applying this to each $j = 1, \ldots, 4$, we obtain the following:

$$\begin{aligned} \#E_i(\mathbb{F}_{p^{4r}}) &= p^{4r} + 1 - (a_1(p^r)^4 - 4p^r a_1(p^r)^2 + 2p^{2r}) \\ &= p^{4r} + 1 - (a_2(p^r)^4 - 4p^r a_2(p^r)^2 + 2p^{2r}) \\ &= p^{4r} + 1 - (a_3(p^r)^4 - 4p^r a_3(p^r)^2 + 2p^{2r}) \\ &= p^{4r} + 1 - (a_4(p^r)^4 - 4p^r a_4(p^r)^2 + 2p^{2r}) \end{aligned}$$

Thus, each $a_i(p^r)$ is a root to the quartic polynomial

$$f(x) = x^4 - 4p^r x^2 + 2p^{2r} - a_1(p^{4r}).$$

□

As $a_i(p^{4r}) = a_j(p^{4r})$ for $1 \leq i, j \leq 4$, we may denote $a_1(p^{4r})$ simply by $a(p^{4r})$. We will use the following fact when further analyzing $a_1(p^r), \ldots, a_4(p^r)$.

Proposition 3.3. *If $p > 3$ is prime, then (-1) is non-quadratic residue in $\mathbb{F}_{p^r}$ if and only if $p^r \equiv 3 \pmod 4$.*

Proof. Suppose $p^r \equiv 3 \pmod 4$. Choose a generator g of $\mathbb{F}_{p^r}^\times$, and let n be an integer such that $p^r - 1 = 4n + 2$. Then $1 = g^{4n+2}$ implies that $-1 = g^{2n+1}$ which is shows that (-1) is non-quadratic residue in $\mathbb{F}_{p^r}$. Now, suppose $p^r \equiv 1 \pmod 4$, and let g be a generator of $\mathbb{F}_{p^r}^\times$. Note that since $p^r - 1 = 4n$ for some n, we have that $1 = g^{4n}$, and $-1 = g^{2n} = (g^n)^2$. But this contradicts the fact that (-1) is non-quadratic residue in $\mathbb{F}_{p^r}$. □

The following proposition shows that $\{a_1(p^r), a_3(p^r)\} \cap \{a_2(p^r), a_4(p^r)\} = \varnothing$.

Proposition 3.4. *Let $p > 3$ be a prime with $p^r \equiv 1 \pmod 4$ and $E(\mathbb{F}_{p^r}) : y^2 = x^3 + Ax$ be an elliptic curve. If A is a quadratic residue in $\mathbb{F}_{p^r}$, then $\#E(\mathbb{F}_{p^r}) \equiv 0 \pmod 4$, and if A is a non-quadratic residue, then $\#E(\mathbb{F}_{p^r}) \equiv 2 \pmod 4$.*

Proof. By Proposition 3.3, it follows that $-1 = d^2$ for some $d \in \mathbb{F}_{p^r}^\times$. Suppose $A = c^2$, for some $c > 0$. Then

$$x^3 + Ax = x(x^2 + A) = x(x^2 - c^2 d^2) = x(x + cd)(x - cd).$$

This equation has three roots: $x = 0, cd, -cd$. Note that if $(x, \pm y)$ is a point on the curve E and $y \neq 0$, then $(-x, \pm dy)$ is also a point on the curve E. Thus, adding the point at infinity and the points $(0, 0), (cd, 0)$, and $(-cd, 0)$, we find that $\#E(\mathbb{F}_{p^r}) \equiv 0 \pmod 4$.

If A is non-quadratic residue in $\mathbb{F}_{p^r}$, then the polynomial $x^2 + A$ has no roots in which case $\#E(\mathbb{F}_{p^r}) \equiv 2 \pmod 4$. □

Lemma 3.5. *Let $a_i(p^r)$ be the trace of $E_i(\mathbb{F}_{p^r}^\times)$ for $1 \leq i \leq 4$. Then the roots of the polynomial*

$$f(x) = x^4 - 4p^r x^2 + 2p^{2r} - a(p^{4r})$$

are exactly the traces $a_1(p^r), \ldots, a_4(p^r)$.

Proof. As demonstrated above, $f(a_i(p^r)) = 0$ for each $1 \leq i \leq 4$. Since the $f(x)$ has no terms of odd order, $\bar{x}$ is a root if and only if $-\bar{x}$ is a root. Since $a_1(p^r) = -a_3(p^r)$ and $a_2(p^r) = -a_4(p^r)$, it suffices to show that $a_1(p^r) \neq a_2(p^r)$ which follows directly from Proposition 3.4. □

3.2 The order of $E(\mathbb{F}_{p^r}) : y^2 = x^3 + Ax$ for $p \equiv 3 \pmod 4$

The point counting arguments for curves $E : y^2 = x^3 + Ax$ rely on facts about quadratic residues in $\mathbb{F}_{p^r}$. Hence, the case of $E(\mathbb{F}_{p^r}) : y^2 = x^3 + Ax$ where r is even will be treated separately from the case where r is odd.

3.2.1 The order of $E(\mathbb{F}_{p^r}) : y^2 = x^3 + Ax$ for r odd

First we will show that $\#E(\mathbb{F}_{p^r}) = p^r + 1$ when $p \equiv 3 \pmod 4$. To prove this, we need the following fact about quadratic residues.

Theorem 3.6. *Let $p > 3$ be prime and $p \equiv 3 \pmod 4$. Then the order of the elliptic curve $E(\mathbb{F}_{p^r}) : y^2 = x^3 + Ax$ is $p^r + 1$.*

Proof. Consider $E(\mathbb{F}_{p^r}) : y^2 = x(x^2 + A)$ when $x \neq 0$. Note that $x^2 + A = (-x)^2 + A$, and that x is a square if and only if $-x$ is not a square by Proposition 3.3.

Thus for every non-zero value of x for which $x(x^2 + A)$ is a square, we have that $(-x)((-x)^2 + A)$ is not a square, and vice-versa. Thus there are $(p^r - 1)/2$ values of x for which $x(x^2 + A)$ is a square.

Furthermore, for each such value of x, there are two y values such that $(x, y) \in E$.

Finally, if $x = 0$, then $y = 0$, and we include also the point at infinity. Adding up all the points on the curve yields $(p^r - 1) + 1 + 1 = p^r + 1$.

□

3.2.2 The order of $E(\mathbb{F}_{p^r}) : y^2 = x^3 + Ax$ for r even

We will use Theorem 1.2 for orders of $E(\mathbb{F}_p)$ to compute the possible orders of $E(\mathbb{F}_{p^r})$ when $p \equiv 3 \pmod 4$ and r is even.

Theorem 3.7. *Let $E(\mathbb{F}_{p^r}) : y^2 = x^3 + Ax$ be an elliptic curve where $p \equiv 3 \pmod 4$ and r is even. Then*

$$\#E(\mathbb{F}_{p^r}) \in \{p^r + 1, p^r \pm 2p^{r/2} + 1\}.$$

Proof. For $1 \leq i \leq 4$, define $E_i(\mathbb{F}_{p^r}) : y^2 = x^3 + A^i x$, and let $a_i(p^r)$ be the trace of E_i for some quadratic non-residue in $\mathbb{F}_{p^r}$. Using the same arguments as in Section 2.1, $a_1(p^r), a_2(p^r), a_3(p^r)$ and $a_4(p^r)$ are the roots of the polynomial

$$f(x) = x^4 - 4p^r x^2 + 2p^{r/2} - a_4(p^{4r}).$$

Without loss of generality we can assume that $A^4 \in \mathbb{F}_p$. By Theorem 3.6 we have that $\#E(\mathbb{F}_p) = p + 1$, i.e. $a(p) = 0$.

By Weil's theorem and the fact that $a(p) = 0$ we have

$$a_4(p^{4r}) = \sum_{i=0}^{2r} \frac{4r}{4r-i}\binom{4r-i}{i}(-p)^i a(p)^{4r-2i}.$$

Hence, $a_1(p^r)$, $a_2(p^r)$, $a_3(p^r)$, and $a_4(p^r)$ are the roots of the polynomial

$$f(x) = x^4 - 4p^r x^2 + 2p^{r/2}a_4(p^{4r}) = x^4 - 4p^r x^2$$

which proves the theorem. □

4 Determining the orders of $E(\mathbb{F}_{p^r}) : y^2 = x^3 + Ax + B$

An elliptic curve with $j \neq 0, 1728$ can have one of exactly two possible orders over a finite field F_{p^r}. We demonstrate this here. To do so, we make use of the following lemma.

Lemma 4.1. *For any quadratic residue $k \in \mathbb{F}_{p^r}^\times$, the elliptic curve $E_1(\mathbb{F}_{p^r}) : y^2 = x^3+Ax+B$ has the same order as the elliptic curve $E_2(\mathbb{F}_{p^r}) : y^2 = x^3 + k^2Ax + k^3B$.*

Proof. Let $m \in \mathbb{F}_q^\times$ satisfy $m^2 = k$. Consider the mapping $\psi : E_1 \to E_2$ defined by $\psi((x, y)) = (m^2x, m^3y)$. If $(x, y) \in E_1$ then

$$(m^3y)^2 = m^6y^2 = m^6(x^3 + Ax + B) = (m^2x)^3 + k^2(m^2x) + k^3B,$$

so $\psi((x, y)) \in E_2$. Similarly, if $(x, y) \in E_2$ then

$$(m^{-3}y)^2 = m^{-6}y^2 = m^{-6}(x^3 + k^2Ax + k^3B) = (m^{-2}x)^3 + A(m^{-2}x) + B,$$

so $\psi^{-1}((x, y))$ (which is clearly well-defined, since $m \in \mathbb{F}_{p^r}^\times$) is on E_1. Thus, ψ defines a bijection between the points on E_1 and the points on E_2, and thus E_1 and E_2 must have the same order, as desired. □

Theorem 4.2. *Let $p \neq 2, 3$ be prime and r be a positive integer. For every $j_0 \in \mathbb{F}_{p^r}$ with $j_0 \neq 0, 1728$, there exists a non-negative integer t such that all elliptic curves $E(\mathbb{F}_{p^r})$ with j-invariant j_0 satisfy $\#E(\mathbb{F}_{p^r}) = p^r + 1 \pm t$.*

Proof. It follows that there are at most two orders of elliptic curves over $\mathbb{F}_{p^r}$ for a fixed j_0, corresponding to the two possible quadratic residue classes of k over $\mathbb{F}_{p^r}$, where, from Lemma 1.4, $(A, B) = (k^2 \cdot 3j(12^3 - j), k^3 \cdot 2j(12^3 - j)^2)$, since for two values of k from the same residue class, the two corresponding elliptic curves have the same order.

All we have left to prove is that these two orders can be expressed as $p^r + 1 \pm t$ for some t. Define $E_1 : y^2 = x^3 + A_0x + B_0$ with A_0 and B_0 as in Lemma 1.4. By this lemma, any curve with j-invariant j_0 can be expressed as (k^2A_0, k^3B_0); let E_2 be a curve where k is a generator of $\mathbb{F}_{p^r}$ (and thus a quadratic non-residue). By Lemma 1.5, $\#E_1(\mathbb{F}_{p^r}) + \#E_2(\mathbb{F}_p^r) = 2(p^r + 1)$. Therefore, these two orders can be expressed as $p^r + 1 \pm t$ for some non-negative integer t, and so we are done. □

References

[1] A. Aabrandt and V. L. Hansen,*A Note on Powers in Finite Fields*, **International Journal of Mathematical Education in Science and Technology** Vol. 47(6) (2016), 987–991.

[2] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*, LNS 265, **Cambridge University Press**, (1999).

[3] D. Boneh, K. Rubin, and A. Silverberg, *Finding composite order ordinary elliptic curves using the Cocks-Pinch method*, **Journal of Number Theory** Vol. 131 (5), (2011), 832–841.

[4] Carella, N.A. "Topic in Elliptic Curves Over Finite Fields: The Groups of Points". arXiv:1103:4560.

[5] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, **John Wiley & Sons**, Vol. 34 (2011).

[6] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, **Springer Science & Business Media**, Vol. 84 (2013).

[7] Y. Morikawa and Y. Nogami, *The orders of elliptic curves of the form $y^2 = x^3 + b$*, **Memoirs of the Faculty of Engineering, Okayama University**, Vol. 40 (2006), 83–94.

[8] René Schoof, *Counting points on elliptic curves over finite fields*, **Journal de Théorie des Nombres de Bordeaux 7** (1995), pp. 219254.

[9] D. Shanks, *Class number, a theory of factorization and genera*, **Proc. Symp. Pure Math., Amer. Math. Soc.**, Vol. 20 (1971), pp. 415–440.

[10] I. E. Shparlinski and A. V. Sutherland, *On the distribution of Atkin and Elkies primes*, **Found. Comp. Math.**,Vol. 14 (2014), 285–297.

[11] L. C. Washington, *Elliptic curves: Number Theory and Cryptography*, **CRC Press**, (2008).

[12] W. Waterhouse, *Abelian varieties over finite fields*, **Annales Scientifiques de l'École Normale Supérieure**, Vol. 2(4) (1969), 521–560.