Isomorphism classes of Edwards curves over finite fields

Reza Rezaeian Farashahi
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
and
Department of Mathematical Sciences
Isfahan University of Technology
P.O. Box 85145 Isfahan, Iran
reza.farashahi@mq.edu.au

Dustin Moody
National Institute of Standards and Technology (NIST)
100 Bureau Drive, Gaithersburg, MD, 20899, USA
dbmoody25@gmail.com

Hongfeng Wu
College of Sciences
North China University of Technology
Beijing 100144, P.R. China
whfmath@gmail.com

Abstract

Edwards curves are an alternate model for elliptic curves, which have attracted notice in cryptography. We give exact formulas for the number of $\mathbb{F}_q$-isomorphism classes of Edwards curves and twisted Edwards curves. This answers a question recently asked by R. Farashahi and I. Shparlinski.

1 Introduction

Elliptic curves have been an object of much study in mathematics. Recall that an elliptic curve is a smooth projective genus 1 curve, with a given rational point. The traditional model for an elliptic curve has been the Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

where the a_i are elements in some field $\mathbb{F}$. While other models for elliptic curves have long been known, in the past few years there has been renewed interest in these alternate models. This attention has primarily come from the cryptographic community.

In 2007, Edwards proposed a new model for elliptic curves [10]. Let $\mathbb{F}$ be a field with characteristic $p \neq 2$. These original *Edwards curves*, defined over $\mathbb{F}$, are given by the equation

$$\mathbf{E}_{\mathrm{E},c}: \quad X^2 + Y^2 = c^2(1 + X^2Y^2), \tag{1}$$

with $c \in \mathbb{F}$ and $c^5 \neq c$. Edwards curves and its variants over finite fields have attracted great interest in elliptic curve cryptography (see [2, 3, 4, 5, 6]). In particular, Bernstein and Lange [3] have considered the closely related family of *Edwards curves*

$$\mathbf{E}_{\mathrm{BL},d}: \quad X^2 + Y^2 = 1 + dX^2Y^2, \tag{2}$$

where $d \in \mathbb{F}$ with $d \neq 0, 1$. They also considered the generalization of this family, the so-called *twisted Edwards* family, [2], given by

$$\mathbf{E}_{\mathrm{TE},a,d}: \quad aX^2 + Y^2 = 1 + dX^2Y^2, \tag{3}$$

where a, d are distinct nonzero elements of $\mathbb{F}$, with $d \neq 1$. In the same paper, they show that a twisted Edwards curve is birationally equivalent to a *Montgomery curve.* We recall, [18], that an elliptic curve given by a Montgomery equation is of the form

$$\mathbf{E}_{\mathrm{M},A,B}: \quad BY^2 = X^3 + AX^2 + X, \tag{4}$$

where $A, B \in \mathbb{F}$ with $A \neq \pm 2$ and $B \neq 0$.

The field of definition for elliptic curves in a cryptographic setting is over a finite field $\mathbb{F}_q$. It is a natural question to count the number of distinct elliptic curves over $\mathbb{F}_q$ up to isomorphism. This has been done for Weierstrass curves [17, 20], and various alternate models of elliptic curves [12, 13, 14, 15, 16]. The number of isomorphism classes of hyperelliptic curves over finite fields has also been of interest [7, 8, 9, 11].

For the Edwards families (1) and (2), Farashahi and Shparlinski gave explicit formulas for the number of distinct elliptic curves (up to isomorphism over the algebraic closure of the ground field). The tool they used was the *j-invariant* of an elliptic curve. They remark that it would be interesting to find exact formulas for the number of distinct curves, up to isomorphism over $\mathbb{F}_q$.

The distinction is subtle. Two curves may be isomorphic over $\overline{\mathbb{F}}_q$ without being isomorphic over $\mathbb{F}_q$. The issue is whether the isomorphism can be given by rational functions defined over $\mathbb{F}_q$ or $\overline{\mathbb{F}}_q \setminus \mathbb{F}_q$. For cryptography, the finite field $\mathbb{F}_q$ is fixed, and calculations are done over $\mathbb{F}_q$ – not its algebraic closure $\overline{\mathbb{F}}_q$. For cryptographic purposes, two elliptic curves which are $\mathbb{F}_q$-isomorphic are essentially the same curve, which is not true if they are only isomorphic over $\overline{\mathbb{F}}_q$.

In this work, we answer the question of Farashahi and Shparlinski. That is, we find precise formulas for the number of distinct elliptic curves in the Edwards curve families (1) and (2), up to isomorphism over a finite field. We are able to do so by elementary methods. We also answer the same question for the families (3) and (4), i.e., the twisted Edwards and Montgomery curves.

This paper is organized as follows. In Section 2 we review some background material about elliptic curves. In Section 3 we find exact formulas for the number of $\mathbb{F}_q$-isomorphism classes of the Edwards curves (1) and (2). We do the same for twisted Edwards (3) and Montgomery curves (4) in section 4. We conclude in Section 5 with some directions for future study.

Throughout the paper, the letter p always denotes a prime number and the letter q always denotes a prime power. Let $\mathbb{F}_q$ be a finite field with characteristic greater than 3. For a field $\mathbb{F}$, denote its algebraic closure by $\overline{\mathbb{F}}$ and its multiplicative subgroup by $\mathbb{F}^*$. Let χ denote the quadratic character in $\mathbb{F}_q$. That is, for $u \in \mathbb{F}_q^*$, $\chi(u) = 1$ if and only if $u = w^2$ for some $w \in \mathbb{F}_q$. Let $\mathcal{Q}$ be the set of quadratic residues of $\mathbb{F}_q \setminus \{0, 1\}$, i.e.,

$$\mathcal{Q} = \{u \in \mathbb{F}_q : \ u = 0, 1, \ \chi(u) = 1\}.$$

The cardinality of a finite set $\mathcal{S}$ is denoted by $\#\mathcal{S}$.

2 Elliptic curves

2.1 Background on isomorphisms

We briefly review some material on isomorphisms between elliptic curves. For more details on isomorphisms, or more generally on elliptic curves, see [21, 22]. Two elliptic curves are isomorphic over a field $\mathbb{F}$, if there is an isomorphism between the two curves which is defined over $\mathbb{F}$. Isomorphisms on Edwards curves have not yet been as well studied as isomorphisms on Weierstrass curves. In order to obtain our results, it will be informative to review what is known about isomorphisms between Weierstrass curves.

It is well known (see e.g. [17]) that two elliptic curves given by Weierstrass equations are isomorphic over $\mathbb{F}$ if and only if there is a change of variables between them of the form:

$$(x, y) \to (\alpha^2 x + r, \alpha^3 y + \alpha^2 sx + t),$$

where $\alpha = 0$, and $\alpha, r, s, t \in \mathbb{F}$. In the case, where $\alpha, r, s, t \in \overline{\mathbb{F}}$, the two elliptic curves are called *isomorphic* over $\overline{\mathbb{F}}$ or *twists* of each other. We will refer to a change of variables of the above form as *an admissible change of variables* over $\mathbb{F}$. When the field $\mathbb{F}$ is clear from context, we will omit it.

The j-invariant is a numerical invariant that can be used to tell when two curves are isomorphic over $\overline{\mathbb{F}}_q$. All of the elliptic curves we will consider in this paper can be represented by the *Legendre equation*

$$\mathbf{E}_{\mathrm{L},u}: \quad Y^2 = X(X-1)(X-u), \tag{5}$$

for some $u \in \mathbb{F}^*$. The j-invariant of $\mathbf{E}_{\mathrm{L},u}$ is given by

$$j(\mathbf{E}_{\mathrm{L},u}) = \frac{2^8(u^2-u+1)^3}{(u^2-u)^2}.$$

Two elliptic curves are $\overline{\mathbb{F}}_q$-isomorphic if and only if they have the same j-invariant. Farashahi and Shparlinski used this fact to prove their results about the number of $\overline{\mathbb{F}}_q$-isomorphism classes. Note, however, that two elliptic curves with the same j-invariant need not be isomorphic over $\mathbb{F}_q$.

In the following, we use $J_{\mathrm{E}}(q)$, $J_{\mathrm{BL}}(q)$, $J_{\mathrm{TE}}(q)$, $J_{\mathrm{M}}(q)$ and $J_{\mathrm{L}}(q)$ to denote the number of distinct j-invariants of the curves defined over $\mathbb{F}_q$ in the families (1), (2), (3), (4) and (5) respectively. Moreover, we use $I_{\mathrm{E}}(q)$, $I_{\mathrm{BL}}(q)$, $I_{\mathrm{TE}}(q)$, $I_{\mathrm{M}}(q)$ and $I_{\mathrm{L}}(q)$ to denote the number of $\mathbb{F}_q$-isomorphism classes of the families (1), (2), (3), (4) and (5) respectively.

2.2 Legendre curves

A Legendre equation is a variant of the Weierstrass equation with just one parameter. Any elliptic curve defined over an algebraically closed field $\mathbb{F}$ of characteristic $p = 2$ can be expressed by the Legendre curve $\mathbf{E}_{\mathrm{L},u}$, given by (5), for some $u \in \mathbb{F}^*$.

We consider the curves $\mathbf{E}_{\mathrm{L},u}$ given by the Legendre equation (5) over a finite field $\mathbb{F}_q$. We require $u = 0, 1$, so that the curve $\mathbf{E}_{\mathrm{L},u}$ is nonsingular. The number of distinct isomorphism classes of Legendre curves over $\mathbb{F}_q$ has been studied in [12, 13, 16]. To be more precise, for the number $J_{\mathrm{L}}(q)$ of distinct values of the j-invariant of the family (5), we have

$$J_{\mathrm{L}}(q) = \lfloor (q+5)/6 \rfloor .$$

Furthermore, the number $I_{\mathrm{L}}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family (5) is

$$I_{\mathrm{L}}(q) = \begin{cases} \lfloor (7q+29)/24 \rfloor & \text{if } q \equiv 1 \pmod{12}, \\ \lfloor (q+2)/3 \rfloor & \text{if } q \equiv 3, 7 \pmod{12}, \\ \lfloor (7q+13)/24 \rfloor & \text{if } q \equiv 5, 9 \pmod{12}, \\ (q-2)/3 & \text{if } q \equiv 11 \pmod{12}. \end{cases}$$

Now we consider the following subfamily of Legendre curves over $\mathbb{F}_q$, and give explicit formulas for its cardinality. We will use the results of this section to count the number of $\mathbb{F}_q$-isomorphism classes of Edwards curves. Recall that $\mathcal{Q}$ is the set of quadratic residues of $\mathbb{F}_q \setminus \{0, 1\}$. Let

$$\mathcal{L}_S = \{\mathbf{E}_{\mathrm{L},u} : \ u \in \mathcal{Q}\} . \tag{6}$$

We also consider two other subfamilies of Legendre curves over $\mathbb{F}_q$. Let

$$\mathcal{L}_{S_1} = \{\mathbf{E}_{\mathrm{L},u} : \ u \in \mathcal{Q}, 1-u \in \mathcal{Q}\} , \tag{7}$$

$$\mathcal{L}_T = \{\mathbf{E}_{\mathrm{L},1-u} : \ u \in \mathcal{Q}\} . \tag{8}$$

As before, we use $I_{\mathrm{L}_S}(q)$, $I_{\mathrm{L}_{S_1}}(q)$ and $I_{\mathrm{L}_T}(q)$ to denote the number of $\mathbb{F}_q$-isomorphism classes of the families (6), (7) and (8) respectively.

Lemma 2.1. *For all elements $u, v \in \mathcal{Q}$, we have $\mathbf{E}_{\mathrm{L},u} \cong_{\mathbb{F}_q} \mathbf{E}_{\mathrm{L},v}$ if and only if u, v satisfy one of the following:*

1. $v \in \left\{u, \frac{1}{u}\right\}$, *2.* $v \in \quad 1-u, \frac{1}{1-u}, \frac{u-1}{u}, \frac{u}{u-1}$ *and* $\chi(-1) = 1$.

Proof. See [13, Lemma 2]. □

Now, we give an exact formula for the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ of the family (6).

Lemma 2.2. *For any prime* $p \geq 3$*, for the number* $I_{\mathrm{L}_S}(q)$ *of* $\mathbb{F}_q$*-isomorphism classes of the family* (6)*, we have*

$$I_{\mathrm{L}_S}(q) = \begin{cases} \left\lfloor \dfrac{q+5}{6} \right\rfloor, & \text{if } q \equiv 1 \pmod 4, \\ \dfrac{q-3}{4}, & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Proof. For a fixed value $u \in \mathcal{Q}$, we let

$$\mathcal{I}_{\mathcal{L}_S,u} = \quad v \ : \ v \in \mathcal{Q}, \ \mathbf{E}_{\mathrm{L},u} \cong_{\mathbb{F}_q} \mathbf{E}_{\mathrm{L},v} \quad .$$

We note that

$$I_{\mathrm{L}_S}(q) = \sum_{u \in \mathcal{Q}} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}}.$$

We partition $\mathcal{Q}$ into the following sets:

$$\mathcal{A} \cup \mathcal{B},$$

where

$$\mathcal{A} = \quad u \in \mathcal{Q} \ : u = -1, 2, 1/2, u^2 - u + 1 = 0 \quad ,$$

and $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ with

$$\mathcal{B}_1 = \{u \in \mathcal{Q} \ : \ u = -1, 2, 1/2\}, \quad \mathcal{B}_2 = \quad u \in \mathcal{Q} \ : \ u^2 - u + 1 = 0 \quad .$$

We further partition $\mathcal{A}$ into the sets

$$\mathcal{A}_1 \cup \mathcal{A}_{-1}$$

where

$$\begin{aligned} \mathcal{A}_1 &= \{u \in \mathcal{Q} \ : \ u \notin \mathcal{B}, \ \chi(1-u) = 1\}, \\ \mathcal{A}_{-1} &= \{u \in \mathcal{Q} \ : \ u \notin \mathcal{B}, \ \chi(1-u) = -1\}. \end{aligned}$$

Now, for all $u \in \mathcal{Q}$, we explicitly express the set $\mathcal{I}_{\mathcal{L}_S,u}$ and compute its cardinality. We note that the sets $\mathcal{B}_1$ and $\mathcal{B}_2$ are disjoint precisely when $p > 3$. If $p = 3$, we have

$$\mathcal{B} = \mathcal{B}_1 = \mathcal{B}_2 = \{u \in \mathcal{Q} : u = -1\}.$$

We know that $-1 \in \mathcal{Q}$ if and only if $q \equiv 1 \pmod 4$. So by Lemma 2.1 we obtain

$$\mathcal{I}_{\mathcal{L}_S,-1} = \mathcal{B} = \{-1\}, \text{ if } q \equiv 9 \pmod{12}.$$

We now use the fact that $\chi(2) = 1$ if and only if $q \equiv \pm 1 \pmod 8$. So, for $p > 3$, we have

$$\mathcal{B}_1 = \begin{cases} \{-1, 2, 1/2\}, & \text{if } \ q \equiv 1 \pmod 8, \\ \{-1\}, & \text{if } \ q \equiv 5 \pmod 8, \\ \{2, 1/2\}, & \text{if } \ q \equiv 7 \pmod 8. \end{cases}$$

Then, using Lemma 2.1 again, we see that

$$\mathcal{I}_{\mathcal{L}_S,u} = \mathcal{B}_1, \text{ if } u \in \mathcal{B}_1.$$

Next, we assume that $u \in \mathcal{B}_2$, i.e., $u \in \mathbb{F}_q$ with $u^2 - u + 1 = 0$. This happens if $\chi(-3) = 1$ which is equivalent to the case where $q \equiv 1 \pmod 6$. Then, $u = \frac{1+\zeta}{2}$, where ζ is a square root of -3 in $\mathbb{F}_q$. Notice u can be written as $u = -(\frac{1-\zeta}{2})^2$. So, $u \in \mathcal{Q}$ if and only if $q \equiv 1 \pmod 4$. In other words, $\mathcal{B}_2 = \emptyset$ if and only $q \equiv 1 \pmod{12}$. From Lemma 2.1, we have

$$\mathcal{I}_{\mathcal{L}_S,u} = \mathcal{B}_2 = \{u, 1/u\}, \text{ if } u \in \mathcal{B}_2.$$

Now we consider $u \in \mathcal{A}$. From Lemma 2.1, we have

$$\mathcal{I}_{\mathcal{L}_S,u} = \{u, 1/u\}, \text{ if } u \in \mathcal{A}, \ q \equiv 3 \pmod 4.$$

Similarly, we also have

$$\mathcal{I}_{\mathcal{L}_S,u} = \{u, 1/u\}, \text{ if } u \in \mathcal{A}_{-1}, \ q \equiv 1 \pmod 4,$$

and

$$\mathcal{I}_{\mathcal{L}_S,u} = \left\{u, \frac{1}{u}, 1-u, \frac{1}{1-u}, \frac{u-1}{u}, \frac{u}{u-1}\right\}, \text{ if } u \in \mathcal{A}_1, \ q \equiv 1 \pmod 4.$$

Putting this all together, for any $u \in \mathcal{Q}$, we have

$$\#\mathcal{I}_{\mathcal{L}_S,u} = \begin{cases} \#\mathcal{B}_1, & \text{if } u \in \mathcal{B}_1, \\ \#\mathcal{B}_2, & \text{if } u \in \mathcal{B}_2, \\ 2, & \text{if } u \in \mathcal{A}, \text{ and } q \equiv 3 \pmod 4, \\ 2, & \text{if } u \in \mathcal{A}_{-1}, \text{ and } q \equiv 1 \pmod 4, \\ 6, & \text{if } u \in \mathcal{A}_1, \text{ and } q \equiv 1 \pmod 4. \end{cases}$$

Now we observe that

$$I_{\mathrm{L}_S}(q) = \textstyle\sum_{u \in \mathcal{Q}} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} = \sum_{u \in \mathcal{B}} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} + \sum_{u \in \mathcal{A}} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}}.$$

We distinguish the following cases for q.

- First, we assume that $\chi(-1) = -1$, i.e., $q \equiv 3 \pmod 4$. The set $\mathcal{B}_2$ is the empty set. Furthermore, the set $\mathcal{B}_1$ is nonempty if and only if $q \equiv 7 \pmod 8$. In the latter case, we have $\#\mathcal{B}_1 = 2$ and $\#\mathcal{A} = \#\mathcal{Q} - \#\mathcal{B}_1 = (q-3)/2 - 2$. If the set $\mathcal{B}_1$ is empty, then $\#\mathcal{A} = \#\mathcal{Q} = (q-3)/2$. We see that either way we obtain

  $$I_{\mathrm{L}_S}(q) = (q-3)/4.$$

- Second, we assume that $\chi(-1) = 1$, i.e., $q \equiv 1 \pmod 4$. If $p = 3$, then $\sum_{u \in \mathcal{B}} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} = 1$. For $p > 3$, we write

  $$\textstyle\sum_{u \in \mathcal{B}} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} = \sum_{u \in \mathcal{B}_1} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} + \sum_{u \in \mathcal{B}_2} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} = \sum_{u \in \mathcal{B}_1} \frac{1}{\#\mathcal{B}_1} + \sum_{u \in \mathcal{B}_2} \frac{1}{\#\mathcal{B}_2}.$$

  In this case, the set $\mathcal{B}_1$ is nonempty and the set $\mathcal{B}_2$ is nonempty if and only if $q \equiv 1 \pmod{12}$. Therefore, we have

  $$\underset{u \in \mathcal{B}}{} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} = \begin{matrix} 2, & \text{if } q \equiv 1 \pmod{12}, \\ 1, & \text{if } q \equiv 5, 9. \pmod{12}. \end{matrix} \tag{9}$$

  Next, we write

  $$\textstyle\sum_{u \in \mathcal{A}} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} = \sum_{u \in \mathcal{A}_1} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} + \sum_{u \in \mathcal{A}_{-1}} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} = \sum_{u \in \mathcal{A}_1} \frac{1}{6} + \sum_{u \in \mathcal{A}_{-1}} \frac{1}{2}.$$

  So, we have

  $$\underset{u \in \mathcal{A}}{} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} = \frac{\#\mathcal{A}_1}{6} + \frac{\#\mathcal{A}_{-1}}{2}. \tag{10}$$

For $j \in \{-1, 1\}$, let

$$S_j = \{u : u \in \mathcal{Q},\ \chi(1-u) = j\}\,.$$

We note that, $\mathcal{A}_j = S_j \setminus \mathcal{B}$. From [13, Lemma 4], for $q \equiv 1 \pmod 4$, we have

$$\#S_j = \begin{array}{ll} (q-5)/4, & \text{if } j = 1, \\ (q-1)/4, & \text{if } j = -1. \end{array}$$

Then, by excluding the elements of $\mathcal{B}$ from the sets S_1, S_{-1}, we obtain the cardinalities of the sets $\mathcal{A}_1$, $\mathcal{A}_{-1}$, where $q \equiv 1 \pmod{24}$; see Table 1, where we let $q \equiv r \pmod{24}$.

r	$\#\mathcal{A}_1$	$\#\mathcal{A}_{-1}$
1	$\frac{q-5}{4} - 5$	$\frac{q-1}{4}$
5	$\frac{q-5}{4}$	$\frac{q-1}{4} - 1$
9	$\frac{q-5}{4} - 1$	$\frac{q-1}{4}$
13	$\frac{q-5}{4} - 2$	$\frac{q-1}{4} - 1$
17	$\frac{q-5}{4} - 3$	$\frac{q-1}{4}$

Table 1: Cardinalities of the sets $\mathcal{A}_1, \mathcal{A}_{-1}$, for $q \equiv 1 \pmod 4$

Finally, combining (9), (10) and Table (1), we compute:

$$I_{\mathrm{L}_S}(q) = \begin{cases} (q+5)/6, & \text{if } q \equiv 1 \pmod{12}, \\ (q+1)/6, & \text{if } q \equiv 5 \pmod{12}, \\ (q+3)/6, & \text{if } q \equiv 9 \pmod{12}, \\ (q-3)/4, & \text{if } q \equiv 3 \pmod{4}, \end{cases}$$

which completes the proof of this lemma.

□

Next we give an exact formula for the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ of the family (7).

Lemma 2.3. *For any prime $p \geq 3$, for the number $I_{\mathrm{L}_{S_1}}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (7)*, we have*

$$I_{\mathrm{L}_{S_1}}(q) = \begin{cases} \lfloor (q+23)/24 \rfloor & \text{if } q \equiv 1, 9, 13, 17 \pmod{24}, \\ (q-5)/24 & \text{if } q \equiv 5 \pmod{24}, \\ (q-3)/4 & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

Proof. Let

$$\mathcal{Q}_1 = \{u \in \mathcal{Q} \ : \ \ \chi(1-u) = 1\}.$$

From [13, Lemma 4], we have $\#\mathcal{Q}_1 = (q-3)/4$. For a fixed value $u \in \mathcal{Q}_1$, we let

$$\mathcal{I}_{\mathcal{L}_{S_1},u} = \quad v \ : \ v \in \mathcal{Q}_1, \ \mathbf{E}_{\mathrm{L},u} \cong_{\mathbb{F}_q} \mathbf{E}_{\mathrm{L},v} \quad .$$

We note that

$$I_{\mathrm{L}_{S_1}}(q) = \underset{u \in \mathcal{Q}_1}{} \frac{1}{\#\mathcal{I}_{\mathcal{L}_{S_1},u}}.$$

So, we need to compute the cardinality of the set $\mathcal{I}_{\mathcal{L}_{S_1},u}$ for all $u \in \mathcal{Q}_1$.

For $q \equiv 3 \pmod 4$, we have $\chi(-1) = -1$. For $u \in \mathcal{Q}_1$, we have

$$\chi(1-1/u) = \chi((u-1)/u) = \chi(u-1) = \chi(-1)\chi(1-u) = -\chi(1-u).$$

So, $1/u \notin \mathcal{Q}_1$. Then, from Lemma 2.1, we have

$$\mathcal{I}_{\mathcal{L}_{S_1},u} = \{u\}, \quad \text{if } u \in \mathcal{Q}_1.$$

Hence,

$$I_{\mathrm{L}_{S_1}}(q) = \underset{u \in \mathcal{Q}_1}{} 1 = \#\mathcal{Q}_1 = (q-3)/4.$$

From now on, we assume that $q \equiv 1 \pmod 4$. We use the proof of Lemma 2.2 and notice that, for $v \in \mathcal{Q}$, we have $v \in \mathcal{I}_{\mathcal{L}_{S_1},u}$ if and only if $v \in \mathcal{I}_{\mathcal{L}_S,u}$ and $v \in \mathcal{Q}_1$.

For $u \in \mathcal{Q}_1$, let $v \in \mathcal{I}_{\mathcal{L}_{S_1},u}$. From Lemma 2.1, we have

$$v \in \{u, 1/u, 1-u, 1/(1-u), u/(1-u), 1-1/u\}.$$

Since $\chi(u) = \chi(1-u) = \chi(-1) = 1$, we see that $\chi(v) = \chi(1-1/v) = 1$. So, $v \in \mathcal{Q}_1$, i.e., for $u \in \mathcal{Q}_1$, we have $\mathcal{I}_{\mathcal{L}_{S_1},u} = \mathcal{I}_{\mathcal{L}_S,u}$ Then, we write

$$I_{\mathrm{L}_{S_1}}(q) = \underset{u \in \mathcal{Q}_1}{} \frac{1}{\#\mathcal{I}_{\mathcal{L}_{S_1},u}} = \underset{u \in \mathcal{Q}_1}{} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} = \underset{u \in \mathcal{B} \cap \mathcal{Q}_1}{} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}} + \underset{u \in \mathcal{A} \cap \mathcal{Q}_1}{} \frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}}.$$

We have

$$\underset{u\in\mathcal{B}\cap\mathcal{Q}_1}{}\frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}}=\underset{u\in\mathcal{B}_1\cap\mathcal{Q}_1}{}\frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}}+\underset{u\in\mathcal{B}_2\cap\mathcal{Q}_1}{}\frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}}.$$

From the proof of Lemma 2.2, we see that, for $p>3$, $\mathcal{B}_1\cap\mathcal{Q}_1$ is nonempty if and only if $q\equiv 1 \pmod 8$ and $\mathcal{B}_2\cap\mathcal{Q}_1$ is nonempty if and only if $q\equiv 1 \pmod{12}$. Furthermore,

$$\underset{u\in\mathcal{B}}{}\frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}}=\begin{cases}2, & \text{if } q\equiv 1 \pmod{24},\\ 0, & \text{if } q\equiv 5. \pmod{24}.\\ 1, & \text{if } q\equiv 9,13,17. \pmod{24}.\end{cases}\tag{11}$$

It is easy to see that $\mathcal{A}\cap\mathcal{Q}_1=\mathcal{A}_1$. Then, from the proof of Lemma 2.2, we have

$$\underset{u\in\mathcal{A}_1}{}\frac{1}{\#\mathcal{I}_{\mathcal{L}_S,u}}=\frac{\#\mathcal{A}_1}{6}.$$

Then, using equation (11) and Table (1), we obtain

$$I_{\mathrm{L}_{S_1}}(q)=\begin{cases}(q+23)/24, & \text{if } q\equiv 1 \pmod{24},\\ (q-5)/24, & \text{if } q\equiv 5 \pmod{24},\\ (q+15)/24, & \text{if } q\equiv 9 \pmod{24},\\ (q+11)/24, & \text{if } q\equiv 13 \pmod{24},\\ (q+7)/24, & \text{if } q\equiv 17 \pmod{24},\end{cases}$$

which completes the proof.

□

The following lemma shows the equality of the values $I_{\mathrm{L}_T}(q)$ and $I_{\mathrm{L}_S}(q)$ for all $p\geq 3$.

Lemma 2.4. *For any prime $p\geq 3$, the number $I_{\mathrm{L}_T}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (6) *is given by*

$$I_{\mathrm{L}_T}(q)=\begin{cases}\lfloor (q+5)/6\rfloor, & \textit{if } q\equiv 1 \pmod 4,\\ \\ (q-3)/4, & \textit{if } q\equiv 3 \pmod 4.\end{cases}$$

Proof. We note that the Legendre curves $\mathbf{E}_{\mathrm{L},u}$ and $\mathbf{E}_{\mathrm{L},1-u}$ are $\mathbb{F}_q$ isomorphic if $\chi(-1)=1$. This can be seen via the admissible change of variables $X\longrightarrow$

$\alpha^2 X + 1$ and $Y \longrightarrow \alpha^3 Y$, where $\alpha^2 = -1$. So, for $q \equiv 1 \pmod 4$, we obviously have $I_{\mathrm{L}_T}(q) = I_{\mathrm{L}_S}(q)$.

If instead $\chi(-1) = -1$ then the curve $\mathbf{E}_{\mathrm{L},1-u}$ is not $\mathbb{F}_q$-isomorphic to $\mathbf{E}_{\mathrm{L},u}$, but rather to the nontrivial quadratic twist of $\mathbf{E}_{\mathrm{L},u}$. So, we have

$$\mathcal{L}_T = \quad E^t : E \in \mathcal{L}_S \quad ,$$

where E^t is the nontrivial quadratic twist of the elliptic curve E. Hence, for $q \equiv 1 \pmod 4$, we see that $I_{\mathrm{L}_T}(q) = I_{\mathrm{L}_S}(q)$.

The result now follow by Lemma 2.2. □

3 Edwards curves

The numbers of distinct j-invariants of the families of Edwards curve (1) and (2) have been studied in [14, Theorems 3 and 5]. More precisely, for any prime $p \geq 3$, the number $J_{\mathrm{E}}(q)$ of distinct values of the j-invariant of the family (1) is

$$J_{\mathrm{E}}(q) = \begin{cases} \lfloor (q+23)/24 \rfloor & \text{if } q \equiv 1, 9, 13, 17 \pmod{24}, \\ (q-5)/24 & \text{if } q \equiv 5 \pmod{24}, \\ \lfloor (q+1)/8 \rfloor & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Also, the number $J_{\mathrm{BL}}(q)$ of distinct values of the j-invariant of the family (2) is given by

$$J_{\mathrm{BL}}(q) = \quad \begin{array}{ll} \lfloor (5q+7)/12 \rfloor & \text{if } q \equiv 1 \pmod 4, \\ \lfloor (3q-1)/8 \rfloor & \text{if } q \equiv 3 \pmod 4. \end{array}$$

In the remainder of this section, we find explicit formulas for the numbers of $\mathbb{F}_q$-isomorphism classes of the Edwards families (1) and (2).

We consider the following family of elliptic curves over $\mathbb{F}_q$ given by

$$\mathbf{E}_{4,c}: \quad Y^2 = X^3 + (1-2c)X^2 + c^2 X, \tag{12}$$

for $c \in \mathbb{F}_q$ with $c = 0, 1/4$. The next lemma shows the equivalence between the above family (12) and the family of Edwards curves (2).

Lemma 3.1. *Every Edwards curve $\mathbf{E}_{\mathrm{BL},d}$ given by* (2) *over $\mathbb{F}_q$ with $d = 0, 1$ is birationally equivalent to the elliptic curve $\mathbf{E}_{4,c}$ given by* (12) *with $c = (1-d)/4$.*

Proof. We recall from [2] that every elliptic curve $E(\mathbb{F}_q)$ with a point of order 4 is birationally equivalent to an Edwards curve $\mathbf{E}_{\mathrm{BL},d}$. It is easy to verify that $P = (c, c)$ is a point of order 4 on the curve $\mathbf{E}_{4,c}$, and so the curve is birationally equivalent to a BL-Edwards curve.

Conversely, via the map $\psi : \mathbf{E}_{\mathrm{BL},d} \to \mathbf{E}_{4,(1-d)/4}$

$$\psi(x, y) = \Big(\frac{c(1 + y)}{1 - y}, \frac{c(1 + y)}{x(1 - y)}\Big),$$

we have that the Edwards curve $\mathbf{E}_{\mathrm{BL},d}$ is birationally equivalent to the elliptic curve $\mathbf{E}_{4,c}$, with $c = (1 - d)/4$. The inverse is the map

$$\psi^{-1}(x, y) = \Big(\frac{x}{y}, \frac{x - c}{x + c}\Big).$$

This proves the lemma. □

We now partition the Edwards curves (2) into two subfamilies. Recall that $\mathcal{Q}$ is the set of quadratic residues of $\mathbb{F}_q \setminus \{0, 1\}$. Let

$$\mathcal{BL}_S = \{\mathbf{E}_{\mathrm{BL},d} : \ d \in \mathcal{Q}\}\,, \tag{13}$$

and

$$\mathcal{BL}_T = \{\mathbf{E}_{\mathrm{BL},d} : \ d \notin \mathcal{Q}\}\,. \tag{14}$$

As before, we use $I_{\mathrm{BL}_S}(q)$ and $I_{\mathrm{BL}_T}(q)$ to denote the numbers of $\mathbb{F}_q$-isomorphism classes of this families (13) and (14).

Note that a point $P = (x, y)$ on the curve $E_{4,c}$ has order 2 if and only if $y = 0$. There is always at least one rational point $(0, 0)$ of order 2, and possibly three points. The next remark shows how the number of $\mathbb{F}_q$-rational points of order 2 relates to $I_{\mathrm{BL}_T}(q)$ and $I_{\mathrm{BL}_S}(q)$.

Remark 3.2. *From Lemma 3.1, we know that every Edwards curve $\mathbf{E}_{\mathrm{BL},d}$ is birationally equivalent to the elliptic curve $\mathbf{E}_{4,c}$ with $d = 1-4c$. Let δ_c be the discriminant of the polynomial $X^2 + (1 - 2c)X + c^2$. We have*

$$\delta_c = (1 - 2c)^2 - 4c^2 = 1 - 4c = d.$$

We see that $\mathbf{E}_{4,c}(\mathbb{F}_q)$ has a single rational point of order 2 if and only if $\chi(\delta_c) = \chi(d) = -1$. Similarly, $\mathbf{E}_{4,c}(\mathbb{F}_q)$ has three rational points of order 2 if and only if $\chi(\delta_c) = \chi(d) = 1$.

Therefore, for the Edwards curve $\mathbf{E}_{\mathrm{BL},d}$, the group $\mathbf{E}_{\mathrm{BL},d}(\mathbb{F}_q)$ has a single point of order 2 if and only if $\mathbf{E}_{\mathrm{BL},d} \in \mathcal{BL}_T$. Also, the group $\mathbf{E}_{\mathrm{BL},d}(\mathbb{F}_q)$ has three points of order 2 if and only if $\mathbf{E}_{\mathrm{BL},d} \in \mathcal{BL}_S$.

Lemma 3.3. *For any prime $p \geq 3$, the number $I_{\mathrm{BL}_T}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (14) *is*

$$I_{\mathrm{BL}_T}(q) = (q-1)/2.$$

Proof. By Lemma 3.1 and Remark 3.2, we can represent Edwards curves $\mathbf{E}_{\mathrm{BL},d}$ with $d \notin \mathcal{Q}$ using elliptic curves of the form $\mathbf{E}_{4,c}$ with $c = (1-d)/4$. There are $(q-1)/2$ non-squares d in $\mathbb{F}_q$.

Suppose two Edwards curve, say $\mathbf{E}_{\mathrm{BL},d_1}$ and $\mathbf{E}_{\mathrm{BL},d_2}$, are isomorphic over $\mathbb{F}_q$. Then the associated curves $\mathbf{E}_{4,c_1}$ and $\mathbf{E}_{4,c_2}$, with $c_1 = (1-d_1)/4$ and $c_2 = (1-d_2)/4$, must be isomorphic over $\mathbb{F}_q$ as well. The only admissible change of variables from $\mathbf{E}_{4,c_1}$ to $\mathbf{E}_{4,c_2}$ has $\alpha = 1$, and $r = s = t = 0$ (see §2.1). Therefore, $c_1 = c_2$ and $d_1 = d_2$. This shows each distinct non-square d leads to a different isomorphism class. Hence, we have $I_{\mathrm{BL}_T}(q) = (q-1)/2$. □

We now turn our attention to the second case, i.e., the curves in $\mathcal{BL}_S$.

Lemma 3.4. *For any prime $p \geq 3$, for the number $I_{\mathrm{BL}_S}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (13)*, we have*

$$I_{\mathrm{BL}_S}(q) = \begin{array}{ll} \lfloor (q+5)/6 \rfloor, & \textit{if } q \equiv 1 \pmod 4, \\ (q-3)/4, & \textit{if } q \equiv 3 \pmod 4. \end{array}$$

Proof. Again, from Lemma 3.1 and Remark 3.2, we can represent an Edwards curve $\mathbf{E}_{\mathrm{BL},d}$ with $d \in \mathcal{Q}$ using the curve $\mathbf{E}_{4,c}$ with $c = (1-d)/4$. We write

$$X^3 + (1-2c)X^2 + c^2X = X(X+s^2)(X+t^2),$$

where $s = \frac{1+\delta}{2}$, $t = \frac{1-\delta}{2}$ and $\delta^2 = d$.

First, we assume that $q \equiv 1 \pmod 4$. We then have $-1 \in \mathcal{Q}$. Let $i \in \mathbb{F}_q$ such that $i^2 = -1$. The elliptic curve $\mathbf{E}_{4,c}$ is isomorphic over $\mathbb{F}_q$ to the Legendre curve $\mathbf{E}_{\mathrm{L},u} : Y^2 = X(X-1)(X-u)$ with $u = (t/s)^2$, via the map

$$(x,y) \to (x/(is)^2, y/(is)^3).$$

Conversely, the Legendre curve $\mathbf{E}_{\mathrm{L},u}$ with $u = \gamma^2$ for some $\gamma \in \mathbb{F}_q$, is isomorphic to the elliptic curve $\mathbf{E}_{4,(1-d)/4}$ with $d = (\frac{1-\gamma}{1+\gamma})^2$. Hence, for $q \equiv 1 \pmod 4$, the curve family $\mathcal{BL}_S$ is isomorphic to the curve family $\mathcal{L}_S$ given by (6). Then, from Lemma 2.2, we have

$$I_{\mathrm{BL}_S}(q) = \begin{cases} (q+5)/6, & \text{if } q \equiv 1 \pmod{12}, \\ (q+1)/6, & \text{if } q \equiv 5 \pmod{12}, \\ (q+3)/6, & \text{if } q \equiv 9 \pmod{12}. \end{cases}$$

Second, we assume that $q \equiv 3 \pmod 4$. The elliptic curve $\mathbf{E}_{4,c}$ is isomorphic over $\mathbb{F}_q$ to the Legendre curve $\mathbf{E}_{\mathrm{L},u}$ with $u = 1 - (t/s)^2$, via the map

$$(x, y) \to (x/s^2 + 1, y/s^3).$$

Conversely, the Legendre curve $\mathbf{E}_{\mathrm{L},u}$ with $\chi(1-u) = 1$, where $1 - u = \gamma^2$ for some $\gamma \in \mathbb{F}_q$, is isomorphic to the elliptic curve $\mathbf{E}_{4,(1-d)/4}$ with $d = (\frac{1-\gamma}{1+\gamma})^2$. Therefore, for $q \equiv 3 \pmod 4$, the curve family $\mathcal{BL}_S$ is isomorphic to the curve family $\mathcal{L}_T$ given by (8). Then, from Lemma 2.4, we have

$$I_{\mathrm{BL}_S}(q) = (q-3)/4, \quad \text{if} \quad q \equiv 3 \pmod 4.$$

This concludes the proof of this lemma. □

Combining everything, we obtain the total number of $\mathbb{F}_q$ isomorphism classes of Edwards curves.

Theorem 3.5. *For any prime $p \geq 3$, the number $I_{\mathrm{BL}}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (2)*, is given by*

$$I_{\mathrm{BL}}(q) = \begin{cases} \dfrac{2q+1}{3} & \text{if } q \equiv 1 \pmod 4, \\ \dfrac{3q-5}{4} & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Proof. We clearly have that

$$I_{\mathrm{BL}}(q) = I_{\mathrm{BL}_S}(q) + I_{\mathrm{BL}_T}(q).$$

From Lemmas 3.4 and 3.3, we obtain

$$I_{\mathrm{BL}}(q) = \begin{cases} (2q+1)/3, & \text{if } q \equiv 1 \pmod{12}, \\ (2q-1)/3, & \text{if } q \equiv 5 \pmod{12}, \\ 2q/3, & \text{if } q \equiv 9 \pmod{12}, \\ (3q-5)/4, & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

which completes the proof. □

We note that any Edwards curve $\mathbf{E}_{\mathrm{E},c}$, given by (1), is isomorphic to an Edwards curve $\mathbf{E}_{\mathrm{BL},c^4}$ of the form

$$X^2 + Y^2 = 1 + c^4X^2Y^2$$

via the map $(x, y) \to (cx, cy)$. Here, we give explicit formulas for the number of $\mathbb{F}_q$-isomorphism classes of the family (1).

Theorem 3.6. *For any prime $p \geq 3$, for the number $I_{\mathrm{E}}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (1)*, we have*

$$I_{\mathrm{E}}(q) = \begin{cases} \lfloor (q+23)/24 \rfloor & \textit{if } q \equiv 1, 9, 13, 17 \pmod{24}, \\ (q-5)/24 & \textit{if } q \equiv 5 \pmod{24}, \\ (q-3)/4 & \textit{if } q \equiv 3 \pmod{4}. \end{cases}$$

Proof. We recall that any Edwards curve $\mathbf{E}_{\mathrm{E},c}$, given by (1), is isomorphic to an Edwards curve $\mathbf{E}_{\mathrm{BL},c^4}$. From the proof of Lemma 3.4, we can represent the Edwards curve $\mathbf{E}_{\mathrm{BL},c^4}$ using the Legendre curve $\mathbf{E}_{\mathrm{L},u}$, where

$$u = \begin{cases} \quad \frac{1-c^2}{1+c^2} \quad {}^{2} & \text{if } q \equiv 1 \pmod{4}, \\ 1 - \quad \frac{1-c^2}{1+c^2} \quad {}^{2} & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

We see that $\chi(u) = \chi(1-u) = 1$. So, $u, 1-u \in \mathcal{Q}$ and $\mathbf{E}_{\mathrm{L},u}$ an elliptic curve in the family $\mathcal{L}_{S_1}$ given by (7).

Conversely, the Legendre curve $\mathbf{E}_{\mathrm{L},u}$ in $\mathcal{L}_{S_1}$ with $u = \gamma^2$ and $1 - u = \lambda^2$ for some $\gamma, \lambda \in \mathbb{F}_q$, is isomorphic to the elliptic curve $\mathbf{E}_{\mathrm{BL},c^4}$ with

$$c = \quad \begin{array}{ll} \frac{\lambda}{1+\gamma} & \text{if } q \equiv 1 \pmod{4}, \\ \frac{\gamma}{1+\lambda} & \text{if } q \equiv 3 \pmod{4}. \end{array}$$

Therefore, the curve family (1) is isomorphic to the curve family $\mathcal{L}_{S_1}$ given by (7). Then, we see that $I_{\mathrm{E}}(q) = I_{\mathrm{L}_{S_1}}(q)$ and from Lemma 2.3, we have

$$I_{\mathrm{L}_{S_1}}(q) = \begin{cases} (q+23)/24, & \text{if } q \equiv 1 \pmod{24}, \\ (q-5)/24, & \text{if } q \equiv 5 \pmod{24}, \\ (q+15)/24, & \text{if } q \equiv 9 \pmod{24}, \\ (q+11)/24, & \text{if } q \equiv 13 \pmod{24}, \\ (q+7)/24, & \text{if } q \equiv 17 \pmod{24}, \\ (q-3)/4, & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

□

4 Twisted Edwards curves

We consider the twisted Edwards curves $\mathbf{E}_{\mathrm{TE},a,d}$ given by the family (3) over a finite field $\mathbb{F}_q$ of characteristic $p = 2$. We note that a, d are in $\mathbb{F}_q$ with $ad(1-d) = 0$.

It has been shown in [2] that twisted Edwards curves are birationally equivalent to Montgomery curves $\mathbf{E}_{\mathrm{M},A,B}$ given by the family (4), where $B(A^2-4)=0$. This can be seen via the map $\psi : \mathbf{E}_{\mathrm{TE},a,d} \to \mathbf{E}_{\mathrm{M},2(a+d)/(a-d),4/(a-d)}$

$$\psi(x,y) = \quad \frac{1+y}{1-y}, \frac{1+y}{x(1-y)} \quad . \tag{15}$$

Furthermore, the Montgomery curve $\mathbf{E}_{\mathrm{M},A,B}$ is birationally equivalent to the twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ where $a=(A+2)/B$ and $d=(A-2)/B$.

We note that, the family (3) is the generalization of the families (1) and (2). Clearly, every Edwards curve $\mathbf{E}_{\mathrm{BL},d}$ is a twisted Edwards. Moreover, a twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ is a twist of the Edwards curve $\mathbf{E}_{\mathrm{BL},\frac{d}{a}}$. We note that a quadratic twist of $\mathbf{E}_{\mathrm{BL},d}$, which is not isomorphic to $\mathbf{E}_{\mathrm{BL},d}$ over $\mathbb{F}_q$, may not be in the family (2). Therefore, the family (3) includes the curves of (2) and the twists of the curves of (2). Moreover, the j-invariant of a curve and the j-invariant of its twist are equal. So, both families have the same number of distinct j-invariants. This establishes the following theorem.

Theorem 4.1. *For any prime $p \geq 3$, for the numbers $J_{\mathrm{TE}}(q)$ and $J_{\mathrm{M}}(q)$ of distinct $\overline{\mathbb{F}}_q$-isomorphism classes of the families* (3) *and* (4) *respectively, we have*

$$J_{\mathrm{TE}}(q) = J_{\mathrm{M}}(q) = \quad \begin{matrix} \lfloor (5q+7)/12 \rfloor & \textit{if } q \equiv 1 \pmod 4, \\ \lfloor (3q-1)/8 \rfloor & \textit{if } q \equiv 3 \pmod 4. \end{matrix}$$

In the remainder of this section, we find explicit formulas for the number of $\mathbb{F}_q$-isomorphism classes of Montgomery curves, which is the same as the number of $\mathbb{F}_q$-isomorphism classes of twisted Edwards curves.

We partition Montgomery curves (4) into the following subfamilies. As usual, let $\mathcal{Q}$ be the set of quadratic residues of $\mathbb{F}_q \setminus \{0,1\}$. Let

$$\mathcal{M}_S = \quad \mathbf{E}_{\mathrm{M},A,B} : \ A^2-4 \in \mathcal{Q} \quad , \tag{16}$$

and

$$\mathcal{M}_T = \quad \mathbf{E}_{\mathrm{M},A,B} : \ A^2-4 \notin \mathcal{Q} \quad . \tag{17}$$

As before, we use $I_{\mathrm{M}_S}(q)$ and $I_{\mathrm{M}_T}(q)$ to denote the numbers of $\mathbb{F}_q$-isomorphism classes of this families (16) and (17). We now compute the values of $I_{\mathrm{M}_S}(q)$ and $I_{\mathrm{M}_T}(q)$.

Lemma 4.2. *For any prime $p \geq 3$, for the number $I_{\mathrm{M}_S}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (16)*, we have*

$$I_{\mathrm{M}_S}(q) = \begin{array}{lll} 2\left\lfloor (q+5)/6 \right\rfloor, & \text{if } q \equiv 1 & \pmod 4, \\ & & \\ (q-3)/4, & \text{if } q \equiv 3 & \pmod 4. \end{array}$$

Proof. We note that the family $\mathcal{M}_S$ is the set of Montgomery curves over $\mathbb{F}_q$ with three 2-torsion points. From Remark 3.2, we know the family $\mathcal{BL}_S$ is the set of Edwards curve $\mathbf{E}_{\mathrm{BL},d}$ with three 2-torsion points.

Suppose first $q \equiv 1 \pmod 4$. We recall from [2, Theorem 3.5] that for every Montgomery curve $\mathbf{E}_{\mathrm{M},A,B}$ with $A^4 - 4 \in \mathcal{Q}$, exactly one of $\mathbf{E}_{\mathrm{M},A,B}$ and its nontrivial quadratic twist $\mathbf{E}_{\mathrm{M},A,cB}$ (with $\chi(c) = -1$) is birationally equivalent to an Edwards curve $\mathbf{E}_{\mathrm{BL},d}$. On the other hand, an Edwards curve $\mathbf{E}_{\mathrm{BL},d}$ via the map (15) is birationally equivalent to the Montgomery curve $\mathbf{E}_{\mathrm{M},2(1+d)/(1-d),4/(1-d)}$. This means, there is a $2:1$ correspondence between the Montgomery curves of the family $\mathcal{M}_S$ and the Edwards curves of $\mathcal{BL}_S$. Therefore, we have $I_{\mathrm{M}_S}(q) = 2I_{\mathrm{BL}_S}(q)$. Thus, from Lemma 3.4, for $q \equiv 1 \pmod 4$, we have

$$I_{\mathrm{M}_S}(q) = \begin{cases} (q+5)/3, & \text{if } q \equiv 1 \pmod{12}, \\ (q+1)/3, & \text{if } q \equiv 5 \pmod{12}, \\ (q+3)/3, & \text{if } q \equiv 9 \pmod{12}. \end{cases}$$

When $q \equiv 3 \pmod 4$, every Montgomery curve over $\mathbb{F}_q$ is birationally equivalent to an Edwards curve [2]. So, the families (16) and (13) are equivalent. So in this case, by Lemma 3.4, we have

$$I_{\mathrm{M}_S}(q) = I_{\mathrm{BL}_S}(q) = (q-3)/4.$$

□

Lemma 4.3. *For any prime $p \geq 3$, then the number $I_{\mathrm{M}_T}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (16) *is*

$$I_{\mathrm{M}_T}(q) = \frac{q-1}{2}.$$

Proof. We observe that the family $\mathcal{M}_T$ is the set of Montgomery curves over $\mathbb{F}_q$ with a single rational 2-torsion point. Again, from Remark 3.2 we recall that the family $\mathcal{BL}_T$ is the set of Edwards curve $\mathbf{E}_{\mathrm{BL},d}$ with single 2-torsion point.

For the Montgomery curve $\mathbf{E}_{\mathrm{M},A,B}$ in $\mathcal{M}_T$, we have $A^2-4 \notin \mathcal{Q}$. Let $a=(A+2)/B$ and $d=(A-2)/B$. It follows that exactly one of a and d is a square element of $\mathbb{F}_q$. If $a \in \mathcal{Q}$, then $\mathbf{E}_{\mathrm{M},A,B}$ has the point $(1,\sqrt{a})$ of order 4. Similarly, if $d \in \mathcal{Q}$, then the point $(-1,\sqrt{d})$ is of order 4. In either case we have that $\mathbf{E}_{\mathrm{M},A,B}$ has a point of order 4, and so is birationally equivalent to an Edwards curve in $\mathcal{BL}_T$. So, we have

$$I_{\mathrm{M}_T}(q)=I_{\mathrm{BL}_T}(q)=(q-1)/2,$$

which completes the proof of this lemma. □

Theorem 4.4. *For any prime $p \geq 3$, for the numbers $I_{\mathrm{TE}}(q)$ and $I_{\mathrm{M}}(q)$ of $\mathbb{F}_q$-isomorphism classes of the families* (3) *and* (4) *respectively, we have*

$$I_{\mathrm{TE}}(q)=I_{\mathrm{M}}(q)=\begin{cases} \dfrac{5q+7}{6} & \textit{if } q \equiv 1,9 \pmod{12}, \\ \dfrac{5q-1}{6} & \textit{if } q \equiv 5 \pmod{12}, \\ \dfrac{3q-5}{4} & \textit{if } q \equiv 3 \pmod{4}. \end{cases}$$

Proof. As we have previously stated, every twisted Edwards curve $\mathbf{E}_{\mathrm{TE},a,d}$ over $\mathbb{F}_q$ is birationally equivalent over $\mathbb{F}_q$ to the Montgomery curve $\mathbf{E}_{\mathrm{M},\frac{4}{a-d},\frac{2(a+d)}{a-d}}$ (see Equation (15)). Conversely, every Montgomery curve $\mathbf{E}_{\mathrm{M},A,B}$ is birationally equivalent over $\mathbb{F}_q$ to the twisted Edwards curve $\mathbf{E}_{\mathrm{TE},\frac{A+2}{B},\frac{A-2}{B}}$ (see [2, Theorem 3.2]). It follows that the families (3) and (4) have the same number of isomorphism classes over $\mathbb{F}_q$. Therefore,

$$I_{\mathrm{TE}}(q)=I_{\mathrm{M}}(q).$$

For the number $I_{\mathrm{M}}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family (4), we clearly have

$$I_{\mathrm{M}}(q)=I_{\mathrm{M}_S}(q)+I_{\mathrm{M}_T}(q).$$

By Lemmas 4.2, and 4.3, we have

$$I_{\mathrm{M}}(q)=\begin{cases} (5q+7)/6 & \text{if } q \equiv 1 \pmod{12}, \\ (5q-1)/6 & \text{if } q \equiv 5 \pmod{12}, \\ (5q+3)/6 & \text{if } q \equiv 9 \pmod{12}, \\ (3q-5)/4 & \text{if } q \equiv 3 \pmod{4}, \end{cases}$$

which completes the proof of this theorem. □

5 Conclusion

In this work we answered a question posed in [14]. That is, we found an exact formula for the number of $\mathbb{F}_q$-isomorphism classes of Edwards curves, original Edwards curves, and twisted Edwards curves.

A natural and related question is to find a formula for the number of distinct isogeny classes for a given family of elliptic curves. Ahmadi and Granger recently were able to do this for Edwards curves [1], and Moody and Wu did the same for Hessian curves [19]. It is an open problem to find similar formulas for most other families of curves. This would include twisted Edwards curves, Jacobi quartics, Jacobi intersections, and Huff curves.

References

[1] O. Ahmadi, R. Granger, On isogeny classes of Edwards curves over finite fields, Preprint, 2011. Available at `http://eprint.iacr.org/2011/135.pdf`. Accessed April 2011.

[2] D. J. Bernstein, P. Birkner, T. Lange, C Peters, Twisted Edwards curves, in: S. Vaudenay (Ed.), Progress in Cryptology – Africacrypt 2008, Lecture Notes in Comput. Sci. 5023, Springer-Verlag, 2008, pp. 389–405.

[3] D. J. Bernstein, T. Lange, Faster addition and doubling on elliptic curves, in: K. Kurosawa (Ed.), Progress in Cryptology – Asiacrypt 2007, Lecture Notes in Comput. Sci. 4833, Springer-Verlag, 2007, pp. 29–50.

[4] D. J. Bernstein, T. Lange, Inverted Edwards coordinates, in: S. Boztas and H.-F. Lu (Eds.), Proceedings of AAECC'2007, Lecture Notes in Comput. Sci. 4851, Springer-Verlag, 2007, pp. 20–27.

[5] D. J. Bernstein, T. Lange, Analysis and optimization of elliptic-curve single-scalar multiplication, in: Finite Fields and Applications - Proceedings of Fq8, Contemp. Math. 461, 2008, pp. 1–20.

[6] D. J. Bernstein, T. Lange, R. Farashahi, Binary Edwards curves, in: Proceedings of CHES'2008, Lecture Notes in Comput. Sci. 5154, Springer-Verlag, 2008, pp. 244–265.

[7] Y. Choie, E. Jeong, Isomorphism classes of elliptic and hyperelliptic curves over finite fields, Finite Fields Appl. 10 4 (2004) 583–614.

[8] Y. Choie, D. Yun, Isomorphism classes of hyperelliptic curves of genus 2 over $\mathbb{F}_q$, in: L.M. Batten and J. Seberry (Eds.), Information Security and Privacy, Lecture Notes in Comput. Sci. 2384, Springer-Verlag, 2002, pp. 190–202.

[9] Y. Deng, Isomorphism classes of hyperelliptic curves of genus 3 over finite fields, Finite Fields Appl. 12 2 (2006) 248–282.

[10] H. M. Edwards, A normal form for elliptic curves, Bull. Amer. Math. Soc. 44 (2007) 393–422.

[11] L.H. Encinas, A.J. Menezes and J.M. Masqué. Isomorphism classes of genus-2 hyperelliptic curves over finite fields, Appl. Algebra Engrg. Comm. Comput. 13 (2002) 57–65.

[12] R. Farashahi, On the Number of Distinct Legendre, Jacobi, Hessian and Edwards Curves (Extended Abstract), in: Proceedings of the Workshop on Coding theory and Cryptology (WCC 2011), 2011, pp. 37–46. Available at `hal.inria.fr/docs/00/60/72/79/PDF/76.pdf`.

[13] R. Farashahi, On the Number of Distinct Legendre, Jacobi, Hessian Curves, to appear, 2011. Available at `http://arxiv.org/`.

[14] R. Farashahi, I. Shparlinski, On the number of distinct elliptic curves in some families, Des. Codes Cryptogr. 54(1) (2010) 83–99.

[15] R. Feng, H. Wu, Elliptic Curves in Huff's model, Preprint, 2010. Available at `http://eprint.iacr.org/2010/390.pdf`. Accessed Dec 2010.

[16] R. Feng, and H. Wu, On the isomorphism classes of Legendre elliptic curves over finite fields, Sci China Math 54(9) (2011) 1885–1890. doi: 10.1007/s11425-011-4255-0.

[17] A.J. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

[18] P. .L Montgomery, Speeding the Pollard and elliptic curve methods of factorization, Math. Comp. 48 (177) (1987) 243–264.

[19] D. Moody, and H, Wu, Families of elliptic curves with rational 3-torsion, Preprint, 2011.

[20] R. Schoof, Nonsingular plane cubic curves over finite field, J. Combin. Theory Ser. A 46 (1987) 183–211.

[21] J. H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, Berlin, 1995.

[22] L. C. Washington, Elliptic curves: Number theory and Cryptography, second ed., CRC Press, 2008.