On the Number of Distinct Legendre, Jacobi,Hessian and Edwards Curves (Extended Abstract)

Reza Rezaeian Farashahi

On the Number of Distinct Legendre, Jacobi, Hessian and Edwards Curves (Extended Abstract)

Reza Rezaeian Farashahi

Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
reza.farashahi@mq.edu.au

Abstract. We give explicit formulas for the number of distinct elliptic curves over a finite field, up to isomorphism, in the families of Legendre, Jacobi, Hessian and Edwards curves.

Keywords: Elliptic curve, Legendre curve, Jacobi curve, Hessian curve, Edwards curve, j-invariant, isomorphism, cryptography

1 Introduction

A nonsingular absolutely irreducible projective curve of genus 1 defined over a field $\mathbb{F}$ with at least one $\mathbb{F}$-rational point is called an elliptic curve over $\mathbb{F}$, see [1, 22] for a general background on elliptic curves. Koblitz [17] and Miller [20] were the first to show that the group of rational points on an elliptic curve over a finite field can be used for the discrete logarithm problem in a public-key cryptosystem.

In particular, an elliptic curve E over $\mathbb{F}$ can be given by the so-called *Weierstrass equation*

$$E: \quad Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{1}$$

where the coefficients $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$, which traditionally has been most commonly used. For a field $\mathbb{F}$ of characteristic $p \neq 2, 3$, the Weierstrass equation (1) can be transformed to the so called *short Weierstrass equation* given by

$$\mathbf{E}_{\mathrm{W},u,v}: \quad Y^2 = X^3 + uX + v, \tag{2}$$

where the coefficients $u, v \in \mathbb{F}$ (see [1, 22]).

There are many other forms of equations to represent elliptic curves such as Legendre equation, Hessian equation, quartic equation and intersection of two quadratic surfaces [24, Chapter 2]. Any equation given by each of the latter forms over a field $\mathbb{F}$ can be transformed to a Weierstrass equation by change of variables that uses rational functions with coefficient in $\mathbb{F}$. Usually, any elliptic curve over an algebraically closed field $\mathbb{F}$ can be defined by each of the latter equations.

A *Legendre equation* is a variant of Weierstrass equation with one parameter. Any elliptic curve defined over an algebraically closed field $\mathbb{F}$ of characteristic $p \neq 2$ can be expressed by an elliptic curve by the Legendre equation

$$\mathbf{E}_{\mathrm{L},u}: \quad Y^2 = X(X-1)(X-u), \tag{3}$$

for some $u \in \mathbb{F}$. Furthermore, an elliptic curve in Legendre form is birationally equivalent to a *Jacobi quartic* curve that is given by the equation

$$\mathbf{E}_{\mathrm{JQ},u}: \quad Y^2 = X^4 + 2uX^2 + 1. \tag{4}$$

for some $u \in \mathbb{F}$ with $u \neq \pm 1$. Moreover, an elliptic curve in Legendre form is birationally equivalent to a so-called *Jacobi intersection* that is defined by the intersection of two quadratics given by

$$\mathbf{E}_{\mathrm{JI},u}: \quad X^2 + Y^2 = 1 \qquad \text{and} \qquad uX^2 + Z^2 = 1, \tag{5}$$

where $u \in \mathbb{F}$ and $u \neq 0, 1$. See [7] for more background on Jacobi curves. The latter two forms over finite fields are used for cryptographic interest in [19]. Also, for the recent improvements on their arithmetic see [10, 15].

A *Hessian curve* over a field $\mathbb{F}$ is given by the cubic equation

$$\mathbf{E}_{\mathrm{H},u}: \quad X^3 + Y^3 + 1 = uXY, \tag{6}$$

for some $u \in \mathbb{F}$ with $u^3 \neq 27$ (see [7]). For the cryptographic interests on Hessian curves over finite fields see [3, 12, 15, 16, 23].

An Edwards curve, [11], over a field $\mathbb{F}$ of characteristic $p \neq 2$, is given by the equation

$$\mathbf{E}_{\mathrm{E},u}: \quad X^2 + Y^2 = u^2(1 + X^2Y^2), \tag{7}$$

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

$$\mathbf{E}_{\mathrm{BL},u}: \quad X^2 + Y^2 = 1 + uX^2Y^2, \tag{8}$$

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

$$\mathbf{E}_{\mathrm{TE},u,v}: \quad vX^2 + Y^2 = 1 + uX^2Y^2, \tag{9}$$

where u, v are distinct nonzero elements of $\mathbb{F}$. In the same paper, they show that a twisted Edwards curve is birationally equivalent to a Montgomery curve. We recall, [21], that an elliptic curve by a *Montgomery equation* is given by

$$\mathbf{E}_{\mathrm{M},u,v}: \quad vY^2 = X^3 + uX^2 + X, \tag{10}$$

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

We note that, above families do not cover all distinct curves over finite fields. Accordingly, a natural question arise about the number of isomorphism classes of these curves.

Lenstra [18] gave explicit estimates for the number of isomorphism classes of elliptic curves over a prime field $\mathbb{F}_p$ with order divisible by a prime $l \neq p$. After that, Howe [14] extended Lenstra's work to arbitrary integers l. Moreover, Castryck and Hubrechts [8] generalized these results giving explicit estimates for the number of isomorphism classes of elliptic curves over a finite field $\mathbb{F}_q$ having order with a fix remainder divided by an integer l.

Furthermore, Farashahi and Shparlinski [13], using the notion of the *j-invariant of an elliptic curve*, see [1, 22, 24], gave exact formulas for the number of distinct elliptic curves over a finite field (up to isomorphism over the algebraic closure of the ground field) in the families of Edwards curves [11] and their generalization due to Bernstein and Lange [4] as well as the curves introduced by Doche, Icart and Kohel [9]. Moreover, the open question of [13] is whether there are explicit formulas for the number of distinct elliptic curves over a finite field in the families of Hessian curves, Jacobi quartic and Jacobi intersections.

In this paper, we give precise formulas for the number of distinct j-invariants of elliptic curves over a finite field in the families of Legendre, Jacobi and Hessian curves. The next interesting and more challenging step is to study isomorphism classes over the ground field of these families. Moreover, we give exact formulas for the number of isomorphism classes over the ground field of above families.

Throughout the paper, for a field $\mathbb{F}$, we denote its algebraic closure by $\overline{\mathbb{F}}$ and its multiplicative subgroup by $\mathbb{F}^*$. The letter p always denotes a prime number and the letter q always denotes a prime power. As usual, $\mathbb{F}_q$ is a finite field of size q. Let χ_2 denote the quadratic character in $\mathbb{F}_q$, where $p \geq 3$. So, for any q where $p \geq 3$, $u = w^2$ for some $w \in \mathbb{F}_q^*$ if and only if $\chi_2(u) = 1$. The cardinality of a finite set $\mathcal{S}$ is denoted by $\#\mathcal{S}$.

2 Background on isomorphisms and outline of our approach

An elliptic curve E over $\mathbb{F}$ given by the Weierstrass equation (1) can be transformed to the elliptic curve $\widetilde{E}$ over $\mathbb{F}$ given by the Weierstrass equation

$$\widetilde{E}: \quad \widetilde{Y}^2 + \widetilde{a}_1\widetilde{X}\widetilde{Y} + \widetilde{a}_3\widetilde{Y} = \widetilde{X}^3 + \widetilde{a}_2\widetilde{X}^2 + \widetilde{a}_4\widetilde{X} + \widetilde{a}_6,$$

via the invertible maps $X \mapsto \alpha^2\widetilde{X}+\beta$ and $Y \mapsto \alpha^3\widetilde{Y}+\alpha^2\gamma\widetilde{X}+\delta$ with $\alpha, \beta, \gamma, \delta \in \overline{\mathbb{F}}$ and $\alpha \neq 0$. In this case, the elliptic curves E and $\widetilde{E}$ are called *isomorphic* over $\overline{\mathbb{F}}$ or *twists* of each other. In case $\alpha, \beta, \gamma, \delta \in \mathbb{F}$, the elliptic curves E and $\widetilde{E}$ are called *isomorphic* over $\mathbb{F}$. We use $E \cong_{\mathbb{F}} \widetilde{E}$ to denote E and $\widetilde{E}$ are $\mathbb{F}$-*isomorphic*.

The elliptic curve E over $\mathbb{F}$ given by the Weierstrass equation (1) has the non-zero discriminant

$$\Delta_E = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

$b_2 = a_1^2+4a_2$, $b_4 = a_1a_3+2a_4$, $b_6 = a_3^2+4a_6$, $b_8 = a_1^2a_6-a_1a_3a_4+4a_2a_6+a_2a_3^2-a_4^2$.

Also, its j-invariant is explicitly defined as

$$j(E) = (b_2^2 - 24b_4)^3/\Delta_E.$$

It is known that two elliptic curves $E, \widetilde{E}$ over a field $\mathbb{F}$ are isomorphic over $\overline{\mathbb{F}}$ if and only if $j(E_1) = j(E_2)$, see [22, Proposition III.1.4(b)].

Note that over a finite field $\mathbb{F}_q$ each of the q values appears as j-invariant of at least one curve. So, the number of distinct elliptic curves over $\mathbb{F}_q$ (up to isomorphism over $\overline{\mathbb{F}}_q$) is equal to q. The same is true for the family (2). Furthermore, for a finite field $\mathbb{F}_q$ with characteristic $p \neq 2, 3$, the number of $\mathbb{F}_q$-isomorphism classes of the family (2) is equal to $2q + 6$, $2q + 2$, $2q + 4$, $2q$ if $q \equiv 1, 5, 7, 11 \pmod{12}$ respectively (e.g. see [18]).

In the following, we use $J_{\mathrm{L}}(q)$, $J_{\mathrm{JQ}}(q)$, $J_{\mathrm{JI}}(q)$, $J_{\mathrm{H}}(q)$, $J_{\mathrm{E}}(q)$, $J_{\mathrm{BL}}(q)$, $J_{\mathrm{TE}}(q)$ and $J_{\mathrm{M}}(q)$ to denote the number of distinct j-invariants of the curves defined over $\mathbb{F}_q$ in the families (3), (4), (5), (6), (7), (8), (9) and (10) respectively.

Moreover, we use $I_{\mathrm{L}}(q)$, $I_{\mathrm{JQ}}(q)$, $I_{\mathrm{JI}}(q)$, $I_{\mathrm{H}}(q)$, $I_{\mathrm{E}}(q)$, $I_{\mathrm{BL}}(q)$, $I_{\mathrm{TE}}(q)$ and $I_{\mathrm{M}}(q)$ to denote the number of $\mathbb{F}_q$-isomorphism classes of the families (3), (4), (5), (6), (7), (8), (9) and (10) respectively.

We compute the number of distinct j-invariants of a family of elliptic curves $\mathbf{E}_u$ over a finite field $\mathbb{F}_q$ with a parameter u, using the general approach mentioned in [13]. In this approach, the j-invariant of $\mathbf{E}_u$ is given by a rational function $F(U) \in \mathbb{F}_q(U)$ of small degree. Next, we consider the bivariate rational function

$$F(U) - F(V) = g(U, V)/l(U, V)$$

with two relatively prime polynomials g and l. We factor $g(U, V)$. Then, studying the number of distinct roots of the polynomials $g_u(V) = g(u, V)$, for $u \in \mathbb{F}_q$, provides the necessary information, which is the cardinality of the set $\mathcal{J}_u$ of all curves $\mathbf{E}_v$ with $j(\mathbf{E}_v) = j(\mathbf{E}_u)$. Then, for several small integers k, we count the number of elements u of $\mathbb{F}_q$ with $\#\mathcal{J}_u = k$. Therefore, we obtain the number of different sets $\mathcal{J}_u$, i.e., the number of distinct $j(\mathbf{E}_u)$ in the family.

We propose an analogous approach to count the number of $\mathbb{F}_q$-isomorphism classes of elliptic curves $\mathbf{E}_u$, for $u \in \mathbb{F}_q$. Considering the set $\mathcal{J}_u$, we study the set $\mathcal{I}_u$ of curves $\mathbf{E}_v$ which are $\mathbb{F}_q$-isomorphic to the curve $\mathbf{E}_u$. Then, counting the number of distinct sets $\mathcal{I}_u$ provides our results.

3 Legendre curves

We consider the curves $\mathbf{E}_{\mathrm{L},u}$ given by Legendre equation (3) over a finite field $\mathbb{F}_q$ with characteristic $p \geq 3$. We note that $u \neq 0, 1$, since the curve $\mathbf{E}_{\mathrm{L},u}$ is nonsingular. The Legendre curve $\mathbf{E}_{\mathrm{L},u}$ over $\mathbb{F}_q$ of characteristic $p > 3$ is isomorphic to the Weierstrass curve $\mathbf{E}_{\mathrm{W},a_u,b_u}$ given by

$$Y^2 = X^3 + a_uX + b_u, \tag{11}$$

where $a_u = -\frac{u^2-u+1}{3}$ and $b_u = -\frac{(u+1)(u-2)(2u-1)}{27}$. The j-invariant of $\mathbf{E}_{\mathrm{L},u}$ is given by $j(\mathbf{E}_{\mathrm{L},u}) = F(u)$ where

$$F(U) = 2^8(U^2 - U + 1)^3/(U^2 - U)^2.$$

Here, we study the cardinality of preimages of $F(u)$, for all elements $u \in \mathbb{F}_q \setminus \{0, 1\}$, under the map $u \mapsto F(u)$. In particular, we see this map is $6:1$, for almost all $u \in \mathbb{F}_q$.

We consider the bivariate rational function $F(U) - F(V) = g(U, V)/l(U, V)$ with two relatively prime polynomials g and l. We see that

$$g(U,V) = 2^8(U-V)(U+V-1)(UV-1)(UV-V+1)(UV-U+1)(UV-U-V).$$

Then, we need to study the number of roots of the polynomial $g_u(V) = g(u, V)$, for $u \in \mathbb{F}_q \setminus \{0, 1\}$. Moreover, for $u \in \mathbb{F}_q \setminus \{0, 1\}$, we let

$$\mathcal{J}_{\mathrm{L},u} = \left\{ v \ : \ v \in \mathbb{F}_q, \ \ \mathbf{E}_{\mathrm{L},u} \cong_{\overline{\mathbb{F}}_q} \mathbf{E}_{\mathrm{L},v} \right\}.$$

We note that, for all $v \in \mathcal{J}_{\mathrm{L},u}$, the curves $\mathbf{E}_{\mathrm{L},u}$ and $\mathbf{E}_{\mathrm{L},v}$ have the same j-invariants. But, these curves may not be isomorphic over $\mathbb{F}_q$. Next, for a fixed value $u \in \mathbb{F}_q \setminus \{0, 1\}$, we let

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

Clearly, for all $u \in \mathbb{F}_q \setminus \{0, 1\}$, we have $\mathcal{I}_{\mathrm{L},u} \subseteq \mathcal{J}_{\mathrm{L},u}$. We see that $j(\mathbf{E}_{\mathrm{L},u}) = j(\mathbf{E}_{\mathrm{W},a_u,b_u}) = 0$ if and only if $a_u = 0$. Furthermore, $j(\mathbf{E}_{\mathrm{L},u}) = 1728$ if and only if $b_u = 0$ (see Equation (11)). Let

$$\mathcal{B} = \{u : u \in \mathbb{F}_q, a_u b_u = 0\}.$$

The following lemma gives the cardinality of $\mathcal{J}_{\mathrm{L},u}$, for all $u \in \mathbb{F}_q \setminus \{0, 1\}$.

Lemma 1. *For all $u \in \mathbb{F}_q \setminus \{0, 1\}$, we have*

$$\#\mathcal{J}_{\mathrm{L},u} = \begin{cases} 1, & \text{if } u = -1 \text{ and } p = 3, \\ 3, & \text{if } u \in \left\{-1, 2, 2^{-1}\right\} \text{ and } p > 3, \\ 2, & \text{if } u^2 - u + 1 = 0 \text{ and } p > 3, \\ 6, & \text{if } u \notin \mathcal{B}. \end{cases}$$

Furthermore, the following lemma gives the cardinality of $\mathcal{I}_{\mathrm{L},u}$, for all $u \in \mathbb{F}_q \setminus \{0, 1\}$.

Lemma 2. *For all $u \in \mathbb{F}_q \setminus \{0, 1\}$, we have*

$$\#\mathcal{I}_{\mathrm{L},u} = \begin{cases} 1, & \text{if } u = -1 \text{ and } p = 3, \\ 3, & \text{if } u \in \left\{-1, 2, 2^{-1}\right\}, \ q \equiv 1, 3, 7 \pmod 8 \text{ and } p > 3, \\ 2, & \text{if } u \in \{-1, 2\}, \ q \equiv 5 \pmod 8, \\ 1, & \text{if } u = 2^{-1}, \ q \equiv 5 \pmod 8, \\ 2, & \text{if } u^2 - u + 1 = 0, \ q \equiv 1 \pmod{12} \text{ and } p > 3, \\ 1, & \text{if } u^2 - u + 1 = 0, \ q \not\equiv 1 \pmod{12}, \\ 3, & \text{if } \chi_2(-1) = -1 \text{ and } u \notin \mathcal{B}, \\ 2, & \text{if } \chi_2(-1) = 1, \chi_2(u) = \chi_2(1-u) = -1 \text{ and } u \notin \mathcal{B}, \\ 4, & \text{if } \chi_2(-1) = 1, \chi_2(u)\chi_2(1-u) = -1 \text{ and } u \notin \mathcal{B}, \\ 6, & \text{if } \chi_2(-1) = 1, \chi_2(u) = \chi_2(1-u) = 1 \text{ and } u \notin \mathcal{B}. \end{cases}$$

In the following, we give a precise formula for the number of distinct curves over $\mathbb{F}_q$, up to isomorphism classes over $\overline{\mathbb{F}}_q$, of the family (3).

Theorem 1. *For any prime $p \geq 3$, for the number $J_{\mathrm{L}}(q)$ of distinct values of the j-invariant of the family* (3)*, we have*

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

Proof. We note that $J_{\mathrm{L}}(q) = \sum_{u \in \mathbb{F}_q \setminus \{0,1\}} \frac{1}{\#\mathcal{J}_{\mathrm{L},u}}$. For any positive integer k, let $N_k = \#\{u : u \in \mathbb{F}_q \setminus \{0,1\},\ \#\mathcal{J}_{\mathrm{L},u} = k\}$. From Lemma 1, we see that $N_k = 0$ for $k = 4, 5$ and $k > 6$. Let r be the remainder of q divided by 3. We have $N_1 = 1$ if $r = 0$, $N_1 = 0$ if $r \neq 0$, $N_2 = 2$ if $r = 1$, $N_2 = 0$ if $r \neq 1$, $N_3 = 0$ if $r = 0$ and $N_3 = 3$ if $r \neq 0$. We also have $N_6 = q-3, q-7, q-5$ if $r = 0, 1, 2$, respectively. Next, we have $J_{\mathrm{L}}(q) = \sum_{k=1}^{6} \frac{N_k}{k}$, so $J_{\mathrm{L}}(q) = \frac{q+3}{6}, \frac{q+5}{6}, \frac{q+1}{6}$ if $q \equiv 0, 1, 2 \pmod 3$ respectively. □

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 (3).

Theorem 2. *For any prime $p \geq 3$, for the number $I_{\mathrm{L}}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (3)*, we have*

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

Proof. We note that $I_{\mathrm{L}}(q) = \sum_{u \in \mathbb{F}_q \setminus \{0,1\}} \frac{1}{\#\mathcal{I}_{\mathrm{L},u}}$. For any positive integer k, let $M_k = \#\{u : u \in \mathbb{F}_q \setminus \{0,1\},\ \#\mathcal{I}_{\mathrm{L},u} = k\}$. From Lemma 2, one can obtain the values of M_k; see Table 1 (where $q \equiv r \pmod{24}$).

r	M_1	M_2	M_3	M_4	M_5	M_6
1	0	$(q+7)/4$	3	$(q-1)/2$	0	$(q-25)/4$
3	1	0	$q-3$	0	0	0
5	1	$(q+3)/4$	0	$(q-5)/2$	0	$(q-5)/4$
7, 19	2	0	$q-4$	0	0	0
9	1	$(q-1)/4$	0	$(q-1)/2$	0	$(q-9)/4$
11, 23	0	0	$q-2$	0	0	0
13	1	$(q+11)/4$	0	$(q-5)/2$	0	$(q-13)/4$
17	0	$(q-1)/4$	3	$(q-1)/2$	0	$(q-17)/4$

Table 1. M_k, for $k = 1, \ldots, 6$.

We have, $I_{\mathrm{L}}(q) = \sum_{k=1}^{6} \frac{M_k}{k}$, so we compute $I_{\mathrm{L}}(q)$ which completes the proof of this theorem. □.

4 Jacobi curves

First, we consider the Jacobi qartic curves $\mathbf{E}_{\mathrm{JQ},u}$ given by (4) over a field $\mathbb{F}$ with characteristic $p \geq 3$. Note that $u \neq \pm 1$, since the curve $\mathbf{E}_{\mathrm{JQ},u}$ is nonsingular. The change of variable $(X, Y) \mapsto (\widetilde{X}, \widetilde{Y})$ defined by $\widetilde{X} = 2(u + \frac{Y+1}{X^2})$ and $\widetilde{Y} = \frac{2\widetilde{X}}{X}$, is a birational equivalence from $\mathbf{E}_{\mathrm{JQ},u}$ to the elliptic curve $\widetilde{\mathbf{E}}_{\mathrm{JQ},u}$ defined by

$$\widetilde{Y}^2 = \widetilde{X}^3 - 4u\widetilde{X}^2 + 4(u^2 - 1)\widetilde{X}$$

with j-invariant $j(\mathbf{E}_{\mathrm{JQ},u}) = F(u)$ where $F(U) = 64(U^2 + 3)^3/(U^2 - 1)^2$.

Lemma 3. *For all $u \in \mathbb{F}$ with $u \neq \pm 1$, the Jacobi curve $\mathbf{E}_{\mathrm{JQ},u}$ is birationally equivalent over $\mathbb{F}$ to the Legendre curve $\mathbf{E}_{\mathrm{L},\frac{1-u}{2}}$.*

Now, we consider the curves $\mathbf{E}_{\mathrm{JI},u}$ given by (5) over a field $\mathbb{F}$ with characteristic $p \geq 3$. We note that $u \neq 0, 1$, since the curve $\mathbf{E}_{\mathrm{JI},u}$ is nonsingular. The change of variable $(X, Y, Z) \mapsto (\widetilde{X}, \widetilde{Y})$ defined by $\widetilde{X} = \frac{u(Y-Z)}{uY-Z+1-u}$ and $\widetilde{Y} = \frac{u(1-u)X}{uY-Z+1-u}$, is a birational equivalence from $\mathbf{E}_{\mathrm{JI},u}$ to the elliptic curve $\widetilde{\mathbf{E}}_{\mathrm{JI},u}$ defined by

$$\widetilde{Y}^2 = \widetilde{X}^3 - (u + 1)\widetilde{X}^2 + u\widetilde{X}.$$

We note that $\widetilde{\mathbf{E}}_{\mathrm{JI},u} = \mathbf{E}_{\mathrm{L},u}$. Moreover, the Jacobi intersection curve $\mathbf{E}_{\mathrm{JI},u}$ is birationally equivalent over $\mathbb{F}$ to the the Jacobi curve $\mathbf{E}_{\mathrm{JQ},1-2u}$.

From Theorem 2, the following lemma gives the numbers of distinct curves over a finite field $\mathbb{F}_q$ of the families (4) and (5).

Lemma 4. *For any prime $p \geq 3$, for the numbers $I_{\mathrm{L}}(q)$, $I_{\mathrm{JQ}}(q)$ and $I_{\mathrm{JI}}(q)$ of $\mathbb{F}_q$-isomorphism classes of the families (3), (4) and (5) respectively, we have*

$$I_{\mathrm{L}}(q) = I_{\mathrm{JQ}}(q) = I_{\mathrm{JI}}(q).$$

5 Hessian curves

We consider the curves $\mathbf{E}_{\mathrm{H},u}$ given by (6) over a finite field $\mathbb{F}_q$ of characteristic p. We note that $u^3 \neq 27$, since the curve $\mathbf{E}_{\mathrm{H},u}$ is nonsingular. The curve $\mathbf{E}_{\mathrm{H},u}$ has the j-invariant $j(\mathbf{E}_{\mathrm{H},u}) = (F(u))^3$ where $F(U) = U(U^3 + 216)/(U^3 - 27)$.

We consider the bivariate rational function $F(U) - F(V) = g(U, V)/l(U, V)$ with two relatively prime polynomials g and l. We see that

$$g(U, V) = (U - V)(UV - 3U - 3V - 18)h(U, V),$$

where $h(U, V) = (U^2 + 3U + 9)V^2 + 3(U^2 + 12U - 18)V + 9(U^2 - 6U + 36)$.

For a fixed value $u \in \mathbb{F}_q$ with $u^3 \neq 27$, let $g_u(V) = g(u, V)$. Next, for $u \in \mathbb{F}_q$ with $u^3 \neq 27$, we investigate the number of roots of the polynomial $g_u(V) = g(u, V)$. Moreover, for $u \in \mathbb{F}_q$ with $u^3 \neq 27$, we let

$$\mathcal{J}_{\mathrm{H},u} = \left\{ v \ : \ v \in \mathbb{F}_q,\ \mathbf{E}_{\mathrm{H},u} \cong_{\overline{\mathbb{F}}_q} \mathbf{E}_{\mathrm{H},v} \right\},\ \mathcal{I}_{\mathrm{H},u} = \left\{ v \ : \ v \in \mathbb{F}_q,\ \mathbf{E}_{\mathrm{H},u} \cong_{\mathbb{F}_q} \mathbf{E}_{\mathrm{H},v} \right\}.$$

Let $A_u = u(u^3 + 6^3)$ and let $B_u = u^6 - 540u^3 - 18^3$. Here, we give the cardinalities of $\mathcal{J}_{\mathrm{H},u}$ and $\mathcal{I}_{\mathrm{H},u}$, for all $u \in \mathbb{F}_q$ with $u^3 \neq 27$.

Lemma 5. *For all $u \in \mathbb{F}_q$ with $u^3 \neq 27$, we have*

$$\#\mathcal{J}_{\mathrm{H},u} = \begin{cases} 1, & \text{if } p = 2 \text{ and } u = 0, \text{ or } p = 3, \\ 4, & \text{if } q \equiv 1 \pmod 3,\ p \neq 2 \text{ and } A_u = 0, \\ 6, & \text{if } q \equiv 1 \pmod 3,\ p \neq 2 \text{ and } B_u = 0, \\ 12, & \text{if } q \equiv 1 \pmod 3 \text{ and } A_u B_u \neq 0, \\ 2, & \text{if } q \equiv 2 \pmod 3,\ p \neq 2 \text{ or } u \neq 0, \end{cases}$$

and

$$\#\mathcal{I}_{\mathrm{H},u} = \begin{cases} 1, & \text{if } q \equiv 0, 2 \pmod 3, \\ \#\mathcal{J}_{\mathrm{H},u}, & \text{if } q \equiv 1 \pmod 3. \end{cases}$$

The following theorems give the number of distinct Hessian curves over $\mathbb{F}_q$.

Theorem 3. *For any prime p, for the number $J_{\mathrm{H}}(q)$ of distinct values of the j-invariant of the family* (6)*, we have*

$$J_{\mathrm{H}}(q) = \begin{cases} q-1, & \text{if } q \equiv 0 \pmod 3, \\ \lfloor (q+11)/12 \rfloor, & \text{if } q \equiv 1 \pmod 3, \\ \lfloor q/2 \rfloor, & \text{if } q \equiv 2 \pmod 3. \end{cases}$$

Proof. We note that $J_{\mathrm{H}}(q) = \sum_{u \in \mathbb{F}_q, u^3 \neq 27} \frac{1}{\#\mathcal{J}_{\mathrm{H},u}}$. For the positive integer k, let $N_k = \#\left\{u : u \in \mathbb{F}_q, u^3 \neq 27,\ \#\mathcal{J}_{\mathrm{H},u} = k\right\}$. From Lemma 5, we can see that $N_k = 0$ for $k = 3, 5, 7, 8, 9, 10, 11$ and $k > 12$. Moreover, we can compute the values of N_k; see Table 2 (where $q \equiv r \pmod{12}$).

r	N_1	N_2	N_4	N_6	N_{12}
1	0	0	4	6	$q-13$
2, 8	1	$q-2$	0	0	0
3, 9	$q-1$	0	0	0	0
4	1	0	0	0	$q-4$
7	0	0	4	0	$q-7$
5, 11	0	$q-1$	0	0	0

Table 2. N_k, for $k = 1, 2, 4, 6, 12$.

Next, we have $J_{\mathrm{H}}(q) = \sum_{k=1}^{12} \frac{N_k}{k}$, so we compute $J_{\mathrm{H}}(q)$, which completes the proof of this theorem. □

Theorem 4. *For any prime p, for the number $I_{\mathrm{H}}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (6)*, we have*

$$I_{\mathrm{H}}(q) = \begin{cases} \lfloor (q+11)/12 \rfloor, & \text{if } q \equiv 1 \pmod 3, \\ q-1, & \text{if } q \equiv 0, 2 \pmod 3. \end{cases}$$

Proof. The proof is given from Lemma 5 and Theorem 3. □

Recently, Farashahi and Joye have considered the generalization of Hessian curves, see [12]. From Theorem 4, the number of distinct *generalized Hessian* curves over $\mathbb{F}_q$ is given by [12, Theorems 4,5].

6 Edwards curves

The numbers of distinct j-invariants of the families (7) and (8) have been studied in [13, Theorms 3 and 5]. In the following theorems, we give the numbers of $\mathbb{F}_q$-isomorphism classes of these families.

Theorem 5. *For any prime $p \geq 3$, for the number $I_{\mathrm{E}}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (7)*, we have*

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

Theorem 6. *For any prime $p \geq 3$, for the number $I_{\mathrm{BL}}(q)$ of $\mathbb{F}_q$-isomorphism classes of the family* (8)*, we have*

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

Now, we consider the families of twisted Edwards curves, given by (9), and the Montgomery curves, given by (10), over a finite field $\mathbb{F}_q$ of odd characteristic.

The twisted Edwards curve $\mathbf{E}_{\mathrm{TE},v,u}$, via the change of variable $(X, Y) \mapsto (\widetilde{X}, \widetilde{Y})$ defined by $\widetilde{X} = (1+Y)/(1-Y)$ and $\widetilde{Y} = \widetilde{X}/X$, is birationally equivalent to the Montgomery curve $\mathbf{E}_{\mathrm{M},\frac{4}{v-u},\frac{2(v+u)}{v-u}}$. Conversely, every Montgomery curve $\mathbf{E}_{\mathrm{M},v,u}$ is birationally equivalent over $\mathbb{F}_q$ to the twisted Edwards curve $\mathbf{E}_{\mathrm{TE},\frac{u+2}{v},\frac{u-2}{v}}$ (see [2, Theorem 3.2]). So, the families (9) and (10) have the same number of isomorphism classes over $\mathbb{F}_q$.

We note that, the family (9) is the generalization of the families (7) and (8). Clearly, every Edwards curve $\mathbf{E}_{\mathrm{BL},u}$ is a twisted Edwards. Moreover, a twisted Edwards curve $\mathbf{E}_{\mathrm{TE},v,u}$ is a twist of the Edwards curve $\mathbf{E}_{\mathrm{BL},\frac{u}{v}}$. We note that a quadratic twist of $\mathbf{E}_{\mathrm{BL},u}$, which is not isomorphic to $\mathbf{E}_{\mathrm{BL},u}$ over $\mathbb{F}_q$, may not be in the family (8). Therefore, the family (9) includes the curves of (8) and the twists of the curves of (8). Moreover, the j-invariant of a curve and the j-invariant of its twist are equal. So, both family have the same number of distinct j-invariants.

Theorem 7. *For any prime $p \geq 3$, for the numbers $J_{\mathrm{BL}}(q)$, $J_{\mathrm{TE}}(q)$ and $J_{\mathrm{M}}(q)$ of distinct $\overline{\mathbb{F}}_q$-isomorphism classes of the families* (8)*,* (9) *and* (10) *respectively, we have*

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

Theorem 8. *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* (9) *and* (10) *respectively, we have*

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

Acknowledgment. The author would like to thank Igor Shparlinski for his interest and support of this work. The author thanks anonymous reviewers for their useful comments.

References

1. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, CRC Press, 2005.
2. D. J. Bernstein, M. Joye, P. Birkner, T. Lange and C. Peters, 'Twisted Edwards curves', *Africacrypt'2008*, LNCS, vol. 5023, Springer-Verlag, 2008, 389–405.
3. D. J. Bersntein, D. Kohel, and T. Lange, 'Twisted Hessian curves', `http://www.hyperelliptic.org/EFD/g1p/auto-twistedhessian.html`.
4. D. J. Bernstein and T. Lange, 'Faster addition and doubling on elliptic curves', *Asiacrypt'2007*, LNCS, vol. 4833, Springer-Verlag, 2007, 29–50.
5. D. J. Bernstein, T. Lange and R. R. Farashahi, 'Binary Edwards curves', *CHES'2008*, LNCS, vol. 5154, Springer-Verlag, 2008, 244–265.
6. O. Billet and M. Joye, 'The Jacobi model of an elliptic curve and side-channel analysis', *AAECC'2003*, LNCS, vol. 2643 Springer-Verlag, 2003, 34–42.
7. J. W. S. Cassels, 'Lectures on elliptic curves', Cambridge University Press, 1991.
8. W. Castryck and H. Hubrechts, 'The distribution of the number of points modulo an integer on elliptic curves over finite fields', *Preprint*, 2009.
9. C. Doche, T. Icart and D. R. Kohel, 'Efficient scalar multiplication by isogeny decompositions', *PKC'2006*, LNCS, vol. 3958, Springer-Verlag, 2006, 191–206.
10. S. Duquesne, 'Improving the arithmetic of elliptic curves in the Jacobi model', *Information Processing Letters*, **104**(3), (2007), 101–105.
11. H. M. Edwards, 'A normal form for elliptic curves', *Bull. Amer. Math. Soc.*, **44** (2007), 393–422,
12. R. R. Farashahi and M. Joye, 'Efficient arithmetic on Hessian curves', *PKC'2010*, LNCS, vol. 6056, Springer-Verlag, 2010, 243–260.
13. R. R. Farashahi and I. E. Shparlinski, 'On the number of distinct elliptic curves in some families', *Designs, Codes and Cryptography*, **54**(1), (2010), 83–99.
14. E. Howe, 'On the group orders of elliptic curves over finite fields', *Compositio Mathematica*, **85**(2), (1993), 229–247.
15. H. Hisil, K. K.-H Wong, G. Carter and E. Dawson, 'Faster group operations on elliptic curves', *Seventh Australasian Information Security Conference - AISC'2009'*, vol. 98, 7-19.
16. M. Joye and J.-J Quisquater, 'Hessian elliptic curves and side-channel attacks', *CHES'2001*, LNCS, vol. 2162, Springer-Verlag, 2001, 402–410.
17. N. Koblitz, 'Elliptic curve cryptosystems', *Math. Comp.*, **48**(177), (1987), 203–209.
18. H. W. Lenstra, 'Factoring integers with elliptic curves', *Annals of Mathematics* **126**(3), (1987), 649–673.
19. P.-Y. Liardet and N. P. Smart, 'Preventing SPA/DPA in ECC systems using the Jacobi form', *CHES'2001*, LNCS, vol. 2162, Springer-Verlag, 2001, 391–401.
20. V. S. Miller, 'Use of elliptic curves in cryptography', *Advances in Cryptology – Crypto 1985*, LNCS, vol. 218, Springer-Verlag, 1986, 417–426.
21. P. L. Montgomery, 'Speeding the Pollard and elliptic curve methods of factorization', *Mathematics of Computation*, **48**(177), (1987), 243–264
22. J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.
23. N. P. Smart, 'The Hessian form of an elliptic curve', *CHES'2001*, LNCS, vol. 2162, Springer-Verlag, 2001, 118-125.
24. L. C. Washington, *Elliptic curves: Number theory and Cryptography*, CRC Press, 2008.