Bol. Soc. Paran. Mat.
©SPM –ISSN-2175-1188 ON LINE
SPM: www.spm.uem.br/bspm

(3s.) **v. 2022 (40)** : 1–6.
ISSN-0037-8712 IN PRESS
doi:10.5269/bspm.51867

Twisted Hessian Curves over the Ring $\mathbb{F}_q[e], e^2 = e$ *

Elhamam Moha Ben Taleb, Abdelhakim Chillali, Lhoussain El Fadil

ABSTRACT: Let $\mathbb{F}_q[e]$ be a finite field of q elements, where q is a power of a prime number p. In this paper, we study the Twisted Hessian curves over the ring $\mathbb{F}_q[e]$, where $e^2 = e$, denoted by $H_{a,d}(\mathbb{F}_q[e])$; $(a, d) \in (\mathbb{F}_q[e])^2$. Using the Twisted Hessian equation, we define the Twisted Hessian curves $H_{a,d}(\mathbb{F}_q[e])$ and we will show that $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$ and $H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ are two Twisted Hessian curves over the field $\mathbb{F}_q$, where π_0 and π_1 are respectively the canonical projection and the sum projection of coordinates from $\mathbb{F}_q[e]$ to $\mathbb{F}_q$. Precisely, we give a bijection between the sets $H_{a,d}(\mathbb{F}_q[e])$ and $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$.

Key Words: Finite field, Finite ring, Local ring, Twisted Hessian curve.

Contents

1. Introduction

Let $\mathbb{K}$ be a finite field of order $q = p^n$ where n is a positive integer and p is a prime number. Daniel, Chitchanok, David and Tanja (2015), in [1], has studied the Twisted Hessian curves $H_{a,d}(\mathbb{K})$ defined over the field $\mathbb{K}$. A. Boulbot et al, study the arithmetic of the ring $\mathbb{F}_q[e], e^2 = e$, in particular we show that this ring is not a local (see [2]). In section 3, we define the Twisted Hessian curves $H_{a,d}(\mathbb{F}_q[e])$ over this ring, we study discriminant and the Twisted Hessian equation which allows us to define two Twisted Hessian curves: $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$ and $H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ defined over the finite field $\mathbb{F}_q$. In the next of this section, we classify the elements of $H_{a,d}(\mathbb{F}_q[e])$ and we give a bijection between the two sets: $H_{a,d}(\mathbb{F}_q[e])$ and $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$, where π_0 and π_1 are surjective morphisms of rings defined by:

$$\begin{array}{cccc} \pi_0 & : & \mathbb{F}_q[e] & \to & \mathbb{F}_q \\ & & x_0 + x_1 e & \mapsto & x_0 \end{array} \quad \text{and} \quad \begin{array}{cccc} \pi_1 & : & \mathbb{F}_q[e] & \to & \mathbb{F}_q \\ & & x_0 + x_1 e & \mapsto & x_0 + x_1 \end{array}$$

2. The ring $\mathbb{F}_q[e], e^2 = e$

$\mathbb{F}_q$ is a finite field of order $q = p^n$ where n is a positive integer and p is a prime number. The ring $\mathbb{F}_q[e], e^2 = e$ can be constructed as an extension of the ring $\mathbb{F}_q$ by using the quotient ring of $\mathbb{F}_q[X]$ by the polynomial $X^2 - X$. An element $X \in \mathbb{F}_q[e]$ is represented by $X = x_0 + x_1 e$ where $(x_0, x_1) \in \mathbb{F}_q$.
The arithmetic operations in $\mathbb{F}_q[e]$ can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:

$$X + Y = (x_0 + y_0) + (x_1 + y_1)e$$

$$X.Y = (x_0 y_0) + (x_0 y_1 + x_1 y_0 + x_1 y_1)e,$$

* Sidi Mohamed Ben Abdellah University, Morocco
2010 *Mathematics Subject Classification:* 11T71, 14G50, 94A60.
Submitted January 21, 2020. Published April 24, 2020

where $X = x_0 + x_1e$ and $Y = y_0 + y_1e$.
We can see ([2]), where the authors have proved the following results:

- $(\mathbb{F}_q[e], +, .)$ is a finite unitary commutative ring.
- $\mathbb{F}_q[e]$ is a vector space over $\mathbb{F}_q$ of dimension 2 and $\{1, e\}$ is it's basis.
- $X.Y = (x_0y_0) + ((x_0 + x_1)(y_0 + y_1) - x_0y_0)e$.
- $X^2 = x_0^2 + ((x_0 + x_1)^2 - x_0^2)e$.
- $X^3 = x_0^3 + ((x_0 + x_1)^3 - x_0^3)e$.
- Let $X = x_0 + x_1e \in \mathbb{F}_q[e]$, then $X \in (\mathbb{F}_q[e])^\times$ if and only if $x_0 \neq 0$ and $x_0 + x_1 \neq 0$. The inverse is given by: $X^{-1} = x_0^{-1} + ((x_0 + x_1)^{-1} - x_0^{-1})e$.
- Let $X \in \mathbb{F}_q[e]$, then X is not invertible if and only if $X = xe$ or $X = x - xe$, such that $x \in \mathbb{F}_q$.
- $\mathbb{F}_q[e]$ is a non local ring.
- π_0 and π_1 are two surjective morphisms of rings.

3. Twisted Hessian curves over the Ring $\mathbb{F}_q[e], e^2 = e$

In this section the elements X, Y, Z, a and d are in the ring $\mathbb{F}_q[e]$ such that $X = x_0+x_1e$, $Y = y_0+y_1e$, $Z = z_0 + z_1e$, $a = a_0 + a_1e$ and $d = d_0 + d_1e$ where $x_0, x_1, y_0, y_1, z_0, z_1, a_0, a_1, d_0$ and d_1 are in $\mathbb{F}_q$. We define an Twisted Hessian curve over the Ring $\mathbb{F}_q[e]$, as a curve in the projective space $P^2(\mathbb{F}_q[e])$, which is given by the equation:

$$aX^3 + Y^3 + Z^3 = dXYZ$$

where the discriminant $\Delta = a(27a - d^3)$ is invertible in $\mathbb{F}_q[e]$.
We denote this curves by: $H_{a,d}(\mathbb{F}_q[e])$.

Remark 3.1.

$$\begin{aligned}\pi_0(\Delta) &= a_0(27a_0 - d_0^3),\\ \pi_1(\Delta) &= (a_0 + a_1)(27(a_0 + a_1) - (d_0 + d_1)^3).\end{aligned}$$

Proposition 3.1. *Let $\Delta_0 = \pi_0(\Delta)$ and $\Delta_1 = \pi_1(\Delta)$, then $\Delta = \Delta_0 + (\Delta_1 - \Delta_0)e$*

Proof. We have:

$$\begin{aligned}\Delta &= a(27a - d^3)\\ &= (a_0 + a_1e)(27(a_0 + a_1e) - (d_0 + d_1e)^3)\\ &= 27a_0(a_0 + a_1e) - a_0(d_0 + d_1e)^3 + 27a_1e(a_0 + a_1e) - a_1e(d_0 + d_1e)^3\\ &= 27a_0^2 + 27a_0a_1e - a_0d_0^3 - a_0(d_0 + d_1)^3e + a_0d_0^3e + 27a_0a_1 + 27a_1^2e - a_1d_0^3e - a_1(d_0 + d_1)^3e + a_1d_0^3e\\ &= a_0(27a_0 - d_0^3) + ((a_0 + a_1)(27(a_0 + a_1) - (d_0 + d_1)^3) - a_0(27a_0 - d_0^3))e\\ &= \Delta_0 + (\Delta_1 - \Delta_0)e.\end{aligned}$$

□

Corollary 3.2. *Δ is invertible in $\mathbb{F}_q[e]$ if and only if $\Delta_0 \neq 0$ and $\Delta_1 \neq 0$.*

Using corrolary3.2, if Δ is invertible in $\mathbb{F}_q[e]$, then $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$ and $H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ are two Twisted Hessian curves over the finite field $\mathbb{F}_q$, and we notice:

$$\begin{aligned}H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) &= \{[x : y : z] \in P^2(\mathbb{F}_q) \mid a_0x^3 + y^3 + z^3 = d_0xyz\}\\ H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q) &= \{[x : y : z] \in P^2(\mathbb{F}_q) \mid (a_0 + a_1)x^3 + y^3 + z^3 = (d_0 + d_1)xyz\}\end{aligned}$$

Proposition 3.2. *Let X, Y and Z in $\mathbb{F}_q[e]$, then $[X : Y : Z] \in P^2(\mathbb{F}_q[e])$ if and only if $[\pi_0(X) : \pi_0(Y) : \pi_0(Z)] \in P^2(\mathbb{F}_q)$ and $[\pi_1(X) : \pi_1(Y) : \pi_1(Z)] \in P^2(\mathbb{F}_q)$.*

Proof. Suppose that $[X : Y : Z] \in P^2(\mathbb{F}_q[e])$, then there exists $(U, V, W) \in (\mathbb{F}_q[e])^3$ such that $UX + VY + WZ = 1$. Hence for $i \in \{0, 1\}$, we have:
$\pi_i(U)\pi_i(X) + \pi_i(V)\pi_i(Y) + \pi_i(W)\pi_i(Z) = 1$, so $(\pi_i(X), \pi_i(Y), \pi_i(Z)) \neq (0, 0, 0)$, which proves that $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in P^2(\mathbb{F}_q)$.
Reciprocally, let $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in P^2(\mathbb{F}_q)$, where $i \in \{0, 1\}$.
Suppose that $x_0 \neq 0$, then we distinguish between two case of $x_0 + x_1$:
a) if $x_0 + x_1 \neq 0$, then X is invertible in $\mathbb{F}_q[e]$, so $[X : Y : Z] \in P^2(\mathbb{F}_q[e])$.
b) if $x_0 + x_1 = 0$, then $y_0 + y_1 \neq 0$ or $z_0 + z_1 \neq 0$.
i) If $y_0 + y_1 \neq 0$ then:

$$x_0 + (y_0 + y_1 - x_0)e = x_0 - x_0 e + (y_0 + y_1)e = X + eY \in (\mathbb{F}_q[e])^\times,$$

so there exists $U \in \mathbb{F}_q[e]$, such that $UX + eUY = 1$, hence $[X : Y : Z] \in P^2(\mathbb{F}_q[e])$.
ii) If $z_0 + z_1 \neq 0$ then $X + eZ \in (\mathbb{F}_q[e])^\times$, so $[X : Y : Z] \in P^2(\mathbb{F}_q[e])$.
We can use the same proof if y_0 not 0 or z_0 not 0.

□

Theorem 3.3. *Let X, Y and Z in $\mathbb{F}_q[e]$, then*
$[X : Y : Z] \in H_{a,d}(\mathbb{F}_q[e])$ *if and only if* $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in H_{\pi_i(a),\pi_i(d)}(\mathbb{F}_q)$, *for* $i \in \{0, 1\}$.

Proof. We have:

$$\begin{aligned}
aX^3 &= (a_0 + a_1 e)(x_0 + x_1 e)^3 \\
&= (a_0 + a_1 e)(x_0^3 + ((x_0 + x_1)^3 - x_0^3)e) \\
&= a_0 x_0^3 + a_0(x_0 + x_1)^3 e - a_0 x_0^3 e + a_1 x_0^3 e + a_1(x_0 + x_1)^3 e - a_1 x_0^3 e \\
&= a_0 x_0^3 + (a_0 + a_1)(x_0 + x_1)^3 e - a_0 x_0^3 e \\
Y^3 &= y_0^3 + ((y_0 + y_1)^3 - y_0^3)e \\
Z^3 &= z_0^3 + ((z_0 + z_1)^3 - z_0^3)e \\
dXYZ &= (d_0 + d_1 e)(x_0 + x_1 e)(y_0 + y_1 e)(z_0 + z_1 e) \\
&= d_0 x_0 y_0 z_0 + d_0 x_0 y_0 z_1 e + d_0 x_0 y_1 z_0 e + d_0 x_0 y_1 z_1 e + d_0 x_1 y_0 z_0 e + d_0 x_1 y_0 z_1 e \\
&\quad + d_0 x_1 y_1 z_0 e + d_0 x_1 y_1 z_1 e + d_1 x_0 y_1 z_1 e + d_1 x_0 y_0 z_0 e + d_1 x_0 y_0 z_1 e \\
&\quad + d_1 x_0 y_1 z_0 e + d_1 x_1 y_0 z_0 e + d_1 x_1 y_0 z_1 e + d_1 x_1 y_1 z_0 e + d_1 x_1 y_1 z_1 e
\end{aligned}$$

Or $\{1, e\}$ is a basis $\mathbb{F}_q$ vector space $\mathbb{F}_q[e]$, then: $aX^3 + Y^3 + Z^3 = dXYZ$
if and only if $a_0 x_0^3 + y_0^3 + z_0^3 = d_0 x_0 y_0 z_0$ and
$(a_0 + a_1)(x_0 + x_1)^3 + (y_0 + y_1)^3 + (z_0 + z_1)^3 = (d_0 + d_1)(x_0 + x_1)(y_0 + y_1)(z_0 + z_1)$.

□

Corollary 3.4. *The mappings $\tilde{\pi_0}$ and $\tilde{\pi_1}$ are well defined, where $\tilde{\pi_i}$ for $i \in \{0, 1\}$ is given by:*

$$\begin{array}{cccc}
\tilde{\pi_i} & : & H_{a,d}(\mathbb{F}_q[e]) & \rightarrow & H_{\pi_i(a),\pi_i(d)}(\mathbb{F}_q) \\
 & & [X : Y : Z] & \mapsto & [\pi_i(X) : \pi_i(Y) : \pi_i(Z)]
\end{array}$$

Proof. From the previous theorem, we have $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in H_{\pi_i(a),\pi_i(d)}(\mathbb{F}_q)$
If $[X : Y : Z] = [X' : Y' : Z']$, then there exist $\lambda \in (\mathbb{F}_q)^\times$ such that: $X' = \lambda X$, $Y' = \lambda Y$ and $Z' = \lambda Z$, then:

$$\begin{aligned}
\tilde{\pi_i}([X' : Y' : Z']) &= [\pi_i(X') : \pi_i(Y') : \pi_i(Z')] \\
&= \underbrace{[\pi_i(\lambda)\pi_i(X) : \pi_i(\lambda)\pi_i(Y) : \pi_i(\lambda)\pi_i(Z)]}_{\pi_i(\lambda)=\lambda\in(\mathbb{F}_q)^\times} \\
&= [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \\
&= \tilde{\pi_i}([X : Y : Z]).
\end{aligned}$$

□

4. Classification of elements in $H_{a,d}(\mathbb{F}_q[e])$

In this subsection, we assume that -3 is not a square in $\mathbb{F}_q$, we will classify the elements of the Twisted Hessian curves into three types, depending on whether the projective coordinate X is invertible or not. The result is in the following proposition.

Proposition 4.1. *The elements of $H_{a,d}(\mathbb{F}_q[e])$ are of the form:*
- $[1 : y_0 + y_1e : z_0 + z_1e]$
- $[0 : -1 : 1]$
- $[e : -1 + y_1e : 1 + z_1e]$
- $[1 - e : -1 - y_1 + y_1e : 1 - z_1 + z_1e]$

Proof. Let $P = [X : Y : Z] \in H_{a,d}(\mathbb{F}_q[e]))$, where $X = x_0 + x_1e$, $Y = y_0 + y_1e$ and $Z = z_0 + z_1e$. We have two cases of the projective coordinate X:
1) first case: X is invertible, then: $[X : Y : Z] \sim [1 : Y : Z]$
2) second case: X is no invertible, in this case we have:
i) $X = xe$, where $x \in \mathbb{F}_q$, then:
- if $x = 0$ then $[X : Y : Z] = [0 : -1 : 1]$, else $x \neq 0$ then:

$$[X : Y : Z] \sim [e : y_0 + y_1e : z_0 + z_1e]$$

we have: $\pi_0([e : y_0 + y_1e : z_0 + z_1e]) = [0 : y_0 : z_0] \in H_{\pi_0(a),\pi_0(d)}$ then:
$y_0 = -1$ and $z_0 = 1$, i.e:

$$[e : y_0 + y_1e : z_0 + z_1e] = [e : -1 + y_1e : 1 + z_1e]$$

ii) $X = x - xe$, where $x \in \mathbb{F}_q$, then:
- if $x = 0$ then $[X : Y : Z] = [0 : -1 : 1]$, else $x \neq 0$ then:

$$[X : Y : Z] \sim [1 - e : y_0 + y_1e : z_0 + z_1e]$$

we have $\pi_1([1 - e : y_0 + y_1e : z_0 + z_1e]) = [0 : y_0 + y_1 : z_0 + z_1] \in H_{\pi_1(a),\pi_1(d)}$ then:
$y_0 + y_1 = -1$ and $z_0 + z_1 = 1$, i.e:

$$[1 - e : y_0 + y_1e : z_0 + z_1e] = [1 - e : -1 - y_1 + y_1e : 1 - z_1 + z_1e]$$

□

From this proposition we deduce the following Corollaries :

Corollary 4.1. $H_{a,d}(\mathbb{F}_q[e]) = [1 : Y : Z] \setminus a + Y^3 + Z^3 = dYZ\}$
$\cup \{[e : -1 + y_1e : 1 + z_1e] \setminus [1 : -1 + y_1 : 1 + z_1] \in H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)\}$
$\cup \{[1 - e : -1 - y_1 + y_1e : 1 - z_1 + z_1e] \setminus [1 : -1 - y_1 : 1 - z_1] \in H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q)\}$
$\cup \{[0 : -1 : 1]\}$

Corollary 4.2. *$\tilde{\pi_0}$ is a surjective mapping.*

Proof. Let $[x : y : z] \in H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$, then:
- if $x = 0$ then $[x : y : z] \sim [0 : -1 : 1]$; hence $[0 : -1 : 1]$ is an antecedent of $[0 : -1 : 1]$
- if $x \neq 0$, then $[x : y : z] \sim [1 : y : z]$; hence $[1 - e : y - (1 + y)e : z + (1 - z)e]$ is an antecedent of $[1 : y : z]$.

□

Corollary 4.3. *$\tilde{\pi_1}$ is a surjective mapping.*

Proof. Let $[x : y : z] \in H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$, then:
- If $x = 0$, then $[x : y : z] \sim [0 : -1 : 1]$; hence $[0 : -1 : 1]$ is an antecedent of $[0 : -1 : 1]$
- If $x \neq 0$, then $[x : y : z] \sim [1 : y : z]$; hence $[e : -1 + (y + 1)e : 1 + (z - 1)e]$ is an antecedent of $[1 : y : z]$.

□

The next proposition gives a bijection between the two sets

$$H_{a,d}(\mathbb{F}_q[e])$$

and

$$H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q).$$

Proposition 4.2. *The $\tilde{\pi}$ mapping defined by:*

$$\begin{array}{cccc} \tilde{\pi} & : & H_{a,d}(\mathbb{F}_q[e]) & \rightarrow & H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q) \\ & & [X:Y:Z] & \mapsto & ([\pi_0(X):\pi_0(Y):\pi_0(Z)],[\pi_1(X):\pi_1(Y):\pi_1(Z)]) \end{array}$$

is a bijection.

Proof. • As $\tilde{\pi_0}$ and $\tilde{\pi_1}$ are well defined, then $\tilde{\pi}$ is well defined.
• Let $([x_0:y_0:z_0],[x_1:y_1:z_1]) \in H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q))$, clearly:
$\tilde{\pi}([x_0+(x_1-x_0)e : y_0+(y_1-y_0)e : z_0+(z_1-z_0)e]) = ([x_0:y_0:z_0],[x_1:y_1:z_1])$, hence $\tilde{\pi}$ is a surjective mapping.
• Lets $[X:Y:Z]$ and $[X':Y':Z']$ are elements of $H_{a,d}(\mathbb{F}_q[e])$, where $X = x_0+x_1e$, $Y = y_0+y_1e$, $Z = z_0+z_1e$, $X' = x'_0+x'_1e$, $Y' = y'_0+y'_1e$ and $Z' = z'_0+z'_1e$.
If $[x_0:y_0:z_0] = [x'_0:y'_0:z'_0]$ and $[x_0+x_1:y_0+y_1:z_0+z_1] = [x'_0+x'_1:y'_0+y'_1:z'_0+z'_1]$, then there exist $(k,l) \in (\mathbb{F}_q^*)^2$ such that:

$$\begin{cases} x'_0 = kx_0 \\ y'_0 = ky_0 \\ z'_0 = kz_0 \end{cases} \text{and} \begin{cases} x'_0+x'_1 = l(x_0+x_1) \\ y'_0+y'_1 = l(y_0+y_1) \\ z'_0+z'_1 = l(z_0+z_1) \end{cases} \text{so} \begin{cases} x'_1 = (l-k)x_0+x_1 \\ y'_1 = (l-k)y_0+y_1 \\ z'_1 = (l-k)z_0+z_1 \end{cases}$$

then: $\begin{cases} X' = kx_0+((l-k)x_0+x_1)e = (k+(l-k)e)X \\ Y' = ky_0+((l-k)y_0+y_1)e = (k+(l-k)e)Y \\ Z' = kz_0+((l-k)z_0+z_1)e = (k+(l-k)e)Z \end{cases}$

Or $k+(l-k)e$ is invertible in $\mathbb{F}_q[e]$, so $[X':Y':Z'] = [X:Y:Z]$, hence $\tilde{\pi}$ is an injective mapping. We can easily show that the mapping $\tilde{\pi}^{-1}$ defined by:

$$\tilde{\pi}^{-1}([x_0:y_0:z_0],[x_1:y_1:z_1]) = [x_0+(x_1-x_0)e : y_0+(y_1-y_0)e : z_0+(z_1-z_0)e]$$

is the inverse of $\tilde{\pi}$.

□

Since there is a bijection between $H_{a,d}(\mathbb{F}_q[e])$ and $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ then we deduce the following corollary:

Corollary 4.4. *The cardinal of $H_{a,d}(\mathbb{F}_q[e])$ is equal to the cardinal of $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$.*

Example 4.5. *In $\mathbb{F}_5[e]$, let $a = 2+2e$, $d = 1+e$. We have:*

$$\begin{aligned} H_{a,d}(\mathbb{F}_5[e]) = \{ & [0:-1:1],[1:0:2+4e],[1:2:4e],[1:e:2+3e],[1:2e:2+2e], \\ & [1:3e:2+e],[1:4e:2],[1:4e:2+2e],[1:2+2e:2e],[1:2+2e:4e], \\ & [e:4:1+e],[e:4:1+3e],[e:4+e:1],[e:4+2e:1+4e], \\ & [e:4+4e:1+2e],[1+4e:4e:2+4e],[1+4e:2+2e:e],[1:2+e:3e], \\ & [1:2+3e:e],[1:2+4e:0],[e:4+3e:1+3e]\} \\ H_{2,1}(\mathbb{F}_5) = \{ & [0:-1:1],[1:0:2],[1:2:0]\} \\ H_{4,2}(\mathbb{F}_5) = \{ & [0:-1:1],[1:0:1],[1:1:0],[1:2:4],[1:3:3],[1:4:2],[1:4:4]\} \end{aligned}$$

So, $card(H_{a,d}(\mathbb{F}_5[e]) = 21$, $card(H_{2,1}(\mathbb{F}_5)) = 3$ and $card(H_{4,3}(\mathbb{F}_5)) = 7$. Note that "card" is the cardinal of a set.

5. Cryptography applications

Several authors have introduced cryptographic applications on projective curves such as elliptic curves, see [3,4,5], in our work, we propose the following cryptographic applications:

- If $card(H_{a,d}(\mathbb{F}_q[e])) := n$ is an odd number, then $n = s \times t$ is the factorization of n, where $s := card(H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q))$ and $t := card(H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q))$, hence the cardinal of $H_{a,d}(\mathbb{F}_q[e])$ is not a prime number.
- The discrete logarithm problem in $H_{a,d}(\mathbb{F}_q[e])$ is equivalent to the discrete logarithm problem in $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$.

6. Conclusion

In this work, we have proved the bijection between $H_{a,d}(\mathtt{F}_q[e])$ and $H_{\pi_0(a),\pi_0(d)}(\mathtt{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathtt{F}_q)$, classified the elements of $H_{a,d}(\mathtt{F}_q[e])$ and it has been proven that its cardinal is never a prime number.

Acknowledgments

The author gratefully acknowledges that his research is supported by Sidi Mohamed Ben Abdellah University, Morocco. We thank the referee by your suggestions.

References

1. Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange, *Twisted Hessian Curves*, In LATINCRYPT 2015, pp 269–294, (2015).http://cr.yp.to/papers.html#hessian
2. A. Boulbot, A. Chillali and A. Mouhib, *Elliptic Curves Over the Ring R*, Bol. Soc. Paran,v. 38 3, pp 193-201, (2015).
3. M. H. Hassib, A. Chillali, M. A. Elomary, *Elliptic curves over a chain ring of characteristic 3*, Journal of Taibah University for Science, 40(9), pages 1687-1700 (2015).
4. M. Joye and J. Quisquater, V.L. *Hessian elliptic curves and sidechannel attacks. Cryptographic Hardware and Embedded Systems - CHES 2001'*, Lecture Notes in Computer Science Vol,2162, Springer, pp. 402-410.(2010).
5. A. Tadmori, A. Chillali, M. Ziane, *Elliptic Curve over Ring* $A_4 = \mathtt{F}_2^d[\varepsilon]$, $\varepsilon^4 = 0$, Applied Mathematical Sciences, Volume 9, Issue 33, Pages 1721-1733(2015).

E. M. Ben Taleb,
Sidi Mohamed Ben Abdellah University,
FSDM, Fez
FP, LSI, Taza
Morocco.
E-mail address: mohaelhomam@gmail.com

and

A. Chillali,
Department of Mathematics,
Physics and Computer Science,
LSI, Polydisciplinary Faculty,
Sidi Mohamed Ben Abdellah University
TAZA; Morocco.
E-mail address: abdelhakim.chillali@usmba.ac.ma

and

L. El Fadil,
Department of Mathematics,
Faculty of Sciences Dhar-El Mahraz Sidi Mohamed Ben Abdellah University,
B.P. 1796-Atlas, Fes, Morocco.
E-mail address: lhouelfadil2@gmail.com