Gulf Journal of Mathematics
Vol 4, Issue 4 (2016) 123-129

ELLIPTIC CURVES OVER THE RING $\mathbb{F}_q[e], e^3 = e^2$

A. BOULBOT[1*], A. CHILLALI[1] AND A. MOUHIB[1]

Abstract. Let $\mathbb{F}_q$ be a finite field of q elements, where q is a power of a prime number p greater than or equal to 5. In this paper, we study the elliptic curve denoted $E_{a,b}(\mathbb{F}_q[e])$ over the ring $\mathbb{F}_q[e]$ where $e^3 = e^2$ and $(a, b) \in (\mathbb{F}_q[e])^2$. In a first time, we we study the arithmetic of the ring $\mathbb{F}_q[e], e^3 = e^2$. In addition, using the Weierstrass equation, we define the elliptic curve $E_{a,b}(\mathbb{F}_q[e])$. The study of this elliptic curve helped us to define two elliptic curve over the finite field $\mathbb{F}_q$. We finish this paper by given a classification of the elements in $E_{a,b}(\mathbb{F}_q[e])$.

1. Introduction

Let $\mathbb{F}_q$ a finite field of order $q = p^d$ where d is a positive integer and $p \geq 5$ is a prime number. In this paper, our objective is to study the elliptic curve defined over the ring $\mathbb{F}_q[X]/(X^3 - X^2)$. In section 2, we define the quotient ring $\mathbb{F}_q[e] := \mathbb{F}_q[X]/(X^3 - X^2)$ where $e^3 = e^2$; we study it's arithmetic and we established some useful results which are necessary for the rest of this paper. In section 3, we define the elliptic curve over $\mathbb{F}_q[e]$; the study of it's discriminant and it's Weierstrass equation, allows us to define two elliptic curves over the finite field $\mathbb{F}_q$ denoted $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ which are necessary to classify the elements of $E_{a,b}(\mathbb{F}_q[e])$. π_0 and π_1 are respectively the canonical projection and the sum projection of coordinates of $X \in \mathbb{F}_q[e]$ defined by:

$$\begin{array}{ccc} \pi_0 : \mathbb{F}_q[e] & \longrightarrow & \mathbb{F}_q \\ x_0 + x_1 e + x_2 e^2 & \longmapsto & x_0 \end{array} \quad \textit{and} \quad \begin{array}{ccc} \pi_1 : \mathbb{F}_q[e] & \longrightarrow & \mathbb{F}_q \\ x_0 + x_1 e + x_2 e^2 & \longmapsto & x_0 + x_1 + x_2 \end{array}.$$

2. The ring $\mathbb{F}_q[e], e^3 = e^2$

In this section, we follow the approach in [2] and [6]; $\mathbb{F}_q$ is a finite field of order $q = p^d$ where d is a positive integer and p is a prime number. The ring $\mathbb{F}_q[e], e^3 = e^2$ 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 $X^3 - X^2$. An element $X \in \mathbb{F}_q[e]$ is represented by $X = x_0 + x_1 e + x_2 e^2$ where $(x_0, x_1, x_2) \in \mathbb{F}_q^3$.

Date: Accepted: Oct 24, 2016.
* Corresponding author.
2010 *Mathematics Subject Classification.* 20K30, 20K40, 20K27.
Key words and phrases. Finite field, Finite ring, Local ring, Elliptic curves, Cryptography.

2.1. **Arithmetic operations.** The arithmetic operations in $\mathbb{F}_q[e]$ can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:

$$X + Y = (x_0 + y_0) + (x_1 + y_1)e + (x_2 + y_2)e^2$$

and

$$X.Y = (x_0y_0) + (x_0y_1 + x_1y_0)\, e + (x_2y_0 + (x_1 + x_2)y_1 + (x_0 + x_1 + x_2)y_2)\, e^2,$$

where $X = x_0 + x_1e + x_2e^2$ and $Y = y_0 + y_1e + y_2e^2$.
One can readily verify the following Lemmas:

Lemma 2.1. *$(\mathbb{F}_q[e], +, .)$ is a finite unitary commutative ring isomorphic to the quotient ring $\mathbb{F}_q[X]/(X^3 - X^2)$.*

Lemma 2.2. *$\mathbb{F}_q[e]$ is a vector space over $\mathbb{F}_q$ of dimension 3 and $\{1, e, e^2\}$ is it's basis.*

Proposition 2.3. *The product law in $\mathbb{F}_q[e]$ can be written as:*

$$X.Y = x_0y_0 + \delta_{XY}e + ((x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0y_0 - \delta_{XY})\, e^2,$$

where $\delta_{XY} = (x_0 + x_1)(y_0 + y_1) - x_0y_0 - x_1y_1 = x_0y_1 + x_1y_0$.

Proof. We have:

$$(x_0 + x_1 + x_2)\,(y_0 + y_1 + y_2))-x_0y_0-\delta_{XY} = x_2y_0+(x_1 + x_2)\,y_1+(x_0 + x_1 + x_2)\,y_2.$$

□

Corollary 2.4. *Let $X = x_0 + x_1e + x_2e^2 \in \mathbb{F}_q[e]$. We have:*

$$X^2 = x_0^2 + \delta_{X^2}e + \left((x_0 + x_1 + x_2)^2 - (x_0 + x_1)^2 + x_1^2\right) e^2$$

and

$$X^3 = x_0^3 + \delta_{X^3}e + \left((x_0 + x_1 + x_2)^3 - (x_0 + x_1)^3 + x_1^3 + 3x_0^2x_1\right) e^2,$$

where: $\delta_{X^2} = (x_0 + x_1)^2 - x_0^2 - x_1^2$ and $\delta_{X^3} = (x_0 + x_1)^3 - x_0^3 - x_1^3 - 3x_0x_1^2$.

The next proposition characterize the set $(\mathbb{F}_q[e])^\times$ of invertible elements in $\mathbb{F}_q[e]$.

Proposition 2.5. *Let $X = x_0 + x_1e + x_2e^2 \in \mathbb{F}_q[e]$. X is invertible if and only if x_0 and $x_0 + x_1 + x_2$ are invertible in $\mathbb{F}_q$. The inverse of X is given by:*

$$X^{-1} = x_0^{-1} - x_1x_0^{-2}e + \left((x_0 + x_1 + x_2)^{-1} + x_1x_0^{-2} - x_0^{-1}\right) e^2.$$

Proof. Let $X = x_0+x_1e+x_2e^2$ and $Y = y_0+y_1e+y_2e^2$ be two elements of $\mathbb{F}_q[e]$. We have $X.Y = x_0y_0 + \delta_{XY}e + ((x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0y_0 - \delta_{XY})\, e^2$ where

$\delta_{XY} = x_0y_1 + x_1y_0$. Then:

$$X.Y = 1 \text{ if and only if } \begin{cases} x_0y_0 = 1 \\ \delta_{XY} = 0 \\ (x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0y_0 - \delta_{XY} = 0 \end{cases}$$

$$\text{if and only if } \begin{cases} x_0y_0 = 1 \\ x_0y_1 + x_1y_0 = 0 \\ (x_0 + x_1 + x_2)(y_0 + y_1 + y_2) = 1 \end{cases}$$

$$\text{if and only if } \begin{cases} y_0 = x_0^{-1} \\ y_1 = -x_1x_0^{-2} \\ y_2 = (x_0 + x_1 + x_2)^{-1} + x_1x_0^{-2} - x_0^{-1} \end{cases},$$

so $X \in (\mathbb{F}_q[e])^\times$ if and only if $x_0 \neq 0$ and $x_0 + x_1 + x_2 \neq 0$. In this case we have:

$$X^{-1} = x_0^{-1} - x_1x_0^{-2}e + \left((x_0 + x_1 + x_2)^{-1} + x_1x_0^{-2} - x_0^{-1}\right)e^2.$$

□

Corollary 2.6. *Let $X \in \mathbb{F}_q[e]$, then X is not invertible if and only if $X = xe+ye^2$ or $X = x + ye - (x + y)\,e^2$ where $(x, y) \in \mathbb{F}_q^2$.*

Now, we consider the set $I \cup J$ of non invertible elements in $\mathbb{F}_q[e]$ where I and J are two ideals of $\mathbb{F}_q[e]$ defined by:

$$I = \left\{xe + ye^2 \mid (x, y) \in \mathbb{F}_q^2\right\} \text{ and } J = \left\{x + ye - (x + y)\,e^2 \mid (x, y) \in \mathbb{F}_q^2\right\}.$$

We have $I \cap J = \{xe - xe^2 \mid x \in \mathbb{F}_q\}$, so $I \cup J$ is not an ideal, then we have the following Lemma:

Lemma 2.7. *$\mathbb{F}_q[e]$ is a non local ring.*

We complete this subsection by the Lemma:

Lemma 2.8. *π_0 and π_1 are two surjective morphisms of rings.*

Proof. From the definition of the sum and product law in $\mathbb{F}_q[e]$, we have:

- ⋆ $\pi_0(X+Y) = x_0+y_0 = \pi_0(X)+\pi_0(Y)$ and $\pi_0(X.Y) = x_0.y_0 = \pi_0(X).\pi_0(Y)$, so π_0 is a morphism of rings.
- ⋆ $\pi_1(X+Y) = x_0+y_0+x_1+y_1+x_2+y_2 = (x_0+x_1+x_2)+(y_0+y_1+y_2) = \pi_1(X)+\pi_1(Y)$ and $\pi_1(X.Y) = (x_0+x_1+x_2).(y_0+y_1+y_2) = \pi_1(X).\pi_1(Y)$, so π_1 is a morphism of rings.

Finally, for all $x \in \mathbb{F}_q \subset \mathbb{F}_q[e]$, we have $\pi_0(x) = \pi_1(x) = x$, so π_0 and π_1 are two surjective morphisms. □

2.2. **Costs of arithmetic operations.** Let s, m and i denote the costs of addition, multiplication and inversion in $\mathbb{F}_q$ respectively and let S, M and I denote the costs of addition, multiplication and inversion in $\mathbb{F}_q[e]$ respectively. We have $S = 3s$, $M = 7s + 4m$ and $I = 4s + m + 3i$ where M is calculated by the Proposition 2.3.

3. Elliptic curves over the ring $\mathbb{F}_q[e]$, $e^3 = e^2$

In this section the prime number p is greater than or equal to 5 and X, Y, Z, a and b are elements of the ring $\mathbb{F}_q[e]$ fixed by $X = x_0 + x_1e + x_2e^2$, $Y = y_0 + y_1e + y_2e^2$, $Z = z_0 + z_1e + z_2e^2$, $a = a_0 + a_1e + a_2e^2$ and $b = b_0 + b_1e + b_2e^2$. We denoted $\Delta := 4a^3 + 27b^2$, $\Delta_0 := \pi_0(\Delta)$ and $\Delta_1 := \pi_1(\Delta)$.

Definition 3.1. We define an elliptic curve over the ring $\mathbb{F}_q[e]$, as a curve in the projective space $\mathbb{P}^2(\mathbb{F}_q[e])$, which is given by the homogeneous equation of degree 3, $Y^2Z = X^3 + aXZ^2 + bZ^3$ where a and b such that the discriminant Δ is invertible in $\mathbb{F}_q[e]$. In this case we denote the elliptic curve over $\mathbb{F}_q[e]$ by $E_{a,b}(\mathbb{F}_q[e])$ and we write:

$$E_{a,b}(\mathbb{F}_q[e]) = \{[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_q[e]) \mid Y^2Z = X^3 + aXZ^2 + bZ^3\}.$$

Proposition 3.2. *The discriminant Δ is invertible in $\mathbb{F}_q[e]$ if and only if Δ_0 and Δ_1 are invertible in $\mathbb{F}_q$.*

Proof. We show easily that $\Delta = \Delta_0 + \delta e + (\Delta_1 - \Delta_0 - \delta)\, e^2$ where $\delta = 4\delta_{a^3} + 27\delta_{b^2}$, then from the Proposition 2.5 we deduce the result. □

Corollary 3.3. *If Δ is invertible in $\mathbb{F}_q[e]$, then we can talk about the elliptic curves $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ defined over the finite field $\mathbb{F}_q$ by:*

$$E_{\pi_0(a),\pi_0(b)}\left(\mathbb{F}_q\right) = \left\{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_q) \mid y^2z = x^3 + a_0xz^2 + b_0z^3\right\} \text{ and}$$

$$E_{\pi_1(a),\pi_1(b)}\left(\mathbb{F}_q\right) = \left\{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_q) \mid y^2z = x^3 + (a_0 + a_1 + a_2)xz^2 + (b_0 + b_1 + b_2)z^3\right\}.$$

Proposition 3.4. *$[X : Y : Z]$ is a point of $\mathbb{P}^2\left(\mathbb{F}_q[e]\right)$ if and only if $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)]$ is a point of $\mathbb{P}^2\left(\mathbb{F}_q\right)$, where $i \in \{0, 1\}$.*

Proof. Suppose that $[X : Y : Z] \in \mathbb{P}^2\left(\mathbb{F}_q[e]\right)$, then there exist $(U, V, W) \in \left(\mathbb{F}_q[e]\right)^3$ 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 $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in \mathbb{P}^2\left(\mathbb{F}_q\right)$.

Reciprocally, let $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in \mathbb{P}^2\left(\mathbb{F}_q\right)$ where $i \in \{0, 1\}$. Suppose that $x_0 \neq 0$, then we distinguish between two case of $x_0 + x_1 + x_2$:

- **(a):** $x_0 + x_1 + x_2 \neq 0$: then X is invertible in $\mathbb{F}_q[e]$, so $[X : Y : Z] \in \mathbb{P}^2\left(\mathbb{F}_q[e]\right)$.
- **(b):** $x_0 + x_1 + x_2 = 0$: then $y_0 + y_1 + y_2 \neq 0$ or $z_0 + z_1 + z_2 \neq 0$.
  - (i) If $y_0 + y_1 + y_2 \neq 0$ then $X + e^2Y \in \left(\mathbb{F}_q[e]\right)^\times$, so there exist $U \in \mathbb{F}_q[e]$ such that $UX + Ue^2Y = 1$, hence $[X : Y : Z] \in \mathbb{P}^2\left(\mathbb{F}_q[e]\right)$.
  - (ii) If $z_0 + z_1 + z_2 \neq 0$ then $X + e^2Z \in \left(\mathbb{F}_q[e]\right)^\times$, so $[X : Y : Z] \in \mathbb{P}^2\left(\mathbb{F}_q[e]\right)$.

In the case where $y_0 \neq 0$ or $z_0 \neq 0$, we follow the same proof. □

Proposition 3.5. *If the point $[X : Y : Z]$ is a solution of the Weierstrass equation in $E_{a,b}\left(\mathbb{F}_q[e]\right)$ then $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)]$ where $i \in \{0, 1\}$ is a solution of the same equation in $E_{\pi_i(a),\pi_i(b)}\left(\mathbb{F}_q\right)$.*

Proof. From the Proposition 2.3 and the Corollary 2.4, we have:

$$\begin{aligned}
Y^2 &= y_0^2 + \delta_{Y^2} e + \left((y_0+y_1+y_2)^2 - y_0^2 - \delta_{Y^2}\right) e^2 \\
Z^2 &= z_0^2 + \delta_{Z^2} e + \left((z_0+z_1+z_2)^2 - z_0^2 - \delta_{Z^2}\right) e^2 \\
aX &= a_0x_0 + \delta_{aX} e + \left((a_0+a_1+a_2)(x_0+x_1+x_2) - a_0x_0 - \delta_{aX}\right) e^2 \\
Z^3 &= z_0^3 + \delta_{Z^3} e + \left((z_0+z_1+z_2)^3 - z_0^3 - \delta_{Z^3}\right) e^2
\end{aligned}$$

then

$$\begin{aligned}
Y^2Z &= y_0^2z_0 + \delta_{Y^2Z} e + \left((y_0+y_1+y_2)^2 (z_0+z_1+z_2) - y_0^2z_0 - \delta_{Y^2Z}\right) e^2 \\
X^3 &= x_0^3 + \delta_{X^3} e + \left((x_0+x_1+x_2)^3 - x_0^3 - \delta_{X^3}\right) e^2 \\
aXZ^2 &= a_0x_0z_0^2 + \delta_{aXZ^2} e \\
&\quad + \left((a_0+a_1+a_2)(x_0+x_1+x_2)(z_0+z_1+z_2)^2 - a_0x_0z_0^2 - \delta_{aXZ^2}\right) e^2 \\
bZ^3 &= b_0z_0^3 + \delta_{bZ^3} e + \left((b_0+b_1+b_2)(z_0+z_1+z_2)^3 - b_0z_0^3 - \delta_{bZ^3}\right) e^2
\end{aligned}$$

hence $Y^2Z = X^3 + aXZ^2 + bZ^3$ if and only if

$$\begin{aligned}
y_0^2z_0 &= x_0^3 + a_0x_0z_0^2 + b_0z_0^3 \\
\delta_{Y^2Z} &= \delta_{X^3} + \delta_{aXZ^2} + \delta_{bZ^3} \\
(y_0+y_1+y_2)^2 (z_0+z_1+z_2) &= (x_0+x_1+x_2)^3 + (a_0+a_1+a_2)(x_0+x_1+x_2)(z_0+z_1+z_2)^2 \\
&\quad + (b_0+b_1+b_2)(z_0+z_1+z_2)^3
\end{aligned}$$

which proves that for $i \in \{0,1\}$, $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)]$ is a solution of the Weierstrass equation in $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$. □

From the Propositions 3.2, 3.4 and 3.5, we deduce the theorem:

Theorem 3.6. *Lets X, Y and Z in $\mathbb{F}_q[e]$. If $[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[e])$ then $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ where $i \in \{0,1\}$.*

Corollary 3.7. *For $i \in \{0,1\}$, the mapping $\widetilde{\pi}_i$ given by:*

$$\begin{array}{ccc} E_{a,b}(\mathbb{F}_q[e]) & \xrightarrow{\widetilde{\pi}_i} & E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q) \\ [X:Y:Z] & \longmapsto & [\pi_i(X):\pi_i(Y):\pi_i(Z)] \end{array},$$

is well defined.

Proof. Let $[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[e])$. From the previous theorem, we have $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ where $i \in \{0,1\}$.
If $[X : Y : Z] = [X' : Y' : Z']$ then there exist $U \in (\mathbb{F}_q[e])^\times$ such that: $X' = UX$, $Y' = UY$ and $Z' = UZ$, then:

$$\begin{aligned}
\widetilde{\pi}_i\left([X' : Y' : Z']\right) &= [\pi_i(X') : \pi_i(Y') : \pi_i(Z')] \\
&= \underbrace{[\pi_i(U)\pi_i(X) : \pi_i(U)\pi_i(Y) : \pi_i(U)\pi_i(Z)]}_{\pi_i(U)\in\mathbb{F}_q^*} \\
&= [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] = \widetilde{\pi}_i\left([X : Y : Z]\right).
\end{aligned}$$

□

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

In this subsection we will classify the elements of the elliptic curve into three types, depending on whether the third projective coordinate Z is invertible or not. The result is in the following proposition.

Proposition 4.1. *We classify the elements of $E_{a,b}(\mathbb{F}_q[e])$ into five sets given by:*

$$\begin{aligned}E_{a,b}(\mathbb{F}_q[e]) = &\left\{[X:Y:1] \mid Y^2 = X^3 + aX + b\right\}\\ &\cup \left\{[xe + x'e^2 : 1 : ze + z'e^2] \mid [x + x' : 1 : z + z'] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)\right\}\\ &\cup \left\{[xe + x'e^2 : 1 + ye - (1+y)\,e^2 : ze + z'e^2] \mid [x + x' : 0 : z + z'] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)\right\}\\ &\cup \left\{[x + x'e - (x + x')\,e^2 : 1 : z + z'e - (z + z')\,e^2] \mid [x : 1 : z] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)\right\}\\ &\cup \left\{[x + x'e - (x + x')\,e^2 : ye + y'e^2 : 1 + ze - (1 + z)\,e^2] \mid y + y' \neq 0 \text{ and } [x : 0 : 1] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)\right\}.\end{aligned}$$

Proof. Let $P = [X : Y : Z] \in E_{a,b}(\mathbb{F}_q[e])$. We have three cases of the third projective coordinate Z:

(1) If Z is invertible, then: $[X : Y : Z] \sim [X : Y : 1]$.

(2) If $Z = z_1e + z_2e^2$ where $(z_1, z_2) \in \mathbb{F}_q^2$, then $\widetilde{\pi_0}\,([X : Y : Z]) = [x_0 : y_0 : 0]$, so $x_0 = 0$ and $y_0 \neq 0$, hence $[X : Y : Z] = [x_1e + x_2e^2 : 1 + y_1e + y_2e^2 : z_1e + z_2e^2]$ and there are two sub-cases of $y_1 + y_2 \in \mathbb{F}_q$:
   (a) $y_1 + y_2 \neq -1$, then $1 + y_1e + y_2e^2$ is invertible in $\mathbb{F}_q[e]$, so we have: $[X : Y : Z] \sim [x_1e + x_2e^2 : 1 : z_1e + z_2e^2]$, where $[x_1 + x_2 : 1 : z_1 + z_2] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.
   (b) $y_1 + y_2 = -1$, then $1 + y_1e - (1 + y_1)\,e^2$ is not invertible in $\mathbb{F}_q[e]$, so we have: $[X : Y : Z] = [x_1e + x_2e^2 : 1 + y_1e - (1 + y_1)\,e^2 : z_1e + z_2e^2]$ where $[x_1 + x_2 : 0 : z_1 + z_2] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

(3) If $Z = z_0 + z_1e - (z_0 + z_1)\,e^2$ where $(z_0, z_1) \in \mathbb{F}_q^2$, then $\widetilde{\pi_1}\,([X : Y : Z]) = [x_0 + x_1 + x_2 : y_0 + y_1 + y_2 : 0]$, so $x_0 + x_1 + x_2 = 0$ and $y_0 + y_1 + y_2 \neq 0$, hence $[X : Y : Z] = [x_0 + x_1e - (x_0 + x_1)\,e^2 : y_0 + y_1e + y_2e^2 : z_0 + z_1e - (z_0 + z_1)\,e^2]$, so we have two sub-cases of $y_0 \in \mathbb{F}_q$:
   (a) $y_0 \neq 0$, then $y_0 + y_1e + y_2e^2$ is invertible in $\mathbb{F}_q[e]$, then: $[X : Y : Z] \sim [x_0 + x_1e - (x_0 + x_1)\,e^2 : 1 : z_0 + z_1e - (z_0 + z_1)\,e^2]$ where $[x_0 : 1 : z_0] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.
   (b) $y_0 = 0$, then $Y = y_1e + y_2e^2$ is not invertible in $\mathbb{F}_q[e]$, so we have: $[X : Y : Z] = [x_0 + x_1e - (x_0 + x_1)\,e^2 : y_1e + y_2e^2 : z_0 + z_1e - (z_0 + z_1)\,e^2]$, where $[x_0 : 0 : z_0] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$, then necessary $z_0 \neq 0$ and $[X : Y : Z] = [x_0 + x_1e - (x_0 + x_1)\,e^2 : y_1e + y_2e^2 : 1 + \alpha e - (1 + \alpha)\,e^2]$, where $y_1 + y_2 \neq 0$ and $[x_0 : 0 : 1] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.

Which proves the proposition. □

From this proposition we deduce that:

Corollary 4.2. *$\widetilde{\pi_1}$ is a surjective mapping.*

Proof. Let $[x : y : z] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$, then:

⋆ If $y \neq 0$ then $[x : y : z] \sim [x : 1 : z]$ hence $[xe^2 : 1 : ze^2]$ is an antecedent of $[x : 1 : z]$.

⋆ If $y = 0$ then $z \neq 0$ and $[x : y : z] \sim [x : 0 : 1]$ hence $[xe^2 : 1 - e^2 : e^2]$ is an antecedent of $[x : 0 : 1]$.

hence $[xe^2 : 1 + (y-1)\,e^2 : ze^2]$ is an antecedent of $[x : y : z]$. □

5. Conclusion

In this work, we have given a classification of elements in the elliptic curves $E_{a,b}(\mathbb{F}_q[e])$ using the elliptic curves $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ defined over the finite field $\mathbb{F}_q$. For the group law over $E_{a,b}(\mathbb{F}_q[e])$ you can see the explicit formulas in the article of [1], [pages : 236—238].

6. ACKNOWLEDGMENT

The authors would like to thank Sidi Mohamed Ben Abdellah Univercity (USMBA), LSI and FP of Taza in MOROCCO for its valued support.

References

1. W. Bosma and H.W. Lenstra; *Complete System of Two Addition Laws for Elliptic Curves*, Journal of Number Theory, (1995).
2. A. Chillali; *Elliptic Curves of the Ring* $\mathbb{F}_q[\varepsilon]$, $\varepsilon^n = 0$, International Mathematical Forum (2011).
3. N. Koblitz; *Elliptic curve cryptosystems*, Math. Compute. 48 (1987) 203209.
4. H.W. Lenstra *Elliptic Curves and Number-Theoretic Algorithms*, Processing of the International Congress of Mathematicians, Berkely, California,USA, (1986).
5. J.H. Silverman *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994.
6. M. Virat; *Courbe elliptique sur un anneau et applications cryptographiques*, PhD thesis, Universite Nice-Sophia Antipolis, Nice, France (2009).

[1]Department of Mathematics, Physics and Computing, LSI, FPT, Taza, Box 1223, University S.M. Ben Abdellah Fez, Morocco.
E-mail address: aziz.boulbot@usmba.ac.ma
E-mail address: abdelhakim.chillali@usmba.ac.ma
E-mail address: ali.mouhib@usmba.ac.ma