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

(3s.) **v. 2022 (40)** : 1–19.
ISSN-0037-8712 IN PRESS
doi:10.5269/bspm.43654

# Elliptic Curve Over a Finite Ring Generated by 1 and an Idempotent Element $e$ with Coefficients in the Finite Field $\mathbb{F}_{3^d}$ *

A. Boulbot, A. Chillali and A. Mouhib

ABSTRACT: An elliptic curve over a ring $\mathcal{R}$ is a curve in the projective plane $\mathbb{P}^2(\mathcal{R})$ given by a specific equation named the Weierstrass equation of the form $f(X,Y,Z) = 0$, where:

$$f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,$$

such that the coefficients $a_1, a_2, a_3, a_4$ and $a_6$ are in the ring $\mathcal{R}$ and with an invertible discriminant in $\mathcal{R}$. In this paper, we consider an elliptic curve over a finite ring of characteristic 3 given by the Weierstrass equation: $Y^2Z = X^3 + aX^2Z + bZ^3$, such that the coefficients $a$ and $b$ are in the quotient ring $\mathcal{R} := \mathbb{F}_{3^d}[X]/(X^2 - X)$, where $d$ is a positive integer and $\mathbb{F}_{3^d}[X]$ is the polynomial ring with coefficients in the finite field $\mathbb{F}_{3^d}$ and such that $-a^3b$ is invertible in $\mathcal{R}$.

Key Words: Finite field, Finite ring, Local ring, Homomorphism, Elliptic curve, Cryptography.

## Contents



## 1. Introduction

Let $\mathbb{F}_{3^d}$ be a finite field of characteristic 3 and order $3^d$ where $d$ is a positive integer and let $\dfrac{\mathbb{F}_{3^d}[X]}{\langle X^2 - X\rangle}$ the quotient ring of the polynomial ring $\mathbb{F}_{3^d}[X]$ by the ideal generated by $\left(X^2 - X\right)$. This ring can be identified to the finite ring $\mathbb{F}_{3^d}[e]$ where $e^2 = e$. Over this ring, we consider the elliptic curve denoted by $E_{a,b}(\mathbb{F}_{3^d}[e])$ and given by all points $[X : Y : Z] \in \mathbb{P}^2\left(\mathbb{F}_{3^d}[e]\right)$ which verify the Weierstrass equation $Y^2Z = X^3 + aX^2Z + bZ^3$, where $(a,b) \in \left(\mathbb{F}_{3^d}[e]\right)^2$ such that $-a^3b$ is invertible in the ring $\mathbb{F}_{3^d}[e]$.

We started this work by studying the arithmetic of the ring $\mathbb{F}_{3^d}[e]$, $e^2 = e$ where we show a useful formulae to compute the product law. By this efficient formulae we characterize the set of invertible elements in the ring $\mathbb{F}_{3^d}[e]$, $e^2 = e$ and we show that the set of non invertible elements is the union of the two distinct ideals $\langle e\rangle$ and $\langle 1 - e\rangle$, which proves that $\mathbb{F}_{3^d}[e]$ is not a local ring.

In the third section, the study of the discriminant and the Weierstrass equation of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$, allows us to define two elliptic curves over the finite field $\mathbb{F}_{3^d}$ denoted by $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d})$ and $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d})$, where $\pi_0$ and $\pi_1$ are two morphisms of rings defined by:

$$\begin{array}{ccc} \pi_0 : \mathbb{F}_{3^d}[e] & \longrightarrow & \mathbb{F}_{3^d} \\ x_0 + x_1e & \longmapsto & x_0 \end{array} \quad \text{and} \quad \begin{array}{ccc} \pi_1 : \mathbb{F}_{3^d}[e] & \longrightarrow & \mathbb{F}_{3^d} \\ x_0 + x_1e & \longmapsto & x_0 + x_1 \end{array}.$$

* USMBA, LSI, FP, Taza, Morocco.
2010 *Mathematics Subject Classification:* 11T71, 14G50, 94A60.
Submitted July 11, 2018. Published November 09, 2018

The morphisms $\pi_0$ and $\pi_1$ gives a bijection between the elliptic curves $E_{a,b}(\mathbb{F}_{3^d}[e])$ and $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d}) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d})$, which help us to define the group law of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$.

In the forth section, we classify the points of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$ on the fact that the third projective coordinate of an element in $E_{a,b}(\mathbb{F}_{3^d}[e])$ is invertible or not. This classification, help us in the last section to give the explicit formulae of the group law of $E_{a,b}(\mathbb{F}_{3^d}[e])$.

In the last section, we use the isomorphism between the elliptic curves $E_{a,b}(\mathbb{F}_{3^d}[e])$ and $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d}) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d})$, the classification points in the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$ and the explicit formulae of addition law for an elliptic curve given by W. Bosma and H. W. Lenstra in [1] to give the explicit formulae of addition law for the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$.

## 2. Arithmetic over the ring $\mathbb{F}_{3^d}[e], e^2 = e$

The ring $\mathbb{F}_{3^d}[e], e^2 = e$ where $d$ is a positive integer can be constructed as an extension of the finite field $\mathbb{F}_{3^d}$ by using the quotient ring of the polynomial ring $\mathbb{F}_{3^d}[X]$ by the polynomial $X^2 - X$. The arithmetic operations in $\mathbb{F}_{3^d}[e]$ can be decomposed into operations in $\mathbb{F}_{3^d}$ and they are computed as follows:

$$X + Y = (x_0 + y_0) + (x_1 + y_1)e \text{ and } X.Y = (x_0y_0) + (x_0y_1 + x_1y_0 + x_1y_1)e,$$

where $X$ and $Y$ are two elements in $\mathbb{F}_{3^d}[e]$ represented by $X = x_0 + x_1e$ and $Y = y_0 + y_1e$ with coefficients $x_0, x_1, y_0$ and $y_1$ are in the field $\mathbb{F}_{3^d}$. One can readily verify the following Lemmas:

**Lemma 2.1.** *$(\mathbb{F}_{3^d}[e], +, .)$ is a finite unitary commutative ring.*

**Lemma 2.2.** *$\mathbb{F}_{3^d}[e]$ is a vector space over $\mathbb{F}_{3^d}$ of dimension 2 and $\{1, e\}$ is its basis.*

The next Lemma give an efficient formulae of the product law, which is very used in the next of this work.

**Lemma 2.3.** *Lets $X = x_0 + x_1e$ and $Y = y_0 + y_1e$ two elements in the ring $\mathbb{F}_{3^d}[e]$. The product law $X.Y$ can be written as:*

$$X.Y = (x_0y_0) + ((x_0 + x_1)(y_0 + y_1) - x_0y_0)\, e.$$

By the Lemma 2.3, we deduce immediately that:

**Corollary 2.4.** *The $X^2$ and $X^3$ power of $X = x_0 + x_1e$ are given by:*

$$X^2 = x_0^2 + \left((x_0 + x_1)^2 - x_0^2\right) e \text{ and } X^3 = x_0^3 + x_1^3 e.$$

**Corollary 2.5.** *An element $X = x_0 + x_1e$ is invertible in the ring $\mathbb{F}_{3^d}[e]$ if and only if $x_0 \not\equiv 0 \mod 3$ and $x_0 + x_1 \not\equiv 0 \mod 3$. In this case we have:*

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

*Proof.* Let $x_0 + x_1e \in \mathbb{F}_{3^d}[e]$. If $x_0 + x_1e$ is invertible in $\mathbb{F}_{3^d}[e]$, then there exist $y_0 + y_1e \in \mathbb{F}_{3^d}[e]$ such that:

$$(x_0 + x_1e)\,.\,(y_0 + y_1e) = x_0y_0 + ((x_0 + x_1)\,(y_0 + y_1) - x_0y_0)\, e = 1,$$

hence we have:

$$\begin{aligned}(x_0 + x_1e)\,.\,(y_0 + y_1e) = 1 &\iff x_0y_0 = 1 \text{ and } (x_0 + x_1)\,(y_0 + y_1) = 1\\ &\implies \begin{cases} x_0 \not\equiv 0\,[3] \text{ and } y_0 = x_0^{-1} \\ x_0 + x_1 \not\equiv 0\,[3] \text{ and } (y_0 + y_1) = (x_0 + x_1)^{-1} \end{cases}\\ &\implies \begin{cases} x_0 \not\equiv 0\,[3] \text{ and } y_0 = x_0^{-1} \\ x_0 + x_1 \not\equiv 0\,[3] \text{ and } y_1 = (x_0 + x_1)^{-1} - x_0^{-1} \end{cases}.\end{aligned}$$

Reciprocally, if $x_0 \not\equiv 0 \mod 3$ and $x_0 + x_1 \not\equiv 0 \mod 3$, then from the Lemma 2.3, we have immediately that:

$$(x_0 + x_1e)\,.\,\left(x_0^{-1} + \left((x_0 + x_1)^{-1} - x_0^{-1}\right) e\right) = 1.$$

□

**Corollary 2.6.** *An element $X = x_0 + x_1 e$ is not invertible in the ring $\mathbb{F}_{3^d}[e]$ if and only if $x_0 \equiv 0 \mod 3$ or $x_0 + x_1 \equiv 0 \mod 3$.*

**Lemma 2.7.** *$\mathbb{F}_{3^d}[e]$ is a non local ring.*

*Proof.* Using the Corollary 2.6, we show that the set of non invertible elements in the ring $\mathbb{F}_{3^d}[e]$ is the union of the two distinct ideals $\langle e\rangle$ and $\langle 1-e\rangle$, hence $\langle e\rangle \cup \langle 1-e\rangle$ is not an ideal, which prove the lemma. □

**Remark 2.8.** *To give a relationship between the elliptic curve defined over the finite ring $\mathbb{F}_{3^d}[e]$ and the same one defined over the finite field $\mathbb{F}_{3^d}$, we use the two mappings $\pi_0$ and $\pi_1$ given in the introduction. This mappings verify the following Lemmas:*

**Lemma 2.9.** *For all $X \in \mathbb{F}_{3^d}[e]$, we have:*

$$X = \pi_0(X) + (\pi_1(X) - \pi_0(X))\, e, \quad Xe = \pi_1(X)e \text{ and } X(1-e) = \pi_0(X)(1-e).$$

*Proof.* If $X = x_0 + x_1 e$, then:

- $\pi_0(X) + (\pi_1(X) - \pi_0(X))\, e = x_0 + (x_0 + x_1 - x_0)\, e = x_0 + x_1 e = X.$
- $Xe = (x_0 + x_1 e)\, e = x_0 e + x_1 e = (x_0 + x_1)\, e = \pi_1(X)e.$
- $X(1-e) = (x_0 + x_1 e)\,(1-e) = x_0 - x_0 e = x_0\,(1-e) = \pi_0(X)(1-e).$

□

**Lemma 2.10.** *$\pi_0$ and $\pi_1$ are two surjective morphisms of rings.*

*Proof.* From the Lemmas 2.3 and 2.9, we have:

$$X + Y = \pi_0(X) + \pi_0(Y) + (\pi_1(X) - \pi_0(X) + \pi_1(Y) - \pi_0(Y))\, e$$

and

$$X.Y = \pi_0(X)\,\pi_0(Y)\, e + (\pi_1(X)\,\pi_1(Y) - \pi_0(X)\,\pi_0(Y))\, e,$$

hence:

- $\pi_0(X+Y) = \pi_0(X) + \pi_0(Y)$ and $\pi_0(X.Y) = \pi_0(X).\pi_0(Y)$
- $\pi_1(X+Y) = \pi_1(X) + \pi_1(Y)$ and $\pi_1(X.Y) = \pi_1(X).\pi_1(Y)$
- For all $x \in \mathbb{F}_{3^d}$, we have $x \in \mathbb{F}_{3^d}[e]$ and $\pi_0(x) = \pi_1(x) = x$,

so $\pi_0$ and $\pi_1$ are two surjective morphisms of rings. □

## 3. Elliptic curve over the ring $\mathbb{F}_{3^d}[e]$, $e^2 = e$

In this section $a$ and $b$ are two elements of the ring $\mathbb{F}_{3^d}[e]$ fixed by $a = a_0 + a_1 e$ and $b = b_0 + b_1 e$. We denoted by $\Delta_0$ and $\Delta_1$ the images of the discriminant $\Delta = -a^3 b$ by the $\pi_0$ and $\pi_1$ morphisms respectively. The important result that we will show in this section is the bijection between the elliptic curves $E_{a,b}(\mathbb{F}_{3^d}[e])$ and $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d}) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d})$. Firstly, we have the followings corollaries:

**Corollary 3.1.** *The discriminant $\Delta$ is invertible in the ring $\mathbb{F}_{3^d}[e]$ if and only if $\Delta_0$ and $\Delta_1$ are not zero in the field $\mathbb{F}_{3^d}$.*

*Proof.* From the Lemma 2.9, we have $\Delta = \Delta_0 + (\Delta_1 - \Delta_0)e$ and from the Corollary 2.5 we deduce the result. □

**Corollary 3.2.** *If $\Delta$ is invertible in the ring $\mathbb{F}_{3^d}[e]$, then the set of all points $[x:y:z]$ in $\mathbb{P}^2(\mathbb{F}_{3^d})$ solution of $y^2z = x^3 + \pi_i(a)x^2z + \pi_i(b)z^3$ where $i \in \{0,1\}$ is an elliptic curve over the finite field $\mathbb{F}_{3^d}$, which is denoted by $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_{3^d})$ and we write:*

$$E_{\pi_i(a),\pi_i(b)}\left(\mathbb{F}_{3^d}\right) = \left\{[x:y:z] \in \mathbb{P}^2(\mathbb{F}_{3^d}) \mid y^2z = x^3 + \pi_i(a)x^2z + \pi_i(b)z^3\right\}.$$

**Proposition 3.3.** *Lets $(X,Y,Z) \in (\mathbb{F}_{3^d}[e])^3$, then:*
*$[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[e])$ if and only if $[\pi_i(X):\pi_i(Y):\pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_{3^d})$ for all $i \in \{0,1\}$.*

*Proof.* Suppose that $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[e])$, then there exist $(U,V,W) \in (\mathbb{F}_{3^d}[e])^3$ such that $UX + VY + WZ = 1$. Hence for all $i \in \{0,1\}$, 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 implies that:

$$[\pi_i(X):\pi_i(Y):\pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_{3^d}) \text{ for all } i \in \{0,1\}.$$

Reciprocally, suppose that $[\pi_i(X):\pi_i(Y):\pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_{3^d})$ for all $i \in \{0,1\}$. If $\pi_0(X)$ is not zero in the field $\mathbb{F}_{3^d}$, then we have two cases of $\pi_1(X)$:

**(i)** If $\pi_1(X)$ is not zero in the field $\mathbb{F}_{3^d}$, then $X$ is invertible in the ring $\mathbb{F}_{3^d}[e]$, hence $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[e])$.

**(ii)** If $\pi_1(X) \equiv 0 \mod 3$, then $[\pi_1(X):\pi_1(Y):\pi_1(Z)] \in \mathbb{P}^2(\mathbb{F}_{3^d})$ implies that $\pi_1(Y) \not\equiv 0 \mod 3$ or $\pi_1(Z) \not\equiv 0 \mod 3$.

- **(a)** If $\pi_1(Y) \not\equiv 0 \mod 3$, then $\pi_0(X) + (\pi_1(Y) - \pi_0(X))\,e = X + eY$ is invertible in $\mathbb{F}_{3^d}[e]$, so there exist $U \in \mathbb{F}_{3^d}[e]$ such that $UX + eUY = 1$, hence $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[e])$.
- **(b)** If $\pi_1(Z) \not\equiv 0 \mod 3$, then similarly $X + eZ$ is invertible in $\mathbb{F}_{3^d}[e]$, hence $[X:Y:Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[e])$.

In the other cases, if $\pi_0(Y) \not\equiv 0 \mod 3$ or $\pi_0(Z) \not\equiv 0 \mod 3$, we follow the same proof. □

**Proposition 3.4.** *Lets $(X,Y,Z) \in (\mathbb{F}_{3^d}[e])^3$, then $Y^2Z = X^3 + aX^2Z + bZ^3$ if and only if $\pi_i^2(Y)\pi_i(Z) = \pi_i^3(X) + \pi_i(a)\pi_i^2(X)\pi_i(Z) + \pi_i(b)\pi_i^3(Z)$ for all $i \in \{0,1\}$.*

*Proof.* By the Lemma 2.9, we have that:

$$\begin{aligned} Y^2Z &= \pi_0(Y^2Z) + \left(\pi_1(Y^2Z) - \pi_0(Y^2Z)\right)e, \text{ and} \\ X^3 + aX^2Z + bZ^3 &= \pi_0\left(X^3 + aX^2Z + bZ^3\right) \\ &\quad + \left(\pi_1\left(X^3 + aX^2Z + bZ^3\right) - \pi_0\left(X^3 + aX^2Z + bZ^3\right)\right)e. \end{aligned}$$

As $\{1, e\}$ is a basis of the $\mathbb{F}_{3^d}$ vector space $\mathbb{F}_{3^d}[e]$, then:

$$Y^2Z = X^3 + aX^2Z + bZ^3$$

if and only if

$$\pi_0(Y^2Z) = \pi_0\left(X^3 + aX^2Z + bZ^3\right)$$

and

$$\pi_1(Y^2Z) = \pi_1\left(X^3 + aX^2Z + bZ^3\right).$$

The result is deduced by using that $\pi_0$ and $\pi_1$ are two morphisms of rings. □

From the Corollary 3.1, the Proposition 3.3 and the Proposition 3.4, we deduce the theorem:

**Theorem 3.5.** *Lets* $(X, Y, Z) \in (\mathbb{F}_{3^d}[e])^3$, *then:*
$[X : Y : Z] \in E_{a,b}(\mathbb{F}_{3^d}[e])$ *if and only if* $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_{3^d})$ *for all* $i \in \{0, 1\}$.

**Corollary 3.6.** *Let* $i \in \{0, 1\}$. *The correspondence* $\widetilde{\pi}_i$ *given by:*

$$\begin{array}{ccc} E_{a,b}(\mathbb{F}_{3^d}[e]) & \xrightarrow{\widetilde{\pi}_i} & E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_{3^d}) \\ [X : Y : Z] & \longmapsto & [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \end{array}$$

*is a mapping.*

*Proof.* From the previous theorem, it is clear that $\widetilde{\pi}_i$ is a correspondence.

Lets $[X : Y : Z]$ and $[X' : Y' : Z']$ two points in the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$ such that $[X : Y : Z] = [X' : Y' : Z']$, then there exist an invertible element $U \in \mathbb{F}_{3^d}[e]$ such that $X' = UX$, $Y' = UY$ and $Z' = UZ$, hence:

$$\begin{aligned} \widetilde{\pi}_i\left([X' : Y' : Z']\right) &= [\pi_i(X') : \pi_i(Y') : \pi_i(Z')] \\ &= \underbrace{[\pi_i(U)\pi_i(X) : \pi_i(U)\pi_i(Y) : \pi_i(U)\pi_i(Z)]}_{\pi_i(U) \in \mathbb{F}_{3^d}^*} \\ &= [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] = \widetilde{\pi}_i\left([X : Y : Z]\right), \end{aligned}$$

so $\widetilde{\pi}_i$ is well defined. □

**Corollary 3.7.** $\widetilde{\pi}_0$ *is a surjective mapping.*

*Proof.* For all $[x : y : z] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d})$, we have:

$$[x : y : z] = \widetilde{\pi}_0\left([x - xe : y + (1 - y)\, e : z - ze]\right).$$

□

**Corollary 3.8.** $\widetilde{\pi}_1$ *is a surjective mapping.*

*Proof.* For all $[x : y : z] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d})$, we have:

$$[x : y : z] = \widetilde{\pi}_1\left([xe : 1 + (y - 1)\, e : ze]\right).$$

□

**Theorem 3.9.** *The* $\widetilde{\pi}$ *mapping defined by:*

$$\begin{array}{ccc} E_{a,b}(\mathbb{F}_{3^d}[e]) & \xrightarrow{\widetilde{\pi}} & E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d}) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d}) \\ [X : Y : Z] & \longmapsto & ([\pi_0(X) : \pi_0(Y) : \pi_0(Z)], [\pi_1(X) : \pi_1(Y) : \pi_1(Z)]) \end{array}$$

*is a bijection and its inverse is given by:*

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

*Proof.* We show to prove that $\widetilde{\pi}$ is well defined, surjective and injective.

(*a*) As $\widetilde{\pi}\left([X : Y : Z]\right) = \left(\widetilde{\pi}_0\left([X : Y : Z]\right), \widetilde{\pi}_1\left([X : Y : Z]\right)\right)$ and $\widetilde{\pi}_0$ and $\widetilde{\pi}_1$ are well defined, then $\widetilde{\pi}$ is well defined.

(*b*) Let $([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]) \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d}) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d})$, then $[x_0 + (x_1 - x_0)\, e : y_0 + (y_1 - y_0)\, e : z_0 + (z_1 - z_0)\, e] \in E_{a,b}(\mathbb{F}_{3^d}[e])$ is an antecedent of $([x_0 : y_0 : z_0], [x_1 : y_1 : z_1])$, hence $\widetilde{\pi}$ is a surjective mapping.

(c) Lets $[x_0+x_1e : y_0+y_1e : z_0+z_1e]$ and $[x'_0+x'_1e : y'_0+y'_1e : z'_0+z'_1e]$ be two elements of $E_{a,b}(\mathbb{F}_{3^d}[e])$ such that:

$$\widetilde{\pi}\left([x_0+x_1e : y_0+y_1e : z_0+z_1e]\right) = \widetilde{\pi}\left([x'_0+x'_1e : y'_0+y'_1e : z'_0+z'_1e]\right),$$

then:

$$[x_0 : y_0 : z_0] = [x'_0 : y'_0 : z'_0]$$

and

$$[x_0+x_1 : y_0+y_1 : z_0+z_1] = [x'_0+x'_1 : y'_0+y'_1 : z'_0+z'_1],$$

so there exists a non zero elements $(\alpha,\beta) \in \left(\mathbb{F}_{3^d}\right)^2$ such that:

$(i)$ $x'_0 = \alpha x_0,\ y'_0 = \alpha y_0$ and $z'_0 = \alpha z_0$

$(ii)$ $x'_0+x'_1 = \beta\left(x_0+x_1\right),\ y'_0+y'_1 = \beta\left(y_0+y_1\right)$ and $z'_0+z'_1 = \beta\left(z_0+z_1\right)$

hence: $x'_1 = (\beta-\alpha)\,x_0+\beta x_1,\ y'_1 = (\beta-\alpha)\,y_0+\beta y_1$ and $z'_1 = (\beta-\alpha)\,z_0+\beta z_1$, so we deduce that:

$$\begin{cases} x'_0+x'_1e = \alpha x_0+\left((\beta-\alpha)\,x_0+\beta x_1\right)e = \left(\alpha+(\beta-\alpha)\,e\right)\left(x_0+x_1e\right) \\ y'_0+y'_1e = \alpha y_0+\left((\beta-\alpha)\,y_0+\beta y_1\right)e = \left(\alpha+(\beta-\alpha)\,e\right)\left(y_0+y_1e\right) \\ z'_0+z'_1e = \alpha z_0+\left((\beta-\alpha)\,z_0+\beta z_1\right)e = \left(\alpha+(\beta-\alpha)\,e\right)\left(z_0+z_1e\right) \end{cases}.$$

As $\alpha+(\beta-\alpha)\,e$ is invertible in the ring $\mathbb{F}_{3^d}[e]$, then:

$$[x_0+x_1e : y_0+y_1e : z_0+z_1e] = [x'_0+x'_1e : y'_0+y'_1e : z'_0+z'_1e],$$

which show that $\widetilde{\pi}$ is an injective mapping.

For the proof of the $\widetilde{\pi}^{-1}$ formulae, we can show easily that:

$$\widetilde{\pi}\circ\widetilde{\pi}^{-1} = id_{E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d})\times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d})} \text{ and } \widetilde{\pi}^{-1}\circ\widetilde{\pi} = id_{E_{a,b}(\mathbb{F}_{3^d}[e])}.$$

□

**Corollary 3.10.** *The cardinal of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$ is equal to the cardinal of $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d})\times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d})$.*

**Corollary 3.11.** *Lets $P$ and $Q$ two points in the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$, then:*

$$P = Q \Longleftrightarrow \widetilde{\pi}\left(P\right) = \widetilde{\pi}\left(Q\right) \Longleftrightarrow \widetilde{\pi_0}\left(P\right) = \widetilde{\pi_0}\left(Q\right) \text{ and } \widetilde{\pi_1}\left(P\right) = \widetilde{\pi_1}\left(Q\right).$$

## 4. Classification of elements of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$

We classify the elements of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$ into two types, depending on whether the third projective coordinate $Z$ is invertible or not. The result is in the following theorem.

**Theorem 4.1.** *Every point of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$ has one of the forms:*

1. $[X : Y : 1]$, *where* $X, Y \in \mathbb{F}_{3^d}[e]$.
2. $[xe : 1 : ze]$, *where* $x, z \in \mathbb{F}_{3^d}$.
3. $[xe : 1-e : ze]$, *where* $(x,z) \in \mathbb{F}_{3^d}\times\mathbb{F}_{3^d}^*$.
4. $[x-xe : 1 : z-ze]$, *where* $x, z \in \mathbb{F}_{3^d}$.
5. $[x-xe : e : z-ze]$, *where* $(x,z) \in \mathbb{F}_{3^d}\times\mathbb{F}_{3^d}^*$.

*Proof.* Lets $X = x_0+x_1e, Y = y_0+y_1e$ and $Z = z_0+z_1e$ such that $[X : Y : Z]$ is in the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$. We have three cases of the third projective coordinate $Z$:

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

$(ii)$ if $Z = ze$, then $\widetilde{\pi_0}([X : Y : Z]) = [x_0 : y_0 : 0]$ implies that $x_0 \equiv 0 \mod 3$ and $y_0 \not\equiv 0 \mod 3$, hence $[X : Y : Z] = [xe : 1 + ye : ze]$ and there are two sub-cases of $y \in \mathbb{F}_{3^d}$ :

$(a)$ if $y + 1 \not\equiv 0 \mod 3$, then $1 + ye$ is invertible in $\mathbb{F}_{3^d}[e]$, hence:

$$[X : Y : Z] \sim [xe : 1 : ze] \text{ where } x, z \in \mathbb{F}_{3^d}.$$

$(b)$ if $y + 1 \equiv 0 \mod 3$, then $1 - e$ is not invertible in $\mathbb{F}_{3^d}[e]$, hence:

$$[X : Y : Z] = [xe : 1 - e : ze] \text{ where } (x, z) \in \mathbb{F}_{3^d} \times \mathbb{F}_{3^d}.$$

Or $\widetilde{\pi_1}([xe : 1 - e : ze]) = [x : 0 : z] \in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d})$, then necessary $z \not\equiv 0 \mod 3$.

$(iii)$ if $Z = z - ze$, then $\widetilde{\pi_1}([X : Y : Z]) = [x_0 + x_1 : y_0 + y_1 : 0]$ implies that $x_0 + x_1 \equiv 0 \mod 3$ and $y_0 + y_1 \not\equiv 0 \mod 3$, hence:

$$[X : Y : Z] = [x - xe : y_0 + y_1 e : z - ze],$$

and there are two sub-cases of $y_0 \in \mathbb{F}_{3^d}$ :

$(a)$ if $y_0 \not\equiv 0 \mod 3$, then $y_0 + y_1 e$ is invertible in the ring $\mathbb{F}_{3^d}[e]$, hence:

$$[X : Y : Z] \sim [x - xe : 1 : z - ze] \text{ where } x, z \in \mathbb{F}_{3^d}.$$

$(b)$ if $y_0 \equiv 0 \mod 3$, then $Y = ye$ where $y \not\equiv 0 \mod 3$, hence:

$$[X : Y : Z] = [x - xe : e : z - ze] \text{ where } (x, z) \in \mathbb{F}_{3^d} \times \mathbb{F}_{3^d}.$$

Or $\widetilde{\pi_0}([x - xe : e : z - ze]) = [x : 0 : z] \in E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d})$, then necessary $z \not\equiv 0 \mod 3$.

□

## 5. The group law of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$

The explicit formulae of the group law for an elliptic curve over is given by W. Bosma and H. W. Lenstra in [1]. The following theorem can be proved by using these explicit formulae.

**Theorem 5.1.** *The set $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_{3^d})$ is an abelian group, which is written additively, and which has $[0 : 1 : 0]$ as its zero element, and for all $P = [x_1 : y_1 : z_1]$ and $Q = [x_2 : y_2 : z_2]$ in $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_{3^d})$ we have $P + Q = [x_3 : y_3 : z_3]$, where:*

$(i)$ *if $P = Q$, then:*

$$\begin{aligned}
x_3 =& (2\pi_i(a)x_1x_2 + y_1y_2)(x_1y_2 + x_2y_1) + 2\pi_i(ab)z_1z_2(y_1z_2 + y_2z_1),\\
y_3 =& y_1^2y_2^2 + 2\pi_i^2(a)x_1^2x_2^2 + \pi_i^2(a)\pi_i(b)z_1z_2(x_1z_2 + x_2z_1),\\
z_3 =& (\pi_i(a)x_1x_2 + y_1y_2)(y_1z_2 + y_2z_1) + \pi_i(a)(x_1y_2 + x_2y_1)(x_1z_2 + x_2z_1).
\end{aligned}$$

$(ii)$ *if $P \neq Q$, then:*

$$\begin{aligned}
x_3 =& (2\pi_i(a)x_1x_2 + y_1y_2)(x_1z_2 + 2x_2z_1) + (x_1y_2 + 2x_2y_1)(y_1z_2 + y_2z_1),\\
y_3 =& y_1y_2(2y_1z_2 + y_2z_1) + \pi_i(a)(x_1y_2 + x_2y_1)(2x_1z_2 + x_2z_1),\\
z_3 =& 2y_1^2z_2^2 + y_2^2z_1^2 + \pi_i(a)x_1^2z_2^2 + 2\pi_i(a)x_2^2z_1^2.
\end{aligned}$$

**Remark 5.2.** *As $\widetilde{\pi}$ is a bijection mapping between the two sets $E_{a,b}(\mathbb{F}_{3^d}[e])$ and $E_{\pi_0(a),\pi_0(b)}(\mathbb{F}_{3^d}) \times E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{3^d})$, then for all points $P$ and $Q$ in $E_{a,b}(\mathbb{F}_{3^d}[e])$, we define the additive law $P+Q$ in $E_{a,b}(\mathbb{F}_{3^d}[e])$ by $P+Q = \widetilde{\pi}^{-1}\left(\widetilde{\pi}(P)+\widetilde{\pi}(Q)\right)$. The following corollaries can be proved immediately:*

**Corollary 5.3.** *The set $(E_{a,b}(\mathbb{F}_{3^d}[e]),+)$ is a commutative group, which has $[0:1:0]$ as its zero element.*

**Corollary 5.4.** *The $\widetilde{\pi}$ mapping is an isomorphism of groups.*

**Remark 5.5.** *By using the Theorem 5.1, the Theorem 4.1 and the Theorem 3.9, we give the explicit formulae of the additive law of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$. All the results are in the following lemmas:*

**Lemma 5.6.** *We have:*

$$[xe:1:ze]+[x'e:1:z'e]=[x_3e:1+(y_3-1)e:z_3e],$$

*where:*

*(i) If $x' \equiv x \mod 3$ and $z' \equiv z \mod 3$, then:*

$$\begin{aligned} x_3 =& 2x+\pi_1(a)\left(x^3+\pi_1(b)z^3\right),\\ y_3 =& 1+2\pi_1^2(a)x\left(x^3+\pi_1(b)z^3\right),\\ z_3 =& 2z. \end{aligned}$$

*(ii) If $x' \not\equiv x \mod 3$ or $z' \not\equiv z \mod 3$, then:*

$$\begin{aligned} x_3 =& (2\pi_1(a)xx'+1)(xz'+2x'z)+(x+2x')(z'+z),\\ y_3 =& 2(z'+2z)+2\pi_1(a)(x+x')(xz'+2x'z),\\ z_3 =& 2z'^2+z^2+\pi_1(a)\left(x^2z'^2+2x'^2z^2\right). \end{aligned}$$

*Proof.* In this case we have:

$$\widetilde{\pi}([xe:1:ze])=([0:1:0],[x:1:z])$$

and

$$\widetilde{\pi}([x'e:1:z'e])=([0:1:0],[x':1:z']),$$

hence:

$$[xe:1:ze]+[x'e:1:z'e]=\widetilde{\pi}^{-1}([0:1:0],[x_3:y_3:z_3])=[x_3e:1+(y_3-1)e:z_3e],$$

where: $[x_3:y_3:z_3]=[x:1:z]+[x':1:z']$.

*(i)* If $x' \equiv x \mod 3$ and $z' \equiv z \mod 3$, then $[x':1:z']=[x:1:z]$, so:

$$\begin{aligned} x_3 =& 2x+\pi_1(a)\left(x^3+\pi_1(b)z^3\right),\\ y_3 =& 1+2\pi_1^2(a)x\left(x^3+\pi_1(b)z^3\right),\\ z_3 =& 2z. \end{aligned}$$

*(ii)* If $x' \not\equiv x \mod 3$ or $z' \not\equiv z \mod 3$, then $[x':1:z'] \neq [x:1:z]$, so:

$$\begin{aligned} x_3 =& (2\pi_1(a)xx'+1)(xz'+2x'z)+(x+2x')(z'+z),\\ y_3 =& 2(z'+2z)+2\pi_1(a)(x+x')(xz'+2x'z),\\ z_3 =& 2z'^2+z^2+\pi_1(a)\left(x^2z'^2+2x'^2z^2\right). \end{aligned}$$

□

**Lemma 5.7.** *We have:*

$$[xe : 1 : ze] + [x'e : 1 - e : z'e] = [x_3e : 1 + (y_3 - 1)\, e : z_3e],$$

*where:*

$$\begin{aligned} x_3 =& 2\pi_1(a)xx'\,(x + 2x'z) + 2x', \\ y_3 =& 2\pi_1(a)x'\,(x + 2x'z)\,, \\ z_3 =& 2 + \pi_1(a)\left(x^2 + 2x'^2z^2\right). \end{aligned}$$

*Proof.* In this case we have:

$$\begin{aligned} [xe : 1 : ze] + [x'e : 1 - e : z'e] &= \widetilde{\pi}^{-1}\left([0 : 1 : 0], [x_3 : y_3 : z_3]\right) \\ &= [x_3e : 1 + (y_3 - 1)\, e : z_3e], \end{aligned}$$

where:

$$[x_3 : y_3 : z_3] = [x : 1 : z] + [x' : 0 : z'] = [x : 1 : z] + [x' : 0 : 1]$$

is given by:

$$\begin{aligned} x_3 =& 2\pi_1(a)xx'\,(x + 2x'z) + 2x', \\ y_3 =& 2\pi_1(a)x'\,(x + 2x'z)\,, \\ z_3 =& 2 + \pi_1(a)\left(x^2 + 2x'^2z^2\right). \end{aligned}$$

□

**Lemma 5.8.** *We have:*

$$[xe : 1 : ze] + [x' - x'e : 1 : z' - z'e] = [x' + (x - x')\, e : 1 : z' + (z - z')\, e].$$

*Proof.* In this case we have:

$$\widetilde{\pi}\left([xe : 1 : ze]\right) + \widetilde{\pi}\left([x' - x'e : 1 : z' - z'e]\right) = \left([x' : 1 : z'], [x : 1 : z]\right),$$

hence:

$$\begin{aligned} [xe : 1 : ze] + [x' - x'e : 1 : z' - z'e] =& \widetilde{\pi}^{-1}\left([x' : 1 : z'], [x : 1 : z]\right) \\ &= [x' + (x - x')\, e : 1 : z' + (z - z')\, e]. \end{aligned}$$

□

**Lemma 5.9.** *We have:*

$$[xe : 1 : ze] + [x' - x'e : e : z' - z'e] = [x' + (x - x')\, e : e : z' + (z - z')\, e].$$

*Proof.* In this case we have:

$$\widetilde{\pi}\left([xe : 1 : ze]\right) + \widetilde{\pi}\left([x' - x'e : e : z' - z'e]\right) = \left([x' : 0 : z'], [x : 1 : z]\right),$$

hence:

$$\begin{aligned} [xe : 1 : ze] + [x' - x'e : e : z' - z'e] =& \widetilde{\pi}^{-1}\left([x' : 0 : z'], [x : 1 : z]\right) \\ &= [x' + (x - x')\, e : e : z' + (z - z')\, e]. \end{aligned}$$

□

**Lemma 5.10.** *We have:*

$$\begin{aligned}[xe:1:ze]+[X:Y:1] &= [\pi_0(X)+(x_3-\pi_0(X))\,e:\\ &\quad \pi_0(Y)+(y_3-\pi_0(Y))\,e:1+(z_3-1)\,e],\end{aligned}$$

*where:*

(*i*) *If $z$ is not zero in $\mathbb{F}_{3^d}$, $\pi_1(Y)=z^{-1}$ and $\pi_1(X)=z^{-1}x$, then:*

$$\begin{aligned}x_3 &= 2x+\pi_1(a)\left(x^3+\pi_1(b)z^3\right),\\ y_3 &= 1+2\pi_1^2(a)x\left(x^3+\pi_1(b)z^3\right),\\ z_3 &= 2z.\end{aligned}$$

(*ii*) *If $z\equiv 0 \mod 3$ or $\pi_1(Y)\neq z^{-1}$ or $\pi_1(X)\neq z^{-1}x$, then:*

$$\begin{aligned}x_3 &= (2\pi_1(a)x\pi_1(X)+\pi_1(Y))\,(x+2\pi_1(X)z)\\ &\quad +(x\pi_1(Y)+2\pi_1(X))\,(1+\pi_1(Y)z),\\ y_3 &= 2\pi_1(Y)\,(1+2\pi_1(Y)z)+2\pi_1(a)\,(x\pi_1(Y)+\pi_1(X))\,(x+2\pi_1(X)z),\\ z_3 &= 2+\pi_1^2(Y)z^2+\pi_1(a)\left(x^2+2\pi_1^2(X)z^2\right).\end{aligned}$$

*Proof.* As $\widetilde{\pi_0}\left([xe:1:ze]\right)=[0:1:0]$, then:

$$\widetilde{\pi}\left([xe:1:ze]\right)+\widetilde{\pi}\left([X:Y:1]\right)=\left(\widetilde{\pi_0}\left([X:Y:1]\right),\widetilde{\pi_1}\left([xe:1:ze]\right)+\widetilde{\pi_1}\left([X:Y:1]\right)\right),$$

hence:

$$\begin{aligned}[xe:1:ze]+[X:Y:1] &= \widetilde{\pi}^{-1}\left([\pi_0(X):\pi_0(Y):1],[x_3:y_3:z_3]\right)\\ &= [\pi_0(X)+(x_3-\pi_0(X))\,e:\\ &\quad \pi_0(Y)+(y_3-\pi_0(Y))\,e:1+(z_3-1)\,e],\end{aligned}$$

where:

$$[x_3:y_3:z_3]=\widetilde{\pi_1}\left([xe:1:ze]\right)+\widetilde{\pi_1}\left([X:Y:1]\right)=[x:1:z]+[\pi_1(X):\pi_1(Y):1].$$

(*i*) If $z\not\equiv 0 \mod 3$, $\pi_1(Y)=z^{-1}$ and $\pi_1(X)=z^{-1}x$, then:

$$[\pi_1(X):\pi_1(Y):1]=[z^{-1}x:z^{-1}:1]=[x:1:z],$$

hence:

$$\begin{aligned}x_3 &= 2x+\pi_1(a)\left(x^3+\pi_1(b)z^3\right),\\ y_3 &= 1+2\pi_1^2(a)x\left(x^3+\pi_1(b)z^3\right),\\ z_3 &= 2z.\end{aligned}$$

(*ii*) If $z\equiv 0 \mod 3$ or $\pi_1(Y)\neq z^{-1}$ or $\pi_1(X)\neq z^{-1}x$, then:

$$[\pi_1(X):\pi_1(Y):1]\neq[x:1:z],$$

hence:

$$\begin{aligned}x_3 &= (2\pi_1(a)x\pi_1(X)+\pi_1(Y))\,(x+2\pi_1(X)z)\\ &\quad +(x\pi_1(Y)+2\pi_1(X))\,(1+\pi_1(Y)z),\\ y_3 &= 2\pi_1(Y)\,(1+2\pi_1(Y)z)+2\pi_1(a)\,(x\pi_1(Y)+\pi_1(X))\,(x+2\pi_1(X)z),\\ z_3 &= 2+\pi_1^2(Y)z^2+\pi_1(a)\left(x^2+2\pi_1^2(X)z^2\right).\end{aligned}$$

□

**Lemma 5.11.** *We have:*

$$[x - xe : 1 : z - ze] + [x' - x'e : 1 : z' - z'e] = [x_3 - x_3e : y_3 + (1 - y_3)\, e : z_3 - z_3e],$$

*where:*

(*i*) *If* $x' \equiv x \mod 3$ *and* $z' \equiv z \mod 3$, *then:*

$$\begin{aligned} x_3 =& 2x + \pi_0(a)\left(x^3 + \pi_0(b)z^3\right), \\ y_3 =& 1 + 2\pi_0^2(a)x\left(x^3 + \pi_0(b)z^3\right), \\ z_3 =& 2z. \end{aligned}$$

(*ii*) *If* $x' \not\equiv x \mod 3$ *or* $z' \not\equiv z \mod 3$, *then:*

$$\begin{aligned} x_3 =& (2\pi_0(a)xx' + 1)(xz' + 2x'z) + (x + 2x')(z' + z), \\ y_3 =& 2(z' + 2z) + 2\pi_0(a)(x + x')(xz' + 2x'z), \\ z_3 =& 2z'^2 + z^2 + \pi_0(a)\left(x^2z'^2 + 2x'^2z^2\right). \end{aligned}$$

*Proof.* As $\widetilde{\pi_1}([x - xe : 1 : z - ze]) = \widetilde{\pi_1}([x' - x'e : 1 : z' - z'e]) = [0 : 1 : 0]$, then:

$$\begin{aligned} [x - xe : 1 : z - ze] + [x' - x'e : 1 : z' - z'e] & \\ = \widetilde{\pi}^{-1}([x_3 : y_3 : z_3], [0 : 1 : 0]) & \\ = [x_3 - x_3e : y_3 + (1 - y_3)\, e : z_3 - z_3e], & \end{aligned}$$

where:

$$\begin{aligned} [x_3 : y_3 : z_3] &= \widetilde{\pi_0}([x - xe : 1 : z - ze]) + \widetilde{\pi_0}([x' - x'e : 1 : z' - z'e]) \\ &= [x : 1 : z] + [x' : 1 : z']. \end{aligned}$$

(*i*) If $x' \equiv x \mod 3$ and $z' \equiv z \mod 3$, then $[x' : 1 : z'] = [x : 1 : z]$, hence:

$$\begin{aligned} x_3 =& 2x + \pi_0(a)\left(x^3 + \pi_0(b)z^3\right), \\ y_3 =& 1 + 2\pi_0^2(a)x\left(x^3 + \pi_0(b)z^3\right), \\ z_3 =& 2z. \end{aligned}$$

(*ii*) If $x' \not\equiv x \mod 3$ or $z' \not\equiv z \mod 3$, then $[x' : 1 : z'] \neq [x : 1 : z]$, hence:

$$\begin{aligned} x_3 =& (2\pi_0(a)xx' + 1)(xz' + 2x'z) + (x + 2x')(z' + z), \\ y_3 =& 2(z' + 2z) + 2\pi_0(a)(x + x')(xz' + 2x'z), \\ z_3 =& 2z'^2 + z^2 + \pi_0(a)\left(x^2z'^2 + 2x'^2z^2\right). \end{aligned}$$

□

**Lemma 5.12.** *We have:*

$$[x - xe : 1 : z - ze] + [x'e : 1 - e : z'e] = [x + (x' - x)\, e : 1 - e : z + (z' - z)\, e].$$

*Proof.* In this case we have:

$$\widetilde{\pi}\left([x-xe:1:z-ze]\right)+\widetilde{\pi}\left([x'e:1-e:z'e]\right)=\left([x:1:z],[x':0:z']\right),$$

hence:

$$\begin{aligned}[x-xe:1:z-ze]+[x'e:1-e:z'e] =&\widetilde{\pi}^{-1}\left([x:1:z],[x':0:z']\right)\\ &=[x+(x'-x)\,e:1-e:z+(z'-z)\,e].\end{aligned}$$

□

**Lemma 5.13.** *We have:*

$$[x-xe:1:z-ze]+[x'-x'e:e:z'-z'e]=[x_3-x_3e:y_3+(1-y_3)\,e:z_3-z_3e],$$

*where:*

$$\begin{aligned}x_3=&2\pi_0(a)xx'\left(x+2x'z\right)+2x',\\ y_3=&2\pi_0(a)x'\left(x+2x'z\right),\\ z_3=&2+\pi_0(a)\left(x^2+2x'^2z^2\right).\end{aligned}$$

*Proof.* In this case we have:

$$\begin{aligned}[x-xe:1:z-ze]+[x'-x'e:e:z'-z'e] =&\widetilde{\pi}^{-1}\left([x_3:y_3:z_3],[0:1:0]\right)\\ &=[x_3-x_3e:y_3+(1-y_3)\,e:z_3-z_3e],\end{aligned}$$

where:

$$\begin{aligned}[x_3:y_3:z_3] =&\widetilde{\pi_0}\left([x-xe:1:z-ze]\right)+\widetilde{\pi_0}\left([x'-x'e:e:z'-z'e]\right)\\ &=[x:1:z]+[x':0:z']=[x:1:z]+[x':0:1],\end{aligned}$$

hence:

$$\begin{aligned}x_3=&2\pi_0(a)xx'\left(x+2x'z\right)+2x',\\ y_3=&2\pi_0(a)x'\left(x+2x'z\right),\\ z_3=&2+\pi_0(a)\left(x^2+2x'^2z^2\right).\end{aligned}$$

□

**Lemma 5.14.** *We have:*

$$\begin{aligned}[x-xe:1:z-ze]+[X:Y:1] \;=\;& [x_3+(\pi_1(X)-x_3)\,e:\\ & y_3+(\pi_1(Y)-y_3)\,e:z_3+(1-z_3)\,e],\end{aligned}$$

*where:*

(*i*) *If* $z\not\equiv 0 \mod 3$, $\pi_0(Y)=z^{-1}$ *and* $\pi_0(X)=z^{-1}x$, *then:*

$$\begin{aligned}x_3=&2x+a_0\left(x^3+b_0z^3\right),\\ y_3=&1+2a_0^2x\left(x^3+2b_0z^3\right),\\ z_3=&2z.\end{aligned}$$

(*ii*) *If* $z \equiv 0 \mod 3$ *or* $\pi_0(Y) \neq z^{-1}$ *or* $\pi_0(X) \neq z^{-1}x$, *then:*

$$\begin{aligned} x_3 =& (2a_0x\pi_1(X) + \pi_1(Y))\,(x + 2\pi_1(X)z) \\ &+ (x\pi_1(Y) + 2\pi_1(X))\,(1 + \pi_1(Y)z)\,, \\ y_3 =& 2\pi_1(Y)\,(1 + 2\pi_1(Y)z) + 2a_0\,(x\pi_1(Y) + \pi_1(X))\,(x + 2\pi_1(X)z)\,, \\ z_3 =& 2 + \pi_1^2(Y)z^2 + a_0x^2 + 2a_0\pi_1^2(X)z^2. \end{aligned}$$

*Proof.* As $\widetilde{\pi_1}\,([x - xe : 1 : z - ze]) = [0 : 1 : 0]$, then:

$$\begin{aligned} [x - xe : 1 : z - ze] + [X : Y : 1] =& \widetilde{\pi}^{-1}\,([x_3 : y_3 : z_3], [\pi_1(X) : \pi_1(Y) : 1]) \\ =& [x_3 + (\pi_1(X) - x_3)\,e : y_3 + (\pi_1(Y) - y_3)\,e : z_3 + (1 - z_3)\,e], \end{aligned}$$

where:

$$\begin{aligned} [x_3 : y_3 : z_3] =& \widetilde{\pi_0}\,([x - xe : 1 : z - ze]) + \widetilde{\pi_0}\,([X : Y : 1]) \\ =& [x : 1 : z] + [\pi_0(X) : \pi_0(Y) : 1]. \end{aligned}$$

(*i*) If $z \not\equiv 0 \mod 3$, $\pi_0(Y) = z^{-1}$ and $\pi_0(X) = z^{-1}x$, then:

$$[z^{-1}x : z^{-1} : 1] = [x : 1 : z],$$

hence:

$$\begin{aligned} x_3 =& 2x + \pi_0(a)\left(x^3 + \pi_0(b)z^3\right), \\ y_3 =& 1 + 2\pi_0^2(a)x\left(x^3 + 2\pi_0(b)z^3\right), \\ z_3 =& 2z. \end{aligned}$$

(*ii*) If $z \equiv 0 \mod 3$ or $\pi_0(Y) \neq z^{-1}$ or $\pi_0(X) \neq z^{-1}x$, then:

$$[\pi_0(X) : \pi_0(Y) : 1] \neq [x : 1 : z],$$

hence:

$$\begin{aligned} x_3 =& (2\pi_0(a)x\pi_1(X) + \pi_1(Y))\,(x + 2\pi_1(X)z) \\ &+ (x\pi_1(Y) + 2\pi_1(X))\,(1 + \pi_1(Y)z)\,, \\ y_3 =& 2\pi_1(Y)\,(1 + 2\pi_1(Y)z) + 2\pi_0(a)\,(x\pi_1(Y) + \pi_1(X))\,(x + 2\pi_1(X)z)\,, \\ z_3 =& 2 + \pi_1^2(Y)z^2 + \pi_0(a)\left(x^2 + 2\pi_1^2(X)z^2\right). \end{aligned}$$

□

**Lemma 5.15.** *We have:*

$$[xe : 1 - e : ze] + [x'e : 1 - e : z'e] = [x_3e : 1 + (y_3 - 1)\,e : z_3e],$$

*where:*

(*i*) *If* $x' \equiv x \mod 3$, *then:*

$$\begin{aligned} x_3 =& z_3 = 0, \\ y_3 =& 2\pi_1^2(a)x\left(x^3 + \pi_1(b)\right). \end{aligned}$$

(*ii*) *If* $x' \not\equiv x \mod 3$, *then:*

$$\begin{aligned} x_3 =& 2\pi_1(a)\,(x+2x')\,xx', \\ y_3 =& 0, \\ z_3 =& \pi_1(a)\left(x^2+2x'^2\right). \end{aligned}$$

*Proof.* In this case we have:

$$\begin{aligned} [xe:1-e:ze]+[x'e:1-e:z'e] =& \widetilde{\pi}^{-1}\left([0:1:0],[x_3:y_3:z_3]\right) \\ =& [x_3e:1+(y_3-1)\,e:z_3e], \end{aligned}$$

where:

$$\begin{aligned} [x_3:y_3:z_3] =& \widetilde{\pi_1}\left([xe:1-e:ze]\right)+\widetilde{\pi_1}\left([x'e:1-e:z'e]\right) \\ =& [x:0:z]+[x':0:z']. \end{aligned}$$

Or $z$ and $z'$ are not zero in the field $\mathbb{F}_{3^d}$, then:

$$[x:0:z]=[x:0:1] \text{ and } [x':0:z']=[x':0:1],$$

so we have two cases:

(*i*) If $x' \equiv x \mod 3$, then $[x':0:1]=[x:0:1]$, hence:

$$\begin{aligned} x_3 =& z_3 = 0, \\ y_3 =& 2\pi_1^2(a)x\left(x^3+\pi_1(b)\right). \end{aligned}$$

(*ii*) If $x' \not\equiv x \mod 3$, then $[x':0:1]\neq[x:0:1]$, hence:

$$\begin{aligned} x_3 =& 2\pi_1(a)\,(x+2x')\,xx', \\ y_3 =& 0, \\ z_3 =& \pi_1(a)\left(x^2+2x'^2\right). \end{aligned}$$

□

**Lemma 5.16.** *We have:*

$$[xe:1-e:ze]+[x'-x'e:e:z'-z'e]=[x'+(x-x')\,e:0:z'+(z-z')\,e].$$

*Proof.* In this case we have:

$$\widetilde{\pi}\left([xe:1-e:ze]\right)+\widetilde{\pi}\left([x'-x'e:e:z'-z'e]\right)=\left([x':0:z'],[x:0:z]\right),$$

hence:

$$\begin{aligned} [xe:1-e:ze]+[x'-x'e:e:z'-z'e] =& \widetilde{\pi}^{-1}\left([x':0:z'],[x:0:z]\right) \\ =& [x'+(x-x')\,e:0:z'+(z-z')\,e]. \end{aligned}$$

□

**Lemma 5.17.** *We have:*

$$\begin{aligned} [xe:1-e:ze]+[X:Y:1] \;=\; & [\pi_0(X)+(x_3-\pi_0(X))\,e: \\ & \pi_0(Y)+(y_3-\pi_0(Y))\,e:1+(z_3-1)\,e], \end{aligned}$$

*where:*

(*i*) *If* $\pi_1(Y) \equiv 0 \mod 3$ *and* $\pi_1(X) \equiv x \mod 3$, *then:*

$$\begin{aligned} x_3 =& z_3 = 0, \\ y_3 =& 2\pi_1^2(a)x\left(x^3 + \pi_1(b)\right). \end{aligned}$$

(*ii*) *If* $\pi_1(Y) \not\equiv 0 \mod 3$ *or* $\pi_1(X) \not\equiv x \mod 3$, *then:*

$$\begin{aligned} x_3 =& 2\pi_1(a)x\pi_1(X)\left(x + 2\pi_1(X)\right) + x\pi_1^2(Y), \\ y_3 =& 2\pi_1(a)\pi_1(Y)\left(x + 2\pi_1(X)\right)x, \\ z_3 =& \pi_1^2(Y)z^2 + \pi_1(a)\left(x^2 + 2\pi_1^2(X)\right). \end{aligned}$$

*Proof.* As $\widetilde{\pi_0}\left([xe : 1 - e : ze]\right) = [0 : 1 : 0]$, then:

$$\begin{aligned} [xe : 1 - e : ze] + [X : Y : 1] =& \widetilde{\pi}^{-1}\left([\pi_0(X) : \pi_0(Y) : 1], [x_3 : y_3 : z_3]\right) \\ =& [\pi_0(X) + (x_3 - \pi_0(X))\, e : \\ & \pi_0(Y) + (y_3 - \pi_0(Y))\, e : 1 + (z_3 - 1)\, e], \end{aligned}$$

where:

$$\begin{aligned} [x_3 : y_3 : z_3] &= \widetilde{\pi_1}\left([xe : 1 - e : ze]\right) + \widetilde{\pi_1}\left([X : Y : 1]\right) \\ &= [x : 0 : 1] + [\pi_1(X) : \pi_1(Y) : 1], \end{aligned}$$

hence we have two cases:

(*i*) If $\pi_1(Y) \equiv 0 \mod 3$ and $\pi_1(X) \equiv x \mod 3$, then:

$$[\pi_1(X) : \pi_1(Y) : 1] = [x : 0 : 1],$$

hence:

$$\begin{aligned} x_3 =& z_3 = 0, \\ y_3 =& 2\pi_1^2(a)x\left(x^3 + \pi_1(b)\right). \end{aligned}$$

(*ii*) If $\pi_1(Y) \not\equiv 0 \mod 3$ or $\pi_1(X) \not\equiv x \mod 3$, then:

$$[\pi_1(X) : \pi_1(Y) : 1] \neq [x : 0 : 1],$$

hence:

$$\begin{aligned} x_3 =& 2\pi_1(a)x\pi_1(X)\left(x + 2\pi_1(X)\right) + x\pi_1^2(Y), \\ y_3 =& 2\pi_1(a)\pi_1(Y)\left(x + 2\pi_1(X)\right)x, \\ z_3 =& \pi_1^2(Y)z^2 + \pi_1(a)\left(x^2 + 2\pi_1^2(X)\right). \end{aligned}$$

□

**Lemma 5.18.** *We have:*

$$[x - xe : e : z - ze] + [x' - x'e : e : z' - z'e] = [x_3 - x_3e : y_3 + (1 - y_3)\, e : z_3 - z_3e],$$

*where:*

(*i*) *If* $x' \equiv x \mod 3$, *then:*

$$\begin{aligned} x_3 =& z_3 = 0, \\ y_3 =& 2\pi_0^2(a)x\left(x^3 + \pi_0(b)\right). \end{aligned}$$

(*ii*) *If* $x' \not\equiv x \mod 3$, *then:*

$$\begin{aligned} x_3 =& 2\pi_0(a)\,(x+2x')\,xx', \\ y_3 =& 0, \\ z_3 =& \pi_0(a)\left(x^2+2x'^2\right). \end{aligned}$$

*Proof.* In this case we have:

$$\begin{aligned} [x-xe:e:z-ze]+[x'-x'e:e:z'-z'e] =& \widetilde{\pi}^{-1}\left([x_3:y_3:z_3],[0:1:0]\right) \\ =& [x_3-x_3e:y_3+(1-y_3)\,e:z_3-z_3e], \end{aligned}$$

where:

$$\begin{aligned} [x_3:y_3:z_3] =& \widetilde{\pi_0}\left([x-xe:e:z-ze]\right)+\widetilde{\pi_0}\left([x'-x'e:e:z'-z'e]\right) \\ =& [x:0:z]+[x':0:z'] = [x:0:1]+[x':0:1], \end{aligned}$$

so we have two cases:

(*i*) If $x' \equiv x \mod 3$, then $[x':0:1]=[x:0:1]$, hence:

$$\begin{aligned} x_3 =& z_3 = 0, \\ y_3 =& 2\pi_0^2(a)x\left(x^3+\pi_0(b)\right). \end{aligned}$$

(*ii*) If $x' \not\equiv x \mod 3$, then $[x':0:1]\neq[x:0:1]$, hence:

$$\begin{aligned} x_3 =& 2\pi_0(a)\,(x+2x')\,xx', \\ y_3 =& 0, \\ z_3 =& \pi_0(a)\left(x^2+2x'^2\right). \end{aligned}$$

□

**Lemma 5.19.** *We have:*

$$\begin{array}{rcl} [x-xe:e:z-ze] & + & [X:Y:1] \\ & = & [x_3+(\pi_1(X)-x_3)\,e:y_3+(\pi_1(Y)-y_3)\,e:z_3+(1-z_3)\,e], \end{array}$$

*where:*

(*i*) *If* $\pi_0(Y)\equiv 0 \mod 3$ *and* $\pi_0(X)\equiv x \mod 3$, *then:*

$$\begin{aligned} x_3 =& z_3 = 0, \\ y_3 =& 2\pi_0^2(a)x\left(x^3+\pi_0(b)\right). \end{aligned}$$

(*ii*) *If* $\pi_0(Y)\not\equiv 0 \mod 3$ *or* $\pi_0(X)\not\equiv x \mod 3$, *then:*

$$\begin{aligned} x_3 =& 2\pi_0(a)x\pi_0(X)\,(x+2\pi_0(X))+x\pi_0(Y)\pi_1(Y), \\ y_3 =& 2\pi_0(a)\pi_0(Y)\,(x+2\pi_0(X))\,x, \\ z_3 =& \pi_0^2(Y)+\pi_0(a)\left(x^2+2\pi_0^2(X)\right). \end{aligned}$$

*Proof.* As $\widetilde{\pi_1}\left([x - xe : e : z - ze]\right) = [0 : 1 : 0]$, then:

$$\begin{aligned}[x - xe : e : z - ze] + [X : Y : 1] = \widetilde{\pi}^{-1}\left([x_3 : y_3 : z_3], [\pi_1(X) : \pi_1(Y) : 1]\right)\\ = [x_3 + (\pi_1(X) - x_3)\, e :\\ y_3 + (\pi_1(Y) - y_3)\, e : z_3 + (1 - z_3)\, e],\end{aligned}$$

where:

$$[x_3 : y_3 : z_3] = [x : 0 : z] + [\pi_0(X) : \pi_0(Y) : 1] = [x : 0 : 1] + [\pi_0(X) : \pi_0(Y) : 1],$$

hence we have two cases:

(*i*) If $\pi_0(Y) \equiv 0 \mod 3$ and $\pi_0(X) \equiv x \mod 3$, then:

$$[\pi_0(X) : \pi_0(Y) : 1] = [x : 0 : 1],$$

hence:

$$\begin{aligned}x_3 =& z_3 = 0,\\ y_3 =& 2\pi_0^2(a)x\left(x^3 + \pi_0(b)\right).\end{aligned}$$

(*ii*) If $\pi_0(Y) \not\equiv 0 \mod 3$ or $\pi_0(X) \not\equiv x \mod 3$, then:

$$[\pi_0(X) : \pi_0(Y) : 1] \neq [x : 0 : 1],$$

hence:

$$\begin{aligned}x_3 =& 2\pi_0(a)x\pi_0(X)\left(x + 2\pi_0(X)\right) + x\pi_0(Y)\pi_1(Y),\\ y_3 =& 2\pi_0(a)\pi_0(Y)\left(x + 2\pi_0(X)\right)x,\\ z_3 =& \pi_0^2(Y) + \pi_0(a)\left(x^2 + 2\pi_0^2(X)\right).\end{aligned}$$

□

**Lemma 5.20.** *We have:*

$$[X : Y : 1] + [X' : Y' : 1] = [x_0 + (x_1 - x_0)\, e : y_0 + (y_1 - y_0)\, e : z_0 + (z_1 - z_0)\, e],$$

*where:*

$$\forall i \in \{0, 1\} : \ [x_i : y_i : z_i] = [\pi_i(X) : \pi_i(Y) : 1] + [\pi_i(X') : \pi_i(Y') : 1]$$

*is such that:*

(*i*) *If* $\pi_i(X') \equiv \pi_i(X) \mod 3$ *and* $\pi_i(Y') \equiv \pi_i(Y) \mod 3$, *then:*

$$\begin{aligned}x_i =& \left(\pi_i(a)\pi_i^2(X) + 2\pi_i^2(Y)\right)\pi_i(XY) + \pi_i(ab)\pi_i(Y),\\ y_i =& \pi_i^4(Y) + 2\pi_i^2(a)\pi_i^4(X) + 2\pi_i^2(a)\pi_i(b)\pi_i(X),\\ z_i =& 2\left(\pi_i^2(Y) + \pi_i(a)\pi_i^2(X)\right)\pi_i(Y) + \pi_i(a)\pi_i(X^2Y).\end{aligned}$$

(*ii*) *If* $\pi_i(X') \not\equiv \pi_i(X) \mod 3$ *or* $\pi_i(Y') \not\equiv \pi_i(Y) \mod 3$, *then:*

$$\begin{aligned}x_i =& \left(2\pi_i(a)\pi_i(XX') + \pi_i(YY')\right)\left(\pi_i(X) + 2\pi_i(X')\right)\\ &+ \left(\pi_i(XY') + 2\pi_i(X'Y)\right)\left(\pi_i(Y) + \pi_i(Y')\right),\\ y_i =& \pi_i(YY')\left(2\pi_i(Y) + \pi_i(Y')\right)\\ &+ 2\pi_i(a)\left(\pi_i(XY') + \pi_i(X'Y)\right)\left(\pi_i(X) + 2\pi_i(X')\right),\\ z_i =& 2\pi_i^2(Y) + \pi_i^2(Y') + \pi_i(a)\pi_i^2(X) + 2\pi_i(a)\pi_i^2(X').\end{aligned}$$

*Proof.* In this case we have:

$$\begin{aligned}[X:Y:1]+[X':Y':1] =& \widetilde{\pi}^{-1}\left([x_0:y_0:z_0],[x_1:y_1:z_1]\right)\\ &= [x_0+(x_1-x_0)\,e : y_0+(y_1-y_0)\,e : z_0+(z_1-z_0)\,e],\end{aligned}$$

where:

$$\forall i\in\{0,1\}:\ [x_i:y_i:z_i]=[\pi_i(X):\pi_i(Y):1]+[\pi_i(X'):\pi_i(Y'):1].$$

(*i*) If $\pi_i(X')\equiv\pi_i(X) \mod 3$ and $\pi_i(Y')\equiv\pi_i(Y) \mod 3$, then:

$$[\pi_i(X):\pi_i(Y):1]=[\pi_i(X'):\pi_i(Y'):1],$$

hence:

$$\begin{aligned}x_i =& \left(\pi_i(a)\pi_i^2(X)+2\pi_i^2(Y)\right)\pi_i(XY)+\pi_i(ab)\pi_i(Y),\\ y_i =& \pi_i^4(Y)+2\pi_i^2(a)\pi_i^4(X)+2\pi_i^2(a)\pi_i(b)\pi_i(X),\\ z_i =& 2\left(\pi_i^2(Y)+\pi_i(a)\pi_i^2(X)\right)\pi_i(Y)+\pi_i(a)\pi_i(X^2Y).\end{aligned}$$

(*ii*) If $\pi_i(X')\not\equiv\pi_i(X) \mod 3$ or $\pi_i(Y')\not\equiv\pi_i(Y) \mod 3$, then:

$$[\pi_i(X):\pi_i(Y):1]\neq[\pi_i(X'):\pi_i(Y'):1],$$

hence:

$$\begin{aligned}x_i =& \left(2\pi_i(a)\pi_i(XX')+\pi_i(YY')\right)\left(\pi_i(X)+2\pi_i(X')\right)\\ &+\left(\pi_i(XY')+2\pi_i(X'Y)\right)\left(\pi_i(Y)+\pi_i(Y')\right),\\ y_i =& \pi_i(YY')\left(2\pi_i(Y)+\pi_i(Y')\right)\\ &+2\pi_i(a)\left(\pi_i(XY')+\pi_i(X'Y)\right)\left(\pi_i(X)+2\pi_i(X')\right),\\ z_i =& 2\pi_i^2(Y)+\pi_i^2(Y')+\pi_i(a)\pi_i^2(X)+2\pi_i(a)\pi_i^2(X').\end{aligned}$$

□

**Remark 5.21.** *The Lemmas from 5.6 to 5.20 can be regrouped in the next theorem which given the additive law of the elliptic curve* $E_{a,b}(\mathbb{F}_{3^d}[e])$.

**Theorem 5.22.** *Lets* $P=[X_0:Y_0:Z_0]$ *and* $Q=[X_1:Y_1:Z_1]$ *in* $E_{a,b}(\mathbb{F}_{3^d}[e])$ *and let* $[x_i:y_i:z_i]=\widetilde{\pi}_i(P)+\widetilde{\pi}_i(Q)$ *the additive law in the group* $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_{3^d})$, *where* $i\in\{0,1\}$. *The set* $(E_{a,b}(\mathbb{F}_{3^d}[e]),+)$ *where* $P+Q=\widetilde{\pi}^{-1}\left(\widetilde{\pi}(P)+\widetilde{\pi}(Q)\right)$ *is a commutative group which has* $[0:1:0]$ *as its zero element, and which its law group* $P+Q=[X_2:Y_2:Z_2]$ *is given by:*

(*i*) *If* $\widetilde{\pi}_0(P)=[0:1:0]$, *then:*

$$\begin{aligned}X_2 =& \pi_0(X_1)+(x_1-\pi_0(X_1))\,e,\\ Y_2 =& \pi_0(Y_1)+(y_1-\pi_0(Y_1))\,e,\\ Z_2 =& \pi_0(Z_1)+(z_1-\pi_0(Z_1))\,e.\end{aligned}$$

(*ii*) *If* $\widetilde{\pi}_1(P)=[0:1:0]$, *then:*

$$\begin{aligned}X_2 =& x_0+(\pi_1(X_1)-x_0)\,e,\\ Y_2 =& y_0+(\pi_1(Y_1)-y_0)\,e,\\ Z_2 =& z_0+(\pi_1(Z_1)-z_0)\,e.\end{aligned}$$

*(iii) If* $\widetilde{\pi_0}(P) \neq [0:1:0]$ *and* $\widetilde{\pi_1}(P) \neq [0:1:0]$*, then:*

$$\begin{aligned} X_2 =& x_0 + (x_1 - x_0)\, e, \\ Y_2 =& y_0 + (y_1 - y_0)\, e, \\ Z_2 =& z_0 + (z_1 - z_0)\, e. \end{aligned}$$

*Proof.* For the proof, we can show easily that the Lemmas 5.6, 5.7, 5.8, 5.9, 5.10, 5.15, 5.16 and 5.17 verify the first case of the theorem, the Lemmas 5.11, 5.12, 5.13, 5.14, 5.18 and 5.19 verify the second case and the Lemma 5.20 verify the last case of the theorem. □

## 6. Conclusion

In this work we have studying in characteristic 3 the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[e])$ defined over the non local ring $\mathbb{F}_{3^d}[e]$ by the Wieirstrass equation:

$$Y^2Z = X^3 + aX^2Z + bZ^3,$$

where we have given explicitly its addition law.

## References


1. W. Bosma, H.W. Lenstra, *Complete System of Two Addition Laws for Elliptic curve*, Journal of Number Theory (1995).
2. A. Chillali, *Cryptography over elliptic curve of the ring* $\mathbb{F}_q[\varepsilon]$ , $\varepsilon^4 = 0$, World Academy of Science, Engineering and Technology, (2011).
3. M. H. Hassib, A. Chillali, *The* $\widetilde{\pi}$ *homomorphism of* $\mathrm{E}_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$, AIP publishing, vol.**1557**, (2013) 12-14.
4. M. H. Hassib, A. Chillali, M. Abdou Elomary, *Elliptic curve over a chain ring of characteristic 3*, (International Workshop of Algebra and Applications, 2014, FST Fez, Morocco), Journal of Taibah University for Science (2015).
5. M. Zeriouh, A. Chillali, A. Boua, *Cryptography based on the matrices*, Boletim da Sociedade Paranaense de Matematica, Vol 37, No 3 (2019) 75-83.
6. M. Sahmoudi, A. Chillali, *Key Exchange over Particular Algebraic Closure Ring*, Tatra Mountains Mathematical Publications, Vol 70, (2017) 151-162.
7. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curve*, Graduate Texts in Mathematics, Vol 151, Springer, 1994.
8. M.Virat, *Courbe elliptique sur un anneau et applications cryptographiques*, Nice-Sophia Antipolis, (Thèse Docteur en Sciences), 2009.



*A. Boulbot,*
*A. Chillali,*
*A. Mouhib,*
*Sidi Mohamed Ben Abdellah University,*
*FP, LSI, Taza, 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