Gulf Journal of Mathematics
Vol 14, Issue 1 (2023) 182-191

ISSN: 2309-4966
https://doi.org/10.56947/gjom.v13i2.902

STUDY OF ELLIPTIC CURVE OVER A FINITE RING $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = \varepsilon^3$

BILEL SELIKH[1*]

Abstract. Let $\mathbb{F}_{3^d}$ be a finite field of order 3^d with $d \in \mathbb{N}^*$. In this paper, we study the elliptic curve over the finite ring $\mathbb{F}_{3^d}[\varepsilon] := \mathbb{F}_{3^d}[X]/(X^4 - X^3)$, where $\varepsilon^4 = \varepsilon^3$ of characteristic 3 given by the homogeneous Weierstrass equation of the form

$$Y^2Z = X^3 + aX^2Z + bZ^3, \text{ where } a, b \in \mathbb{F}_{3^d}[\varepsilon].$$

Such that we study the arithmetic operations of this ring and define the elliptic curve over it. Next, we show that $E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$ and $E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$ are two elliptic curves over the finite field $\mathbb{F}_{3^d}$, such that Π_0 is a canonical projection and Π_1 is a sum projection of coordinate of element in $\mathbb{F}_{3^d}[\varepsilon]$ and we conclude by given a classification of elements in elliptic curve over the finite ring $\mathbb{F}_{3^d}[\varepsilon]$.

1. Introduction

Elliptic curves play an important role in many areas of mathematics (geometry, algebra and numbers theory...etc). The study of elliptic curves by algebraists, algebraic geometers and number theorists dates back to the middle of the nineteenth century. They are the basis of the demonstration of fermat's great theorem by Andrew Wiles, it was proposed for the asymmetrical cryptography by Neal Koblitz [6] and Victor Miller [7] in 1985 separately.

In 2016, A. Boulbot et al. published their article [2] were constructed a non local ring $\mathbb{F}_q[e] = \mathbb{F}_q[X]/(X^3 - X^2)$, $e^3 = e^2$, defined an elliptic curve over $\mathbb{F}_q[e]$ and they had given the classification of elements in $E_{a,b}(\mathbb{F}_q[e])$, and in 2018 [4] they studied elements classification and the group law of an elliptic curve over $\mathbb{F}_{3^d}[e], e^2 = e$.

In 2021, B. Selikh et al. published their article [8] were introduced the classification of elements in elliptic curve over the ring $\mathbb{F}_q[\varepsilon] := \mathbb{F}_q[X]/(X^4 - X^3), \varepsilon^4 = \varepsilon^3$ with $q = p^r$ where r be a positive integer and $p \geq 5$ is a prime number.

Our goal of this work is to study the elliptic curve over the ring $\mathbb{F}_{3^d}[\varepsilon] := \mathbb{F}_{3^d}[X]/(X^4 - X^3)$, we start this work by studying the arithmetic of the ring $\mathbb{F}_{3^d}[\varepsilon]$, $\varepsilon^4 = \varepsilon^3$, in particular we show that $\mathbb{F}_{3^d}[\varepsilon]$ is not a local ring. In section 3, the study of the discriminant and the homogeneous Weierstrass equation of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$, allow us to define the two elliptic curves $E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$

Date: Received: Apr 12, 2022; Accepted: Sep 4, 2022.

* Corresponding author.

2010 *Mathematics Subject Classification.* Primary 11T55, 20K27 ; Secondary 20K30,14H52.
Key words and phrases. Elliptic curve, finite ring, finite field, Weierstrass equation.

and $E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$ over the finite field $\mathbb{F}_{3^d}$, where Π_0 and Π_1 two surjective morphisms of rings. In the last section, we classify the elements of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ into three types.

2. The finite ring $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = \varepsilon^3$

We will follow the approach in [3, 4, 8]. The ring $\mathbb{F}_{3^d}[\varepsilon]$, where $\varepsilon^4 = \varepsilon^3$ can be constructed by using the quotient ring of $\mathbb{F}_{3^d}[X]$ by the polynomial $X^4 - X^3$. $\mathbb{F}_{3^d}$ is a finite field of order 3^d where d be a positive integer. Every element $X \in \mathbb{F}_{3^d}[\varepsilon]$ written in the form $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ where $(x_0, x_1, x_2, x_3) \in \mathbb{F}_{3^d}^4$.

2.1. **Arithmetic operations.** The arithmetic operations in $\mathbb{F}_{3^d}[\varepsilon]$ can be decomposed into operations in $\mathbb{F}_{3^d}$ and they are computed as follows:
$X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2 + (x_3 + y_3)\varepsilon^3$ and

$$\begin{aligned} X \cdot Y &= (x_0y_0) + (x_0y_1 + x_1y_0)\varepsilon + (x_0y_2 + x_1y_1 + x_2y_0)\varepsilon^2 \\ &\quad + ((x_0 + x_1 + x_2 + x_3)y_3 + (x_1 + x_2 + x_3)y_2 + (x_2 + x_3)y_1 + x_3y_0)\varepsilon^3, \end{aligned}$$

where $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ with $x_i, y_i \in \mathbb{F}_{3^d}$ and $0 \leq i \leq 3$.

Example 2.1. Let $X = 1 + \varepsilon + \varepsilon^2 + 2\varepsilon^3$ and $Y = 2 + \varepsilon^2 + \varepsilon^3$ are two elements in $\mathbb{F}_3[\varepsilon]$, we have:

$$X + Y = \varepsilon + 2\varepsilon^2, \text{ and } X \cdot Y = 2 + 2\varepsilon + \varepsilon^3.$$

Lemma 2.2. *$(\mathbb{F}_{3^d}[\varepsilon], +, \cdot)$ is a finite unitary commutative ring isomorphic to the quotient ring $\mathbb{F}_{3^d}[X]/(X^4 - X^3)$.*

Lemma 2.3. *The ring $\mathbb{F}_{3^d}[\varepsilon]$ is a vector space over $\mathbb{F}_{3^d}$ of dimension 4. And have $\{1, \varepsilon, \varepsilon^2, \varepsilon^3\}$ as basis, then: $\mathbb{F}_{3^d}[\varepsilon] = \mathbb{F}_{3^d} + \mathbb{F}_{3^d}\varepsilon + \mathbb{F}_{3^d}\varepsilon^2 + \mathbb{F}_{3^d}\varepsilon^3$.*

Proof. Let X and Y in $\mathbb{F}_{3^d}[\varepsilon]$ and k in the ring $\mathbb{F}_{3^d}$, we have:

- ❖ $X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2 + (x_3 + y_3)\varepsilon^3$.
- ❖ $k \cdot X = k\sum_{i=0}^{3} x_i\varepsilon^i = \sum_{i=0}^{3} kx_i\varepsilon^i = kx_0 + kx_1\varepsilon + kx_2\varepsilon^2 + kx_3\varepsilon^3$.

□

Proposition 2.4. *The product law in $\mathbb{F}_{3^d}[\varepsilon]$ can be written as:*
$X \cdot Y = x_0y_0 + \Theta_{XY}\varepsilon + \Omega_{XY}\varepsilon^2$

$$+ ((x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0y_0 - \Theta_{XY} - \Omega_{XY})\varepsilon^3,$$

where:

$$\Theta_{XY} = (x_0 + x_1)(y_0 + y_1) - x_0y_0 - x_1y_1 = x_0y_1 + x_1y_0 \text{ and}$$

$$\begin{aligned} \Omega_{XY} &= (x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0(y_0 + y_1) - x_1(y_0 + y_2) - x_2(y_1 + y_2) \\ &= x_0y_2 + x_1y_1 + x_2y_0. \end{aligned}$$

Proof. We have:
$(x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0y_0 - \Theta_{XY} - \Omega_{XY}$
$= (x_0 + x_1 + x_2 + x_3)y_3 + (x_1 + x_2 + x_3)y_2 + (x_2 + x_3)y_1 + x_3y_0.$ □

Corollary 2.5. *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_{3^d}[\varepsilon]$, we have:*
$X^2 = x_0^2 + \Theta_{X^2}\varepsilon + \Omega_{X^2}\varepsilon^2 + ((x_0 + x_1 + x_2 + x_3)^2 - x_0^2 - x_1^2 + x_0x_1 + x_0x_2)\varepsilon^3,$

$X^3 = x_0^3 + (x_1^3 + x_2^3 + x_3^3)\varepsilon^3$,
where: $\Theta_{X^2} = (x_0+x_1)^2 - x_0^2 - x_1^2$ *and* $\Omega_{X^2} = (x_0+x_1+x_2)^2 - x_0^2 - x_2^2 + x_0x_1 + x_1x_2$.

The next proposition characterize the set $(\mathbb{F}_{3^d}[\varepsilon])^\times$of invertible elements in $\mathbb{F}_{3^d}[\varepsilon]$.

Proposition 2.6. *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_{3^d}[\varepsilon]$. The element X is invertible if and only if x_0 and $x_0+x_1+x_2+x_3$ are invertible in $\mathbb{F}_{3^d}$. The inverse of X is given by:*
$X^{-1} = x_0^{-1} - x_1x_0^{-2}\varepsilon + (x_1^2x_0^{-3} - x_2x_0^{-2})\varepsilon^2$
$\quad + ((x_0 + x_1 + x_2 + x_3)^{-1} + x_1x_0^{-2} + x_2x_0^{-2} - x_1^2x_0^{-3} - x_0^{-1})\varepsilon^3$.

Proof. Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ be two elements of $\mathbb{F}_{3^d}[\varepsilon]$, we have:

$$\begin{aligned} X \cdot Y &= x_0y_0 + \Theta_{XY}\varepsilon + \Omega_{XY}\varepsilon^2 \\ &+ ((x_0 + x_1 + x_2 + x_3)(y_0 + y_1 + y_2 + y_3) - x_0y_0 - \Theta_{XY} - \Omega_{XY})\varepsilon^3, \end{aligned}$$

where $\Theta_{XY} = x_0y_1 + x_1y_0$ and $\Omega_{XY} = x_0y_2 + x_1y_1 + x_2y_0$. Then:

$$X \cdot Y = 1 \iff \begin{cases} x_0y_0 = 1; \\ \Theta_{XY} = 0; \\ \Omega_{XY} = 0; \\ (\sum_{i=0}^3 x_i)(\sum_{i=0}^3 y_i) - x_0y_0 - \Theta_{XY} - \Omega_{XY} = 0. \end{cases}$$

$$\iff \begin{cases} x_0y_0 = 1; \\ x_0y_1 + x_1y_0 = 0; \\ x_0y_2 + x_1y_1 + x_2y_0 = 0; \\ (\sum_{i=0}^3 x_i)(\sum_{i=0}^3 y_i) = 1. \end{cases}$$

$$\iff \begin{cases} y_0 = x_0^{-1}, \text{ and } \ x_0 \not\equiv 0[3]; \\ y_1 = -x_1x_0^{-2}; \\ y_2 = -x_2x_0^{-2} + x_1^2x_0^{-3}; \\ y_3 = (\sum_{i=0}^3 x_i)^{-1} + x_1x_0^{-2} + x_2x_0^{-2} - x_1^2x_0^{-3} - x_0^{-1}, \text{ and } \sum_{i=0}^3 x_i \not\equiv 0[3]. \end{cases}$$

So, $X \in (\mathbb{F}_{3^d}[\varepsilon])^\times$ if and only if $x_0 \not\equiv 0[3]$ and $x_0 + x_1 + x_2 + x_3 \not\equiv 0[3]$.
In this case, we have:
$X^{-1} = x_0^{-1} - x_1x_0^{-2}\varepsilon + (x_1^2x_0^{-3} - x_2x_0^{-2})\varepsilon^2$
$\quad + ((x_0 + x_1 + x_2 + x_3)^{-1} + x_1x_0^{-2} + x_2x_0^{-2} - x_1^2x_0^{-3} - x_0^{-1})\varepsilon^3$. □

Corollary 2.7. *Let $X \in \mathbb{F}_{3^d}[\varepsilon]$, then is not invertible if and only if $x_0 \equiv 0[3]$ or $x_0 + x_1 + x_2 + x_3 \equiv 0[3]$, where $(x_0, x_1, x_2, x_3) \in \mathbb{F}_{3^d}^4$.*

Example 2.8. Let $X = 1 + 2\varepsilon + \varepsilon^3 \in \mathbb{F}_3[\varepsilon]$, we have $x_0 = 1 \not\equiv 0[3]$ and $x_0 + x_1 + x_2 + x_3 = 1 \not\equiv 0[3]$ then X is invertible in $\mathbb{F}_3[\varepsilon]$. The inverse of X is $X^{-1} = 1 + \varepsilon + \varepsilon^2 + \varepsilon^3$.

Lemma 2.9. $\mathbb{F}_{3^d}[\varepsilon]$ *is a non local ring.*

Proof. Let $X \in \mathbb{F}_{3^d}[\varepsilon]$, then the element X is not invertible if and only if $X = x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ or $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0+x_1+x_2)\varepsilon^3$, such that $(x_0, x_1, x_2, x_3) \in \mathbb{F}_{3^d}^4$. Now, we consider I_0, I_1 be two ideals of $\mathbb{F}_{3^d}[\varepsilon]$ defined by:

$$I_0 = \{x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \mid (x_1, x_2, x_3) \in \mathbb{F}_{3^d}^3\} \text{ and}$$
$$I_1 = \{x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 \mid (x_0, x_1, x_2) \in \mathbb{F}_{3^d}^3\},$$

it's clear that $I_0 \cup I_1$ is the set of non invertible elements in $\mathbb{F}_{3^d}[\varepsilon]$, and for all x_0, x_1, x_2, a, b and c in $\mathbb{F}_{3^d}$, we have:
$x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 = a\varepsilon + b\varepsilon^2 + c\varepsilon^3$
$\Longrightarrow x_0 + (x_1 - a)\varepsilon + (x_2 - b)\varepsilon^2 - (x_0 + x_1 + x_2 + c)\varepsilon^3 = 0$

$$\Longrightarrow \begin{cases} x_0 = 0; \\ x_1 - a = 0; \\ x_2 - b = 0; \\ x_0 + x_1 + x_2 + c = 0. \end{cases} \Longrightarrow \begin{cases} x_0 = 0; \\ x_1 = a; \\ x_2 = b; \\ x_1 + x_2 = -c. \end{cases}$$

We have $I_0 \cap I_1 = \{a\varepsilon + b\varepsilon^2 - c\varepsilon^3 \mid (a, b, c) \in \mathbb{F}_{3^d}^3\}$ then I_0 and I_1 are two distinct ideals of $\mathbb{F}_{3^d}[\varepsilon]$, so $I_0 \cup I_1$ is not ideal. Finally, the ring $\mathbb{F}_{3^d}[\varepsilon]$ is not local. □

Definition 2.10. Let Π_0 be a canonical projection and Π_1 be a sum projection of coordinate of element in $\mathbb{F}_{3^d}[\varepsilon]$ defined as given below:

$$\Pi_0 : \left| \begin{array}{ccc} \mathbb{F}_{3^d}[\varepsilon] & \longrightarrow & \mathbb{F}_{3^d} \\ X = \sum_{i=0}^{3} x_i\varepsilon^i & \longmapsto & x_0 \end{array} \right. \text{ and } \Pi_1 : \left| \begin{array}{ccc} \mathbb{F}_{3^d}[\varepsilon] & \longrightarrow & \mathbb{F}_{3^d} \\ X = \sum_{i=0}^{3} x_i\varepsilon^i & \longmapsto & \sum_{i=0}^{3} x_i \end{array} \right.$$

Lemma 2.11. *The mappings Π_0 and Π_1 are two surjective morphisms of rings.*

Proof. Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ be two elements of $\mathbb{F}_{3^d}[\varepsilon]$. From the definition of the sum and product law in $\mathbb{F}_{3^d}[\varepsilon]$, we have:

$$\Pi_0(X + Y) = x_0 + y_0 = \Pi_0(X) + \Pi_0(Y), \text{ and}$$
$$\Pi_0(X \cdot Y) = x_0 \cdot y_0 = \Pi_0(X) \cdot \Pi_0(Y).$$

So, Π_0 is morphism of rings.

$$\begin{aligned} \Pi_1(X + Y) &= x_0 + y_0 + x_1 + y_1 + x_2 + y_2 + x_3 + y_3 \\ &= \Pi_1(X) + \Pi_1(Y), \text{ and} \\ \Pi_1(X \cdot Y) &= (x_0 + x_1 + x_2 + x_3) \cdot (y_0 + y_1 + y_2 + y_3) \\ &= \Pi_1(X) \cdot \Pi_1(Y). \end{aligned}$$

So, Π_1 is morphism of rings.
Finally, for all $x \in \mathbb{F}_{3^d} \subset \mathbb{F}_{3^d}[\varepsilon]$, we have $\Pi_0(x) = \Pi_1(x) = x$, so Π_0 and Π_1 are two surjective morphisms. □

Lemma 2.12. *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_{3^d}[\varepsilon]$. If X is invertible in $\mathbb{F}_{3^d}[\varepsilon]$, then:*

$$\Pi_0(X^{-1}) = (\Pi_0(X))^{-1} \text{ and } \Pi_1(X^{-1}) = (\Pi_1(X))^{-1}.$$

Proof. Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 \in \mathbb{F}_{3^d}[\varepsilon]$. By using the Proposition 2.6, we have:

$$\begin{aligned} \Pi_0(X^{-1}) &= x_0^{-1} \\ &= (\Pi_0(X))^{-1}, \end{aligned} \quad \text{and} \quad \begin{aligned} \Pi_1(X^{-1}) &= (x_0 + x_1 + x_2 + x_3)^{-1} \\ &= (\Pi_1(X))^{-1}. \end{aligned}$$

□

3. Elliptic curve over $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = \varepsilon^3$

In this section, we consider X, Y, Z, a and b are elements of the ring $\mathbb{F}_{3^d}[\varepsilon]$ fixed by $X = x_0+x_1\varepsilon+x_2\varepsilon^2+x_3\varepsilon^3$, $Y = y_0+y_1\varepsilon+y_2\varepsilon^2+y_3\varepsilon^3$, $Z = z_0+z_1\varepsilon+z_2\varepsilon^2+z_3\varepsilon^3$, $a = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3$ and $b = b_0 + b_1\varepsilon + b_2\varepsilon^2 + b_3\varepsilon^3$, with d be a positive integer.
The discriminant of elliptic curve over the ring $\mathbb{F}_{3^d}[\varepsilon]$ is $\triangle := -a^3b$, and we denoted by $\triangle_0'$ and $\triangle_1'$ the images of the discriminant $\triangle$ by Π_0 and Π_1 the morphisms respectively,

$$\triangle_0' = \Pi_0(\triangle) = \Pi_0(-a^3b) = \Pi_0(-a^3)\Pi_0(b) = -a_0^3b_0, \text{ and}$$
$$\triangle_1' = \Pi_1(\triangle) = \Pi_1(-a^3b) = \Pi_1(-a^3)\Pi_1(b) = -(a_0 + a_1 + a_2 + a_3)^3(b_0 + b_1 + b_2 + b_3)$$
$$= -(a_0^3 + a_1^3 + a_2^3 + a_3^3)(b_0 + b_1 + b_2 + b_3).$$

The j-invariant of elliptic curve over the ring $\mathbb{F}_{3^d}[\varepsilon]$ is $j := \dfrac{-a^3}{b}$, and we denoted by j_0' and j_1' the images of the j-invariant j by Π_0 and Π_1 the morphisms respectively. By using the Lemma 2.12, we have:

$$j_0' = \Pi_0(j) = \Pi_0\left(\frac{-a^3}{b}\right) = \Pi_0(-a^3b^{-1}) = \Pi_0(-a^3)\Pi_0(b^{-1}) = (-\Pi_0(a))^3(\Pi_0(b))^{-1}$$
$$= -a_0^3b_0^{-1} = \frac{-a_0^3}{b_0}, \text{ and}$$
$$j_1' = \Pi_1(j) = \Pi_1\left(\frac{-a^3}{b}\right) = \Pi_1(-a^3b^{-1}) = \Pi_1(-a^3)\Pi_1(b^{-1}) = (-\Pi_1(a))^3(\Pi_1(b))^{-1}$$
$$= -(a_0 + a_1 + a_2 + a_3)^3(b_0 + b_1 + b_2 + b_3)^{-1} = \frac{-(a_0^3 + a_1^3 + a_2^3 + a_3^3)}{(b_0 + b_1 + b_2 + b_3)}.$$

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

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

Proposition 3.2. *The discriminant $\triangle$ is invertible in $\mathbb{F}_{3^d}[\varepsilon]$ if and only if $\triangle_0' \not\equiv 0[3]$ and $\triangle_1' \not\equiv 0[3]$.*

Proof. We show easily that $\triangle = \triangle_0' + A\varepsilon + B\varepsilon^2 + (\triangle_1' - \triangle_0' - A - B)\varepsilon^3$ where $A = -a_0^3b_1$ and $B = -a_0^3b_2$, then from the Proposition 2.6 we deduce the result. □

Corollary 3.3. *If the discriminant $\triangle$ is invertible in $\mathbb{F}_{3^d}[\varepsilon]$, then we can talk about the elliptic curves $E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$ and $E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$ defined over the finite field $\mathbb{F}_{3^d}$ by:*

$$E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d}) = \{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_{3^d}) |\ y^2z = x^3 + a_0x^2z + b_0z^3\}, \text{ and}$$
$$E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d}) = \{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_{3^d}) |\ y^2z = x^3 + (\sum_{i=0}^{3} a_i)x^2z + (\sum_{i=0}^{3} b_i)z^3\}.$$

Proposition 3.4. *Let X, Y and Z be three elements in the ring $\mathbb{F}_{3^d}[\varepsilon]$, then $[X : Y : Z]$ is a point of $\mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$ if and only if $[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)]$ is a point of $\mathbb{P}^2(\mathbb{F}_{3^d})$, where $i \in \{0, 1\}$.*

Proof. Suppose that $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$, then there exist the triple $(\alpha_1, \alpha_2, \alpha_3) \in (\mathbb{F}_{3^d}[\varepsilon])^3$ such that $\alpha_1 X + \alpha_2 Y + \alpha_3 Z = 1$. Hence, we have:

$$\Pi_0(\alpha_1)\Pi_0(X) + \Pi_0(\alpha_2)\Pi_0(Y) + \Pi_0(\alpha_3)\Pi_0(Z) = 1, \text{ and}$$
$$\Pi_1(\alpha_1)\Pi_1(X) + \Pi_1(\alpha_2)\Pi_1(Y) + \Pi_1(\alpha_3)\Pi_1(Z) = 1.$$

So, $(\Pi_0(X), \Pi_0(Y), \Pi_0(Z)) \neq (0, 0, 0)$ and $(\Pi_1(X), \Pi_1(Y), \Pi_1(Z)) \neq (0, 0, 0)$, which proves that $[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_{3^d})$ for $i \in \{0, 1\}$.
Reciprocally, let $[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)] \in \mathbb{P}^2(\mathbb{F}_{3^d})$ where $i \in \{0, 1\}$. Suppose that $x_0 \not\equiv 0[3]$, then we distinguish between two cases of $\Pi_1(X) = x_0 + x_1 + x_2 + x_3$:

(1) $\Pi_1(X) \not\equiv 0[3]$: then X is invertible in $\mathbb{F}_{3^d}[\varepsilon]$, so the projective point $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$.
(2) $\Pi_1(X) \equiv 0[3]$: then $\Pi_1(Y) \not\equiv 0[3]$ or $\Pi_1(Z) \not\equiv 0[3]$.
   (i) If $\Pi_1(Y) \not\equiv 0[3]$ then:
   $x_0 + x_1\varepsilon + x_2\varepsilon^2 + (y_0 + y_1 + y_2 + y_3 - x_0 - x_1 - x_2)\varepsilon^3$
   $= x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 + (y_0 + y_1 + y_2 + y_3)\varepsilon^3$
   $= X + \varepsilon^3 Y \in (\mathbb{F}_{3^d}[\varepsilon])^\times$,
   so there exist $\Phi \in \mathbb{F}_{3^d}[\varepsilon]$: $\Phi X + \varepsilon^3 \Phi Y = 1$, hence $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$.
   (ii) If $\Pi_1(Z) \not\equiv 0[3]$ then:
   $x_0 + x_1\varepsilon + x_2\varepsilon^2 + (z_0 + z_1 + z_2 + z_3 - x_0 - x_1 - x_2)\varepsilon^3$
   $= x_0 + x_1\varepsilon + x_2\varepsilon^2 - (x_0 + x_1 + x_2)\varepsilon^3 + (z_0 + z_1 + z_2 + z_3)\varepsilon^3$
   $= X + \varepsilon^3 Z \in (\mathbb{F}_{3^d}[\varepsilon])^\times$,
   so there exist $\Phi' \in \mathbb{F}_{3^d}[\varepsilon]$: $\Phi' X + \varepsilon^3 \Phi' Z = 1$, hence $[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_{3^d}[\varepsilon])$.

In the case where $\Pi_0(Y) \not\equiv 0[3]$ or $\Pi_0(Z) \not\equiv 0[3]$, we follow the same proof. □

Example 3.5. Let $X = 1+\varepsilon+\varepsilon^2+2\varepsilon^3$, $Y = 1+2\varepsilon+\varepsilon^3$ and $Z = 2+\varepsilon+\varepsilon^2$ in $\mathbb{F}_3[\varepsilon]$, then $[X : Y : Z]$ is a point of $\mathbb{P}^2(\mathbb{F}_3[\varepsilon]) \Longleftrightarrow [\Pi_0(X) : \Pi_0(Y) : \Pi_0(Z)] = [1 : 1 : 2]$ and $[\Pi_1(X) : \Pi_1(Y) : \Pi_1(Z)] = [2 : 1 : 1]$ are two points of $\mathbb{P}^2(\mathbb{F}_3)$.

Proposition 3.6. *Let X, Y and Z in $\mathbb{F}_{3^d}[\varepsilon]$, if the point $[X : Y : Z]$ is a solution of the Weierstrass equation in $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ then $[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)]$ is a solution of the same equation in $E_{\Pi_i(a),\Pi_i(b)}(\mathbb{F}_{3^d})$, where $i \in \{0, 1\}$.*

Proof. From the Proposition 2.4 and the Corollary 2.5, we have:

$$Y^2 = y_0^2 + \Theta_{Y^2}\varepsilon + \Omega_{Y^2}\varepsilon^2 + ((\sum_{i=0}^{3} y_i)^2 - y_0^2 - \Theta_{Y^2} - \Omega_{Y^2})\varepsilon^3,$$

$$Z^2 = z_0^2 + \Theta_{Z^2}\varepsilon + \Omega_{Z^2}\varepsilon^2 + ((\sum_{i=0}^{3} z_i)^2 - z_0^2 - \Theta_{Z^2} - \Omega_{Z^2})\varepsilon^3,$$

$$aX^2 = a_0x_0^2 + \Theta_{aX^2}\varepsilon + \Omega_{aX^2}\varepsilon^2 + ((\sum_{i=0}^{3} a_i)(\sum_{i=0}^{3} x_i)^2 - a_0x_0^2 - \Theta_{aX^2} - \Omega_{aX^2})\varepsilon^3,$$

$$Z^3 = z_0^3 + (\sum_{i=1}^{3} z_i^3)\varepsilon^3.$$

Then:

$$Y^2Z = y_0^2z_0 + \Theta_{Y^2Z}\varepsilon + \Omega_{Y^2Z}\varepsilon^2 + ((\sum_{i=0}^{3} y_i)^2(\sum_{i=0}^{3} z_i) - y_0^2z_0 - \Theta_{Y^2Z} - \Omega_{Y^2Z})\varepsilon^3,$$

$$X^3 = x_0^3 + (\sum_{i=1}^{3} x_i^3)\varepsilon^3,$$

$$aX^2Z = a_0x_0^2z_0 + \Theta_{aX^2Z}\varepsilon + \Omega_{aX^2Z}\varepsilon^2 + ((\sum_{i=0}^{3} a_i)(\sum_{i=0}^{3} x_i)^2(\sum_{i=0}^{3} z_i) - a_0x_0^2z_0 - \Theta_{aX^2Z} - \Omega_{aX^2Z})\varepsilon^3,$$

$$bZ^3 = b_0z_0^3 + b_1Z_0^3\varepsilon + b_2Z_0^3\varepsilon^2 + ((\sum_{i=0}^{3} b_i)(\sum_{i=0}^{3} z_i^3) - b_0z_0^3 - b_1Z_0^3 - b_2Z_0^3)\varepsilon^3.$$

Hence,

$$Y^2Z = X^3+aX^2Z+bZ^3 \Longleftrightarrow \begin{cases} y_0^2z_0 = x_0^3 + a_0x_0^2z_0 + b_0z_0^3; \\ \Theta_{Y^2Z} = \Theta_{aX^2Z} + b_1Z_0^3; \\ \Omega_{Y^2Z} = \Omega_{aX^2Z} + b_2Z_0^3; \\ (\sum_{i=0}^{3} y_i)^2(\sum_{i=0}^{3} z_i) = (\sum_{i=1}^{3} x_i^3) + (\sum_{i=0}^{3} a_i)(\sum_{i=0}^{3} x_i)^2(\sum_{i=0}^{3} z_i) \\ \qquad\qquad + (\sum_{i=0}^{3} b_i)(\sum_{i=0}^{3} z_i^3). \end{cases}$$

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 $E_{\Pi_i(a),\Pi_i(b)}(\mathbb{F}_{3^d}[\varepsilon])$. □

Example 3.7. Let $E_{a,b} : Y^2Z = X^3 + aX^2Z + bZ^3$, where $a = 2 + \varepsilon + \varepsilon^2$ and $b = 1 + 2\varepsilon^2 + \varepsilon^3$ in $\mathbb{F}_3[\varepsilon]$, the discriminant $\triangle = -a^3b = 1 + 2\varepsilon^2 + 2\varepsilon^3$ is invertible in $\mathbb{F}_3[\varepsilon]$, because $\Pi_0(\triangle) = 1 \not\equiv 0[3]$ and $\Pi_1(\triangle) = 2 \not\equiv 0[3]$ then $E_{a,b}(\mathbb{F}_3[\varepsilon])$ is an elliptic curve.
Let $X = 1 + \varepsilon$, $Y = 1 + \varepsilon$ and $Z = 1$ in $\mathbb{F}_3[\varepsilon]$, the point $[X : Y : Z]$ is a solution of the Weierstrass equation $E_{a,b}$, then $[\Pi_0(X) : \Pi_0(Y) : \Pi_0(Z)] = [x, y, z] = [1 : 1 : 1]$ is a solution of equation:

$$E_{\Pi_0(a),\Pi_0(b)} : y^2z = x^3 + \Pi_0(a)x^2z + \Pi_0(b)z^3 = x^3 + 2x^2z + z^3,$$

and $[\Pi_1(X) : \Pi_1(Y) : \Pi_1(Z)] = [x, y, z] = [2 : 2 : 1]$ is a solution of equation:

$$E_{\Pi_1(a),\Pi_1(b)} : y^2z = x^3 + \Pi_1(a)x^2z + \Pi_1(b)z^3 = x^3 + x^2z + z^3.$$

From the propositions 3.2, 3.4 and 3.6, we deduce the following theorem:

Theorem 3.8. *Let X, Y and Z in $\mathbb{F}_{3^d}[\varepsilon]$. If $[X : Y : Z] \in E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ then $[\Pi_i(X) : \Pi_i(Y) : \Pi_i(Z)] \in E_{\Pi_i(a),\Pi_i(b)}(\mathbb{F}_{3^d})$, where $i \in \{0, 1\}$.*

Corollary 3.9. *The mappings $\overline{\Pi}_0$ and $\overline{\Pi}_1$ are well defined, where $\overline{\Pi}_i$ for $i \in \{0,1\}$ is given by:*

$$\overline{\Pi}_i : \left| \begin{array}{ccc} E_{a,b}(\mathbb{F}_{3^d}[\varepsilon]) & \longrightarrow & E_{\Pi_i(a),\Pi_i(b)}(\mathbb{F}_{3^d}) \\ [X:Y:Z] & \longmapsto & [\Pi_i(X):\Pi_i(Y):\Pi_i(Z)] \end{array} \right.$$

Proof. Let $[X:Y:Z] \in E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$. From the previous Theorem 3.8, we have $[\Pi_i(X):\Pi_i(Y):\Pi_i(Z)] \in E_{\Pi_i(a),\Pi_i(b)}(\mathbb{F}_{3^d})$ where $i \in \{0,1\}$.
If $[X:Y:Z] = [X':Y':Z']$ then there exist $\Psi \in (\mathbb{F}_{3^d}[\varepsilon])^\times$ such that: $X' = \Psi X$, $Y' = \Psi Y$ and $Z' = \Psi Z$, then:

$$\begin{aligned} \overline{\Pi}_i([X':Y':Z']) &= [\Pi_i(X'):\Pi_i(Y'):\Pi_i(Z')] \\ &= [\Pi_i(\Psi X):\Pi_i(\Psi Y):\Pi_i(\Psi Z)] \\ &= \underbrace{[\Pi_i(\Psi)\Pi_i(X):\Pi_i(\Psi)\Pi_i(Y):\Pi_i(\Psi)\Pi_i(Z)]}_{\Pi_i(\Psi)\in\mathbb{F}_{3^d}^*} \\ &= [\Pi_i(X):\Pi_i(Y):\Pi_i(Z)] \\ &= \overline{\Pi}_i([X:Y:Z]). \end{aligned}$$

So, the mapping $\overline{\Pi}_i$ is well defined with $i \in \{0,1\}$. □

Corollary 3.10. *The mapping $\overline{\Pi}_0$ is a surjective.*

Proof. Let $[x:y:z] \in E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$, then:

- ❖ If $y \not\equiv 0[3]$ then $[x:y:z] \sim [x:1:z]$ hence $[x(1+2\varepsilon+2\varepsilon^2+\varepsilon^3):1:z(1+2\varepsilon+2\varepsilon^2+\varepsilon^3)]$ is an antecedent of $[x:1:z]$.
- ❖ If $y \equiv 0[3]$ then $z \not\equiv 0[3]$ and $[x:y:z] \sim [x:0:1]$ hence $[x(1+2\varepsilon+2\varepsilon^2+\varepsilon^3):\varepsilon+\varepsilon^2+\varepsilon^3:1+2\varepsilon+2\varepsilon^2+\varepsilon^3]$ is an antecedent of $[x:0:1]$.

□

Corollary 3.11. *The mapping $\overline{\Pi}_1$ is a surjective.*

Proof. Let $[x:y:z] \in E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$ then:

- ❖ If $y \not\equiv 0[3]$ then $[x:y:z] \sim [x:1:z]$ hence $[x(\varepsilon+2\varepsilon^2+\varepsilon^3):1:z(\varepsilon+2\varepsilon^2+\varepsilon^3)]$ is an antecedent of $[x:1:z]$.
- ❖ If $y \equiv 0[3]$ then $z \not\equiv 0[3]$ and $[x:y:z] \sim [x:0:1]$ hence $[x(\varepsilon+2\varepsilon^2+\varepsilon^3):1+\varepsilon+2\varepsilon^2-\varepsilon^3:\varepsilon+2\varepsilon^2+\varepsilon^3]$ is an antecedent of $[x:0:1]$.

□

4. Classification of elements in $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$

In this section, we will classify the elements of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ 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. *Every element of the elliptic curve $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$ has one of the forms:*

(1) $[X:Y:1]$, *where* $X, Y \in \mathbb{F}_{3^d}[\varepsilon]$.

(2) $[x_1\varepsilon+x_2\varepsilon^2+x_3\varepsilon^3 : 1 : z_1\varepsilon+z_2\varepsilon^2+z_3\varepsilon^3]$, *such that* $[x_1+x_2+x_3 : 1 : z_1+z_2+z_3]$ *in* $E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$.
(3) $[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 - (1 + y_1 + y_2)\varepsilon^3 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$, *such that* $[x_1 + x_2 + x_3 : 0 : z_1 + z_2 + z_3]$ *in* $E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$.
(4) $[x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : 1 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, *such that* $[x_0 : 1 : z_0]$ *in* $E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$.
(5) $[x_0+x_1\varepsilon+x_2\varepsilon^2-\sum_{i=0}^{2} x_i\varepsilon^3 : y_1\varepsilon+y_2\varepsilon^2+y_3\varepsilon^3 : z_0+z_1\varepsilon+z_2\varepsilon^2-\sum_{i=0}^{2} z_i\varepsilon^3]$, *such that* $y_1 + y_2 + y_3 \not\equiv 0[3]$ *and* $[x_0 : 0 : 1]$ *in* $E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$.

Proof. Let $\mathcal{T} = [X : Y : Z]$ be a point in $E_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$, we have three cases of third projective coordinate Z:

(1) If Z is invertibe, then: $[X : Y : Z] \sim [X : Y : 1]$.
(2) If $Z = z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3$ where $(z_1, z_2, z_3) \in (\mathbb{F}_{3^d})^3$, then:
$\overline{\Pi}_0([X : Y : Z]) = [\Pi_0(X) : \Pi_0(Y) : \Pi_0(Z)] = [x_0 : y_0 : 0]$, so $x_0 \equiv 0[3]$ and $y_0 \not\equiv 0[3]$, hence
$[X : Y : Z] = [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$,
and there are two sub-cases of $y_1 + y_2 + y_3 \in \mathbb{F}_{3^d}$:
  (i) $y_1 + y_2 + y_3 \not\equiv -1[3]$, then $1 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ is invertible in $\mathbb{F}_{3^d}[\varepsilon]$, so we have:
  $[X : Y : Z] \sim [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3]$, where
  $[x_1 + x_2 + x_3 : 1 : z_1 + z_2 + z_3] \in E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$.
  (ii) $y_1+y_2+y_3 \equiv 1[3]$, then $1+y_1\varepsilon+y_2\varepsilon^2-(1+y_1+y_2)\varepsilon^3$ is not invertible in $\mathbb{F}_{3^d}[\varepsilon]$, so we have:
  $[X : Y : Z] = [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 + y_1\varepsilon + y_2\varepsilon^2 - (1 + y_1 + y_2)\varepsilon^3 : z_1\varepsilon+z_2\varepsilon^2+z_3\varepsilon^3]$, where $[x_1+x_2+x_3 : 0 : z_1+z_2+z_3] \in E_{\Pi_1(a),\Pi_1(b)}(\mathbb{F}_{3^d})$, then necessary $z_1 + z_2 + z_3 \not\equiv 0[3]$.
(3) If $Z = z_0 + z_1\varepsilon + z_2\varepsilon^2 - (z_0 + z_1 + z_2)\varepsilon^3$ where $(z_0, z_1, z_2) \in (\mathbb{F}_{3^d})^3$, then:
$\overline{\Pi}_1([X : Y : Z]) = [\Pi_1(X) : \Pi_1(Y) : \Pi_1(Z)] = [x_0 + x_1 + x_2 + x_3 : y_0 + y_1 + y_2 + y_3 : 0]$,
so $x_0 + x_1 + x_2 + x_3 \equiv 0[3]$ and $y_0 + y_1 + y_2 + y_3 \not\equiv 0[3]$, hence
$[X : Y : Z] = [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$,
so we have two sub-cases of $y_0 \in \mathbb{F}_{3^d}$:
  (i) $y_0 \not\equiv 0[3]$, then $y_0 + y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3$ is invertible in $\mathbb{F}_{3^d}[\varepsilon]$, then:
  $[X : Y : Z] \sim [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : 1 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, where $[x_0 : 1 : z_0] \in E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$.
  (ii) $y_0 \equiv 0[3]$, then $y_1\varepsilon+y_2\varepsilon^2+y_3\varepsilon^3$ is not invertible in $\mathbb{F}_{3^d}[\varepsilon]$, so we have:
  $[X : Y : Z] = [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : z_0 + z_1\varepsilon + z_2\varepsilon^2 - \sum_{i=0}^{2} z_i\varepsilon^3]$, where $[x_0 : 0 : z_0] \in E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$, then necessary $z_0 \not\equiv 0[3]$ and $[X : Y : Z] = [x_0 + x_1\varepsilon + x_2\varepsilon^2 - \sum_{i=0}^{2} x_i\varepsilon^3 : y_1\varepsilon + y_2\varepsilon^2 + y_3\varepsilon^3 : 1 + \alpha\varepsilon + \beta\varepsilon^2 - (1 + \alpha + \beta)\varepsilon^3]$, where $y_1 + y_2 + y_3 \not\equiv 0[3]$ and $[x_0 : 0 : 1] \in E_{\Pi_0(a),\Pi_0(b)}(\mathbb{F}_{3^d})$.

Which proves the proposition. □

Acknowledgement

The authors are deeply grateful to the referees and the editors for their kind comments on improving the presentation of this paper.

References

1. W. Bosma and H.W. Lenstra, *Complete System of Two Addition Laws for Elliptic Curves*, Journal of Number Theory, **53**(2), (1995), 229–240. https://doi.org/10.1006/jnth.1995.1088
2. A. Boulbot, A. Chillali and A. Mouhib, *Elliptic curves over the ring* $\mathbb{F}_q[e]$, $e^3 = e^2$, Gulf Journal of Mathematics, **4**(4), (2016), 123-129. https://doi.org/10.56947/gjom.v4i4.271
3. A. Boulbot, A. Chillali and A. Mouhib, *Elliptic curves over the ring R*, Boletim da Sociedade Paranaense de Matematica, **38**(3), (2017). https://doi.org/10.5269/bspm.v38i3.39868
4. A. Boulbot, A. Chillali and A. Mouhib, *Elliptic curve over a finite ring generated by* 1 *and an idempotent element* ε *with coefficients in the finite field* $\mathbb{F}_{3^d}$, Boletim da Sociedade Paranaense de Matematica, **40**, (2022). https://doi.org/10.5269/bspm.43654
5. A. Chillali, *Elliptic Curves of the Ring* $\mathbb{F}_q[\varepsilon]$, $\varepsilon^n = 0$, International Mathematical Forum, (2011).
6. N. Koblitz, *Elliptic curve cryptosystems*, Math. Compute. **48**, (1987), 203-209. https://doi.org/10.1090/S0025-5718-1987-0866109-5
7. V. Miller, *Use of elliptic curves in cryptography*. Advanced cryptology-CRYPTO'85, Lecture Notes in Computer Science, **218**. Springer, (1986), 417-426. https://doi.org/10.1007/3-540-39799-X_31
8. B. Selikh, D. Mihoubi and N. Ghadbane, *Classification of elements in elliptic curve over the ring* $\mathbb{F}_q[\varepsilon]$, Discussiones Mathematicae General Algebra and Applications, **41**(2), (2021), 283-298. https://doi.org/10.7151/dmgaa.1371
9. J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, **151**, Springer, (1994). https://doi.org/10.1007/978-1-4612-0851-8
10. M. Virat, *Courbe elliptique sur un anneau et applications cryptographiques*, PhD thesis, University of Nice-Sophia Antipolis, Nice, France, (2009).

[1] Laboratory of Pure and Applied Mathematics, Department of Mathematics, Mohamed Boudiaf University of M'sila, P.O. Box 166 Ichbilia, M'sila 28000, Algeria.

Email address: bilel.selikh@univ-msila.dz