Bol. Soc. Paran. Mat. (3s.) **v. 38** 3 (2020): 193–201.
©SPM –ISSN-2175-1188 ON LINE ISSN-00378712 IN PRESS
SPM: www.spm.uem.br/bspm doi:10.5269/bspm.v38i3.39868

Elliptic Curves Over the Ring R *

A. Boulbot, A. Chillali, A. Mouhib

ABSTRACT: Let $\mathtt{F}_q$ 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 $E_{a,b}(\mathtt{F}_q[e])$ over the ring $\mathtt{F}_q[e]$, where $e^2 = e$ and $(a,b) \in (\mathtt{F}_q[e])^2$. In a first time, we study the arithmetic of this ring. In addition, using the Weierstrass equation, we define the elliptic curve $E_{a,b}(\mathtt{F}_q[e])$ and we will show that $E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$ are two elliptic curves over the field $\mathtt{F}_q$, where π_0 and π_1 are respectively the canonical projection and the sum projection of coordinates of $X \in \mathtt{F}_q[e]$. Precisely, we give a bijection between the sets $E_{a,b}(\mathtt{F}_q[e])$ and $E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$.

Key Words: Finite field, Finite ring, Local ring, Elliptic curves, Cryptography.

Contents

1. Introduction

Let $\mathtt{F}_q$ be a finite field of order $q = p^d$ where d is a positive integer and $p \geq 5$ is a prime number. M. Virat see([9]) has studied the elliptic curve $E_{a,b}(\mathtt{F}_p[\epsilon])$ defined over the local ring $\mathtt{F}_p[\epsilon] := \mathtt{F}_p[X]/(X^2)$, where $\epsilon^2 = 0$ and $(a,b) \in (\mathtt{F}_p[\epsilon])^2$. A. Chillali see([2]) has generalized the work of M. Virat and extended it to the ring $\mathtt{F}_q[\epsilon] := \mathtt{F}_q[X]/(X^n)$ where $\epsilon^n = 0$. In this article, our objective is to study the elliptic curve defined over the ring $\mathtt{F}_q[X]/(X^2 - X)$. In section 2, we study the arithmetic of this ring, in particular we show that $\mathtt{F}_q[e]$ is not a local ring. In section 3, we define the elliptic curve $E_{a,b}(\mathtt{F}_q[e])$. The study of it's discriminant and it's Weierstrass equation, allows us to define two elliptic curves $E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)$

* USMBA, LSI, FP, Taza, Morocco
2010 *Mathematics Subject Classification:* 11T71, 14G50, 94A60.
Submitted October 01, 2017. Published November 19, 2017

and $E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$ defined over the finite field $\mathtt{F}_q$. In the next of this section, we classify the elements of $E_{a,b}(\mathtt{F}_q[e])$ and we give a bijection between the two sets $E_{a,b}(\mathtt{F}_q[e])$ and $E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)\times E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$ where π_0 and π_1 are two surjective morphisms of rings defined by:

$$\begin{array}{rcl} \pi_0: \mathtt{F}_q[e] & \longrightarrow & \mathtt{F}_q \\ x_0 + x_1 e & \longmapsto & x_0 \end{array} \quad \textit{and} \quad \begin{array}{rcl} \pi_1: \mathtt{F}_q[e] & \longrightarrow & \mathtt{F}_q \\ x_0 + x_1 e & \longmapsto & x_0 + x_1 \end{array}.$$

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

In this section, we follow the approach in [4], [3], [7], [8] and [9]. $\mathtt{F}_q$ is a finite field of order $q = p^d$ where d is a positive integer and p is a prime number. The ring $\mathtt{F}_q[e], e^2 = e$ can be constructed as an extension of the ring $\mathtt{F}_q$ by using the quotient ring of $\mathtt{F}_q[X]$ by the polynomial $X^2 - X$. An element $X \in \mathtt{F}_q[e]$ is represented by $X = x_0 + x_1 e$ where $(x_0, x_1) \in \mathtt{F}_q^2$.

2.1. Arithmetic operations

The arithmetic operations in $\mathtt{F}_q[e]$ can be decomposed into operations in $\mathtt{F}_q$ and they are computed as follows: $X + Y = (x_0 + y_0) + (x_1 + y_1)e$ and $X.Y = (x_0y_0) + (x_0y_1 + x_1y_0 + x_1y_1)e$, where $X = x_0 + x_1e$ and $Y = y_0 + y_1e$.
One can readily verify the following Lemmas:

Lemma 2.1. *$(\mathtt{F}_q[e], +, .)$ is a finite unitary commutative ring.*

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

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

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

Proof: We have: $(x_0 + x_1)(y_0 + y_1) - x_0y_0 = x_0y_1 + x_1y_0 + x_1y_1$. □

Corollary 2.4. *For all $X = x_0 + x_1e \in \mathtt{F}_q[e]$, we have:*

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

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

Proposition 2.5. *Let $X = x_0 + x_1e \in \mathtt{F}_q[e]$, then $X \in (\mathtt{F}_q[e])^\times$ if and only if $x_0 \neq 0$ and $x_0 + x_1 \neq 0$. The inverse is given by:*

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

Proof: Let $X = x_0 + x_1e$ and $Y = y_0 + y_1e$ be two elements of $\mathtt{F}_q[e]$. We have $X.Y = x_0y_0 + ((x_0 + x_1)(y_0 + y_1) - x_0y_0)e$, then:

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

$$\text{if and only if } \begin{cases} y_0 = x_0^{-1}, \ x_0 \neq 0 \\ y_1 = (x_0 + x_1)^{-1} - x_0^{-1}, \ x_0 + x_1 \neq 0 \end{cases}$$

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

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

□

Corollary 2.6. *Let $X \in \mathtt{F}_q[e]$, then X is not invertible if and only if $X = xe$ or $X = x - xe$, such that $x \in \mathtt{F}_q$.*

Now, we consider the two ideals of $\mathtt{F}_q[e]$, $I = \{xe \in \mathtt{F}_q[e] \mid x \in \mathtt{F}_q\}$ and $J = \{x - xe \in \mathtt{F}_q[e] \mid x \in \mathtt{F}_q\}$. It's clear that $I \cup J$ is the set of non invertible elements in $\mathtt{F}_q[e]$, and for all $(x, y) \in \mathtt{F}_q^2$ we have:

$$x - xe = ye \Rightarrow x - (x + y)e = 0 \Rightarrow x = x + y = 0 \Rightarrow x = y = 0,$$

so I and J are two distinct ideals of $\mathtt{F}_q[e]$ and $I \cup J$ is not an ideal. Finally, we have:

Lemma 2.7. *$\mathtt{F}_q[e]$ 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: Let $X = x_0 + x_1e$ and $Y = y_0 + y_1e$ be two elements of $\mathtt{F}_q[e]$. We have: $X + Y = (x_0 + y_0) + (x_1 + y_1)e$ and $X.Y = (x_0y_0) + ((x_0 + x_1)(y_0 + y_1) - x_0y_0)e$, then:

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

Finally, for all $x \in \mathtt{F}_q \subset \mathtt{F}_q[e]$, 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 $\mathtt{F}_q$ respectively, and let S, M and I denote the costs of addition, multiplication and inversion in $\mathtt{F}_q[e]$ respectively; we have $S = 2s$, $M = 2s + 4m$ and $I = s + 2i$. From the Proposition 2.3, we have $M = 3s+2m$, so $3s+2m < 2s+4m$, then the formula in the Proposition 2.3 is more efficient to compute the multiplication law in $\mathtt{F}_q[e]$.

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

In this section the prime number p is greater than or equal to 5, and the elements X, Y, Z, a and b are in the ring $\mathtt{F}_q[e]$ such that $X = x_0 + x_1e$, $Y = y_0 + y_1e$, $Z = z_0 + z_1e, a = a_0 + a_1e$ and $b = b_0 + b_1e$ where $x_0, x_1, y_0, y_1, z_0, z_1, a_0, a_1, b_0$ and b_1 are in $\mathtt{F}_q$. We denoted $\Delta := 4a^3 + 27b^2$, $\Delta_0 := \pi_0(\Delta) = 4a_0^3 + 27b_0^2$ and $\Delta_1 := \pi_1(\Delta) = 4(a_0 + a_1)^3 + 27(b_0 + b_1)^2$. For more details of an elliptic curves in characteristics 2 and 3, see the appendix A in [6].

3.1. The elliptic curves $E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$

Definition 3.1. *We define an elliptic curve over the ring $\mathtt{F}_q[e]$, as a curve in the projective space $\mathtt{P}^2(\mathtt{F}_q[e])$, which is given by the Weierstrass equation: $Y^2Z = X^3 + aXZ^2 + bZ^3$, where the discriminant Δ is invertible in $\mathtt{F}_q[e]$.*

Notation:
If Δ is invertible in $\mathtt{F}_q[e]$, we denote the elliptic curve over $\mathtt{F}_q[e]$ by $E_{a,b}(\mathtt{F}_q[e])$, and we write:

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

Proposition 3.2. $\Delta = \Delta_0 + (\Delta_1 - \Delta_0)e$.

From the Propositions 2.5 and 3.2, we deduce that:

Corollary 3.3. *Δ is invertible in $\mathtt{F}_q[e]$ if and only if $\Delta_0 \neq 0$ and $\Delta_1 \neq 0$.*

Corollary 3.4. *If Δ is invertible in $\mathtt{F}_q[e]$, then $E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)$ and $E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$ are two elliptic curves over the finite field $\mathtt{F}_q$, and we write:*

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

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

Proposition 3.5. *Let X, Y and Z in $\mathtt{F}_q[e]$, then $[X : Y : Z] \in \mathtt{P}^2\left(\mathtt{F}_q[e]\right)$ if and only if $[\pi_0(X) : \pi_0(Y) : \pi_0(Z)] \in \mathtt{P}^2\left(\mathtt{F}_q\right)$ and $[\pi_1(X) : \pi_1(Y) : \pi_1(Z)] \in \mathtt{P}^2\left(\mathtt{F}_q\right)$.*

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

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

(a) $x_0 + x_1 \neq 0$: then X is invertible in $\mathtt{F}_q[e]$, so $[X : Y : Z] \in \mathtt{P}^2\left(\mathtt{F}_q[e]\right)$.

(b) $x_0 + x_1 = 0$: then $y_0 + y_1 \neq 0$ or $z_0 + z_1 \neq 0$.

- **(i)** If $y_0 + y_1 \neq 0$ then:

$$x_0 + (y_0 + y_1 - x_0)\,e = x_0 - x_0e + (y_0 + y_1)\,e = X + eY \in \left(\mathtt{F}_q[e]\right)^{\times},$$

  so there exist $U \in \mathtt{F}_q[e]$: $UX + eUY = 1$, hence $[X : Y : Z] \in \mathtt{P}^2\left(\mathtt{F}_q[e]\right)$.

- **(ii)** If $z_0 + z_1 \neq 0$ then $X + eZ \in \left(\mathtt{F}_q[e]\right)^{\times}$, so $[X : Y : Z] \in \mathtt{P}^2\left(\mathtt{F}_q[e]\right)$.

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

Proposition 3.6. *Let X, Y and Z in $\mathbb{F}_q[e]$, then the point $[X : Y : Z]$ is a solution of the Weierstrass equation in $E_{a,b}(\mathbb{F}_q[e])$ if and only if $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)]$ is a solution of the same equation in $E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$ where $i \in \{0, 1\}$.*

Proof: We have:

$$Y^2Z = y_0^2z_0 + ((y_0 + y_1)^2(z_0 + z_1) - y_0^2z_0)e$$
$$X^3 = x_0^3 + ((x_0 + x_1)^3 - x_0^3)e$$
$$aXZ^2 = a_0x_0z_0^2 + ((a_0 + a_1)(x_0 + x_1)(z_0 + z_1)^2 - a_0x_0z_0^2)e$$
$$bZ^3 = b_0z_0^3 + ((b_0 + b_1)(z_0 + z_1)^3 - b_0z_0^3)e.$$

Or $\{1, e\}$ is a basis of $\mathbb{F}_q$ vector space $\mathbb{F}_q[e]$, then: $Y^2Z = X^3 + aXZ^2 + bZ^3$ if and only if $y_0^2z_0 = x_0^3 + a_0x_0z_0^2 + b_0z_0^3$ and $(y_0 + y_1)^2(z_0 + z_1) = (x_0 + x_1)^3 + (a_0 + a_1)(x_0 + x_1)(z_0 + z_1)^2 + (b_0 + b_1)(z_0 + z_1)^3$. □

From the Corollary 3.3, the Proposition 3.5 and the Proposition 3.6, we deduce the theorem:

Theorem 3.7. *Let X, Y and Z in $\mathbb{F}_q[e]$, then $[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[e])$ if and only if $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$, where $i \in \{0, 1\}$.*

Corollary 3.8. *The mappings $\widetilde{\pi_0}$ and $\widetilde{\pi_1}$ are well defined, where $\widetilde{\pi_i}$ for $i \in \{0, 1\}$ is given by:*

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

Proof: From the previous theorem, we have

$$[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q).$$

If $[X : Y : Z] = [X' : Y' : Z']$, then there exist $\Phi \in (\mathbb{F}_q[e])^\times$ such that: $X' = \Phi X$, $Y' = \Phi Y$ and $Z' = \Phi Z$, then:

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

□

3.2. 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 3.9. *Every element of* $E_{a,b}(\mathtt{F}_q[e])$ *is of the form* $[X : Y : 1]$ *or* $[xe : 1 : ze]$ *such that* $[x : 1 : z] \in E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$ *or* $[x - xe : 1 : z - ze]$ *such that* $[x : 1 : z] \in E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)$ *or* $[xe : y - ye : e]$ *such that* $y \neq 0$ *and* $[x : 0 : 1] \in E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$ *or* $[x - xe : ye : 1 - e]$ *such that* $y \neq 0$ *and* $[x : 0 : 1] \in E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)$. *We write:*

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

Proof: Let $P = [X : Y : Z] \in E_{a,b}(\mathtt{F}_q[e])$, where $X = x_0 + x_1 e$ and $Y = y_0 + y_1 e$. 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 $Z = ze$, where $z \in \mathtt{F}_q$, then $\tilde{\pi_0}\,([X : Y : Z]) = [x_0 : y_0 : 0]$, so $x_0 = 0$ and $y_0 \neq 0$; hence $[X : Y : Z] = [xe : 1 + ye : ze]$ and there are two sub-cases of $y \in \mathtt{F}_q$:
   (a) $y \neq -1$, then $1 + ye$ is invertible in $\mathtt{F}_q[e]$, so we have: $[X : Y : Z] \sim [xe : 1 : ze]$, where $[x : 1 : z] \in E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$.
   (b) $y = -1$, then $1 - e$ is not invertible in $\mathtt{F}_q[e]$, so we have: $[X : Y : Z] = [xe : 1 - e : ze]$, where $[x : 0 : z] \in E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$, then necessary $z \neq 0$, hence $[X : Y : Z] = [\alpha e : \beta - \beta e : e]$, where $\beta = z^{-1} \neq 0$ and $[\alpha : 0 : 1] \in E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$.
3. If $Z = z - ze$, where $z \in \mathtt{F}_q$, then $\tilde{\pi_1}\,([X : Y : Z]) = [x_0 + x_1 : y_0 + y_1 : 0]$, so $x_0 + x_1 = 0$ and $y_0 + y_1 \neq 0$; hence $[X : Y : Z] = [x - xe : y_0 + y_1 e : z - ze]$, where $y_0 + y_1 \neq 0$. We have two sub-cases of $y_0 \in \mathtt{F}_q$:
   (a) $y_0 \neq 0$, then $y_0 + y_1 e$ is invertible in $\mathtt{F}_q[e]$, so we have: $[X : Y : Z] \sim [x - xe : 1 : z - ze]$, where $[x : 1 : z] \in E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)$.
   (b) $y_0 = 0$, then $Y = ye$, where $y \neq 0$ is not invertible in $\mathtt{F}_q[e]$, so we have: $[X : Y : Z] = [x - xe : ye : z - ze]$, where $[x : 0 : z] \in E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)$, then necessary $z \neq 0$ and $[X : Y : Z] = [x - xe : ye : 1 - e]$, where $y \neq 0$ and $[x : 0 : 1] \in E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)$.

Which proves the proposition. □

From this proposition we deduce that:

Corollary 3.10. $\tilde{\pi_0}$ *is a surjective mapping.*

Proof: Let $[x : y : z] \in E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)$, then:

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

□

Corollary 3.11. *$\widetilde{\pi_1}$ is a surjective mapping.*

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

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

□

The next proposition gives a bijection between the two sets $E_{a,b}(\mathtt{F}_q[e])$ and $E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$.

Proposition 3.12. *The $\widetilde{\pi}$ mapping defined by:*

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

is a bijection.

Proof:

- ⋆ As $\widetilde{\pi_0}$ and $\widetilde{\pi_1}$ are well defined, then $\widetilde{\pi}$ is well defined.
- ⋆ Let $([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]) \in E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$, then $[x_0 + (x_1 - x_0)\, e : y_0 + (y_1 - y_0)\, e : z_0 + (z_1 - z_0)\, e] \in E_{a,b}\,(\mathtt{F}_q[e])$ and it is clear that

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

  hence $\widetilde{\pi}$ is a surjective mapping.
- ⋆ Lets $[X : Y : Z]$ and $[X' : Y' : Z']$ be elements of $E_{a,b}(\mathtt{F}_q[e])$, where $X = x_0 + x_1 e, Y = y_0 + y_1 e, Z = z_0 + z_1 e, X' = x'_0 + x'_1 e, Y' = y'_0 + y'_1 e$ and $Z' = z'_0 + z'_1 e$. If $[x_0 : y_0 : z_0] = [x'_0 : y'_0 : z'_0]$ and $[x_0 + x_1 : y_0 + y_1 : z_0 + z_1] = [x'_0 + x'_1 : y'_0 + y'_1 : z'_0 + z'_1]$, then there exist $(\alpha, \beta) \in \left(\mathtt{F}_q^*\right)^2$ such

that: $\begin{cases} x_0' = \alpha x_0 \\ y_0' = \alpha y_0 \\ z_0' = \alpha z_0 \end{cases}$ and $\begin{cases} x_0' + x_1' = \beta\,(x_0 + x_1) \\ y_0' + y_1' = \beta\,(y_0 + y_1) \\ z_0' + z_1' = \beta\,(z_0 + z_1) \end{cases}$, so $\begin{cases} x_1' = (\beta - \alpha)\,x_0 + \beta x_1 \\ y_1' = (\beta - \alpha)\,y_0 + \beta y_1 \\ z_1' = (\beta - \alpha)\,z_0 + \beta z_1 \end{cases}$,

then:

$$\begin{cases} X' = \alpha x_0 + ((\beta - \alpha)\,x_0 + \beta x_1)\,e = (\alpha + (\beta - \alpha)\,e)\,X \\ Y' = \alpha y_0 + ((\beta - \alpha)\,y_0 + \beta y_1)\,e = (\alpha + (\beta - \alpha)\,e)\,Y \\ Z' = \alpha z_0 + ((\beta - \alpha)\,z_0 + \beta z_1)\,e = (\alpha + (\beta - \alpha)\,e)\,Z \end{cases}.$$

Or $\alpha + (\beta - \alpha)\,e$ is invertible in $\mathtt{F}_q[e]$, so $[X' : Y' : Z'] = [X : Y : Z]$, hence $\widetilde{\pi}$ is an injective mapping.

We can easily show that the mapping $\widetilde{\pi}^{-1}$ defined by:

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

is the inverse of $\widetilde{\pi}$. □

Corollary 3.13. *The cardinal of $E_{a,b}(\mathtt{F}_q[e])$ is equal to the cardinal of*

$$E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q) \times E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q).$$

3.3. Example

In $\mathtt{F}_5[e]$, lets $a = 1 + 3e$ and $b = 1 + 2e$. We have:

$$\begin{aligned} E_{a,b}(\mathtt{F}_5[e]) = \{&[0 : 1 : 0], [0 : 1 : 1 + 4e], [0 : 1 : 4 + e], [2 : 1 + e : 1], \\ &[2 : 1 + 2e : 1], [2 : 4 + 3e : 1], [2 : 4 + 4e : 1], [e : 1 : 3e], \\ &[2e : 1 + e : 1], [2e : 1 + 2e : 1], [2e : 4 + 3e : 1], [2e : 4 + 4e : 1], \\ &[4e : 1 : 2e], [2 + 3e : 1 : 1 + 4e], [2 + 3e : 1 : 3 + 2e], \\ &[2 + 3e : 1 : 4 + e], [3 + 2e : 1 : 1 + 4e], [3 + 2e : 1 : 2 + 3e], \\ &[3 + 2e : 1 : 4 + e], [3 + 4e : 1 + e : 1], [3 + 4e : 1 + 2e : 1], \\ &[3 + 4e : 4 + 3e : 1], [3 + 4e : 4 + 4e : 1], [4 + 3e : 2 : 1], \\ &[4 + 3e : 3 : 1], [4 + 3e : 2 + e : 1], [4 + 3e : 3 + 4e : 1]\}, \\ E_{1,1}(\mathtt{F}_5) = \{&[0 : 1 : 0], [0 : 1 : 1], [0 : 4 : 1], [2 : 1 : 1], [2 : 4 : 1], [3 : 1 : 1], \\ &[3 : 4 : 1], [4 : 2 : 1], [4 : 3 : 1]\}, \\ E_{4,3}(\mathtt{F}_5) = \{&[0 : 1 : 0], [2 : 2 : 1], [2 : 3 : 1]\}, \end{aligned}$$

so $card(E_{a,b}(\mathtt{F}_5[e])) = 27, card(E_{1,1}(\mathtt{F}_5)) = 9$ and $card(E_{4,3}(\mathtt{F}_5)) = 3$.

3.4. Cryptography applications

In cryptography applications, we have:

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

4. Conclusion

In this work, we have proved the bijection between $E_{a,b}(\mathtt{F}_q[e])$ and $E_{\pi_0(a),\pi_0(b)}(\mathtt{F}_q)\times E_{\pi_1(a),\pi_1(b)}(\mathtt{F}_q)$. For the group law over $E_{a,b}(\mathtt{F}_q[e])$ see the explicit formulas in the article of [1], [pages : 236-238].

Acknowledgments

The author gratefully acknowledges that his research is supported by Sidi Mohamed Ben Abdellah University, Polydisciplinary Faculty of Taza (FPT), and the Laboratory of Engineering Sciences (LSI) at FP, Taza, Morocco. We thank the referee by your suggestions.

References

1. W. Bosma, H. W. Lenstra, *Complete System of Two Addition Laws for Elliptic Curves*, Journal of Number Theory, Volume 53, Series B, Pages 229-240 (1995).
2. A. Chillali, *Cryptosystème à clef publique et courbes elliptique sur l'anneau* $\mathtt{F}_q[\varepsilon]$, $\varepsilon^n = 0$, Université Sidi Mohamed Ben Abdellah, Fès, Maroc (2013).
3. A. Chillali, *Cryptography over elliptic curve of the ring*, World Academy of Science, Engineering and Technology, Volume 78, Pages 848-850 (2011).
4. M. H. Hassib, A. Chillali, M. A. Elomary, *Elliptic curves over a chain ring of characteristic 3*, Journal of Taibah University for Science, 40(9), pages 1687-1700 (2015).
5. H. W. Lenstra, *Elliptic Curves and Number-Theoretic Algorithms*, Processing of the International Congress of Mathematicians, Berkely, California,USA, Volume 29, No. 2, Pages 156-163 (1986).
6. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer-Verlag, New York, Volume 106 (1986).
7. A. Tadmori, A. Chillali, M. Ziane, *Elliptic Curve over Ring* $A_4 = \mathtt{F}_2^d[\varepsilon]$, $\varepsilon^4 = 0$, Applied Mathematical Sciences, Volume 9, Issue 33, Pages 1721-1733(2015).
8. A. Tadmori, A. Chillali, M. Ziane, *The binary operations calculus in* $E_{a,b,c}$, International Journal of Mathematical Models and Methods in Applied Sciences, Volume 9, Pages 171-175(2015).
9. M. Virat, *Courbe elliptique sur un anneau et applications cryptographiques*, Université Nice-Sophia Antipolis, Nice, France(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