Gulf Journal of Mathematics
Vol 3, Issue 2 (2015) 49-53

THE ELLIPTIC CURVE $E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$

A. CHILLALI[1*] AND S. ABDELALIM[2]

Abstract. In this paper, we study the elliptic curve $E_{a,b}$ over ring $\mathbb{F}_p[e_1, e_2, e_3]$, where $e_ie_i = e_i$ and $e_ie_j = 0$ if $i \neq j$. We characterize the invertible elements of $\mathbb{F}_p[e_1, e_2, e_3]$, and we determine the relation between $E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$ and $E_{a,b}(\mathbb{F}_p)$. Finally we show that $Card(E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])) \geq (Card(E_{a,b}(\mathbb{F}_p)) - 3)^3 + Card(E_{a,b}(\mathbb{F}_p))$.

1. Introduction

Let p be a prime number, we consider the ring $\mathbb{F}_p[e_1, e_2, e_3] = \{a_0 + a_1e_1 + a_2e_2 + a_3e_3/a_0, a_1, a_2, a_3 \in \mathbb{F}_p,\ e_ie_i = e_i \text{ and } e_ie_j = 0 \text{ if } i \neq j\}$, $\mathbb{F}_p[e_1, e_2, e_3]$ is vector space over $\mathbb{F}_p$ with basis $(1, e_1, e_2, e_3)$. Let $X, Y \in \mathbb{F}_p[e_1, e_2, e_3]$ with $X = x_0 + x_1e_1 + x_2e_2 + x_3e_3$ and $Y = y_0 + y_1e_1 + y_2e_2 + y_3e_3$, we have: $X + Y = x_0 + y_0 + (x_1 + y_1)e_1 + (x_2 + y_2)e_2 + (x_3 + y_3)e_3$ and $XY = t_0 + t_1e_1 + t_2e_2 + t_3e_3$ where $t_i = \begin{cases} x_0y_0 & \text{if } i = 0 \\ x_0y_i + x_iy_0 + x_iy_i & \text{if } i \neq 0. \end{cases}$

Proposition 1.1. *If $X \in \mathbb{F}_p[e_1, e_2, e_3]$ with $X = x_0+x_1e_1+x_2e_2+x_3e_3$, then X is invertible in $\mathbb{F}_p[e_1, e_2, e_3]$ if and only if $x_0 \in \mathbb{F}_p^*$ and $x_i \neq -x_0$ for all $i \in \{1, 2, 3\}$.*

Proof. Let $X \in \mathbb{F}_p[e_1, e_2, e_3]$, such that $X = x_0 + x_1e_1 + x_2e_2 + x_3e_3$ is invertible then there exist $Y \in \mathbb{F}_p[e_1, e_2, e_3]$ such that $Y = y_0 + y_1e_1 + y_2e_2 + y_3e_3$ and $XY = t_0+t_1e_1+t_2e_2+t_3e_3$. We have: $t_0 = x_0y_0 = 1$ and $t_i = x_0y_i+x_iy_0+x_iy_i = 0$, *for all* $1 \leq i \leq 3$ so, $y_0 = x_0^{-1} \in \mathbb{F}_p$. Assumes that $x_i = -x_0$ for all $i \in \{1, 2, 3\}$. Then $t_i = x_0y_i - x_0y_0 - x_0y_i = -x_0y_0 = -1 = 0$ which is absurd,we result that $x_0 \in \mathbb{F}_p^*$ and $x_i \neq -x_0$ for all$1 \leq i \leq 3$. Let $x_0 \in \mathbb{F}_p^*$ such that $x_0 \neq -x_i$ for all $1 \leq i \leq 3$, then $(x_0 + x_i) \in \mathbb{F}_p^*$. And let $Y = y_0 + y_1e_1 + y_2e_2 + y_3e_3$ such that $y_i = \begin{cases} x_0^{-1} & \text{if } i = 0 \\ -(x_0 + x_i)^{-1}x_iy_0 & \text{if } i \neq 0 \end{cases}$. We have $XY = t_0+t_1e_1+t_2e_2+t_3e_3$, then

$$\begin{aligned} t_0 &= x_0y_0 \\ &= x_0x_0^{-1} \\ &= 1 \end{aligned}$$

and for all $1 \leq i \leq 3$, we have:

Date: Received: Feb 28, 2015.

* Corresponding author.

2010 *Mathematics Subject Classification.* 14H52, 94A60, 11T71.

Key words and phrases. Finite Ring, Elliptic Curves, Chain Ring, Isomorphism.

$$\begin{array}{rcc} t_i & = & x_0y_i + x_iy_0 + x_iy_i \\ & = & (x_i + x_0)y_i + x_iy_0 \\ & = & (x_i + x_0)(-(x_0 + x_i)^{-1}x_iy_0) + x_iy_0 \\ & = & -(x_iy_0) + x_iy_0 \\ & = & 0. \end{array}$$

We deduce that X is invertible. □

2. The Elliptic Curve $E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$

In this section we will study various propriety over the elliptic curve $E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$ over the ring $\mathbb{F}_p[e_1, e_2, e_3]$. We show that if $[x : 1 : z] \in E_{a,b}(\mathbb{F}_p)$ then $[xe_i : 1 : ze_i] \in E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$ and $Card(E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])) \geq (Card(E_{a,b}(\mathbb{F}_p)) - 3)^3 + Card(E_{a,b}(\mathbb{F}_p))$. Let $a, b \in \mathbb{F}_p$ we denote in [1], [2], [3] and [6]:

$$E_{a,b}(\mathbb{F}_p) = \{[x : y : z] \in P^2(\mathbb{F}_p)/y^2z = x^3 + axz^2 + bz^3\}$$

$$E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3]) = \{[X : Y : Z] \in P^2(\mathbb{F}_p[e_1, e_2, e_3])/Y^2Z = X^3 + aXZ^2 + bZ^3\}.$$

Theorem 2.1. *Let p a prime number. The following properties are equivalent:*

(1) $([x : y : z], [x_1 : y, z_1]) \in (E_{a,b}(\mathbb{F}_p))^2$

(2) $([xe_i : y : ze_i], [x_1e_j : y : z_1e_j]) \in (E_{(a,b)}(\mathbb{F}_p[e_1, e_2, e_3]))^2$ *with* $i, j \in \{1, 2, 3\}$ *and* $i \neq j$.

(3) $[xe_i + x_1e_j : y : ze_i + z_1e_j] \in E_{(a,b)}(\mathbb{F}_p[e_1, e_2, e_3])$ *with* $i, j \in \{1, 2, 3\}$ *and* $i \neq j$.

Proof. **(1) $\Longleftrightarrow$ (2)**

$([x : y : z], [x_1 : y, z_1]) \in (E_{a,b}(\mathbb{F}_p))^2$ if only if $zy^2 = x^3 + axz^2 + bz^3$ and $z_1y^2 = x_1^3 + ax_1z_1^2 + bz_1^3$. It is clear that:

$$\begin{array}{rcc} (xe_i)^3 & = & x^3e_i \\ (ze_i)y^2 & = & zy^2e_i \\ axe_i(ze_i)^2 & = & axz^2e_i \\ b(ze_i)^3 & = & bz^3e_i. \end{array}$$

So, we have: $zy^2e_i = x^3e_i + axz_1^2e_i + bz^3e_i$ if only if $(ze_i)y^2 = (xe_i)^3 + a(xe_i)(ze_i)^2 + b(ze_i)^3$ i.e, $[xe_i : y : ze_i] \in E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$.

(2) $\Longleftrightarrow$ (3) Let $([xe_i : y : ze_i], [x_1e_j : y : z_1e_j]) \in (E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3]))^2$ with $i, j \in \{1, 2, 3\}$ and $i \neq j$. We have:

$$\begin{array}{rcc} (xe_i + x_1e_j)^3 & = & (xe_i)^3 + 3(xe_i)^2x_1e_j + 3(e_i(x_1e_j)^2 + (x_1e_j)^3 \\ & = & (xe_i)^3 + (x_1e_j)^3 \\ (ze_i + z_1e_j)^3 & = & (ze_i)^3 + 3(ze_i)^2x_1e_j + 3(e_i(z_1e_j)^2 + (z_1e_j)^3 \\ & = & ze_i)^3 + (z_1e_j)^3 \\ a(xe_i + x_1e_j)(ze_i + z_1e_j)^2 & = & a(xe_i + x_1e_j)((ze_i)^2 + 2(ze_i)(z_1e_j)^2 + (z_1e_j)^2) \\ & = & a(xe_i + x_1e_j)((ze_i)^2 + (z_1e_j)^2) \\ & = & a(xe_i)(ze_i)^2 + a(x_1e_j)(z_1e_j)^2) \end{array}$$

then

$$\begin{array}{rcl}(ze_i)y^2 & = & (xe_i)^3+a(xe_i)(ze_i)^2+b(ze_i)^3\\ (z_1e_j)y^2 & = & (x_1e_j)^3+a(x_1e_j)(z_1e_j)^2+b(z_1e_j)^3\\ (ze_i)y^2+(z_1e_j)y^2 & = & (xe_i)^3+(x_1e_j)^3+a(xe_i)(ze_i)^2+a(x_1e_j)(z_1e_j)^2+b(ze_i)^3+b(z_1e_j)^3\\ (ze_i+z_1e_j)y^2 & = & (xe_i+x_1e_j)^3+a(xe_i+x_1e_j)(ze_i+z_1e_j)^2+b(ze_i+z_1e_j)^3\end{array}$$

so, $[xe_i+x_1e_j : y : ze_i+z_1e_j]\in E_{a,b}(\mathbb{F}_p[e_1,e_2,e_3])$. □

Lemma 2.2. *Let π be a homomorphism from $\mathbb{F}_p[e_1,e_2,e_3]$ to $\mathbb{F}_p$ defined by:*

$$\begin{array}{ccc}\mathbb{F}_p[e_1,e_2,e_3] & \xrightarrow{\pi} & \mathbb{F}_p\\ a_0+a_1e_1+a_2e_2+a_3e_3 & \mapsto & a_0\end{array}$$

π is a surjective homomorphism of rings.

Proof. Let X,Y be two elements of the ring $\mathbb{F}_p[e_1,e_2,e_3]$ such that $X=x_0+x_1e_1+x_2e_2+x_3e_3$ and $Y=y_0+y_1e_1+y_2e_2+y_3e_3$. We have:

$$\begin{array}{rcl}X+Y & = & x_0+y_0+(x_1+y_1)e_1+(x_2+y_2)e_2+(x_3+y_3)e_3\\ \textit{and}\quad XY & = & x_0y_0+(x_0y_1+x_1y_0+x_1y_1)e_1+(x_0y_2+x_2y_0+x_2y_2)e_2+(x_0y_3+x_3y_0+x_3y_3)e_3\end{array}$$

then

$$\begin{array}{rcl}\pi(X+Y) & = & x_0+y_0\\ & = & \pi(X)+\pi(Y)\\ \textit{and}\quad \pi(XY) & = & x_0y_0\\ & = & \pi(X)\pi(Y)\end{array}$$

We deduce that π is an homomorphism. Let $a\in\mathbb{F}_p$ then $a\in\mathbb{F}_p[e_1,e_2,e_3]$ and $\pi(a)=a$. We result that π is surjective homomorphism. □

Corollary 2.3. *If $b=t^2$ with $t\in\mathbb{F}_p$ then $[0:t:e_i]\in E_{a,b}(\mathbb{F}_p[e_1,e_2,e_3])$ for all $i\in\{1,2,3\}$.*

Proposition 2.4. *Let $[0:1:ze_i],[0:1:z_1e_j]\in E_{a,b}(\mathbb{F}_p[e_1,e_2,e_3])$.*
If $i\neq j$ then $[0:1:ze_i]+[0:1:z_1e_j]=[0:1:ze_i+z_1e_j]$ else

$[0:1:ze_i]+[0:1:z_1e_j]=[a^2(z^2z_1+zz_1^2)e_i : 1+(-a^3-9b^2)z^2z_1^2e_i : (1+3bzz_1)(z+z_1)e_i]$.

Proof. By using the explicit formulas of W. Bosma and H. Lenstra (see [8], [4] and [5]). □

Proposition 2.5. *If $[X:Y:Z]\in E_{a,b}(\mathbb{F}_p[e_1,e_2,e_3])$ then $[\pi(X):\pi(Y):\pi(Z)]\in E_{a,b}(\mathbb{F}_p)$.*

Proof. Let $[X:Y:Z]\in E_{a,b}(\mathbb{F}_p[e_1,e_2,e_3])$ then $Y^2Z=X^3+aZ^2X+bZ^3$.
We have:

$$\pi(Y^2Z)=\pi(X^3)+\pi(aZ^2X)+\pi(bZ^3)$$

so,

$$(\pi(Y))^2\pi(Z)=(\pi(X))^3+\pi(a)(\pi(Z))^2\pi(X)+\pi(b)(\pi(Z))^3.$$

We deduce that $[\pi(X):\pi(Y):\pi(Z)]\in E_{a,b}(\mathbb{F}_p)$. □

Theorem 2.6. *Let a and b two elements of the ring $\mathbb{F}_p$ then*

$$Card(E_{a,b}(\mathbb{F}_p[e_1,e_2,e_3]))\geq(Card(E_{a,b}(\mathbb{F}_p))-3)^3+Card(E_{a,b}(\mathbb{F}_p)).$$

Proof. We consider the set:

$$\begin{aligned} T &= \{[x:y:z] \in P^2(\mathbb{F}_p)/y^2z = x^3 + axz^2 + bz^3 \ \texttt{and} \ y = 0\} \\ &= \{[x:0:z] \in P^2(\mathbb{F}_p)/0 = x^3 + axz^2 + bz^3\} \\ &= \{[xz^{-1}:0:1] \in P^2(\mathbb{F}_p)/0 = (xz^{-1})^3 + axz^{-1} + b\} \\ &= \{[x:0:1] \in P^2(\mathbb{F}_p)/0 = x^3 + ax + b\} \end{aligned}$$

then $Card(T)$ is exactly the number of the solution of the equation $0 = x^3 + ax + b$, therefore $Card(T) \leq 3$. We put

$$\begin{aligned} G &= (E_{a,b}(\mathbb{F}_p)) \setminus T \\ &= \{[x:y:z] \in P^2(\mathbb{F}_p)/y^2z = x^3 + axz^2 + bz^3 \ \texttt{and} \ y \neq 0\} \\ &= \{[x:1:z] \in P^2(\mathbb{F}_p)/z = x^3 + axz^3 + bz^3\} \\ &= \{[x:1:z] \in P^2(\mathbb{F}_p)/[x:1:z] \in E_{a,b}(\mathbb{F}_p)\} \end{aligned}$$

then $Card(G) \geq Card(E_{a,b}(\mathbb{F}_p)) - 3$. Now let α be a map from G to $E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$ defined by:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\alpha} & E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3]) \\ ([x_1:1:z_1], [x_2:1:z_2], [x_3:1:z_3]) & \mapsto & [x_1e_1 + x_2e_2 + x_3e_3 : 1 : z_1e_1 + z_2e_2 + z_3e_3] \end{array}$$

We have:

$$(x_1e_1 + x_2e_2 + x_3e_3)^3 = (x_1e_1)^3 + (x_2e_2)^3 + (x_3e_3)^3$$

$$(z_1e_1 + z_2e_2 + z_3e_3)^2 = (z_1e_1)^2 + (z_2e_2)^2 + (z_3e_3)^2$$

$$a(x_1e_1+x_2e_2+x_3e_3)(z_1e_1+z_2e_2+z_3e_3)^2 = a(x_1e_1)((z_1e_1)^2)+a(x_2e_2)((z_2e_2)^2)+a(x_3e_3)((z_3e_3)^2$$

Since $[x_i : 1 : z_i] \in E_{a,b}(\mathbb{F}_p)$ then $z_i = x_i^3 + ax_iz_i^2 + bz_i^3$. It is clear that

$$\begin{aligned} z_ie_i &= (x_ie_i)^3 + a(x_ie_i)(z_ie_i)^2 + b(z_ie_i)^3, \forall i \in \{1,2,3\} \\ \sum_{i=1}^{3} z_ie_i &= \sum_{i=1}^{3}(x_ie_i)^3 + a\sum_{i=1}^{3}(x_ie_i)(z_ie_i)^2 + b\sum_{i=1}^{3}(z_ie_i)^3 \\ &= (\sum_{i=1}^{3}(x_ie_i))^3 + a(\sum_{i=1}^{3}(x_ie_i))(\sum_{i=1}^{3}(z_ie_i))^2 + b(\sum_{i=1}^{3}(z_ie_i))^3 \end{aligned}$$

we deduce that $[x_1e_1 + x_2e_2 + x_3e_3 : 1 : z_1e_1 + z_2e_2 + z_3e_3] \in E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$.

α is injective. Indeed

$$E_{a,b}(\mathbb{F}_p) \subset E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3]),$$

$$\alpha(G^3) \subset E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$$

and

$$\alpha(G^3) \cap E_{a,b}(\mathbb{F}_p) = \{[0:1:0]\}.$$

We result that $Card(E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])) \geq card(\alpha(G^3)) + Card(E_{a,b}(\mathbb{F}_p)) - 1$. Since α is injective then $card(\alpha(G^3)) = Card(G)^3 \geq (card(E_{a,b}(\mathbb{F}_p)) - 3)^3$, we deduce that $Card(E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])) \geq (Card(E_{a,b}(\mathbb{F}_p)) - 3)^3 + Card(E_{a,b}(\mathbb{F}_p))$. □

3. Cryptographic Applications

In this section, we give hastily, some results in cryptography, other more practical applications, will be given in our future work. We deduce the following results:

- The Cardinal of $E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$ is bigger than that of $E_{a,b}(\mathbb{F}_p)$.
- The Discrete Logarithm Problem, [7], on the elliptic curve $E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$ is equivalent to the one on $E_{a,b}(\mathbb{F}_p)$.

4. Conclusion

In this work, we have extended the results of elliptic curve over $\mathbb{F}_p[e_1, e_2, e_3]$, and we deduce that the Discrete Logarithm Problem (DLP) on this elliptic curve is equivalent to the one on $E_{a,b}(\mathbb{F}_p)$ but the Cardinal of this elliptic curve is bigger than that of $E_{a,b}(\mathbb{F}_p)$.

References

1. A. Chillali; *Elliptic curve over ring*, International Mathematical Forum, Vol.6, no.31 (2011), 1501-1505.
2. A. Tadmori, A. Chillali and M. Ziane; *Elliptic Curves Over SPIR of characteristic Two*, Proceeding of the 2013 international conference on applied mathematics and Computational Methode, AMCM-05 (2013), 41-44.
3. J.H. Silverman; *The Arithmetic of Elliptic curves*, Graduate Texts in Mathematcs, 106 Springer (1985).
4. J.H. Silverman; *Advanced Topics in the Arithmetic of Elliptic curves*, Graduate Texts in Mathematics, Volume 151, Springer (1994).
5. J. Lenstra; *Elliptic curves and number-theoretic algorithms*, Proceeding of the International Congress of Mathematicians, Berkely, California, USA, (1986).
6. M. Virat; *Courbe elliptique sur un anneau et applications cryptographiques*, These Docteur en Sciences, Nice-Sophia Antipolis (2009).
7. N. Koblitz; *Elliptic Curve Cryptosystems*, Math. Comp. 48 (1987), 203-209.
8. W. Bosma and H. Lenstra; *Complete system of two addition laws for elliptic curved*, Journal of Number theory, 53 (1995) 229-240.

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

[2]Department of Mathematical and Computer Sciences, Labo TAGESUP, Faculty of Sciences Ain Choc, University of Hassan II Casablanca, Morocco.
E-mail address: seddikabd@hotmail.com