Elliptic Curve Over $\mathbb{F}_p[i]$

Seddik.Abdelalim, Abdelhakim. Chillali and Said. Elhajji

Abstract—In this paper we study the elliptic curve $E_{a,b}$ and $E_{a,-b}$ over ring $\mathbb{F}_p[\, i]$, where $i^2 = -1$. More precisely we will establish a isomorphism between $E_{a,b}$and $E_{a,-b}$. After we define an internal composition law$*$ on the set$\mathrm{E} = \mathrm{E}_{\mathrm{a,b}} \cup \mathrm{E}_{\mathrm{a,-b}}$ and we proof that $\mathrm{Card(E)} = 2\mathrm{Card}(\mathrm{E}_{\mathrm{a,b}}) - 1$. At the end we give an example of cryptography.

Keywords—Ellipticcurves,Ring, Finite Field,Isomorphism.

I. INTRODUCTION

Let p be a prime number. We consider the ring

$$A = \{\, a + ib \,/ a, b \in \mathbb{F}_p, \qquad i^2 = -1\}.$$

$A$is vector space with basis $(1, i)$.

Lemma 1.1:
$a + ib$is invertible in$\mathbb{F}_p[\, i]$ if and only if $a^2 + b^2 \neq 0\ [p]$
Proof:
$\Longrightarrow$)Let $a + ib$be invertible then there exist$c + id in$ $\mathbb{F}_p[\, i]$ such that$(a + ib)(c + id) = 1$.
So, $ac - bd + i(bc + ad) = 1$, therefore$\begin{cases} ac - bd = 1 \\ bc + ad = 0 \end{cases}$.
We have

$$(a + ib)(a - ib)(c + id)(c - id) = (a^2 + b^2)(c^2 + d^2)$$

and

$$(a + ib)(a - ib)(c + id)(c - id) = (a - ib)(c - id) = 1$$

We deduce $(a^2 + b^2)(c^2 + d^2) = 1$, so $a^2 + b^2 \neq 0\ [p]$
$\Longleftarrow$)Assume$a^2 + b^2 \neq 0\ [p]$then there exist $t$in$\mathbb{F}_p$such that $(a^2 + b^2)t = 1$. We can write$(a + ib)(a - ib)t = 1$■

Lemma 1.2:
Let $p$be a prime number. Then the following propriety are equivalent:

1. $\mathbb{F}_p[\, i]$is field
2. $p \neq 1$ and $p \neq 3\ [4]$

Proof:

$$1 \Longleftarrow 2)$$

Assume that $\mathbb{F}_p[\, i]$ isn't field then there exist $a + ib$is not invertible.

This work was supported in part by the Laboratory of Mathematics, Computing and Application , Faculty of sciences University of Mohamed V Agdal, BP.1014 . Rabat, Morocco.
S. Abdelalim: Laboratory of Mathematics, Computing and Application, Department of Mathematical and computer, Faculty of sciences University of Mohamed V Agdal, BP.1014 . Rabat, Morocco. seddikabd@hotmail.com
A. Chillali: Department of Mathematics, USMBA, FPT, TAZA, MOROCCO. chil2015@hotmail.fr
S. Elhajji: Laboratory of Mathematics, Computing and Application, Department of Mathematical and computer, Faculty of sciences University of Mohamed V Agdal, BP.1014 . Rabat, Morocco.elhajji@fsr.ac.ma.

By lemma 1.1, we have $a^2 + b^2 = 0\ [p]$. So, $a^2 + b^2 = k$, $k \in \mathbb{Z}$. We can write $a = ta_1$, $b = tb_1$with$a_1 \wedge b_1 = 1$.
Suppose a is not divisible by p then p doesnot divise$t$ and hence$p/(a_1^2 + b_1^2)$, then $a_1^2 + b_1^2 = kp$.
Since, see (proposition 1.2 [10, 11]), we have $p \neq 3\ [4]$.
We deduce that $p = 2$ or $p = 1\ [4]$.

$$1 \Longrightarrow 2)$$

Suppose $p = 2$, we can write $1^2 + 1^2 = 0\ [2]$, then $1 + i$isnotinvertible absurd.
Assume $p = 1\ [4]$ then$\frac{p-1}{2} = 2k$. There exist $c$in$\mathbb{F}_p$ such that$c^{\frac{p-1}{2}} \neq 1$, since $c^{p-1} = 1$ then $c^{\frac{p-1}{2}} = -1$and hence $(c^k)^2 = c^{2k} = -1$. So $1^2 + (c^k)^2 = 1 - 1 = 0$.
We deduce that $c^k + i$ isnot invertible absurd.■

II. THE SET $\mathrm{E} = \mathrm{E}_{\mathrm{A,B}} \cup \mathrm{E}_{\mathrm{A,-B}}$

Let $(G,*)$ and $(H,\nabla)$are two abeliangroups with the same unit element e such that G and H are isomorphism.

We put φ the isomorphism between two groups $(G,*)$ and (H,∇).

Theorem 1.2:
Let $E = G \cup H$ andΔ the mapping defined by:

$$\Delta: E \times E \to E$$
$$(x, y) \mapsto x\Delta y$$

$$\text{Where } x\Delta y = \begin{cases} x * y \text{ if } x, y \in G \\ x\nabla y \text{ if } x, y \in H \\ \varphi(x)\nabla y \text{ if } x \in G, y \notin G \\ x\nabla\varphi(y) \text{ if } x \notin G, y \in G \end{cases}$$

Then $\Delta$is an internal composition law, commutative with identity element e and all elements in E are invertible.
Proof:
It is clearly that $\Delta$is an internal composition law over E.
Show that e isidentity elementof Δ.
Let $x$in E.
If $x \in G$then $x\Delta e = x * e = e * x = e\Delta\, x = x$,
because$x \in G$ and e is unit element of $(G,*)$.
Else, $x \in H$then$x\Delta\, e = x\nabla\, e = e\nabla\, x = e\Delta\, x = x$,
because$x \in H, \varphi(e) = e$and$e$ is unit element of (H,∇).
$\Delta$is commutatif ?
We have $(\mathrm{G},*)$ and (H,∇) two abeliangroups with the same unit element e. Let $\mathrm{x,y} \in \mathrm{E}$.
If $\mathrm{x,y} \in \mathrm{G}$ then $\mathrm{x\Delta\, y = x * y = y * x = y\Delta\, x}$.
If $\mathrm{x,y} \in \mathrm{H}$ then $\mathrm{x\Delta\, y = x\nabla\, y = y\nabla\, x = y\Delta\, x}$.
If $\mathrm{x} \in \mathrm{G}, \mathrm{y} \notin \mathrm{G}$then $\mathrm{x\Delta\, y} = \varphi(\mathrm{x})\nabla\mathrm{y} = \mathrm{y}\nabla\varphi(\mathrm{x}) = \mathrm{y\Delta x}$.
If $\mathrm{x} \notin \mathrm{G}, \mathrm{y} \in \mathrm{G}$ then $\mathrm{x\Delta\, y} = \mathrm{x}\nabla\varphi(\mathrm{y}) = \varphi(\mathrm{y})\nabla\mathrm{x} = \mathrm{y\Delta x}$. ■
Let p a prime number such that $\mathrm{p} = 3[4]$and $\mathrm{E_{a,b}}$, $\mathrm{E_{a,-b}}$ are two elliptic curves defined over the field$\mathbb{F}_\mathrm{p}[\,\mathrm{i}]$ by:

$$\mathrm{E_{a,b}} = \{ (\mathrm{x,y}) / \mathrm{y}^2 = \mathrm{x}^3 + \mathrm{ax} + \mathrm{b}\} \cup \{\infty\}$$

$$\mathrm{E_{a,-b}} = \{ (\mathrm{x,y}) / \mathrm{y}^2 = \mathrm{x}^3 + \mathrm{ax} - \mathrm{b}\} \cup \{\infty\}$$

Proposition 2.2 :
If $b \neq 0$ then $E_{a,b} \cap E_{a,-b} = \{\infty\}$
Proof :
Assume that $(x, y) \in E_{a,b} \cap E_{a,-b} = \{\infty\}$,then $y^2 = x^3 + ax + b$and $y^2 = x^3 + ax - b$, so $b = -b$, i.e :$b = 0$, absurd. ■

Theorem2.3:
The mapping ρdefined by :

$$\rho: E_{a,b} \rightarrow E_{a,-b}$$
$$(x, y) \longmapsto (-x, iy)$$

and$\rho(\infty) = \infty$, is an isomorphism of groups.
Proof :
$\rho$is defined?.
Let $(x, y) \in E_{a,b}$ then $y^2 = x^3 + ax + b$, then $-y^2 = -x^3 - ax - b$, i.e: $(iy)^2 = (-x)^3 + a(-x) - b$therefore$\rho((x, y)) = (-x, iy) \in E_{a,-b}$.
$\rho$is injective?.
Let$(x_0, y_0), (x_1, y_1) \in E_{a,b}$ such that$\rho\big((x, y)\big) = \rho((x_1, y_1))$ then$(-x_0, iy_0) = (-x_1, iy_1)$ so, $(x_0, y_0) = (x_1, y_1)$ i.e: ρ is injective.
ρissurjective?
Let $(x, y) \in E_{a,-b}$then $y^2 = x^3 + ax - b$. It is clearly that$-y^2 = -x^3 - ax + b$ so, $(iy)^2 = (-x)^3 + a(-x) + b$ therefore $(-x, iy) \in E_{a,b}$ and $\rho((-x, iy)) = (x, y)$ i.e: ρ issurjective.
$\rho$is homomorphism?.
Let $(x_0, y_0), (x_1, y_1) \in E_{a,b}$ there is three cases:
1[st]case$x_0 \neq x_1$:

$$\rho\big((x_0, y_0) + (x_1, y_1)\big) = \begin{cases} \rho(\mathrm{m}_{a,b}^2 - \mathrm{x}_0 - \mathrm{x}_1, \mathrm{m}_{a,b}(\mathrm{x}_1 - \mathrm{x}_3) - \mathrm{y}_1) \\ (-\mathrm{m}_{a,b}^2 + \mathrm{x}_0 + \mathrm{x}_1, \mathrm{im}_{a,b}(\mathrm{x}_1 - \mathrm{x}_3) - \mathrm{iy}_1) \end{cases}$$

with$m_{a,b} = \frac{y_1 - y_0}{x_1 - x_0}$ and $x_3 = m_{a,b}^2 - x_0 - x_1$. See [7, P27].

$$\rho((x_0, y_0)) + \rho((x_1, y_1)) = \begin{cases} (-x_0, iy_0) + (-x_1, iy_1) \\ (\mathrm{m}_{a,-b}^2 + \mathrm{x}_0 + \mathrm{x}_1, \mathrm{m}_{a,-b}(-\mathrm{x}_1 - \mathrm{x}_4) - \mathrm{iy}_1) \end{cases}$$

with$m_{a,-b} = \frac{iy_1 - iy_0}{-x_1 + x_0}$ and $x_4 = m_{a,-b}^2 + x_0 + x_1$.
It is clear that $m_{a,-b} = \frac{i(y_1 - y_{0)}}{-(x_1 - x_0)} = -im_{a,b}$ then, $m_{a,b}^2 = -m_{a,-b}^2$and$x_3 = -x_4$. So hence,
$\rho\big((x_0, y_0) + (x_1, y_1)\big) = \rho((x_0, y_0)) + \rho((x_1, y_1))$.
2[nd]case $x_0 = x_1$and $y_0 = y_1$:

$$\rho\big((x_0, y_0) + (x_1, y_1)\big) = \begin{cases} \rho(\mathrm{m}_{a,b}^2 - 2\mathrm{x}_0, \mathrm{m}_{a,b}(\mathrm{x}_0 - \mathrm{x}_3) - \mathrm{y}_0) \\ (-\mathrm{m}_{a,b}^2 + 2\mathrm{x}_0, \mathrm{im}_{a,b}(\mathrm{x}_0 - \mathrm{x}_3) - \mathrm{iy}_0) \end{cases}$$

with$m_{a,b} = \frac{3x_0^2}{2y_0}$ and $x_3 = m_{a,b}^2 - 2x_0$. See [7, P27].

$$\rho((x_0, y_0)) + \rho((x_1, y_1)) = \begin{cases} (-x_0, iy_0) + (-x_1, iy_1) \\ (\mathrm{m}_{a,-b}^2 + 2\mathrm{x}_0, \mathrm{m}_{a,-b}(-\mathrm{x}_0 - \mathrm{x}_4) - \mathrm{iy}_0) \end{cases}$$

with$m_{a,-b} = \frac{3(-x_0)^2}{2y_0}$ and $x_4 = m_{a,-b}^2 + x_0 + x_1$.
It is clear that $m_{a,-b} = -i\frac{3x_0^2}{2y_0} = -im_{a,b}$ then, $m_{a,b}^2 = -m_{a,-b}^2$and$x_3 = -x_4$. So hence,
$\rho\big((x_0, y_0) + (x_1, y_1)\big) = \rho((x_0, y_0)) + \rho((x_1, y_1))$.
3[th]case $x_0 = x_1$and $y_0 = -y_1$:
We have:

$$\rho\big((x_0, y_0) + (x_1, y_1)\big) = \rho(\infty) = \infty$$

and

$$\rho((x_0, y_0)) + \rho((x_1, y_1)) = \begin{cases} (-x_0, iy_0) + (-x_1, iy_1) \\ \infty \\ \rho\big((x_0, y_0) + (x_1, y_1)\big) \end{cases}$$

So, ρ isan homomorphism.■

Corollary2.4:
Let $E = E_{a,b} \cup E_{a,-b}$and $+$ the mapping defined by:

$$+: E \times E \rightarrow E$$
$$(P, Q) \longmapsto P + Q$$

Such that:

$$P + Q = \begin{cases} P + Q \ if \ P, Q \in E_{a,b} \\ P + Q \ if \ P, Q \in E_{a,-b} \\ \rho(P) + Q \ if \ P \in E_{a,b}, Q \notin E_{a,b} \\ P + \rho(Q) \ if \ P \notin E_{a,b}, Q \in E_{a,b} \end{cases}$$

Then $+$isan internal composition law, commutative with identity element ∞ and all elements in E are invertible.
Proof:
Since theorem 2.1, proposition 2.2 and theorem 2.3, we have $+$is an internal composition law, commutative with identity element ∞ and all elements in E are invertible. ■

Corollary 2.5:
$Card\ (E) = 2Card(E_{a,b}) - 1$.
Proof:
We have:$E_{a,b}$ is isomorphic to$E_{a,-b}$. Then $Card(E) = Card\big(E_{a,b}\big) + Card\big(E_{a,-b}\big) - Card(E_{a,b} \cap E_{a,-b})$, so

$$Card\ (E) = 2Card(E_{a,b}) - 1. ■$$

III. CryptographicExample

Let $p = 7$,$a = 2 + 3i$ and $b = 1 + i$.
We have:

$$\mathrm{E_{a,b}} = \{ (\mathrm{x,y}) / \mathrm{y}^2 = \mathrm{x}^3 + \mathrm{ax} + \mathrm{b}\} \cup \{[0:1:0]\}$$
$$\mathrm{E_{a,-b}} = \{ (\mathrm{x,y}) / \mathrm{y}^2 = \mathrm{x}^3 + \mathrm{ax} - \mathrm{b}\} \cup \{[0:1:0]\}$$

Coding of elementsof $E = E_{a,b} \cup E_{a,-b}$.
We will give a code to each element $P \in E$ defined as it follows:
if $P = [x_0 + x_1 i: y_0 + y_1 i: z]$, where $x_j, y_j \in \mathbb{F}_p$for $j = 0\ or\ 1$and $z = 0\ or\ 1$, then we code P as follows:

$$x_0 x_1 y_0 y_1 z.$$

We conclude,
E={00100,00131,00361,00411,00641,01021,01051,01351,01421,02111,02661,03141,03631,04311,04461,05161,05611,06201,06231,06501,06541,10121,10241,10531,10651,12251,12521,14031,14041,14111,14661,15021,15051,15351,15421,16201,16231,16501,16541,20011,20061,23141,23631,25251,25521,26311,26461,31141,31631,33001,33321,33451,35301,35401,36341,36431,41331,41441,42031,42041,44001,44241,44531,46311,46461,50101,50601,51141,51631,52221,52551,54311,54461,60261,60321,60451,60511,61021,61051,61351,61421,62201,62231,62501,62541,63161,63301,63401,63611,

65221,65551}.

We have: $Card\ (E) = 91$

Remark:

With this application, we can encrypt and decrypt any message of any length.This application was implemented by Maple.

IV. CONCLUSION

In this paper, we present an example of cryptography that is not associative.

ACKNOWLEDGMENT

I would thank Laboratory of Mathematics, Computing and Application for his helpful comments and suggestions.

REFERENCES

[1] A. Chillali, The j-invariant over $E_{3^d}{}^n$, Int.j.Open problems Compt. Math.Vol.5, No 4,December 2012,ISSN 1998-6262, Copyright ICSRS Publication, (WWW.i-csrs.org,pp.106-111, 2012).

[2] A. Chillali, , Cryptography over elliptic curve of the ring $\mathbb{F}_q[\varepsilon], \varepsilon^4 = 0$ World Academy of science Engineering and Technology,78 (2011),pp.848-850

[3] A. Chillali, Elliptic curve over ring, International Mathematical Forum, Vol.6, no.31, 2011 pp.1501-1505

[4] 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, www.europment.org/library/2013/AMCM-05.

[5] A. Tadmori, A. Chillali and M. Ziane, Normal Form of the elliptic Curves over the finite ring, Journal of Mathematics and system sience, 4 (2014) 194-196.

[6] A. Tadmori, A. Chillali and M. Ziane, Coding over elliptic curves in the ring of characteristic two, International journal of Applied Mathemathics and Informatics, (Volume 8. 2014).

[7] J.H. SILVERMAN, The Arithmetic of Elliptic curves, Graduate Texts in Mathematcs, Springer, Volume 106(1985).2,19,20,21

[8] J.H. ~SILVERMAN, Advanced Topics in the Arithmetic of Elliptic curves, Graduate Texts in Mathematcs, Volume 151, Springer,(1994).

[9] W. Bosma and H. Lenstra, Complete system of two addition laws for elliptic curved, Journal of Number theory, (1995).J. U. Duncombe, “Infrared navigation—Part I: An assessment of feasibility (Periodical style),” IEEE Trans. Electron Devices, vol. ED-11, pp. 34–39, Jan. 1959.

[10] Duverney, D., Th\'eorie des nombres. Dunod, 1998.

[11] G. H. Hardy and E. M.Wright, An introduction to the theory of numbers, Oxford UniversityPress