Gulf Journal of Mathematics
Vol 3, Issue 2 (2015) 38-43

THE BINARY CALCULUS IN $E^2_{a,b}$

MY HACHEM HASSIB[1*]
ABDELHAKIM CHILLALI[2] AND MOHAMED ABDOU ELOMARY[1]

Abstract. In [11, p.52-57], M.Virat has established the group law on the elliptic curve defined over the ring $\mathbb{F}_{p^d}[\varepsilon], \varepsilon^n = 0$, where p a prime number $\geqslant 5$, $d \in \mathbb{N}^*$ and $n = 2$; and in [4] A.Chillali has, on his part studied the same case for p and extend it to $n = 3$.

In this article we will study the elliptic curve over the ring $A_2 = \mathbb{F}_{3^d}[\varepsilon]$, where $\varepsilon^2 = 0$. More precisely we will give many various explicit formulas describing the binary operations calculus in $E^2_{a,b}$, where $E^2_{a,b}$ is the elliptic curve over A_2, and we will reduce the cost of the complexity of the calculus found in theorem 1.1, by proving the lemmas 3.1, 3.2, 3.3, 3.4, 3.5 and 3.6; as it is shown in the section 3.

1. Introduction

Let d be an integer. We consider the quotient ring $A_2 = \mathbb{F}_{3^d}[X]/(X^2)$, where $\mathbb{F}_{3^d}$ is the finite field of order 3^d. Then the ring A_2 is identified to the ring $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^2 = 0$:

$$A_2 = \{a_0 + a_1\varepsilon \mid a_0, a_1 \in \mathbb{F}_{3^d}\}.$$

We consider the elliptic curve over the ring A_2 which is given by the equation: [3]

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

where $a, b \in A$ and $-a^3b$ is invertible in A_2.

We denote the elliptic curve over A_2 by $E^2_{a,b}$.

We consider the canonical projection π defined by:

$$\begin{aligned} \pi : \ \mathbb{F}_{3^d}[\varepsilon] &\longrightarrow \mathbb{F}_{3^d} \\ x_0 + x_1\varepsilon &\longrightarrow x_0 \end{aligned}$$

Theorem 1.1. *Let $P = [X_1 : Y_1 : Z_1]$ and $Q = [X_2 : Y_2 : Z_2]$ two points in $E^2_{a,b}$, and*
$P + Q = [X_3 : Y_3 : Z_3]$.

Date: Received: Feb 28, 2015.
* Corresponding author.
2010 *Mathematics Subject Classification.* 11T71, 14H52, 94A60.
Key words and phrases. Elliptic curve, ring, characteristic 3, finite field, finite ring.

- *If* $[\pi(X_1) : \pi(Y_1) : \pi(Z_1)] = [\pi(X_2) : \pi(Y_2) : \pi(Z_2)]$ *then :*

$X_3 = Y_1Y_2^2X_1 + {Y_1}^2Y_2X_2 + 2a{X_1}^2X_2Y_2 + 2aX_1{X_2}^2Y_1 + 2Z_1{Z_2}^2abY_1 + 2{Z_1}^2Z_2abY_2$

$Y_3 = {Y_1}^2{Y_2}^2 + 2a^2{X_1}^2{X_2}^2 + a^2bX_1Z_1{Z_2}^2 + a^2bX_2{Z_1}^2Z_2$

$Z_3 = aX_1X_2(Y_1Z_2+Y_2Z_1)+a(X_1Y_2+X_2Y_1)(X_1Z_2+X_2Z_1)+Y_1Y_2(Y_1Z_2+Y_2Z_1)$

- *If* $[\pi(X_1) : \pi(Y_1) : \pi(Z_1)] \neq [\pi(X_2) : \pi(Y_2) : \pi(Z_2)]$ *then :*

$X_3 = 2X_1Y_2Y_1Z_2 + X_1{Y_2}^2Z_1 + 2X_2{Y_1}^2Z_2 + X_2Y_1Y_2Z_1 + 2a{X_1}^2X_2Z_2 + aX_1{X_2}^2Z_1$

$Y_3 = 2{Y_1}^2Y_2Z_2 + Y_1{Y_2}^2Z_1 + 2aX_1X_2Y_1Z_2 + aX_1X_2Y_2Z_1 + 2a{X_1}^2Y_2Z_2 + a{X_2}^2Y_1Z_1$

$Z_3 = 2{Y_1}^2{Z_2}^2 + {Y_2}^2{Z_1}^2 + a{X_1}^2{Z_2}^2 + 2a{X_2}^2{Z_1}^2$

Proof. By using the explicit formulas in W.Bosma and H.W. Lenstra's article [1, p.236 to 238] we prove the theorem.

□

2. Classification of elements of $E^2_{a,b}$

Let $[X : Y : Z] \in E^2_{a,b}$, where X, Y and $Z \in A_2$.
We have two cases for Z:

- Z **invertible**: then $[X : Y : Z] = [XZ^{-1} : YZ^{-1} : 1] \sim [X : Y : 1]$.
- Z **noninvertible**: so $Z = z_1\varepsilon$ (see [4]), then we have two cases for Y:
  - Y **invertible**:
    then $[X : Y : Z] = [XY^{-1} : 1 : ZY^{-1}] \sim [X : 1 : z_1\varepsilon]$. So $[X : 1 : z_1\varepsilon] \in E^2_{a,b}$, then $z_1\varepsilon = x_0^3 + a_0x_0^2z_1\varepsilon$, where:

$$\begin{aligned} a &= a_0 + a_1\varepsilon, \\ b &= b_0 + b_1\varepsilon, \\ \text{and} \quad X &= x_0 + x_1\varepsilon. \end{aligned}$$

    Since $(1, \varepsilon)$ is a base of the vector space A_2 over $\mathbb{F}_{3^d}$, then $x_0 = 0$ and $z_1 = 0$ hence $[X : Y : Z] \sim [x_1\varepsilon : 1 : 0]$.
  - Y **noninvertible**:
    We have $Y = y_1\varepsilon$, so $[X : Y : Z] \sim [1 : y_1\varepsilon : z_1\varepsilon]$, thus $0 = 1 + az_1\varepsilon$, wich is absurd.

Proposition 2.1. *Every element of* $E^2_{a,b}$ *is in the form* $[X : Y : 1]$ *or* $[x\varepsilon : 1 : 0]$*; where* $x \in \mathbb{F}_{3^d}$*, and* $X, Y \in A_2$*, so we write:*

$$E^2_{a,b}= \{[X:Y:1] \in \mathbb{P}_2(A_2) \mid Y^2 = X^3 + aX^2 + b\} \cup \{[x\varepsilon : 1 : 0] \mid x \in \mathbb{F}_{3^d}\}.$$

3. Main results

3.1. **Binary operations.**

Lemma 3.1. *Let $P = [\alpha\varepsilon : 1 : 0]$ and $Q = [\beta\varepsilon : 1 : 0]$ two points in $E^2_{a,b}$ then:*

$$P + Q = [(\alpha + \beta)\varepsilon : 1 : 0]$$

.

Proof. As $[\pi(\alpha\varepsilon) : \pi(1) : \pi(0)] = [\pi(\beta\varepsilon) : \pi(1) : \pi(0)]$, then by applying the first case of theorem 1.1 we find the result.

□

The following lemmas may be proved by using the explicit formulas in [1, p. 236—238].

Lemma 3.2. *Let $P = [x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : 1]$ and $Q = [l\varepsilon : 1 : 0]$ two points in $E^2_{a,b}$, then:*

$$P + Q = [x_0 + (x_1 + ly_0)\varepsilon : y_0 + (y_1 + la_0x_0)\varepsilon : 1]$$

.

Lemma 3.3. *Let $P = [x_0 + x_1\varepsilon : y_1\varepsilon : 1]$ and $Q = [x_0 + t_1\varepsilon : s_1\varepsilon : 1]$ two points in $E^2_{a,b}$, then:*

$$P + Q = \Big[\frac{y_1 + s_1}{a_0x_0}\varepsilon : 1 : 0\Big]$$

Lemma 3.4. *Let $P = [x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : 1]$ and $Q = [x_0 + t_1\varepsilon : -y_0 + s_1\varepsilon : 1]$ two points of $E^2_{a,b}$ where $y_0 \neq 0$ then:*

$$P + Q = \Big[\frac{2t_1 + x_1}{y_0}\varepsilon : 1 : 0\Big]$$

Lemma 3.5. *Let $P = [t_0 + t_1\varepsilon : s_0 + s_1\varepsilon : 1]$ and $Q = [t_0 + l_1\varepsilon : s_0 + k_1\varepsilon : 1]$ two points in $E^2_{a,b}$ where $s_0 \neq 0$, then:*

$$P + Q = [X_0 + X_1\varepsilon : Y_0 + Y_1\varepsilon : 1],$$

where:

$$\begin{aligned} X_0 &= \lambda^2 - a_0 + t_0, \\ Y_0 &= \lambda(t_0 - X_0) - s_0, \\ \text{and} \quad \lambda &= \frac{a_0t_0}{s_0}\ . \end{aligned}$$

Lemma 3.6. *Let $P = [x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : 1]$ and $Q = [t_0 + t_1\varepsilon : s_0 + s_1\varepsilon : 1]$ two points of $E^2_{a,b}$ where $x_0 \neq t_0$, then:*

$$P + Q = [X_0 + X_1\varepsilon : Y_0 + Y_1\varepsilon : 1]$$

where:

$$\begin{aligned} X_0 &= \lambda^2 - a_0 - t_0 - x_0, \\ Y_0 &= \lambda(t_0 - X_0) - s_0, \\ \textit{and} \quad \lambda &= \frac{y_0 - s_0}{x_0 - t_0}\ . \end{aligned}$$

3.2. **Summary.** Similar as in [11], we summarize the results in the following table:

Table 1: Complexity reduction of the sum law in the elliptic curve $E^2_{a,b}$

	P	Q	$P+Q$
1	$[\alpha\varepsilon : 1 : 0]$	$[\beta\varepsilon : 1 : 0]$	$[(\alpha+\beta)\varepsilon : 1 : 0]$
2	$[\alpha\varepsilon : 1 : 0]$	$[x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : 1]$	$[x_0 + (x_0 + \alpha y_0)\varepsilon : y_0 + (y_1 + \alpha a_0 x_0)\varepsilon : 1]$
3	$[x_0 + x_1\varepsilon : y_1\varepsilon : 1]$	$[x_0 + t_1\varepsilon : s_1\varepsilon : 1]$	$[\frac{y_1 + s_1}{a_0 x_0}\varepsilon : 1 : 0]$
4	$[x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : 1]$	$[x_0 + t_1\varepsilon : -y_0 + s_1\varepsilon : 1]$ and $y_0 \neq 0$	$[\frac{2t_1 + x_1}{y_0}\varepsilon : 1 : 0]$
5	$[t_0 + t_1\varepsilon : s_0 + s_1\varepsilon : 1]$	$[t_0 + l_1\varepsilon : s_0 + k_1\varepsilon : 1]$ and $s_0 \neq 0$	$[X_0 + X_1\varepsilon : Y_0 + Y_1\varepsilon : 1]$, where: $X_0 = \lambda^2 - a_0 + t_0$, $Y_0 = \lambda(t_0 - X_0) - s_0$, and $\lambda = \frac{a_0 t_0}{s_0}$
6	$[x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : 1]$	$[t_0 + t_1\varepsilon : s_0 + s_1\varepsilon : 1]$ and $x_0 \neq t_0$	$[X_0 + X_1\varepsilon : Y_0 + Y_1\varepsilon : 1]$ where: $X_0 = \lambda^2 - a_0 - t_0 - x_0$, $Y_0 = \lambda(t_0 - X_0) - s_0$ and $\lambda = \frac{y_0 - s_0}{x_0 - t_0}$

4. Reduction of complexity

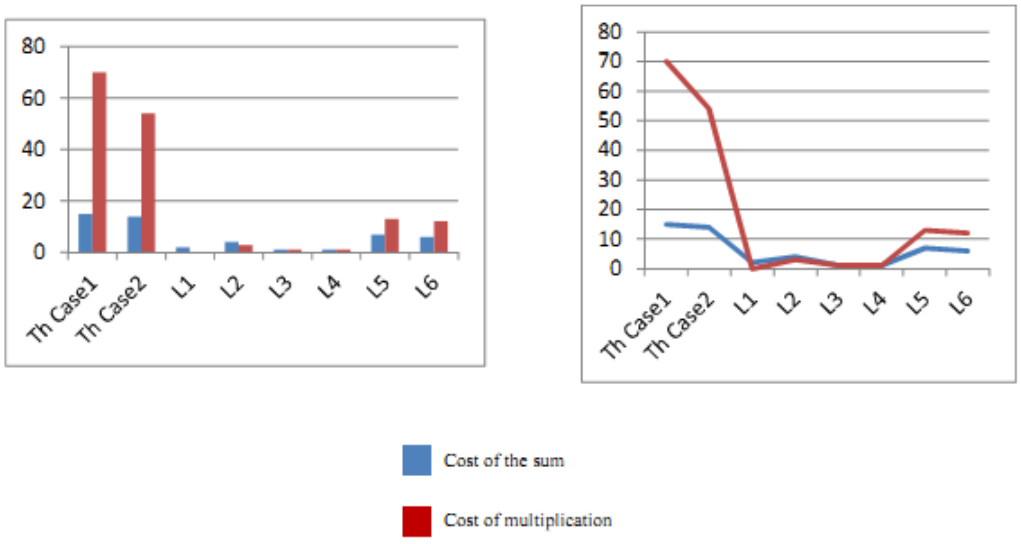
Let s, m and i are respectively the costs of the sum, the multiplication and the inverse in the field $\mathbb{F}_{3^d}$. It is clear that : $s \leqslant m \leqslant i$. We neglect the costs of the inverse and the comparison. We have the following table:

4.1. **Complexity cost.**

Table 2: Complexity reduction of the sum law in the elliptic curve $E^2_{a,b}$

case	Sum cost	multiplication cost
Theorem- case1	$15 \times s$	$70 \times m$
Theorem- case2	$14 \times s$	$54 \times m$
Lemma 1	$2 \times s$	$0 \times m$
Lemma 2	$4 \times s$	$3 \times m$
Lemma 3	$1 \times s$	$1 \times m$
Lemma 4	$1 \times s$	$1 \times m$
Lemma 5	$10 \times s$	$13 \times m$
Lemma 6	$16 \times s$	$12 \times m$

4.2. **Graphics interpretation.** the following graphics illustrate the above results:



5. Conclusion

The above results show that, the cost of the sum and the multiplication in the lemmas 3.1, 3.2, 3.3, 3.4, 3.5 and 3.6, are less than those in the theorem 1.1. Hence the complexity time in the lemmas is lower than the one in the theorem. This shows the importance of these lemmas.

References

1. W. Bosma and H. Lenstra, *Complete system of two addition laws for elliptic curved*, Journal of Number Theory, (1995).
2. A. Chillali, *Elliptic curves of the ring* $\mathbb{F}_q[\varepsilon]$, $\varepsilon^n = 0$, International Mathematical Forum, (2011).
3. A. Chillali, *The j-invariant over* $E^n_{3^d}$, Int.J.Open Problem, (2012).

4. A. Chillali and M. Cherkani, *Explicit formulas describing the binary operations calculus in $E_{a,b}$*, J. of Commun. & Comput. Eng., 2 (2012), pp. 16–20.
5. M. H. Hassib and A. Chillali, *Example of cryptography over the ring $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^2 = 0$*, Latest trends in Applied Informatics and Computing , ISBN 978-1-61804-130-2, (2012), pp. 71–73.
6. M. H. Hassib and A. Chillali, *The $\widetilde{\pi}$ homomorphism of $\mathrm{E}_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$*, AIP publishing, 1557 (2013), pp. 12–14.
7. M. H. Hassib, A. Chillali, and M. A. Elomary, *Special ideal ring A_3 and cryptography*, in Security Days (JNS3), 2013 National, April 2013, pp. 1–4.
8. M. H. Hassib, A. Chillali, and M. A. Elomary, *Elliptic curve over the ring $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^4 = 0$*, International Mathematical Forum, 9 (2014), pp. 1191 – 1196.
9. J. Lenstra, H.W, *Elliptic curves and number-theoretic algorithms*, Processing of the International Congress of Mathematicians,Berkely,California,USA, (1986).
10. J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, 2009.
11. M. Virat, *Courbe elliptique sur un anneau et application*, PhD thesis, Nice-Sophia Antipolis, 2009.

[1*] Moulay Ismail University FSTE Errachidia, Morocco.
E-mail address: hachem71@gmail.com

[1] Moulay Ismail University FSTE Errachidia, Morocco.
E-mail address: elomaryabdou@yahoo.fr

[2] USMBA, LSI, FPT, Taza, Morocco.
E-mail address: abdelhakim.chillali@usmba.ac.ma