Chapter

# Elliptic Curve over a Local Finite Ring $R_n$

*Abdelhakim Chillali and Lhoussain El Fadil*


## Abstract

The goal of this chapter is to study some arithmetic proprieties of an elliptic curve defined by a Weierstrass equation on the local ring $R_n = \mathbb{F}_q[X]/(X^n)$, where $n \geq 1$ is an integer. It consists of, an introduction, four sections, and a conclusion. In the first section, we review some fundamental arithmetic proprieties of finite local rings $R_n$, which will be used in the remainder of the chapter. The second section is devoted to a study the above mentioned elliptic curve on these finite local rings for arbitrary characteristics. A restriction to some specific characteristic cases will then be considered in the third section. Using these studies, we give in the fourth section some cryptography applications, and we give in the conclusion some current research perspectives concerning the use of this kind of curves in cryptography. We can see in the conclusion of research in perspectives on these types of curves.


**Keywords:** elliptic curve, finite ring, cryptography

## 1. Introduction

Elliptic curves are especially important in number theory and constitute a major area of current research; for example, they were used in Andrew Wiles's proof of Fermat's Last Theorem. They also find applications in elliptic curve cryptography (ECC), integer factorization, classical mechanics in the description of the movement of spinning tops, to produce efficient codes … For these reasons, the subject is well known, presented, and worth exploring.

The purpose of cryptography is to ensure the security of communications and data stored in the presence of adversaries [1–3]. It offers a set of techniques for providing confidentiality, authenticity, and integrity services. Cryptology, also known as the science of secrecy, combines cryptography and cryptanalysis. While the role of cryptographers is to design, build, and prove cryptosystems, among other things, the goal of cryptanalysis is to "break" these systems. The history of cryptography has long been the history of secret codes and along all previous times, this has affected the fate of men and nations [4]. In fact, until 1970, the main goal of cryptography was to build a signature encryption systems [5, 6], but thanks to cryptanalysis, the army and the black cabinets of diplomats were able to wage their wars in the shadows controlling the communication networks, especially of their enemies [7, 8]. The internet revolution and the increasingly massive use of information in digital form facilitated communications but in counterparty it weakened the security level of information. Indeed, "open" networks create security holes, which allow access to the information. Cryptography, or the art of encrypting messages, a science that sites today in the crossroads of mathematics, computer sciences, and some applied physics, has then become a necessity for today's civilization to keep its secrets from adversaries. Confusion is often made between cryptography and cryptology, but the difference exists. Cryptology is the "science of secrecy," and combines two branches on the one hand, cryptography, which makes it possible to encrypt messages, and on the other hand, cryptanalysis, which serves to decrypt them. Our focus in this chapter is to show how some elliptic curves, mathematical objects studied particularly in algebraic geometry [9–12]. You can give several definitions depending on the person you are talking to. Cryptography indeed used elliptic curves for more than 40 years the appearance of the Diffie-Hellman key exchange protocol and the ElGamal cryptogram [13–15]. These cryptographic protocols use in particular group structures, for by applying these methods to groups defined by elliptic curves, a new speciality was born at the end of the 1980: ECC, Elliptic Curve Cryptography. Recall that Diffie-Hellman key exchange which is based on the difficulty of the discrete logarithm problem (DLP) [16–18]. The success of elliptic curves in public key cryptographic systems has then created a new interest in the study of the arithmetic of these geometric objects. The group of points on an elliptical curve is an interesting group in cryptography because there is no known sub-exponential algorithm for sound (DLP) [19–21]. In general, the DLP is difficult to be solved, but not as much as in a generic group as in the case of finite field. We know sub-exponential algorithms to solve it depending on the size of the group to use, which impose criteria for the PLD to be infeasible. The prime number p which is the characteristic of our base ring must then have at least 1024 bits, which offers a security level similar to the one given by a generic order group of 160 bits. Recall that a generic group for the DLP is a group for which there is no a specific algorithm to solve the DLP [22], so that the only available algorithms are those for all groups.

In [23], Elhassani et al. have built an encryption method based on DLP and Lattice. Boulbot et al. in [24] have studied elliptic curves on a non-local ring to compare these curves on local and non-local rings, while in [25], Sahmoudi et al. have studied these types of curves on a family of finite rings in the authors have introduced a cryptosystem on these types of curves, see [26].

In this chapter, $d$ and $n$ are a positive integers and $q = p^d$ is a power of a prime natural number $p$.

## 2. The ring $R_n = \mathbb{F}_q[X]/(X^n)$

Let $R_n = \mathbb{F}_q[X]/(X^n)$ be a $\mathbb{F}_q$-algebra of dimension $n$, with $(1, \epsilon, \ldots, \epsilon^{n-1})$ as a $\mathbb{F}_q$-basis, where $\epsilon = \overline{X}$, $\epsilon^n = 0$, $\mathbb{F}_q$ is the finite field of order $q = p^r$, and $p$ being a prime integer [27–29].

### 2.1 Internal laws in $R_n$

Recall that the two laws "+" and "." are naturally defined on $R_n$ [30, 31]: for every two elements $X = \sum_{i=0}^{n-1} x_i \epsilon^i$ and $Y = \sum_{i=0}^{n-1} y_i \epsilon^i$ in $R_n$, with $x_1, \ldots, x_n, y_1, \ldots, y_n$ in $\mathbb{F}_q$,

$$X + Y = \sum_{i=0}^{n-1} z_i \epsilon^i, \text{where } z_j = x_j + y_j \text{ in } \mathbb{F}_q \tag{1}$$

$$X.Y=\sum_{i=0}^{n-1} z_i\epsilon^i, \text{where} z_j=\sum_{i=0}^{j} x_i y_{\ j-i}(\text{The cauchy product}) \tag{2}$$

**Corollary 2.1** *Let* $X=\sum_{i=0}^{n-1}x_i\epsilon^i\in R_n$, *then* $X^2=\sum_{i=0}^{n-1}x'_i\epsilon^i$ *where*

$$\forall k\geq 0, \begin{cases} x'_{2k}=x_k^2+2\sum_{i=0}^{k-1}x_ix_{2k-i} \\ x'_{2k+1}=2\sum_{i=0}^{k}x_ix_{2k+1-i} \end{cases} \tag{3}$$

**Proof.**
By formula (2), we have

$$\forall j\geq 0, x'_j=\sum_{i=0}^{j} x_i x_{\ j-i}. \tag{4}$$

$$\text{For} j=2k, x'_{2k}=\sum_{i=0}^{2k} x_i x_{2k-i}, \tag{5}$$

$$\text{so}, x'_{2k}=x_k^2+2\sum_{i=0}^{k-1} x_i x_{2k-i}. \tag{6}$$

$$\text{Similarly, for} j=2k+1, x'_{2k+1}=\sum_{i=0}^{2k+1} x_i x_{2k+1-i}, \tag{7}$$

$$\text{then}, x'_{2k+1}=2\sum_{i=0}^{k} x_i x_{2k+1-i}. \tag{8}$$

Under the same hypotheses of the corollary (2.1) and by an analogous proof, we have the following corollary:

**Corollary 2.2** $X^3=\sum_{i=0}^{n-1}x''_i\epsilon^i$, *where*

$$\forall k\geq 0, \begin{cases} x''_{2k}=x'_{2k}x_0+\sum_{l=0}^{k-1}\left(x'_{2l}x_{2k-2l}+x'_{2l+1}x_{2k-1-2l}\right) \\ x''_{2k+1}=\sum_{l=0}^{k}\left(x'_{2l}x_{2k+1-2l}+x'_{2l+1}x_{2k-2l}\right) \end{cases} \tag{9}$$

**Lemma 2.3** *Let* $Y=\sum_{i=0}^{n-1}y_i\epsilon^i$ *the inverse of* $X=\sum_{i=0}^{n-1}x_i\epsilon^i$. *Then*

$$\begin{cases} y_0=x_0^{-1} \\ y_j=-x_0^{-1}\sum_{i=0}^{j-1}y_ix_{\ j-i}, \qquad \forall j>0 \end{cases} \tag{10}$$

**Proof.**
Let $Y=\sum_{i=0}^{n-1}y_i\epsilon^i$ be the inverse of $X=\sum_{i=0}^{n-1}x_i\epsilon^i$. Then $XY=1$, by formula (2), we have

$$XY=\sum_{i=0}^{n-1} z_i\epsilon^i, \text{where } z_j=\sum_{i=0}^{j} x_i y_{j-i}. \tag{11}$$

So,

$$z_0=1 \text{and } \forall j>0, z_j=0, \tag{12}$$

which means that,

$$\begin{cases} y_0 = x_0^{-1} \\ y_j = -x_0^{-1}\sum_{i=0}^{j-1} y_i x_{j-i}, \qquad \forall j > 0 \end{cases} \tag{13}$$

**Lemma 2.4** *The non inverse elements in* $R_n$ *are the elements of the form* $\sum_{i=1}^{n-1} x_i \epsilon^i$ *where* $x_i \in \mathbb{F}_q^{n-1}$ *for all* $1 \leq i \leq n-1$.

**Proof.**

Let $X = \sum_{i=0}^{n-1} x_i \epsilon^i \in R_n$. By lemma (2.3), $X$ is invertible in $R_n$ if and only if $x_0$ is invertible in $\mathbb{F}_q$. As $\mathbb{F}_q$ is a field, this means $x_0 \neq 0$.

**Corollary 2.5** *The ring* $R_n$ *is local, with maximal ideal* $I_n = \epsilon R_n$.

Notation.

Let $k \geq 2$, we denote:

1.

$$\pi_k : \left| \begin{array}{ccc} R_k & \rightarrow & R_{k-1} \\ \sum_{i=0}^{k-1} x_i \epsilon^i & \mapsto & \sum_{i=0}^{k-2} x_i \delta^i \end{array} \right.$$

the projection of $R_k$ on $R_{k-1}$.

2.

$$k^\pi : \left| \begin{array}{ccc} R_k & \rightarrow & R_1 \\ \sum_{i=0}^{k-1} x_i \epsilon^i & \mapsto & x_0 \end{array} \right.$$

the canonical projection of $R_k$ on $R_1 = \mathbb{F}_q$.

**Corollary 2.6** $\pi_k$ *et* $k^\pi$ *are two ring homomorphisms.*

**Proof.**

We have,

$$\begin{aligned} \pi_k\left(\sum_{i=0}^{k-1} x_i \epsilon^i + \sum_{i=0}^{k-1} y_i \epsilon^i\right) &= \pi_k\left(\sum_{i=0}^{k-1} (x_i + y_i)\epsilon^i\right) \\ &= \sum_{i=0}^{k-2} (x_i + y_i)\delta^i \\ &= \pi_k\left(\sum_{i=0}^{k-1} x_i \epsilon^i\right) + \pi_k\left(\sum_{i=0}^{k-1} y_i \epsilon^i\right) \end{aligned} \tag{14}$$

and

$$\begin{gathered} \left(\sum_{i=0}^{k-1} x_i \epsilon^i\right)\left(\sum_{i=0}^{k-1} y_i \epsilon^i\right) = \sum_{i=0}^{k-1} z_i \epsilon^i, \text{where } z_j = \sum_{i=0}^{j} x_i y_{j-i}. \\ \pi_k\left(\sum_{i=0}^{k-1} z_i \epsilon^i\right) = \sum_{i=0}^{k-2} z_i \delta^i \\ \pi_k\left(\sum_{i=0}^{k-1} x_i \epsilon^i\right)\pi_k\left(\sum_{i=0}^{k-1} y_i \epsilon^i\right) = \sum_{i=0}^{k-2} z_i \delta^i \end{gathered} \tag{15}$$

Note that in addition, for every $k \geq 1$,

$$k^{\pi} = \pi_2 \circ \pi_3 \circ \pi_4 \ldots\ldots \circ \pi_k \tag{16}$$

So, $\pi_k$ and $k^{\pi}$ are tow rings morphisms.

**Theorem 2.7** *Let $n \geq 2$ be an integer,*
$a = \tilde{a} + a_{n-1}\epsilon^{n-1}$, $b = \tilde{b} + b_{n-1}\epsilon^{n-1}$, $X = \tilde{X} + x_{n-1}\epsilon^{n-1}$, $Y = \tilde{Y} + y_{n-1}\epsilon^{n-1}$ *and* $Z = \tilde{Z} + z_{n-1}\epsilon^{n-1}$ *be elements of $R_n$ with:*

$$Y^2 Z = X^3 + aXZ^2 + bZ^3. \tag{17}$$

*Then*

$$\tilde{Y}^2 \tilde{Z} = \tilde{X}^3 + \tilde{a}\tilde{X}\tilde{Z}^2 + \tilde{b}\tilde{Z}^3 + \left[D - \left(Ay_{n-1} + Bz_{n-1} + Cx_{n-1}\right)\right]\epsilon^{n-1} \tag{18}$$

where,

$$A = 2y_0 z_0, \tag{19}$$

$$B = y_0^2 - 3z_0^2 b_0 - 2z_0 a_0 x_0, \tag{20}$$

$$C = -\left(3x_0^2 + a_0 z_0^2\right) \tag{21}$$

and

$$D = b_{n-1} z_0^3 + a_{n-1} x_0 z_0^2. \tag{22}$$

**Proof.**
We have:

$$\begin{aligned}
Y^2 Z &= \left(\tilde{Y} + y_{n-1}\epsilon^{n-1}\right)^2 \left(\tilde{Z} + z_{n-1}\epsilon^{n-1}\right) \\
&= \tilde{Y}^2 \tilde{Z} + \left(y_0^2 z_{n-1} + 2y_0 z_0 y_{n-1}\right)\epsilon^{n-1} \\
X^3 &= \left(\tilde{X} + x_{n-1}\epsilon^{n-1}\right)^3 \\
&= \tilde{X}^3 + 3x_0^2 x_{n-1}\epsilon^{n-1} \\
aXZ^2 &= \tilde{a}\tilde{X}\tilde{Z}^2 + \left(2z_{n-1}z_0 a_0 x_0 + a_0 x_{n-1} z_0^2 + a_{n-1} x_0 z_0^2\right)\epsilon^{n-1} \\
bZ^3 &= \tilde{b}\tilde{Z}^3 + \left(b_{n-1} z_0^3 + 3z_0^2 z_{n-1} b_0\right)\epsilon^{n-1}
\end{aligned} \tag{23}$$

If

$$Y^2 Z = X^3 + aXZ^2 + bZ^3, \tag{24}$$

then, $\tilde{Y}^2 \tilde{Z} = \tilde{X}^3 + \tilde{a}\tilde{X}\tilde{Z}^2 + \tilde{b}\tilde{Z}^3 + (3x_0^2 x_{n-1} + 2z_{n-1} z_0 a_0 x_0 + a_0 x_{n-1} z_0^2 + a_{n-1} x_0 z_0^2 3z_0^2 z_{n-1} b_0 - y_0^2 z_{n-1} - 2y_0 z_0 y_{n-1})\epsilon^{n-1}$ and therefore,

$$\tilde{Y}^2 \tilde{Z} = \tilde{X}^3 + \tilde{a}\tilde{X}\tilde{Z}^2 + \tilde{b}\tilde{Z}^3 + \left[D - \left(Ay_{n-1} + Bz_{n-1} + Cx_{n-1}\right)\right]\epsilon^{n-1} \tag{25}$$

where,

$$A = 2y_0z_0, \tag{26}$$

$$B = y_0^2 - 3z_0^2b_0 - 2z_0a_0x_0, \tag{27}$$

$$C = -\left(3x_0^2 + a_0z_0^2\right) \tag{28}$$

and

$$D = b_{n-1}z_0^3 + a_{n-1}x_0z_0^2. \tag{29}$$

### 2.2 Primitive triples

**Definition 2.8** *Let $R$ be a ring. We say that an element $(x, y, z) \in R^3$ is primitive if: $xR + yR + zR = R$. The set of these primitive triplets will be denoted $\mathcal{P}(R)$.*

**Remark 2.9** *The equality $xR + yR + zR = R$ means that there exists $(\alpha, \beta, \lambda) \in R^3$ such that $1_R = \alpha x + \beta y + \lambda z$.*

**Proposition 2.10** *Let $R$ be a local ring, then $(x, y, z) \in R^3$ is a primitive triple if and only if at least one of the elements $x$, $y$, and $z$ is invertible in $R$.*

**Proof.**

Suppose that $x, y$ and $z$ are not invertible in $R$, then:
$(x, y, z) \in \mathcal{M}^3$ where $\mathcal{M}$ is the unique maximal ideal of $R$, hence

$$xR + yR + zR \subset \mathcal{M} \subsetneq R, \tag{30}$$

which contradicts that $(x, y, z)$ is a primitive triple.

Conversely, suppose, for example, that $x$ is invertible in $R$, then $xR = R$, so $xR + yR + zR = R$.

**Remark 2.11** *If $R$ is a field, then an element $(x, y, z) \in R^3$ is primitive if and only if $(x, y, z) \neq (0, 0, 0)$.*

### 2.3 The projective plane on a finite ring

Let $R$ is a ring. The projective plane on $R$ is the set of equivalence classes of $\mathcal{P}(R)$ modulo; the equivalence relation $\sim R$ defined by:

$$(x_1, y_1, z_1) \sim R(x_2, y_2, z_2) \Leftrightarrow \exists \lambda \in R^\times : \quad (x_2, y_2, z_2) = \lambda(x_1, y_1, z_1). \tag{31}$$

We denote the projective plane on $R$ by $\mathbb{P}^2(R)$, it is the quotient set $\frac{\mathcal{P}(R)}{\sim R}$, and we write $[x : y : z]$ for the equivalence class of $(x, y, z) \in \mathcal{P}(R)$. Thus, we have:

$$[x_1 : y_1 : z_1] = [x_2 : y_2 : z_2] \Leftrightarrow \exists \lambda \in R^\times : x_2 = \lambda x_1, y_2 = \lambda y_1 \text{ and } z_2 = \lambda z_1. \tag{32}$$

**Example 2.12** *We Consider the finite ring $\mathbb{F}_2[e] = \{\alpha + \beta e / \alpha \in \mathbb{F}_2 \, and \, \beta \in \mathbb{F}_2\}$, where $e$ is an indeterminate satisfying $e^2 = 0$. The group of units for this ring is $(\mathbb{F}_2[e])^\times = \{1, 1 + e\}$.*

*As this ring is local with maximal ideal $e\mathbb{F}_2[e]$, then an element $(x, y, z)$ of $\mathbb{F}_2[e]^3$ is non primitive if and only if $(x, y, z) \in \{0, e\}^3$. As one can see, there are eight elements which are not primitive, and therefore the set $\mathcal{P}(\mathbb{F}_2[e])$ contains $64 - 8 = 56$ primitive triples as given below:*

$$
\begin{aligned}
\mathcal{P}(\mathbb{F}_2[e]) = \{&(0,0,1),(0,1,1+e),(0,1,0),(0,1,1),(0,1,e),(0,1,1+e),(0,e,1),\\
&(0,e,1+e),(0,1+e,0),\ (0,1+e,1),\ (0,1+e,e),(0,1+e,1+e),\\
&(1,0,0),(1,0,1),(1,0,e),(1,0,1+e),(1,1,0),(1,1,1),(1,1,e),\\
&(1,1,1+e),(1,e,0),(1,e,1),(1,e,e),(1,e,1+e),(1,1+e,0),\\
&(1,1+e,1),(1,1+e,e),(1,1+e,1+e),(e,0,1),(e,0,1+e),(e,1,0),\\
&(e,1,1),(e,1,e),(e,1,1+e),(e,e,1),(e,e,1+e),(e,1+e,0),(e,1+e,1),\\
&(e,1+e,e),(e,1+e,1+e),(1+e,0,0),(1+e,0,1),(1+e,0,e),\\
&(1+e,0,1+e),(1+e,1,0),(1+e,1,1),(1+e,1,e),(1+e,1,1+e),\\
&(1+e,e,0),(1+e,e,1),(1+e,e,e),(1+e,e,1+e),(1+e,1+e,0),\\
&(1+e,1+e,1),(1+e,1+e,e),(1+e,1+e,1+e)\}.
\end{aligned}
\tag{33}
$$

*Let* $(x,y,z)$ *and* $(x',y',z')$ *be two elements in* $\mathcal{P}(\mathbb{F}_2[e])$*, then:*
$[x':y':z'] = [x:y:z] \Leftrightarrow (x',y',z') = (x,y,z)$ *or* $(x',y',z') = (x+xe, y+ye, z+ze)$
*so every class in* $\mathbb{P}^2(\mathbb{F}_2[e])$ *contains two representatives, that is, the projective plane* $\mathbb{P}^2(\mathbb{F}_2[e])$ *contains exactly the following 28 elements:*

$$
\begin{aligned}
\mathbb{P}^2(\mathbb{F}_2[e]) = \{&[0:1:0],[0:0:1],[0:1:1],[0:1:e],[0:1:1+e],[0:e:1],[1:0:0],\\
&[1:0:1],[1:0:e],[1:0:1+e],[1:1:0],[1:1:1],[1:1:e],[1:1:1+e],\\
&[1:e:0],[1:e:1],[1:e:e],[1:e:1+e],[1:1+e:0],[1:1+e:1],\\
&[1:1+e:e],[1:1+e:1+e],[e:0:1],[e:1:0],[e:1:1],[e:1:e],\\
&[e:1:1+e],[e:e:1]\}.
\end{aligned}
\tag{34}
$$

## 3. Elliptic curve over $R_n$

In this section, we study the elliptic curves defined on finite local rings $R_n$ of characteristic a prime number p;

1. A projective Weierstrass equation on $R_n$ is an equation of the form:

$$\mathbf{E}: \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4X + a_6Z^3 \tag{35}$$

2. A affine Weierstrass equation on $R_n$ is an equation of the form:

$$\mathbf{E}': \quad Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{36}$$

where $(a_1, a_2, a_3, a_4, a_6) \in {R_n}^5$.

### 3.1 Elliptic curve form

To an affine (or projective) Weierstrass Eqs. (3) and (4), we associate the following quantities:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j &= \frac{c_4^3}{\Delta} if\, \Delta \neq 0
\end{aligned} \tag{37}$$

$\Delta$ is called the discriminant of $\mathbf{E}$ and $j$ its $j$ – invariant.

**Remark 3.1** *On the field $R_1 = \mathbb{F}_q$, we denote the discriminant by $\Delta_0$ and the j-invariant by $j_0$, while on the ring $R_n$, $n > 1$ we denote the discriminant by $\Delta_{\varepsilon,n}$ and the j-invariant by $j_{\varepsilon,n}$.*

*We have $n^\pi(\Delta_{\varepsilon,n}) = \Delta_0$ and $n^\pi\left(j_{\varepsilon,n}\right) = j_0$.*

**Definition 3.2** *Let R be a finite ring and let $a = (a_1, a_2, a_3, a_4, a_6) \in R^5$. An elliptic curve on R corresponding to a, which we write $E_a(R)$, is the set of zeros in the projective plane $\mathbb{P}^2(R)$ of the Weierstrass Eq. (3), for which the discriminant $\Delta$ is invertible in R.*

**Remark 3.3** *According to the characteristic of the ring R; $chra(R)$ we have the following cases:*

1. If $char(R) \neq 2$ and $char(R) \neq 3$, then:

$$E_{a,b}(R) = \{[X : Y : Z] \in \mathbb{P}^2(R)/Y^2Z = X^3 + aXZ^2 + bZ^3\} \tag{38}$$

*for $(a, b) \in R \times R$, with $\Delta = \Delta_{a,b} = -16(4a^3 + 27b^2) \in R^\times$.*

2. If $char(R) = 2$, then $E_{a,b}(R)$ has one of the following forms:

$$E_{a,b}(R) = \{[X : Y : Z] \in \mathbb{P}^2(R)/Y^2Z + XYZ = X^3 + aX^2Z + bZ^3\} \tag{39}$$

for $(a, b) \in R^2$, with $\Delta = \Delta_{a,b} = b \in R^\times$.
*Or:*

$$E_a(R) = \{[X : Y : Z] \in \mathbb{P}^2(R)/Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_4XZ^2 + a_6Z^3\} \tag{40}$$

for $a = (a_1, a_3, a_4, a_6) \in R^4$, with $a_1$ non invertible and

$$\Delta = \Delta_a = a_1^3(a_1^3a_6 + a_1^2a_3a_4 + a_1a_4^2 + a_3^3) + a_3^4 \in R^\times. \tag{41}$$

3. If $char(R) = 3$, then $E_{a,b}(R)$ has one of the following forms:

$$E_{a,b}(R) = \{[X : Y : Z] \in \mathbb{P}^2(R)/Y^2Z = X^3 + aX^2Z + bZ^3\} \tag{42}$$

*for $(a, b) \in R^2$, with $\Delta = \Delta_{a,b} = -a^3b \in R^\times$.*
*Or:*

$$E_{a,b}(R) = \{[X : Y : Z] \in \mathbb{P}^2(R)/Y^2Z = X^3 + aXZ^2 + bZ^3\} \tag{43}$$

for $(a, b) \in R^2$, with $\Delta = \Delta_{a,b} = -a^3 \in R^\times$.

**Remark 3.4** *A projective elliptic curve on a field K has one of the following normal forms (**Table 1**):*

| | | Normal form | |
|---|---|---|---|
| $char(\mathbf{K}) \neq 2,3$ | | $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$ | |
| | | $\Delta = -16(4a_4^3 + 27a_6^2)$ | $j = 1728\frac{4a_4^3}{4a_4^3+27a_6^2}$ |
| $char(\mathbf{K}) = 3$ | $j = 0$ | $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$ | |
| | | $\Delta = -a_4^3$ | |
| | $j \neq 0$ | $Y^2Z = X^3 + a_2X^2Z + a_6Z^3$ | |
| | | $\Delta = -a_2^3a_6$ | $j = -\frac{a_2^3}{a_6}$ |
| $char(\mathbf{K}) = 2$ | $j = 0$ | $Y^2Z + a_3YZ^2 = X^3 + a_4XZ^2 + a_6Z^3$ | |
| | | $\Delta = a_3^4$ | |
| | $j \neq 0$ | $Y^2Z + XYZ = X^3 + a_2X^2Z + a_6Z^3$ | |
| | | $\Delta = a_6$ | $j = \frac{1}{a_6}$ |

**Table 1.**
*Elliptic curve form on a field.*

### 3.2 Projective coordinates and group law

In this subsection, we give in projective coordinates the formulas for adding the points on an elliptic curve defined by Eq. (3) on the ring $R_n$, according to the normal form.

Using Bosma and Lenstra's theorem see [32], we can deduce the explicit formulas for the commutative additive law of the group $E_a(R_n)$. The results are given in the next theorems following the values of the characteristic of ring $R_n$ [33–36]. Let

$$[X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2] = [X_3 : Y_3 : Z_3]. \tag{44}$$

**Theorem 3.5** *[Characteristic two case]:*

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

$$\begin{aligned} X_3 = {} & X_1Y_1Y_2^2 + X_2Y_1^2Y_2 + X_2^2Y_1^2 + X_1X_2^2Y_1 + aX_1^2X_2Y_2 + aX_1X_2^2Y_1 + aX_1^2X_2^2 + \\ & bX_1Y_1Z_2^2 + bX_2Y_2Z_1^2 + bX_1^2Z_2^2 + bY_1Z_2^2Z_1 + bY_2Z_1^2Z_2 + bX_1Z_2^2Z_1. \end{aligned} \tag{45}$$

$$\begin{aligned} Y_3 = {} & Y_1^2Y_2^2 + X_2Y_1^2Y_2 + aX_1X_2^2Y_1 + a^2X_1^2X_2^2 + bX_1^2X_2Z_2 + bX_1X_2^2Z_1 + \\ & bX_1Y_1Z_2^2 + bX_1^2Z_2^2 + abX_2^2Z_1^2 + abX_1^2Z_2^2 + bY_1Z_1Z_2^2 + bX_1Z_1Z_2^2 + abX_1Z_1Z_2^2 + \\ & abX_2Z_1^2Z_2 + b^2Z_1^2Z_2^2 \end{aligned} \tag{46}$$

$$\begin{aligned} Z_3 = {} & X_1^2X_2Y_2 + X_1X_2^2Y_1 + Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + X_1^2X_2^2 + Y_1^2X_2Z_2 + X_1^2Y_2Z_2 + \\ & aX_1^2Y_2Z_2 + aX_2^2Y_1Z_1 + X_1^2X_2Z_2 + aX_1X_2^2Z_1 + bY_1Z_1Z_2^2 + bY_2Z_1^2Z_2 + bX_1Z_1Z_2^2. \end{aligned} \tag{47}$$

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

$$\begin{aligned} X_3 = {} & X_1Y_2^2Z_1 + X_2Y_1^2Z_2 + X_1^2Y_2Z_2 + X_2^2Y_1Z_1 + aX_1^2X_2Z_2 + aX_1X_2^2Z_1 + \\ & bX_1Z_1Z_2^2 + bX_2Z_1^2Z_2. \end{aligned} \tag{48}$$

$$Y_3 = X_1^2X_2Y_2 + X_1X_2^2Y_1 + Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + X_1^2Y_2Z_2 + X_2^2Y_1Z_1 + aX_1^2Y_2Z_2 + aX_2^2Y_1Z_1 + aX_1^2X_2Z_2 + aX_1X_2^2Z_1 + bY_1Z_1Z_2^2 + bY_2Z_1^2Z_2 + bX_1Z_1Z_2^2 + bX_2Z_1^2Z_2. \tag{49}$$

$$Z_3 = X_1^2X_2Z_2 + X_1X_2^2Z_1 + Y_1^2Z_2^2 + Y_2^2Z_1^2 + X_1Y_1Z_2^2 + X_2Y_2Z_1^2 + aX_1^2Z_2^2 + aX_2^2Z_1^2. \tag{50}$$

**Theorem 3.6** *[Characteristic three case]:*

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

$$X_3 = Y_1Y_2^2X_1 + Y_1{}^2Y_2X_2 + 2aX_1{}^2X_2Y_2 + 2aX_1X_2{}^2Y_1 + 2Z_1Z_2{}^2abY_1 + 2Z_1{}^2Z_2abY_2. \tag{51}$$

$$Y_3 = Y_1{}^2Y_2{}^2 + 2a^2X_1{}^2X_2{}^2 + a^2bX_1Z_1Z_2{}^2 + a^2bX_2Z_1{}^2Z_2. \tag{52}$$

$$Z_3 = aX_1X_2(Y_1Z_2 + Y_2Z_1) + a(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) + Y_1Y_2(Y_1Z_2 + Y_2Z_1). \tag{53}$$

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

$$X_3 = 2X_1Y_2Y_1Z_2 + X_1Y_2{}^2Z_1 + 2X_2Y_1{}^2Z_2 + X_2Y_1Y_2Z_1 + 2aX_1{}^2X_2Z_2 + aX_1X_2{}^2Z_1. \tag{54}$$

$$Y_3 = 2Y_1{}^2Y_2Z_2 + Y_1Y_2{}^2Z_1 + 2aX_1X_2Y_1Z_2 + aX_1X_2Y_2Z_1 + 2aX_1{}^2Y_2Z_2 + aX_2{}^2Y_1Z_1. \tag{55}$$

$$Z_3 = 2Y_1{}^2Z_2{}^2 + Y_2{}^2Z_1{}^2 + aX_1{}^2Z_2{}^2 + 2aX_2{}^2Z_1{}^2. \tag{56}$$

**Theorem 3.7** *[The case where the characteristic is different from two and from three]:*

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

$$X_3 = Y_1^2X_2Z_2 - Z_1X_1Y_2^2a(Z_1X_2 + X_1Z_2)(Z_1X_2 - X_1Z_2) + (2Y_1Y_2 - 3bZ_1Z_2)(Z_1X_2 - X_1Z_2) \tag{57}$$

$$Y_3 = Y_1Y_2(Z_2Y_1 - Z_1Y_2) - a\left(X_1Y_1Z_2^2 - Z_1^2X_2Y_2\right) + (-2aZ_1Z_2 - 3X_1X_2)(X_2Y_1 - X_1Y_2) - 3bZ_1Z_2(Z_2Y_1 - Z_1Y_2) \tag{58}$$

$$Z_3 = (Z_1Y_2 + Z_2Y_1)(Z_2Y_1 - Z_1Y_2) + (3X_1X_2 + aZ_1Z_2)(Z_1X_2 - X_1Z_2) \tag{59}$$

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

$$X_3 = (Y_1Y_2 - 6bZ_1Z_2)(X_2Y_1 + X_1Y_2) + \left(a^2Z_1Z_2 - 2aX_1X_2\right)(Z_1Y_2 + Z_2Y_1) - 3b\left(X_1Y_1Z_2^2 + Z_1^2X_2Y_2\right) - a\left(Y_1Z_1X_2^2 + X_1^2Y_2Z_2\right) \tag{60}$$

$$Y_3 = Y_1^2Y_2^2 + 3aX_1^2X_2^2 + \left(-a^3 - 9b^2\right)Z_1^2Z_2^2 - a^2(Z_1X_2 + X_1Z_2)^2 - 2a^2Z_1X_1Z_2X_2 + (9bX_1X_2 - 3abZ_1Z_2)(Z_1X_2 + X_1Z_2) \tag{61}$$

$$Z_3 = (Y_1Y_2 + 3bZ_1Z_2)(Z_1Y_2 + Z_2Y_1) + (3X_1X_2 + 2aZ_1Z_2)(X_2Y_1 + X_1Y_2) + a\left(X_1Y_1Z_2^2 + Z^1X_2Y_2\right). \tag{62}$$

## 4. Elliptic curve on $R_n$ where $char(\mathbf{R_n}) \neq 2, 3$

The objective of this chapter is to study elliptic curves defined by a Weierstrass equation with coefficients in a ring $R_n$ such that $char(\mathbf{R_n}) \neq 2, 3$. We denote it by $E^n_{a,b}$. Let

$$k_\theta : \left| \begin{array}{ccc} \mathbb{F}_q^{k-1} & \rightarrow & E_{a,b}^k \\ (x_1, x_2, \ldots, x_{k-1}) & \mapsto & \left[\sum_{i=1}^{k-1} x_i \epsilon^i : 1 : \sum_{i=3}^{k-1} z_i \epsilon^i\right] \end{array} \right. \tag{63}$$

we denote, $k_G = k_\theta\left(\mathbb{F}_q^{k-1}\right)$.

### 4.1 The morphisms $\pi^k$ et $\theta_k$

**Lemma 4.1** *The application*

$$\pi^k : \left| \begin{array}{c} E_{a,b}^k \rightarrow E_{\pi_k(a),\pi_k(b)}^{k-1} \\ [X : Y : Z] \mapsto [\pi_k(X) : \pi_k(Y) : \pi_k(Z)] \end{array} \right. \tag{64}$$

is a surjective group homomorphism.
**Proof.**
*$\pi^k$ is well defined because $\pi_k$ is a morphism of rings. According to theorem (2.7), we have $AY_{k-1} + BZ_{k-1} + CX_{k-1} = D \bmod p$, with*

$$A = 2y_0 z_0, \tag{65}$$

$$B = y_0^2 - 3z_0^2 b_0 - 2z_0 a_0 x_0, \tag{66}$$

$$C = -\left(3x_0^2 + a_0 z_0^2\right) \tag{67}$$

and

$$D = b_{n-1} z_0^3 + a_{n-1} x_0 z_0^2. \tag{68}$$

*The coefficients A, B and $-C$ are the partial derivatives of the function*

$$F(X, Y, Z) = Y^2 Z - X^3 - a_0 X Z^2 - b_0 Z^3 \tag{69}$$

calculated starting from $(x_0, y_0, z_0)$, which are not all equal to zero and deducing the existence of $\left[x_{k-1} : y_{k-1} : z_{k-1}\right]$. Hence, $\pi^k$ est surjectif.
*Using corollary (2.6), we deduce that $\pi^k$ is a group homomorphism.*
**Lemma 4.2** *For all $k \geq 2$,*

$$Ker\left(\pi^k\right) = \left\{\left[l\epsilon^{k-1} : 1 : 0\right] \mid \quad l \in \mathbb{F}_q\right\}. \tag{70}$$

**Proof.**
We have:

$$Ker\left(\pi^k\right) = \left\{P \in E_{a,b}^k \mid \quad \pi^k(P) = [0 : 1 : 0] \ \right\}. \tag{71}$$

Then, $P = \left[x_{k-1}\epsilon^{k-1} : 1 + y_{k-1}\epsilon^{k-1} : z_{k-1}\epsilon^{k-1}\right] = \left[x_{k-1}\epsilon^{k-1} : 1 : z_{k-1}\epsilon^{k-1}\right]$..
As $P \in E_{a,b}^k$, we have

$$\begin{aligned} z_{k-1}\epsilon^{k-1} &= \left(x_{k-1}\epsilon^{k-1}\right)^3 + a x_{k-1}\epsilon^{k-1}\left(z_{k-1}\epsilon^{k-1}\right)^2 + b\left(z_{k-1}\epsilon^{k-1}\right)^3 \\ &= 0, \end{aligned} \tag{72}$$

so, $z_{k-1} = 0$.

This yields $Ker(\pi^k) = \{[l\epsilon^{k-1} : 1 : 0] | \quad l \in \mathbb{F}_q\}$.

**Lemma 4.3** *The application*

$$\theta_k : \left| \begin{array}{lcl} \mathbb{F}_q & \to & E^k_{a,b} \\ l & \mapsto & [l\epsilon^{k-1} : 1 : 0] \end{array} \right. \tag{73}$$

is an injective group homomorphism.

**Proof.**

The application $\theta_k$ is injective by construction.

Let $[l\epsilon^{k-1} : 1 : 0]$ and $[h\epsilon^{k-1} : 1 : 0]$ be two elements in $E^k_{a,b}$, then:

$$\begin{aligned} k^\pi(l\epsilon^{k-1}) &= k^\pi(h\epsilon^{k-1}) \\ k^\pi(1) &= k^\pi(1) \\ k^\pi(0) &= k^\pi(0). \end{aligned} \tag{74}$$

so, using theorem (3.7),

$$\begin{aligned} X_3 &= (l+h)\epsilon^{k-1} \\ Y_3 &= 1 \\ Z_3 &= 0. \end{aligned} \tag{75}$$

This yields

$$\theta_k(l+h) = \theta_k(l) + \theta_k(h). \tag{76}$$

Thus, $\theta_k$ is an injective group homomorphism.

### 4.2 Main applications

In this subsection, we consider a prime $p$ which does not divide $N$, where $N = \sharp E^1_{k^\pi(a),k^\pi(b)}$.

**Corollary 4.4** *Let* $P \in E^k_{a,b}$, *then*

$$NP = [0 : 1 : 0] \Leftrightarrow P \in E^1_{k^\pi(a),k^\pi(b)}. \tag{77}$$

**Proof.**

If $P \in E^1_{k^\pi(a),k^\pi(b)}$, then $NP = [0 : 1 : 0]$.

Let $P = [x_0 + X : y_0 + Y : z_0 + Z] \in E^k_{a,b}$ and $Q = [x_0 : y_0 : z_0] \in E^1_{k^\pi(a),k^\pi(b)}$.

If $NP = [0 : 1 : 0]$, then $N(P - Q) = [0 : 1 : 0]$.

So, $P - Q = k_\theta(l_1, l_2, ...., l_{k-1})$.

We deduce that $Nl_i \equiv 0\ [p], i = 1, 2, ..., k - 1,$ where $pgcd(N, p) = 1,$ which proves that $l_i = 0$ et $P = Q$.

**Corollary 4.5**

$$\forall P \in E^k_{a,b}, we\ have\ pNP = [0 : 1 : 0]. \tag{78}$$

*DOI: http://dx.doi.org/10.5772/intechopen.93476*

**Proof.**
$\forall P \in E^k_{a,b}, NP \in k_G,$ so $pNP = [0:1:0]$..

**Lemma 4.6** *If p do not divide N, then there exists a unique homomorphism*

$$v_k : E^1_{a_0,b_0} \to E^k_{a,b} \tag{79}$$

for which the following diagram is commutative; (named Diagram(d)).

$$\begin{tikzcd} E^k_{a,b} \arrow[rr, "\pi_k"] \arrow[dr, "{[p]}"'] & & E^1_{a_0,b_0} \arrow[dl, "v_k"] \\ & E^k_{a,b} & \end{tikzcd}$$

**Proof.**
Let $P \in k_G,$ we have $pP = [0:1:0]$.

Then

$$k_G \subset ker([p]). \tag{80}$$

Hence, there is a unique homomorphism

$$v_k : E^1_{a_0,b_0} \to E^k_{a,b} \tag{81}$$

which makes the diagram(d) commutative.

**Theorem 4.7** *If p do not divide N, then there exists a unique homomorphism*

$$s_k : E^1_{a_0,b_0} \to E^k_{a,b} \tag{82}$$

such that $\pi_k o s_k = id_{E^1_{a_0,b_0}}$.

**Proof.**
Let $N' \in \mathbb{Z}$ as it exists $t \in \mathbb{Z}$ checking $1 - NN' = tp$. Then,

$$[1 - NN'] = [t]o[p]. \tag{83}$$

According to Lemma (4.6), there is a unique homomorphism

$$s_k : E^1_{a_0,b_0} \to E^k_{a,b} \tag{84}$$

which makes the following diagram commutative; (named Diagram(d')):

$$\begin{tikzcd} E^k_{a,b} \arrow[rr, "\pi_k"] \arrow[dr, "{[tp]}"'] & & E^1_{a_0,b_0} \arrow[dl, "s_k"] \\ & E^k_{a,b} & \end{tikzcd}$$

Let $P \in E^1_{a_0,b_0}$, then there exists $P' \in E^k_{a,b}$ such that $\pi_k(P') = P$. So,

$$\begin{aligned}\pi_k o s_k(P) &= \pi_k o s_k o \pi_k(P') \\ &= \pi_k([1 - NN'](P')) \\ &= \pi_k(P' - NN'P') \\ &= P - NN'P \\ &= P.\end{aligned} \tag{85}$$

**Theorem 4.8** *If p do not divide N, then* $E^k_{a,b} \cong E^1_{a_0,b_0} \times k_G$.
**Proof.**
The isomorphism

$$f_k : \left| \begin{array}{ll} E^1_{a_0,b_0} \times k_G & \to E^k_{a,b} \\ (P, Q) & \mapsto s_k(P) + Q \end{array} \right. \tag{86}$$

admits an inverse application

$$F_k : \left| \begin{array}{ll} E^k_{a,b} & \to E^1_{a_0,b_0} \times k_G \\ P & \mapsto (\pi_k(P), NN'P) \end{array} \right. . \tag{87}$$

Indeed,

$$\begin{aligned}f_k o F_k(P) &= f_k((\pi_k(P), NN'P)) \\ &= s_k o \pi_k(P) + NN'P \\ &= (1 - NN')P + NN'P \\ &= P.\end{aligned} \tag{88}$$

Likewise,

$$\begin{aligned}F_k o f_k(P, Q) &= F_k(s_k(P) + Q) \\ &= (\pi_k(s_k(P) + Q), NN'(s_k(P) + Q)).\end{aligned} \tag{89}$$

So,

$$\begin{aligned}\pi_k(s_k(P) + Q) &= \pi_k(s_k(P)) + \pi_k(Q) \\ &= P + [0 : 1 : 0] \\ &= P. \\ NN^{'}(s_k(P) + Q) &= NN'(s_k(P)) + NN'Q \\ &= NN'(1 - NN')P' + NN'Q \\ &= N'tpNP' + NN'Q \\ &= [0 : 1 : 0] + NN'Q \\ &= NN'Q.\end{aligned} \tag{90}$$

As, $pQ = [0:1:0]$, then we have

$$\begin{aligned} NN'Q &= (1-tp)Q \\ &= Q - tpQ \\ &= Q. \end{aligned} \tag{91}$$

We conclude,

$$F_k o f_k(P,Q) = (P,Q). \tag{92}$$

**Corollary 4.9** *If p do not divide N, then* $E^k_{a,b} \cong E^1_{a_0,b_0} \times \mathbb{F}_q^{k-1}$.
**Proof.**
We have, $k_G \cong \mathbb{F}_q^{k-1}$, see [27, 30, 33].
**Corollary 4.10** *If p do not divide N, then*

$$\begin{aligned} &E^k_{a,b} \cong C_N \times \mathbb{F}_q^{k-1}, \textit{with } C_N \textit{ cyclic} \\ &\quad \textit{or} \\ &E^k_{a,b} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{F}_q^{k-1}, \textit{where } n_2|(n_1 \wedge p-1). \end{aligned} \tag{93}$$

**Proof.**
We have

$$\begin{aligned} &E^1_{a_0,b_0} \cong C_N, \text{with } C_N \text{ cyclic} \\ &\quad \textit{or} \\ &E^1_{a_0,b_0} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}, \text{where } n_2|(n_1 \wedge p-1). \end{aligned} \tag{94}$$

And

$$E^k_{a,b} \cong E^1_{a_0,b_0} \times \mathbb{F}_q^{k-1}. \tag{95}$$

**Corollary 4.11** *If p do not divide N, then* $\left(\sqrt{q}-1\right)^2 q^{k-1} \leq \sharp\left(E^k_{a,b}\right) \leq \left(\sqrt{q}+1\right)^2 q^{k-1}$.
**Proof.**
According to Haas' theorem, we have:

$$|q+1-N| \leq 2\sqrt{q} \tag{96}$$

so

$$\left(\sqrt{q}-1\right)^2 q^{k-1} \leq \sharp\left(E^k_{a,b}\right) \leq \left(\sqrt{q}+1\right)^2 q^{k-1}. \tag{97}$$

## 5. Applications

In this section, we are interested in ECC using elliptic curves over the ring $R_n$.

### 5.1 The discrete logarithm on $\mathrm{E}^n_{a,b}$

The discrete logarithm problem that we denote DLP, (Discrete logarithm problem), is a generally difficult problem which depends on the considered group $\mathcal{G}$. In many situations, due to the asymmetry existing between problems concerning the calculation of logarithms and calculation of powers which is more easier and so of great interest in cryptograph, the above mentioned makes Diffie and Hellman were the first to build a cryptosystem from this situation [37, 38].

**Definition 5.1** *Let $\mathcal{G}$ be a finite cyclic group of order $\rho$ and $s, r$ two elements of $\mathcal{G}$. We call discrete logarithm of base s of r, the only element m in $[[0, \rho - 1]]$ such that $s^m = r$. The discrete logarithm for elliptic curves is defined in an analogous way to be, the only element m in $[[0, \rho - 1]]$ such that $mP = Q$, where $P$, and $Q$ are two points of an additive subgroup $\mathcal{G}$ of $\mathbf{E}^n_{a,b}$.*

By using the isomorphism proved given in theorem (4.8), we get the results gathered in the next theorem:

**Theorem 5.2** *If p does not divide N, then.*

- $\#\mathbf{E}^n_{a,b} = p^{d(n-1)} \times N$.
- The problem of the discrete logarithm on the elliptic curve $\mathbf{E}^n_{a,b}$ is equivalent to that of $\mathbf{E}^1_{a_0,b_0}$.
- If the problem of the discrete logarithm on $\mathbf{E}^n_{a,b}$ is trivial, then it is also trivial on the elliptic curve $\mathbf{E}^1_{a_0,b_0}$.

### 5.2 Cryptography based on elliptic curves $\mathbf{E}^n_{a,b}$

Elliptic curve cryptography (ECC) is public key cryptography, which relies on the use of curves over finite fields. Essentially, there are two families of these curves which are used in cryptography. The first uses elliptic curves on a finite field $\mathbb{F}_{p^d}$, where $p$ is a large prime number. This family is the best choice for a high software level when implementing ECC. The second family uses elliptic curves on a binary field $\mathbb{F}_{2^d}$ where $d$ is a large positive integer, this family is more appropriate at the material level point of view when implementing ECC. Another family which is also interesting in ECC implementations is the family of elliptic curves on the previously seen rings $\mathbf{R_n}$. The most important advantage presented by the use of elliptic curves in cryptography (ECC) consists in the high security they provide for wireless applications compared to other asymmetric key cryptosystems, also their small key size. Indeed, a 160-bit key for (ECC) can replace a 1024-bit key for (RSA). Given $d$; a large integer, $P \in \mathbf{E}^n_{a,b}$ and $Q \in \mathcal{G} \subset \mathbf{E}^n_{a,b}$. The discrete elliptical logarithm problem (DLEP) consists in finding $k \in \mathbb{Z}\, such\ \ that\ Q = [k]P$, where

$$[k]P = \underbrace{P + P + \cdots P}_{ktimes} = kP. \tag{98}$$

This is in fact a difficult problem, whose resolution is exponential.

### 5.3 Elliptical Diffie-Hellman cryptosystem

Recall that Alice and Bob can publicly agree on a common secret (that we describe below).

1. They choose on a large integer $d$, $\mathbf{E}^n_{a,b}\ \ and\ \ P \in \mathbf{E}^n_{a,b}$.

2. Alice chooses $t \in \mathbb{Z}$ and calculates $tP$.

3. Bob chooses $s \in \mathbb{Z}$ and calculates $sP$.

4. Alice let public $tP$ and keep private $t$.

5. Bob let public $sP$ and keep private $s$.

6. Then, Alice and Bob build their common secret key $K = tsP = stP$.

**Remark 5.3**

1. Unlike the classic Diffie-Hellman algorithm, we do not ask that $P$ be a generator of $\mathbf{E}^n_{a,b}$. The analogue of the subgroup $\mathbb{F}_p^*$ of order $p-1$, is the cyclic subgroup of $\mathbf{E}^n_{a,b}$, generated by the point $P$.

2. As soon as we have a group $\mathbf{E}^n_{a,b}$, and an element $P \in \mathbf{E}^n_{a,b}$ of finite order we can consider a Diffie-Hellman system on $\mathcal{G} = <P>$ which is cyclic. For this construction to have a cryptographic interest, $log_{\,P}(tP) = t$ must be not easy to calculate.

3. $\mathbf{E}^n_{a,b}$, is not always cyclical.

4. If, Oscar (program) is giving $d, \mathbf{E}^n_{a,b}, tP\ and\ sP$, then it is able to solve the discrete elliptical logarithm problem and find $t\ or\ s$.

### 5.4 Elliptical ElGamal cryptosystem

Let $P_m \in \mathbf{E}^n_{a,b}$ be the point representing the message m, to encrypt $P_m$ :

1. Key generation algorithm

    - Bob chooses the private key $t \in \mathbb{Z}$ known only to him.

    - $d \in \mathbb{N}, P \in \mathbf{E}^n_{a,b}\ and\ R = [t]P$ are public.

2. Encryption algorithm

    - Alice Randomly chooses $k \in \mathbb{Z}$;

    - She calculates $c_1 = [k]P \in \mathbf{E}^n_{a,b}$;

    - She also calculates $c_2 = P_m + [k]R$;

    - Then, he makes public $c_1, c_2$, or $C = (c_1; c_2)$.

3. To decrypt received message $(c_1, c_2)$, Bob calculates:

$$P_m = c_2 - [k]R = c_2 - [k][t]P = c_2 - [t]c_1. \tag{99}$$

Now, Oscar encounters the discrete elliptic logarithm problem, because to decipher the message $P_m$ he must know $t$ (i.e.; calculate $t$ such that $R = [t]P$).

### 5.5 Coding example

Let $d$ be a positive integer, we consider the quotient ring $\mathbf{R}_2 = \frac{\mathbb{F}_{2^d}[X]}{(X^2)}$, where $\mathbb{F}_{2^d}$ is the finite field of order $2^d$.

Then the ring $\mathbf{R}_2$ is identified with the ring $\mathbb{F}_{2^d}[\varepsilon]$, where $\varepsilon^2 = 0$, i.e.,

$$\mathbf{R}_2 = \left\{ a_0 + a_1 \cdot \varepsilon | a_0, a_1 \in \mathbb{F}_{2^d} \right\}. \tag{100}$$

We consider the elliptic curve on the ring $\mathbf{R}_2$ given by the equation:

$$Y^2Z + XYZ = X^3 + aX^2Z + bZ^3. \tag{101}$$

where $a, b$ in $\mathbf{R}_2$ and $b$ is invertible in $\mathbf{R}_2$. Each element of $\mathbf{E}^2_{a,b}$ is of the form; $[X : Y : 1]$ or $[x\varepsilon : 1 : 0]$, with $x \in \mathbb{F}_{2^d}$. Write:

$$\mathbf{E}^2_{a,b} = \left\{ [X : Y : 1] \in \mathbb{P}^2_2 | Y^2 + XY = X^3 + aX^2 + b \right\} \cup \left\{ [x\varepsilon : 1 : 0] | x \in \mathbb{F}_{2^d} \right\}. \tag{102}$$

Let $\mathbf{E}^2_{a,b}$ be the elliptic curve over $R_2$ and consider the irreducible polynomial $T(X) = 1 + X + X^3$ in $\mathbb{F}_2[X]$. Let $\alpha$ be such that $T(\alpha) = 0$ in $\mathbb{F}_8 = \frac{\mathbb{F}_2[X]}{(T(X))}$, then $(1, \alpha, \alpha^2)$ is a vector space base of $\mathbb{F}_8$ over $\mathbb{F}_2$.

$$\mathbb{F}_8 = \left\{ 0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^2 + 1, \alpha^2 + \alpha + 1 \right\} \tag{103}$$

$\star$ Put:

$$a = 1 + \alpha; \tag{104}$$

$$b = 1 + \alpha^2\varepsilon. \tag{105}$$

We have: $\mathbf{R}_2 = \mathbb{F}_8[\varepsilon]$ and $\mathbf{E}^2_{a,b} : Y^2 + XY = X^3 + (1 + \alpha)X^2 + (1 + \alpha^2\varepsilon)$. Consider $P \in \mathbf{E}^2_{a,b}$ of order $l$, and consider the subgroup $\mathcal{G} = <P>$, generated by $P$, to encrypt and decrypt our messages.

1. Coding of elements of $\mathcal{G}$

We will give a code to each element $Q = mP$, where $m \in \{1, 2, .., l\}$, defined as follows:
If $Q = [x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : Z]$, where $x_i, y_i \in \mathbb{F}_8$ for $i = 0, 1$, and $Z = 0 \, or \, 1$, then we set:

$$x_i = c_{0i} + c_{1i}\alpha + c_{2i}\alpha^2; \tag{106}$$

$$y_i = d_{0i} + d_{1i}\alpha + d_{2i}\alpha^2, \tag{107}$$

where $\alpha$ is the primitive root of the irreducible polynomial $T(X) = 1 + X + X^3$, and $c_{ij}, d_{ij} \in \mathbb{F}_2$.
So, we code $Q$ as follows:
If $Z = 1$: $Q = c_{00}c_{10}c_{20}c_{01}c_{11}c_{21}d_{00}d_{10}d_{20}d_{01}d_{11}d_{21}1$.
If $Z = 0$: $Q = 00c_{01}c_{11}c_{21}d_{01}d_{11}d_{21}10000$.

2. Example: with the same $a$ and $b$;

$$a = 1 + \alpha; \tag{108}$$

$$b = 1 + \alpha^2 \varepsilon. \tag{109}$$

The elliptic curve $\mathbf{E}^2_{a,b}$ contains 112 elements to know:

$$\mathbf{E}_{a,b}(\mathbb{A}_2) = \{[(\alpha^2+\alpha+1)\varepsilon : 1 : 0], [(\alpha^2+1)\varepsilon : 1 : 0], [(1+\alpha)\varepsilon : 1 : 0], [(\alpha^2+\alpha)\varepsilon : 1 : 0], [\alpha^2\varepsilon : 1 : 0], [\alpha\varepsilon : 1 : 0], [\varepsilon+\alpha^2+1 : \alpha\varepsilon+\alpha : 1], [\alpha^2+\alpha : (\alpha^2+\alpha+1)\varepsilon : 1], [\alpha^2\varepsilon : \varepsilon+1 : 1], [(\alpha^2+1)\varepsilon+\alpha^2+1 : (\alpha^2+\alpha)\varepsilon+\alpha : 1], [(1+\alpha)\varepsilon+\alpha^2 : (\alpha^2+\alpha+1)\varepsilon+\alpha^2+1 : 1], [(\alpha^2+\alpha)\varepsilon+1+\alpha : (\alpha^2+\alpha+1)\varepsilon+\alpha^2 : 1], [(1+\alpha)\varepsilon+\alpha^2+1 : \alpha : 1], [\alpha^2\varepsilon+\alpha^2+\alpha+1 : \varepsilon+1 : 1], [1+\alpha : (\alpha^2+1)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha : (\alpha^2+1)\varepsilon+\alpha^2+\alpha : 1], [\alpha\varepsilon+\alpha^2 : (\alpha^2+1)\varepsilon+\alpha^2+1 : 1], [(1+\alpha)\varepsilon+\alpha^2+\alpha+1 : (1+\alpha)\varepsilon+1 : 1], [\alpha^2\varepsilon : (1+\alpha)\varepsilon+1 : 1], [\alpha^2\varepsilon+1+\alpha : \alpha^2\varepsilon+\alpha^2+\alpha+1 : 1], [\alpha\varepsilon+\alpha^2+1 : \varepsilon+\alpha : 1], [(1+\alpha)\varepsilon+\alpha^2+\alpha : (\alpha^2+1)\varepsilon+\alpha^2+\alpha : 1], [\alpha^2\varepsilon+\alpha^2+\alpha+1 : (\alpha^2+1)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+1)\varepsilon+1+\alpha : (\alpha^2+\alpha)\varepsilon+\alpha^2 : 1], [\alpha\varepsilon+\alpha^2+\alpha : \tag{110}$$

$$0 : 1], [\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2 : (1+\alpha)\varepsilon+1 : 1], [\alpha^2\varepsilon+\alpha^2+1 : (\alpha^2+\alpha+1)\varepsilon+\alpha : 1], [(1+\alpha)\varepsilon+\alpha^2+\alpha : (\alpha^2+\alpha)\varepsilon : 1], [(\alpha^2+\alpha+1)\varepsilon+1+\alpha : \varepsilon+\alpha^2 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+1)\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+1)\varepsilon+1+\alpha : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [\varepsilon+\alpha^2 : \alpha\varepsilon+1 : 1], [(\alpha^2+1)\varepsilon+\alpha^2+\alpha+1 : \alpha\varepsilon+1 : 1], [\alpha^2\varepsilon : \alpha\varepsilon+1 : 1], [\varepsilon+\alpha^2+\alpha : \varepsilon : 1], [(1+\alpha)\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [\alpha^2\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [\alpha\varepsilon+\alpha^2+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha+1 : \alpha^2\varepsilon+1 : 1], [(1+\alpha)\varepsilon+\alpha^2 : \alpha^2\varepsilon+1 : 1], [\alpha^2\varepsilon : \alpha^2\varepsilon+1 : 1], [\alpha^2+\alpha+1 : (\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha : 1], [\alpha^2\varepsilon : 1 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2 : 1 : 1], [\varepsilon+\alpha, (1+\alpha)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha+1 : (1+\alpha)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha : (1+\alpha)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+\alpha)\varepsilon+1+\alpha : \varepsilon+\alpha^2+\alpha+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha : (1+\alpha)\varepsilon : 1], [\varepsilon+\alpha^2+\alpha+1 : \alpha^2\varepsilon+\alpha^2+\alpha : 1], [\varepsilon+1+\alpha : \alpha\varepsilon+\alpha^2+\alpha+1 : 1], [\alpha : \alpha\varepsilon+\alpha^2+\alpha : 1], [\alpha\varepsilon+\alpha^2+\alpha+1 : \alpha\varepsilon+\alpha^2+\alpha : 1], [\alpha\varepsilon+\alpha^2+\alpha+1 : 1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha : \alpha^2\varepsilon+\alpha^2+\alpha : 1], [\alpha^2 : \varepsilon+\alpha^2+1 : 1], [(1+\alpha)\varepsilon+1+\alpha : (\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha+1 : 1], [\alpha^2+\alpha : (\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha : 1], [\varepsilon+\alpha^2+\alpha : \alpha^2+\alpha : 1], [\alpha\varepsilon+1+\alpha : \alpha^2+\alpha+1 : 1], [\alpha^2 : \varepsilon+1 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha+1 : (\alpha^2+\alpha+1)\varepsilon+1 : 1], [\alpha^2\varepsilon : (\alpha^2+\alpha+1)\varepsilon+1 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2+1 : (\alpha^2+1)\varepsilon+\alpha : 1], [\varepsilon+\alpha^2 : (1+\alpha)\varepsilon+\alpha^2+1 : 1], [\varepsilon+1+\alpha : (1+\alpha)\varepsilon+\alpha^2 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2 : (\alpha^2+\alpha)\varepsilon+\alpha^2+1 : 1], [(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha : (\alpha^2+1)\varepsilon : 1], [\varepsilon+\alpha^2+\alpha+1 : (\alpha^2+1)\varepsilon+1 : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2+1 : \alpha^2\varepsilon+\alpha : 1], [\alpha^2\varepsilon+\alpha^2+\alpha : \alpha\varepsilon : 1], [(\alpha^2+\alpha)\varepsilon+\alpha : \alpha^2\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+\alpha)\varepsilon+\alpha : \alpha\varepsilon+\alpha^2 : 1], [(\alpha^2+1)\varepsilon+\alpha : \alpha\varepsilon+\alpha^2 : 1], [(1+\alpha)\varepsilon+\alpha : \alpha\varepsilon+\alpha^2 : 1], [(1+\alpha)\varepsilon+\alpha : \varepsilon+\alpha^2+\alpha : 1], [(1+\alpha)\varepsilon+\alpha^2+\alpha+1 : \alpha^2+\alpha : 1], [\alpha^2+\alpha+1 : (\alpha^2+\alpha)\varepsilon+1 : 1], [\alpha^2\varepsilon : (\alpha^2+\alpha)\varepsilon+1 : 1], [\alpha^2\varepsilon+\alpha : \alpha\varepsilon+\alpha^2 : 1], [\alpha\varepsilon+1+\alpha : \alpha\varepsilon+\alpha^2 : 1], [\alpha\varepsilon+\alpha : \alpha\varepsilon+\alpha^2 : 1], [(\alpha^2+1)\varepsilon+\alpha^2 : \alpha^2+1 : 1], [\alpha\varepsilon+\alpha : \alpha^2+\alpha : 1], [(1+\alpha)\varepsilon+1+\alpha : \alpha^2\varepsilon+\alpha^2 : 1], [(\alpha^2+1)\varepsilon+\alpha^2+\alpha : \varepsilon+\alpha^2+\alpha : 1], [\alpha\varepsilon+\alpha^2+\alpha : \alpha\varepsilon+\alpha^2+\alpha : 1], [\alpha^2\varepsilon+\alpha^2 : \alpha\varepsilon+\alpha^2+1 : 1], [(\alpha^2+1)\varepsilon+\alpha^2+\alpha+1 : (\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+1)\varepsilon+\alpha : (\alpha^2+\alpha+1)\varepsilon+\alpha^2+\alpha : 1], [(\alpha^2+\alpha+1)\varepsilon+\alpha^2 : \alpha^2\varepsilon+\alpha^2+1 : 1], [\alpha^2\varepsilon : \tag{111}$$

$$(\alpha^2+1)\varepsilon+1:1], [\alpha^2\varepsilon+\alpha:(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha:1], [1+\alpha:(\alpha^2+1)\varepsilon+\alpha^2:1], [(\alpha^2+\alpha+1)\varepsilon+1+\alpha:(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha+1:1], [\alpha^2\varepsilon+\alpha^2:(\alpha^2+\alpha)\varepsilon+1:1], [\alpha^2+1:(1+\alpha)\varepsilon+\alpha:1], [(\alpha^2+1)\varepsilon+\alpha^2+\alpha:\alpha^2\varepsilon:1], [\alpha^2\varepsilon+1+\alpha:\alpha^2:1], [0:1:0], [\alpha:\alpha\varepsilon+\alpha^2:1], [\varepsilon+\alpha:\alpha\varepsilon+\alpha^2:1], [(\alpha^2+\alpha+1)\varepsilon+\alpha:\alpha\varepsilon+\alpha^2:1], [(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha+1:\varepsilon+\alpha^2+\alpha:1], [\alpha^2\varepsilon+\alpha^2+\alpha:(\alpha^2+\alpha)\varepsilon+\alpha^2+\alpha:1], [\alpha\varepsilon+\alpha^2:(\alpha^2+\alpha+1)\varepsilon+1:1], [\varepsilon:1:0], [(\alpha^2+1)\varepsilon+\alpha^2:(\alpha^2+1)\varepsilon+1:1]\} \tag{112}$$

We consider: $P=[\alpha:\alpha+\alpha^2+\alpha\varepsilon:1]=0100000110101,$ then $\mathcal{G}=<P>$ is of order 28. We attach to each point $Q\in\mathcal{G}$ a letter of the alphabet and a code. We collect the results in the following **Table 2**:

| | **mP** | **Codefor mP** | **Symbol** |
|---|---|---|---|
| 1 | $[\alpha:\alpha+\alpha^2+\alpha\varepsilon:1]$ | 0100000110101 | *a* |
| 2 | $[1+\alpha+\varepsilon:\alpha^2+(1+\alpha)\varepsilon:1]$ | 1101000011101 | *b* |
| 3 | $[\alpha^2+\alpha\varepsilon:1+\alpha^2+(\alpha^2+1)\varepsilon:1]$ | 0010101011011 | *c* |
| 4 | $[1+\alpha+\alpha^2+(1+\alpha)\varepsilon:\alpha+\alpha^2:1]$ | 1111100110001 | *d* |
| 5 | $[\alpha+\alpha^2+(1+\alpha+\alpha^2)\varepsilon:(1+\alpha)\varepsilon:1]$ | 0111110001101 | *e* |
| 6 | $[1+\alpha^2+(1+\alpha+\alpha^2)\varepsilon:\alpha+\alpha^2\varepsilon:1]$ | 1011110100011 | *f* |
| 7 | $[\alpha^2\varepsilon:1+(1+\alpha^2)\varepsilon:1]$ | 0000011001011 | *g* |
| 8 | $[1+\alpha^2+(1+\alpha^2)\varepsilon:1+\alpha+\alpha^2+(1+\alpha)\varepsilon:1]$ | 1011011111101 | *h* |
| 9 | $[\alpha+\alpha^2+\alpha\varepsilon:\alpha+\alpha^2+\alpha\varepsilon:1]$ | 0110100110101 | *i* |
| 10 | $[1+\alpha+\alpha^2+\alpha\varepsilon:1:1]$ | 1110101000001 | *j* |
| 11 | $[\alpha^2+\alpha^2\varepsilon:1+(\alpha+\alpha^2)\varepsilon:1]$ | 0010011000111 | *k* |
| 12 | $[1+\alpha+(\alpha+\alpha^2)\varepsilon:1+\alpha+\alpha^2+\varepsilon:1]$ | 1100111111001 | *l* |
| 13 | $[\alpha+(1+\alpha)\varepsilon:\alpha^2+\alpha\varepsilon:1]$ | 0101100010101 | *m* |
| 14 | $[\alpha^2\varepsilon:1:0]$ | 0000100010000 | *n* |
| 15 | $[\alpha+(1+\alpha)\varepsilon:\alpha+\alpha^2+\varepsilon:1]$ | 0101100111001 | *o* |
| 16 | $[1+\alpha+(\alpha+\alpha^2)\varepsilon:\alpha^2+(1+\alpha+\alpha^2)\varepsilon:1]$ | 1100110011111 | *p* |
| 17 | $[\alpha^2+\alpha^2\varepsilon:1+\alpha^2+\alpha\varepsilon:1]$ | 0010011010101 | *q* |
| 18 | $[1+\alpha+\alpha^2+\alpha\varepsilon:\alpha+\alpha^2+\alpha\varepsilon:1]$ | 1110100110101 | *r* |
| 19 | $[\alpha+\alpha^2+\alpha\varepsilon:0:1]$ | 0110100000001 | *s* |
| 20 | $[1+\alpha^2+(1+\alpha^2)\varepsilon:\alpha+(\alpha+\alpha^2)\varepsilon:1]$ | 1011010100111 | *t* |
| 21 | $[\alpha^2\varepsilon:1+\varepsilon:1]$ | 0000011001001 | *u* |
| 22 | $[1+\alpha^2+(1+\alpha+\alpha^2)\varepsilon:1+\alpha+\alpha^2+(1+\alpha)\varepsilon:1]$ | 1011111111101 | *v* |
| 23 | $[\alpha+\alpha^2+(1+\alpha+\alpha^2)\varepsilon:\alpha+\alpha^2+\alpha^2\varepsilon:1]$ | 0111110110011 | *w* |
| 24 | $[1+\alpha\alpha^2+(1+\alpha)\varepsilon:1+(1+\alpha)\varepsilon:1]$ | 1111101001101 | *x* |
| 25 | $[\alpha^2+\alpha\varepsilon:1+(1+\alpha+\alpha^2)\varepsilon:1]$ | 0010101001111 | *y* |
| 26 | $[1+\alpha+\varepsilon:1+\alpha+\alpha^2+\alpha\varepsilon:1]$ | 1101001110101 | *z* |
| 27 | $[\alpha:\alpha^2+\alpha\varepsilon:1]$ | 0100000010101 | *space* |
| 28 | $[0:1:0]$ | 0000000010000 | , |

**Table 2.**
*Points coding.*

### 5.6 Encryption and decryption procedures

- The encryption of our message “for the elliptical curve”, is;

$$
\begin{array}{l}
0111110110011011111000110101000000010101000000\\
11001001011010000000101111100011010100000010\\
1011011010100111101101111110101111000110101\\
000000101010111110001101110011111100111001 11\\
11100101101001101011100110011111101101010011\\
10110100110101001010101101101000000101010010\\
1010110110000011001001111010011010110111111 1\\
110101111100011010000000010000
\end{array}
\tag{113}
$$

- Decryption of this message:

$$
\begin{array}{l}
0100000110101110100001110111111001100010111 1\\
10001101110011111100110110111111010100000110\\
1010101100010101011010011010111111001100010 1\\
000000101011011010100111010000011010111111 00\\
110001010110001010101011001110011110100110101 0\\
110100110101
\end{array}
\tag{114}
$$

is: hello to abdelhakim.

## 6. Conclusion

The results obtained are very important from theoretical points of view because to study an elliptic curve on a finite local ring it suffices to study these curves on finite fields, for the applications of these curves they can be applied in cryptography to reinforce security and we can use them in cryptanalysis to solve the PDL on special curves. This results are very imploring and give applications in different fields such as classical mechanics, number theory, cryptology, information theory … and we can quote here:

1. The generalization of Hass’s theorem, corollary 4.9.
2. The result of the corollary 4.11, then in [24], we have the result of the Proposition 3.12.

## Acknowledgements

The authors thank professor Karim Mounirh for his correcting typographical, grammatical, spelling, and punctuation errors to ensure the clear and accurate communication.

## Author details

Abdelhakim Chillali* and Lhoussain El Fadil
Sidi Mohamed Ben Abdellah University, Morocco

*Address all correspondence to: abdelhakim.chillali@usmba.ac.ma

## References

[1] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. SIAM Journal on Computing. 2003;**32**(3): 586-615

[2] Hoffstein J, Pipher J, Silverman JH. An Introduction to Mathematical Cryptography. Springer, New York, NJ, USA: Undergraduate Texts in Mathematics; 2008

[3] Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation. 1987;**48**:203-209

[4] Diffie W, Hellman ME. New directions in cryptography. In: IEEE Transactions on Information Theory. Vol. 22. IEEE Xplore; 1976. pp. 644-654

[5] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security. 2001;**1**(1):36-63

[6] Tzer-Shyong C, Gwo-Shiuan H, Tzuoh-Pyng L, Yu-Fang C. Digital signature scheme resulted from identification protocol by elliptic curve cryptosystem. In: Tencon '02. Proceedings. 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering. Vol. 1. Beijing: IEEE; 2002. pp. 192-195

[7] Shannon CE. Communication theory of secrecy systems. Bell System Technical Journal. 1949;**28**(4):656-715

[8] Shannon CE. A mathematical theory of communication. Bell System Technical Journal. 1948;**27**(4):379-423

[9] Beutelspacher A, Rosenbaum U. Projective Geometry: From Fondations to Application. Cambridge: Cambridge University Press; 1998

[10] Hartshorne J. Algebraic Geometry. Vol. 52. Springer-Verlag, GTM; 1977

[11] Lang S. Algebraic Number Theory. New York: Springer; 1986

[12] Lenstra AK, Lenstra HW Jr, editors. The Development of the Number Field Sieve, Volume 1554 of Lecture Notes in Mathematics. Berlin: Springer-Verlag; 1993

[13] Joux A. A one round protocol for tripartite Diffie-Hellman. Journal of Cryptology. 2004;**17**(4):263-276

[14] Joux A, Pierrot C. Improving the Polynomial Time Precomputation of Frobenius Representation Discrete Logarithm Algorithms Simplified Setting for Small Characteristic Finite Fields. Springer-Verlag; 2014

[15] Joux A, Vitse V. Elliptic curve discrete logarithm problem over small degree extension fields application to the static Diffie-Hellman problem on $\mathbf{E}(\mathbb{F}_{q^5})$. Journal of Cryptology. 2013;**26**(1):119-143

[16] Maurer UM, Wolf S. Diffie Hellman oracles. In: Crypto, 96, LNCS. 1109. Springer-Verlag; 1996. pp. 268-282

[17] Menezes AJ, Okamoto T, Vanstone SA. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory. 1993;**39**(5):1639-1646

[18] Popescu C. An identification scheme based on the elliptic curve discrete logarithm problem. In: Proceedings of the Fourth International Conference/ Exhibition on High Performance Computing in the Asia-Pacific Region. Vol. 2. Beijing: IEEE; 2000. pp. 624-625

[19] Fontein F. Elliptic Curves over Rings with a Point of View on Cryptography and Factoring. Vol. 28. Company, Reading, Massachusetts:

Diplomarbeit, Carl von Ossietzky Universität Oldenburg Diplomstudiengang Mathematik; 2005

[20] Silverman JH. Advanced topics in the arithmetic of elliptic curves. In: Volume 151 of Graduate Texts in Mathematics. Springer; 1994

[21] Silverman JH. The arithmetic of elliptic curves. In: Graduate Texts in Mathematics. Vol. 106. Springer; 1986

[22] Semaev I. New algorithm for the discrete logarithm problem on elliptic curves. Computer Science and Security. 2015; Cryptology ePrint Archive, Report 2015/310

[23] Elhassani M, Chillali A, Mouhib A. Elliptic curve and lattice cryptosystem. In: Proceedings - 2019 International Conference on Intelligent Systems and Advanced Computing Sciences. ISACS; 2019

[24] Boulbot A, Chillali A, Mouhib A. Elliptic curves over the ring R. Boletim da Sociedade Paranaense de Matematica (BSPM). 2020;**38**(3):193-201

[25] Sahmoudi M, Chillali A. Elliptic curve on a family of finite ring. WSEAS Transactions on Mathematics. 2019;**18**: 415-422

[26] Sahmoudi M, Chillali A. SCC-cryptosystem on an algebraic closure ring. Journal of Discrete Mathematical Sciences and Cryptography. 2019. DOI: 10.1080/09720529.2019.1624338

[27] Chillali A. Identification methods over. In: ICACM'11 Proceedings of the 2011 International Conference on Applied & Computational Mathematics, ACM Digital Library. Recent Researches in Applied and Computational Mathematics. 2011. pp. 133-138

[28] Hassib MH, Chillali A, Elomary MA. Special ideal ring A3 and cryptography. In: Proceedings of the International Conference JNS3. IEEE; 2013. pp. 1-4

[29] Tadmori A, Chillali A, Ziane M. The binary operations calculus in $\mathbf{E}_{a,b,c}$. International Journal of Mathematical Models and Methods in Applied Sciences. 2015;**9**:171-175

[30] Chillali A. The $J_{\varepsilon,n}$-invariant of $\mathbf{E}^n_{A,B}$. In: Recent Advances in Computers, Communications, Applied Social Science and Mathematics -Proceedings of ICANCM'11, ICDCC'11, IC-ASSSE-DC'11. 2011

[31] Tadmori A, Chillali A, Ziane M. Elliptic curve over ring $\mathbf{A_4} = \mathbb{F}_{2^d}[\varepsilon]; \varepsilon^4 = 0$. Applied Mathematical Sciences. 2015;**9**(35):1721-1733

[32] Bosma W, Lenstra H. Complete system of two addition laws for elliptic curved. Journal of Number Theory. 1995;**53**:229-240

[33] Chillali A. Cryptography over elliptic curve of the ring $\mathbb{F}_q[\varepsilon], \varepsilon^4 = 0$. World Academy of Science, Engineering and Technology. 2011;**5**:917-919

[34] Hassib MH, Chillali A, Elomary MA. Elliptic curves over a chain ring of characteristic 3. Journal of Taibah University for Science. 2014;**9**(3): 276-287

[35] Tadmori A, Chillali A, Ziane M. Normal form of the elliptic curve over the finite ring. Journal of Mathematics and System Science. 2014;**4**:194-196

[36] Tadmori A, Chillali A, Ziane M. Elliptic curve over SPIR of characteristic two. In: Proceeding of the 2013 International Conference on Applied Mathematics and Computational Methodes. 2013. pp. 41-44

[37] Okamoto T, Uchiyama S. A new pubic-key cryptosystem as secure as factoring. In: Eurocrypt, 98, LNCS. 1403. Springer-Verlag; 1998. pp. 308-318

[38] Washington LC. Elliptic curves number theory and cryptography. In: Discrete Mathematics and its Applications. Chapman and Hall/CRC; 2003