IJAMML 17:1 (2023) 1-26 March 2023
ISSN: 2394-2258
Available at http://scientificadvances.co.in
DOI: http://dx.doi.org/10.18642/ijamml_7100122261

AN MODAL ϴ-VALENT APPROACH OF THE RSA CRYPTOSYSTEM

Jean Armand Tsimi

Department of Mathematics and Computer Sciences, Faculty of Sciences, University of Douala, PO Box: 24157 Douala, Cameroon

Abstract

In this note, from the appropriate modal Θ-valent mathematical notions, we define a modal Θ-valent view of the RSA cryptosystem, and then, we propose an practical application.

Keywords: $m\Theta$ Fermat-Euler's theorem, formal $m\Theta$ Euler's function, formal $m\Theta$ exponentiation, $m\Theta$ congruence, RSA cryptosystem.

1. Introduction

In 1976, Diffie and Hellman introduced in [3] the concept of the public-key cryptosystem. Since then, a number of public-key cryptosystems have been proposed. The RSA cryptosystem was proposed

*Corresponding author.
E-mail address: tsimije@yahoo.fr (Jean Armand Tsimi).

2020 Mathematics Subject Classification: 94A60, 11A99, 11T71, 03G25, 03B45.
Submitted by Jianqiang Gao.
Received August 22, 2022

in 1978 by Ronald Rivest et al. in [4] as an example of public-key system. This means that everyone can know the encryption key, but it is computationally infeasible for an unauthorized person to deduce the corresponding decryption key. In the RSA cryptosystem, the public modulus $N = pq$ is a product of two primes of the same bit size. The public and private exponent e and d satisfy the congruence $ed \equiv 1(\mathrm{mod}\, \phi(N))$, where $\phi(N) = (p-1)(q-1)$ is the Euler totient function. Encryption, decryption, signature and signature-verification in RSA require the computation of heavy exponentiations. Although the RSA algorithm is indeed among the strongest, the question that arises is whether it could withstand the test of time. But, as without a doubt nothing can withstand the test of time, we intend to present a modal Θ-valent view of the RSA cryptosystem in order to improve its robustness. We understand by the modal Θ-valent view that we will present the RSA cryptosystem from the mathematical algebraic structures specific to a new logic defined by Eteme in [1] named the modal Θ-valent chrysippian logic which appears as a modal Θ-valent chrysippian extension of the boolean logic. The modal Θ-valent chrysippian logic admits states of truth other than true and false, and has as algebraic representation the modal Θ-valent chrysippian ring introduced in [1]. From the modal Θ-valent chrysippian logic, the notions of modal Θ-valent $(m\Theta)$ sets, of $m\Theta$ algebraic structures as soon as the notions of the modal Θ-valent congruence, the formal modal Θ-valent exponentiation, the formal modal Θ-valent Euler's function, and the modal Θ-valent Fermat-Euler theorem are defined in [1]. In this note, we intend to propose a modal Θ-valent view of the RSA cryptosystem. The rest of the paper is structured as follows: In the Section 2, we will present the basic necessary modal Θ-valent mathematical notions useful for our purpuse. In the Section 3, we will present a modal Θ-valent approach of the RSA cryptosystem. A practical application will be presented in the Section 4.

2. The Modal Θ-Valent Sets

2.1. Generalities

2.1.1. The notion of modality over a classical set

Let E be a non empty set.

Definition 2.1. One calls structure of modalities over E, every tuple $(E, (f_\alpha)_{\alpha\in I_*})$ such that:

(1) I is a closed chain $0, 1$ and $I_* = I\setminus\{0\}$.

(2) $\forall\alpha \in I\setminus\{0\}$, $f_\alpha : E \to E$ is a map fulfulling:

- $\bigcap_{\alpha\in I_*} f_\alpha(E) \neq \emptyset$;
- $\forall\alpha, \beta \in I_*$, $\alpha \neq \beta \Rightarrow f_\alpha \neq f_\beta$;
- $\forall\alpha, \beta \in I_*$, $f_\beta o f_\alpha = f_\alpha$.

Notation 2.1. We write (E, f_α) instead of $(E, (f_\alpha)_{\alpha\in I_*})$ for short.

Remark 2.1. If Θ (resp., Θ_*) is the ordinal of I (resp., I_*), then the chain I is said Θ-valent and (E, f_α) is called an $m\Theta$ structure of modalities over the set E.

Proposition 2.1. *Let (E, f_α) be an $m\Theta$ structure of modalities over E.*

For every $\alpha \in I_*$, let R_α be the equivalence relation defined on E by: $xR_\alpha y \Leftrightarrow f_\alpha(x) = f_\alpha(y)$.

Let R_Θ be the binary relation over E defined by:

$$xR_\Theta y \Leftrightarrow \forall\alpha \in I_*, f_\alpha(x) = f_\alpha(y)$$

$$\Leftrightarrow \forall\alpha \in I_*, xR_\alpha y$$

R_Θ is an equivalence relation on E.

Proof ([1]). $R_\Theta = \bigwedge_{\alpha\in I_*} R_\alpha$ by definition.

Proposition 2.2. *Let* $\frac{E}{\Theta} = \frac{E}{R_\Theta}$ *be the quotient of* E *by* R_Θ.

Let $x \in E$ *and* $\frac{x}{\Theta} = \frac{x}{R_\Theta} = \{y \in E/\forall\alpha \in I_*, f_\alpha(x) = f_\alpha(y)\}$ *be the equivalence class of* x *modulo* R_Θ. *For every* $\alpha \in I_*$, *let set* $F_\alpha : \frac{E}{\Theta} \to \frac{E}{\Theta}$ *by* $F_\alpha(\frac{x}{\Theta}) = \frac{f_\alpha(y)}{\Theta}$, $y \in \frac{x}{\Theta}$. *We have*:

(1) $(\frac{E}{\Theta}, F_\alpha)$ *is an* $m\Theta$ *structure of modalities over* $\frac{E}{\Theta}$.

(2) *In* $(\frac{E}{\Theta}, F_\alpha)$, $\frac{x}{\Theta} = \frac{y}{\Theta} \Leftrightarrow A\alpha \in I_*, F_\alpha(\frac{x}{\Theta}) = F_\alpha(\frac{y}{\Theta})$.

Proof. (1) Let $\alpha, \beta \in I_*$.

- $\alpha \neq \beta \Rightarrow \exists a \in E, f_\alpha(a) \neq f_\beta(a)$. Then, $\forall\lambda \in I_*, f_\lambda o f_\alpha(a) \neq f_\lambda o f_\beta(a)$.

Thus $F_\alpha(\frac{a}{\Theta}) = \frac{f_\alpha(a)}{\Theta} \neq \frac{f_\beta(a)}{\Theta} = F_\beta(\frac{a}{\Theta})$.

Therefore $\alpha \neq \beta \Rightarrow F_\alpha \neq F_\beta$.

- $F_\beta o F_\alpha = F_\alpha$.

(2)

$$\frac{x}{\Theta} = \frac{y}{\Theta} \Leftrightarrow xR_\Theta y$$

$$\Leftrightarrow \forall\alpha \in I_*, f_\alpha(x) = f_\alpha(y)$$

$$\Rightarrow \forall\alpha \in I_*, \frac{f_\alpha(x)}{\Theta} = \frac{f_\alpha(y)}{\Theta}$$

$$\Rightarrow \forall\alpha \in I_*, F_\alpha(\frac{x}{\Theta}) = F_\alpha(\frac{y}{\Theta}).$$

Conversely, let suppose that $\forall\alpha \in I_*$,

$$F_\alpha(\frac{x}{\Theta}) = F_\alpha(\frac{y}{\Theta}) \Leftrightarrow \forall\alpha \in I_*, \frac{f_\alpha(x)}{\Theta} = \frac{f_\alpha(y)}{\Theta}$$

$$\Leftrightarrow \forall\alpha \in I_*, f_\alpha(x) R_\Theta f_\alpha(y)$$

$$\Rightarrow \forall\alpha, \lambda \in I_*, f_\lambda o f_\alpha(x) = f_\lambda o f_\alpha(y)$$

$$\Rightarrow \forall\alpha \in I_*, f_\alpha(x) = f_\alpha(y)$$

$$\Rightarrow \frac{x}{\Theta} = \frac{y}{\Theta}.$$

Definition 2.2. One calls an $m\Theta$ set, every structure of modalities (E, F_α) over E that satisfies: $\forall\alpha \in I_*, (F_\alpha(x) = F_\alpha(y) \Leftrightarrow x = y)$.

Definition 2.3. Let (E, F_α) be an $m\Theta$ set. $C(E, F_\alpha) = \bigcap_{\alpha\in I_*} F_\alpha(E)$ is called the subset of $m\Theta$ invariant elements of (E, F_α).

Definition 2.4. Let (E, F_α) and (E', F'_α) be two $m\Theta$ sets. One calls $m\Theta$ map from (E, F_α) to (E', F'_α) every map $F_\alpha : E \to E'$ verifying $\forall\alpha \in I_*, F'_\alpha o f = f o F_\alpha$.

2.1.2. The $m\Theta$ completion of an $m\Theta$ set

Observation 2.1. Let (E, F_α) be an $m\Theta$ set and $C(E, F_\alpha)$ be the subset of modal Θ-valent invariant elements of (E, F_α).

Let $(C(E, F_\alpha))^{I_*}$ be the set of I_*-families of elements of $C(E, F_\alpha)$. Let $(x_\lambda) \in (C(E, F_\alpha))^{I_*}$.

For every $a \in C(E, F_\alpha)$, one can identify a to the I_*-families of elements of $C(E, F_\alpha)$, (a_α) with $\lambda \in I_*, a_\lambda = a$.

For every $\alpha \in I_*$, one defines $\hat{F}_\alpha : (C(E, F_\alpha))^{I_*} \to (C(E, F_\alpha))^{I_*}$ by $\hat{F}_\alpha(x_\lambda) = x_\alpha \in C(E, F_\alpha)$.

Then $((C(E, F_\alpha))^{I_*}, \hat{F}_\alpha)$ is an $m\Theta$ set and the map $t : x \mapsto (F_\alpha(x))_{\alpha \in I_*}$ is an injection from E to $(C(E, F_\alpha))^{I_*}$. We also have $\forall \alpha \in I_*, \hat{F}_\alpha o t = t o F_\alpha$. Thus, $t : x \mapsto (F_\alpha(x))_{\alpha \in I_*}$ is an $m\Theta$ injective map, so one can consider (E, F_α) as a sub-structure of $m\Theta$ set of $((C(E, F_\alpha))^{I_*}, \hat{F}_\alpha)$. We will denote the $m\Theta$ set $((C(E, F_\alpha))^{I_*}, \hat{F}_\alpha)$ by $B^\Theta(E, F_\alpha)$.

Definition 2.5. One calls $m\Theta$ completion of an $m\Theta$ set (E, F_α) every $m\Theta$ set (E', F'_α) that is $m\Theta$ isomorphic to $B^\Theta(E, F_\alpha)$.

Theorem 2.1. *Every $m\Theta$ set admits a unique completion of $m\Theta$ set up to an isomorphism.*

Proof. [1].

2.1.3. The modal Θ-valent expression

Let (E, F_α) be an $m\Theta$ set and $x \in E$.

Observation 2.2. Let define $x^\Theta = (F_\alpha(x))_{\alpha \in I_*}$, $x^\Theta \in (C(E, F_\alpha))^{I_*}$. $\forall \alpha \in I_*$, $(F_\alpha(x))^\Theta = (F_\lambda(F_\alpha(x)))_\lambda = (F_\alpha(x))_\lambda \equiv F_\alpha(x)$. Thus, we can identify $(F_\alpha(x))^\Theta$ to $F_\alpha(x) \in C(E, F_\alpha)$.

Let set $E^\Theta = \{x^\Theta / x \in E\}$. Let define $\hat{F}_\alpha : E^\Theta \to E^\Theta$ by $\hat{F}_\alpha(x^\Theta) = (F_\alpha(x))^\Theta = F_\alpha(x) \in C(E, F_\alpha)$, $\forall \alpha \in I_*$. We have

(1) $\forall \alpha, \beta \in I_*, \alpha \neq \beta \Rightarrow \hat{F}_\alpha \neq \hat{F}_\beta$;

(2) $\forall \alpha, \beta \in I_*, \hat{F}_\beta o \hat{F}_\alpha = \hat{F}_\alpha$;

(3) $(\forall \alpha \in I_*, \hat{F}_\alpha(x^\Theta) = \hat{F}_\alpha(y^\Theta)) \Rightarrow (x = y \Rightarrow x^\Theta = y^\Theta)$.

Therefore $(E^{\Theta}, \hat{F}_{\alpha})$ is an $m\Theta$ set. Let $t : E \to E^{\Theta}$ the map defined by $x \mapsto x^{\Theta}$. t is a bijection such that $\forall \alpha \in I_*$, $\hat{F}_{\alpha} o t = t o F_{\alpha}$. Thus $t : x \mapsto x^{\Theta}$ is an $m\Theta$ isomorphism from (E, F_{α}) to $(E^{\Theta}, \hat{F}_{\alpha})$. In (E, F_{α}), $x = y \Leftrightarrow (\forall \alpha \in I_*, F_{\alpha}(x) = F_{\alpha}(y))$. In $(E^{\Theta}, \hat{F}_{\alpha})$, $x^{\Theta} = y^{\Theta} \Leftrightarrow (\forall \alpha \in I_*, F_{\alpha}(x) = F_{\alpha}(y))$.

Definition 2.6. (1) One calls $m\Theta$ expression of x in (E, F_{α}) the element x^{Θ} defined as above.

(2) One calls $m\Theta$ expression of (E, F_{α}) the $m\Theta$ set $(E^{\Theta}, \hat{F}_{\alpha})$.

Remark 2.2. (1) According to what proceeds, one can identify (E, F_{α}) to $(E^{\Theta}, \hat{F}_{\alpha})$ by the bijective map $x \mapsto x^{\Theta}$. So $(E^{\Theta}, \hat{F}_{\alpha})$ as (E, F_{α}) can be identified to a sub-structure of $m\Theta$ set of $B^{\Theta}(E, F_{\alpha})$.

(2) If the $m\Theta$ set (E, F_{α}) is a completion of $m\Theta$ set, we have the following identifications $(E^{\Theta}, \hat{F}_{\alpha}) \equiv (E, F_{\alpha}) \subset^{\Theta} B^{\Theta}(E, F_{\Theta})$ and $x \mapsto (F_{\alpha}(x))_{\alpha}$, $x \mapsto x^{\Theta}$.

Definition 2.7. Let (E, F_{α}) and (E', F'_{α}) be two $m\Theta$ sets and let X be a non-empty set.

(1) (E', F'_{α}) is an $m\Theta$ subset of (E, F_{α}) if $E' \subseteq E$ and $\forall \alpha \in I_*$, $F'_{\alpha} = F_{\alpha|E'}$.

(2) X is an $m\Theta$ subset of (E, F_{α}) if $X \subseteq E$ and $\left(X, F_{\alpha|X}\right)$ is an $m\Theta$ set.

Proposition 2.3. *Let* (E, F_α) *be an* $m\Theta$ *set and* $\emptyset \neq E' \subseteq E$. $\left(E', F_{\alpha|E'}\right)$ *is an* $m\Theta$ *set if and only if*:

(1) $C\left(E', F_{\alpha|E'}\right) \neq \emptyset$;

(2) $\forall x \in E', F_\alpha(x) \in E'$;

(3) $\alpha \neq \beta \Rightarrow F_{\alpha|E'} \neq F_{\beta|E'}$.

Proof. [1].

2.1.4. Some examples of $m\Theta$ sets

(a) The canonical Lukasiewicz algebra of a chain

Let I be a closed chain $0, 1$. For every $\forall \alpha \in I_*$, one defines $F_\alpha : I \to I$ by:

$$\forall x \in I, F_\alpha(x) = \begin{cases} 1 & \text{if } \alpha \leqslant x, \\ 0 & \text{if } \alpha > x, \end{cases}$$

$\forall x, y \in I, (x \leq y \Rightarrow \forall \alpha \in I_*, F_\alpha(x) \leq F_\alpha(y))$. We also observe that $\forall \alpha, \beta \in I_*, \alpha \leq \beta \Rightarrow F_\beta \leq F_\alpha$. Then (I, F_α) is a $m\Theta$ set that is a Θ-valent Lukasiewicz algebra.

Notation 2.2. Let denote $I_\Theta = (I, F_\alpha)$ and $(2^\Theta, w^\alpha) = B^\Theta(I_\Theta)$. Recall that $(2^\Theta, w_\alpha) = B^\Theta(I_\Theta)$ is the completion of $m\Theta$ set of the $m\Theta$ set $I_\Theta = (I, F_\alpha)$. If $\Theta = 3$, $I = \{0, \alpha, 1\}$ with $0 < \alpha < 1$, $I_\Theta = (I, F_\alpha, F_1)$, $(2^\Theta, w_\alpha) = B^\Theta(I_\Theta) = \{0, \alpha, \overline{\alpha}, 1\}$.

$B^\Theta(I_\Theta)$	0	α	$\overline{\alpha}$	1
w_α	0	1	0	1
w_1	0	0	1	1

$\Theta = 4$; $I = \{0, \alpha, \beta, 1\}$; $0 < \alpha < \beta < 1$; $I_\Theta = \left(I, F_\alpha, F_\beta, F_1\right)$ and $B^\Theta(I_\Theta) = \{0, \alpha, \overline{\alpha}, \beta, \overline{\beta}, \beta \wedge \overline{\alpha}, \alpha \vee \overline{\beta}, 1\}$.

$B^{\Theta}(I_{\Theta})$	0	α	$\overline{\beta}$	$\beta \wedge \overline{\alpha}$	β	$\overline{\alpha}$	$\alpha \vee \overline{\beta}$	1
w_{α}	0	1	0	0	1	0	1	1
w_{β}	0	0	0	1	1	1	0	1
w_1	0	0	1	0	0	1	1	1

.

(b) *The structures of* $m\Theta$ *set* $\mathbb{Z}$.

Let $n \in \mathbb{N}\backslash\{0, 1\}$.

$\forall x \in \mathbb{Z}, \exists!(p, r)$ such that $0 \leq r \leq n-1$ and $p \in \mathbb{Z}$ with $x = pn + r$.

If $n = 2$ take the chain $I = \{0, 1, 2\}$.

If $n \geq 3$ take the chain $I = \mathbb{N}_{n-1} = \{0, 1, \cdots, n-1\}$.

For every $\forall \alpha \in I_*$, let define $F_{\alpha} : \mathbb{Z} \to \mathbb{Z}$ by $F_{\alpha}(x) = n(p + \alpha r)$.

Proposition 2.4. (1) $(\mathbb{Z}, F_{\alpha})$ *is an* $m\Theta$ *set such that* $C(\mathbb{Z}, F_{\alpha}) = n\mathbb{Z}$.

(2) $\left(\mathbb{N}, F_{\alpha|\mathbb{N}}\right)$ *is an* $m\Theta$ *subset of* $(\mathbb{Z}, F_{\alpha})$.

Proof. [1].

(c) The $m\Theta$ set of $m\Theta$ relative integers $(\mathbb{Z}_{n\mathbb{Z}}, F'_{\alpha})$

Let $n \in \mathbb{N}\backslash\{0, 1\}$.

$$\forall x \in \mathbb{Z}, \exists!(p, r) \in \mathbb{Z} \times [|0, n-1|] \text{ such that } x = pn + r.$$

Let set $x_{nZ} = (p + \alpha r)_{\alpha \in I_*}$ if $\neg(x \equiv 0[n])$. Let's set $\mathbb{Z}_{n\mathbb{Z}} = \mathbb{Z} \cup \{x_{n\mathbb{Z}} : x \in \mathbb{Z} \text{ and } \neg(x \equiv 0[n])\}$. Let define for every $\forall \alpha \in I_*$, $F'_{\alpha} : \mathbb{Z}_{n\mathbb{Z}} \to \mathbb{Z}_{n\mathbb{Z}}$ by:

$$F'_{\alpha}(a) = \begin{cases} a & \text{if } a \in \mathbb{Z}, \\ p + \alpha r & \text{if } a \in \mathbb{Z}_{n\mathbb{Z}}\backslash\mathbb{Z} \text{ with } a = x_{n\mathbb{Z}},\ x = pn + r. \end{cases}$$

Proposition 2.5. *$(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$ is an $m\Theta$ set such that $C(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha) = \mathbb{Z}$.*

Proof. [1].

Proposition 2.6. *Let define $Spec_{n\mathbb{Z}}$ from $(\mathbb{Z}, n\mathbb{Z}, F_\alpha)$ to $(\mathbb{Z}_{n\mathbb{Z}}, \mathbb{Z}, F'_\alpha)$ by:*

$$\forall x \in \mathbb{Z},\ Spec_{n\mathbb{Z}}(x) = \begin{cases} p & if\ x = np, \\ x_{n\mathbb{Z}} & if\ \neg(x \equiv 0[n]). \end{cases}$$

$Spec_{n\mathbb{Z}}$ is an $m\Theta$ isomorphism, i.e., $Spec_{n\mathbb{Z}}$ is a bijective $m\Theta$ map such that $\forall \alpha \in I_*$, $Spec_{n\mathbb{Z}} o F_\alpha = F'_\alpha o Spec_{n\mathbb{Z}}$.

Proof. [1].

2.2. Modal Θ-valent algebraic structures

2.2.1. Algebraic structure of $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$

Definition 2.8. (1) Let $a \in \mathbb{Z}_{n\mathbb{Z}}$, one calls the support of a the element denoted by $s(a)$ and defined as follows:

$$s(a) = \begin{cases} a & \text{if } a \in \mathbb{Z}, \\ x & \text{if } a = x_{n\mathbb{Z}},\ \neg(x \equiv 0[n]). \end{cases}$$

(2) Let $\top$ be a binary law over $\mathbb{Z}$. Let $a, b \in \mathbb{Z}_{n\mathbb{Z}}$, we define an $m\Theta$ binary law in $\mathbb{Z}_{n\mathbb{Z}}$ induct by $\top$ and denoted also $\top$ as follows:

$$a \top b = \begin{cases} s(a) \top s(b) & \text{if } \begin{cases} a, b \in \mathbb{Z}, \\ (s(a) \top s(b)) \equiv 0[n] \end{cases} \text{ otherwise,} \\ (s(a) \top s(b))_{n\mathbb{Z}} & \text{otherwise} \end{cases}$$

$\top$ as defined above on $\mathbb{Z}_{n\mathbb{Z}}$ is called an $m\Theta$ law on $\mathbb{Z}_{n\mathbb{Z}}$: $a \top b \in \mathbb{Z}_{n\mathbb{Z}}$ for every $a, b \in \mathbb{Z}_{n\mathbb{Z}}$.

Thus we can define $a + b \in \mathbb{Z}_{n\mathbb{Z}}$ and $a \times b \in \mathbb{Z}_{n\mathbb{Z}}$ for every $a, b \in \mathbb{Z}_{n\mathbb{Z}}$, where $+$ and $\times$ are $m\Theta$ addition and $m\Theta$ multiplication, respectively.

In $\mathbb{Z}_{n\mathbb{Z}}$, the $m\Theta$ addition and the $m\Theta$ multiplication are commutative and not associative.

The $m\Theta$ multiplication is not distributive in comparison with the $m\Theta$ addition. However, one defines similar concepts to the structure of $m\Theta$ set of $\mathbb{Z}_{n\mathbb{Z}}$. These laws are then said $m\Theta$ associative and the $m\Theta$ multiplication is $m\Theta$ distributive in comparison with the $m\Theta$ addition.

The respective restrictions of these $m\Theta$ laws in $\mathbb{Z} = \bigcap_{\alpha\in I_*} F'_\alpha(\mathbb{Z}_{n\mathbb{Z}})$ are the classical laws of $\mathbb{Z}$. The $m\Theta$ associativity and the $m\Theta$ distributivity in $\mathbb{Z}_{n\mathbb{Z}}$. Let $x, y, z \in \mathbb{Z}$ such that $\urcorner(x \equiv 0[n])$ or $\urcorner(y \equiv 0[n])$ or $\urcorner(z \equiv 0[n])$.

(a) Let $\top$ be an $m\Theta$ binary law in $\mathbb{Z}_{n\mathbb{Z}}$, $\forall x_{n\mathbb{Z}}, y_{n\mathbb{Z}}, z_{n\mathbb{Z}} \in \mathbb{Z}_{n\mathbb{Z}}$, we have

$$(x_{n\mathbb{Z}} \top y_{n\mathbb{Z}}) \top z_{n\mathbb{Z}} = \begin{cases} (x \top y) \top z & \text{if } ((x \top y) \top z) \equiv 0[n] \\ ((x \top y) \top z)_{n\mathbb{Z}} & \text{otherwise} \end{cases}$$

$$= \begin{cases} x \top (y \top z) & \text{if } (x \top (y \top z)) \equiv 0\,[n] \\ (x \top (y \top z))_{n\mathbb{Z}} & \text{otherwise} \end{cases}$$

$$= x_{n\mathbb{Z}} \top (y_{n\mathbb{Z}} \top z_{n\mathbb{Z}}).$$

(b) Let $+$ and $\times$ be the $m\Theta$ addition and the $m\Theta$ multiplication in $\mathbb{Z}_{n\mathbb{Z}}$, $\forall x_{n\mathbb{Z}}, y_{n\mathbb{Z}}, z_{n\mathbb{Z}} \in \mathbb{Z}_{n\mathbb{Z}}$,

$$x_{n\mathbb{Z}}(y_{n\mathbb{Z}} + z_{n\mathbb{Z}}) = \begin{cases} x(y+z) & \text{if } x(y+z) \equiv 0[n] \\ (x(y+z))_{n\mathbb{Z}} & \text{otherwise} \end{cases}$$

$$= \begin{cases} xy + xz & \text{if } xy + xz \equiv 0[n] \\ (xy + xz)_{n\mathbb{Z}} & \text{otherwise} \end{cases}$$

$$= x_{n\mathbb{Z}} y_{n\mathbb{Z}} + x_{n\mathbb{Z}} z_{n\mathbb{Z}}.$$

Definition 2.9. One calls:

(1) The modal Θ-valent identity element of $(\mathbb{Z}_{n\mathbb{Z}}, F'_{\alpha})$ for the $m\Theta$ multiplication the $m\Theta$ element $1_{n\mathbb{Z}} = Spec_{n\mathbb{Z}}(1)$.

(2) The $m\Theta$ inverse of $a \in \mathbb{Z}_{n\mathbb{Z}}$, every $b \in \mathbb{Z}_{n\mathbb{Z}}$ when it exists that is a solution of the equation $ab = 1_{n\mathbb{Z}}$.

Remark 2.3. The $m\Theta$ inverse when it exists is not necessary unique.

Definition 2.10. One calls:

(1) A modal Θ-valent monoïd a pair $((A, F_{\alpha}), \top)$ consisting of a modal Θ-valent set (A, F_{α}) and an $m\Theta$ binary operation $\top$ on (A, F_{α}) which satisfies the $m\Theta$ associative law. The $m\Theta$ monoïd is said $m\Theta$ unitary if it has an $m\Theta$ identity element.

(2) A modal Θ-valent group, every modal Θ-valent unitary modal Θ-valent monoïd that has at least an $m\Theta$ identity element.

(3) A modal Θ-valent ring every triple $((A, F_{\alpha}), +, \times)$, where (A, F_{α}) is an $m\Theta$ set and $+$ and $\times$ are $m\Theta$ binary operations on (A, F_{α}) such that the following properties hold:

- $((A, F_{\alpha}), +)$ is an abelian $m\Theta$ group.
- $((A, F_{\alpha}), \times)$ is an $m\Theta$ monoïd.
- The $m\Theta$ distributive $m\Theta$ laws hold.

(4) A modal Θ-valent field $(m\Theta f)$, every $m\Theta$ ring $(m\Theta r)$ in which every non zero $m\Theta$ element has at least a modal Θ-valent inverse.

Proposition 2.7. $((\mathbb{Z}_{n\mathbb{Z}}, F'_{\alpha}), +, \times)$ *is an* $m\Theta$ *ring with no zero divisors.*

Proof. [1].

Remark 2.1. 1 (resp., $1_{n\mathbb{Z}}$) is an identity element (resp., an $m\Theta$ identity element) for the $m\Theta$ multiplication in $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$.

2.2.2. The modal Θ-valent congruence of $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$

Let $n \in \mathbb{N}$ such that $n \geq 2$. $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$ is the $m\Theta$ ring of the modal Θ-valent relative integers. Let set $\Theta_0 = \{a : a \in \mathbb{Z}_{n\mathbb{Z}}, \exists \mu \in I_*, F'_\mu(a) = 0\}$, $\mathbb{N}_{n\mathbb{Z}} = \mathbb{N} \cup \{x_{n\mathbb{Z}} : \urcorner(x \equiv 0 \,(\mathrm{mod}\, n)), x \in \mathbb{N}\}$.

Proposition 2.8. *Let* $P \in \mathbb{N}_{n\mathbb{Z}} \backslash \Theta_0$ *and* ρ_P *be a binary relation on* $\mathbb{Z}_{n\mathbb{Z}}$ *defined by*:

For every $a, b \in \mathbb{Z}_{n\mathbb{Z}}$, $a\rho_P b \Leftrightarrow \forall \alpha \in I_*, F'_\alpha(a) \equiv F'_\alpha(b)[F'_\alpha(P)]$. *We have*:

(1) ρ_P *is an equivalence relation on* $\mathbb{Z}_{n\mathbb{Z}}$.

(2) $\rho_{P|\mathbb{Z}}$ *is the classical congruence of* $\mathbb{Z}$.

(3) ρ_P *is compactible with the structure of* $m\Theta$ *set of* $(\mathbb{Z}_{n\mathbb{Z}}, F'_\alpha)$, *i.e., for every* $a, b \in \mathbb{Z}_{n\mathbb{Z}}$, $a\rho_P b \Leftrightarrow \forall \alpha \in I_*, F'_\alpha(a)\rho_P F'_\alpha(b)$.

Proof. [1].

Notation 2.3.

- ρ_P will be denoted by $P\mathbb{Z}_{n\mathbb{Z}}$ in what follows.
- We will denote the equivalence class of an element $a \in \mathbb{Z}_{n\mathbb{Z}}$ modulo $P\mathbb{Z}_{n\mathbb{Z}}$ by $\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}}$.
- Let set $\frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}} = \{\frac{a}{P\mathbb{Z}_{n\mathbb{Z}}}, a \in \mathbb{Z}_{n\mathbb{Z}}\}$.

Proposition 2.9. *Let* $(\mathbb{Z}_{n\mathbb{Z}}, F'_{\alpha})$ *be the* $m\Theta$ *set of* $m\Theta$ *relative integers and* $P \in \mathbb{N}_{n\mathbb{Z}} \backslash \Theta_0$. *For every* $\forall \alpha \in I_*$, *let* $F_{\alpha, P}$ *be defined as follows*:

$$F_{\alpha, P} : \begin{array}{c} \frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}} \to \frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}} \\ \frac{a}{P\mathbb{Z}_{n\mathbb{Z}}} \mapsto F_{\alpha, P}\left(\frac{a}{P\mathbb{Z}_{n\mathbb{Z}}}\right) = \frac{F'_{\alpha}(a)}{F'_{\alpha}(P)\mathbb{Z}_{n\mathbb{Z}}} \end{array}$$

$(\frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}}, F_{\alpha, P})$ *is an* $m\Theta$ *set if and only if* $P \in \mathbb{N}^*$.

Proof. [1].

Remark 2.4. If $P \in \mathbb{N}^*$, then $\frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}} = \frac{\mathbb{Z}}{P\mathbb{Z}} \bigcup \{\frac{x_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}} : \urcorner(x \equiv 0 \,(\mathrm{mod}\, n))\}$ and $C(\frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}}, F_{\alpha, P}) = \frac{\mathbb{Z}}{P\mathbb{Z}}$.

Definition 2.11. One calls:

(1) The $m\Theta$ congruence in $(\mathbb{Z}_{n\mathbb{Z}}, F'_{\alpha})$, the $m\Theta$ equivalence relation denoted by $P\mathbb{Z}_{n\mathbb{Z}}$, $P \in \mathbb{N}^*$.

(2) A modal Θ-valent residual class modulo P, the equivalence class modulo $P\mathbb{Z}_{n\mathbb{Z}}$ of every $a \in \mathbb{Z}_{n\mathbb{Z}}$ and denoted by $\frac{a}{P\mathbb{Z}_{n\mathbb{Z}}}$.

(3) The α-modality of $\frac{a}{P\mathbb{Z}_{n\mathbb{Z}}}$, the integer modulo P defined as follows: $\forall \alpha \in I_*$, $F_{\alpha, P}(\frac{a}{P\mathbb{Z}_{n\mathbb{Z}}}) = \frac{F'_{\alpha}a}{P\mathbb{Z}} \in \frac{\mathbb{Z}}{P\mathbb{Z}}$.

(4) $(\frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}}, F_{\alpha, P})$ the $m\Theta$ set of $m\Theta$ relative integers modulo P also denoted by $\frac{(\mathbb{Z}_{n\mathbb{Z}}, F'_{\alpha})}{P\mathbb{Z}_{n\mathbb{Z}}}$.

(5) The set of integers modulo P, the following set $C(\frac{(\mathbb{Z}_{n\mathbb{Z}}, F'_{\alpha})}{P\mathbb{Z}_{n\mathbb{Z}}}) = \frac{\mathbb{Z}}{P\mathbb{Z}}$.

Proposition 2.10. *Let* $a, b \in \mathbb{Z}_{n\mathbb{Z}}$.

$$a \rho_P b \Leftrightarrow \begin{cases} a \equiv b[P] & \text{if } a \in \mathbb{Z} \text{ (therefore } b \in \mathbb{Z}), \\ x \equiv y[nP] & \text{if } a = x_{n\mathbb{Z}},\ \neg(x \equiv 0[n]) \text{ (therefore } b = y_{n\mathbb{Z}},\ \neg(y \equiv 0[n])). \end{cases}$$

Proof. [1].

Notation 2.4. In all what follows, we shall denote $x_{n\mathbb{Z}} \rho_P y_{n\mathbb{Z}}$ by $x_{n\mathbb{Z}} \equiv y_{n\mathbb{Z}}[P\mathbb{Z}_{n\mathbb{Z}}]$.

Definition 2.12. One calls a modal Θ-valent representing of the element $\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}}$ with $a \in \mathbb{Z}_{n\mathbb{Z}}$, every $b \in \mathbb{Z}_{n\mathbb{Z}}$ satisfying the following conditions:

- If $a \in \mathbb{Z}$, therefore $b \in \mathbb{Z}$ and then $b \equiv a[nP]$.
- If not, $a = x_{n\mathbb{Z}}$ therefore $b = y_{n\mathbb{Z}}$ and then $x \equiv y[nP]$, with $\neg(x \equiv 0[n])$ and $\neg(y \equiv 0[n])$.

Notation 2.5. Let denote the set of $m\Theta$ representings of $\frac{a}{P\mathbb{Z}_{n\mathbb{Z}}}$ by $rm\frac{a}{P\mathbb{Z}_{n\mathbb{Z}}}$.

Definition 2.13. Let $a, b \in \mathbb{Z}_{n\mathbb{Z}}$. One defines the addition $+$ and the multiplication $\times$ in $\frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}}$ as follows:

$$\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}} + \frac{b}{p\mathbb{Z}_{n\mathbb{Z}}} = \frac{x+y}{p\mathbb{Z}_{n\mathbb{Z}}} \text{ with } x \in rm\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}} \text{ and } y \in rm\frac{b}{p\mathbb{Z}_{n\mathbb{Z}}}.$$

$$\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}} \times \frac{b}{p\mathbb{Z}_{n\mathbb{Z}}} = \frac{x \times y}{p\mathbb{Z}_{n\mathbb{Z}}} \text{ with } x \in rm\frac{a}{p\mathbb{Z}_{n\mathbb{Z}}} \text{ and } y \in rm\frac{b}{p\mathbb{Z}_{n\mathbb{Z}}}.$$

$x + y$ and xy are respectively, the $m\Theta$ addition and the $m\Theta$ multiplication.

Theorem 2.2. *Let* $+$ *and* $\times$ *defined in* $\frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}}$ *as above.* $((\frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}}, F_\alpha), +, \times)$ *is an* $m\Theta$ *ring with as identity element* $\frac{1}{P\mathbb{Z}}$ *and as an* $m\Theta$ *identity element* $\frac{1_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}}$.

Proof. [1].

Theorem 2.3. *Let* $P, n \in \mathbb{Z}$ *with* $2 \leq n \leq P$. *The following statements are equivalent*:

(1) $(\frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}}, F_\alpha)$ *is an* $m\Theta$ *field.*

(2) $\forall a \in \mathbb{Z}_{n\mathbb{Z}}, \exists b \in \mathbb{Z}_{n\mathbb{Z}}$ *such that*:

(i) *Or* $a \in \mathbb{Z}$, *then* $b = x_{n\mathbb{Z}}, \urcorner(y \equiv 0[n])$ *and* $ay \equiv 1[nP]$.

(2i) *Or if* $a \notin \mathbb{Z}$, $a = x_{n\mathbb{Z}}, \urcorner(y \equiv 0[n])$ *then*

(a) *If* $\exists b \in \mathbb{Z}$, *then* $xb \equiv 1[nP]$.

(b) *If not*, $b = y_{n\mathbb{Z}}, \urcorner(y \equiv 0[n])$ *and* $xy \equiv 1[nP]$.

Proof. [1].

Corollary 2.1. *If* $(\frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}}, F_\alpha)$ *is an* $m\Theta$ *field, then* P *is a prime integer.*

Proof. [1].

Definition 2.14. $\frac{a}{P\mathbb{Z}_{n\mathbb{Z}}}$ is a divisor of zero in $(\frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}}, F_\alpha)$ if it exists $b \in \mathbb{Z}_{n\mathbb{Z}}$ such that $\frac{a}{P\mathbb{Z}_{n\mathbb{Z}}} \frac{b}{P\mathbb{Z}_{n\mathbb{Z}}} = 0$.

Proposition 2.11. *If* $2 \leq n \leq P$, *then* $Card \frac{\mathbb{Z}_{n\mathbb{Z}}}{P\mathbb{Z}_{n\mathbb{Z}}} = nP$.

Proof. [1].

Proposition 2.12. *Let* $a, b \in \mathbb{Z}_{n\mathbb{Z}}$ *and* $P, P' \in \mathbb{N}^*$. *If* $a \equiv b(P\mathbb{Z}_{n\mathbb{Z}})$ *and* $a \equiv b(P'\mathbb{Z}_{n\mathbb{Z}})$, *then* $a \equiv b(ppcm(P, P')\mathbb{Z}_{n\mathbb{Z}})$.

Proof. [1].

Proposition 2.13. *Let* $a, b, K \in \mathbb{Z}_{n\mathbb{Z}}$, *the following statements are equivalent*:

(i) $Ka \equiv Kb(P\mathbb{Z}_{n\mathbb{Z}})$.

(2i) $a \equiv b(\frac{P}{pgcd(s(K),\ P)}\mathbb{Z}_{n\mathbb{Z}})$.

Proof. [1].

2.3. Some intrinsic *m*Θ parameters in $\mathbb{Z}_{n\mathbb{Z}}$

2.3.1. Formal *m*Θ exponentiation in $\mathbb{Z}_{n\mathbb{Z}}$

Definition 2.15. Let $a \in \mathbb{Z}_{n\mathbb{Z}}$ and $b \in \mathbb{N}_{n\mathbb{Z}}$.

(1) a^b is defined as follows:

$$a^b = \begin{cases} s(a)^{s(b)} & \text{if } a, b \in \mathbb{Z} \text{ or } s(a)^{s(b)} \equiv 0[n], \\ (s(a)^{s(b)})_{n\mathbb{Z}} & \text{if not.} \end{cases}$$

(2) $(a, b) \mapsto a^b$ is an $m\Theta$ map from $\mathbb{Z}_{n\mathbb{Z}} \times \mathbb{N}_{n\mathbb{Z}}$ to $\mathbb{Z}_{n\mathbb{Z}}$ and $s(a^b) = s(a)^{s(b)}$.

2.3.2. Formal *m*Θ Euler's function in $\mathbb{Z}_{n\mathbb{Z}}$

Definition 2.16. The formal $m\Theta$ Euler's function in $\mathbb{Z}_{n\mathbb{Z}}$ denoted by $\rho_{n\mathbb{Z}}$ is defined as an $m\Theta$ map from $\mathbb{N}_{n\mathbb{Z}}$ to $\mathbb{N}_{n\mathbb{Z}}$ as follows:

Let $m \in \mathbb{N}_{n\mathbb{Z}}$

$$\rho_{n\mathbb{Z}}(m) = \begin{cases} \rho(s(m)) & \text{if } m \in \mathbb{N} \text{ or if } \rho(s(m)) \equiv 0[n], \\ (\rho(s(m)))_{n\mathbb{Z}} & \text{if not.} \end{cases}$$

Remark 2.5. (1) $\rho_{n\mathbb{Z}}(m) \in \mathbb{N} \Leftrightarrow \begin{cases} m \in \mathbb{N}, & \text{or} \\ \rho(s(m)) \equiv 0[n]. \end{cases}$

(2) $s(\rho_{n\mathbb{Z}}(m)) = \rho(s(m)) \in \mathbb{N}$.

(3) If $\gcd(s(m), s(m')) = 1$, then $\rho_{n\mathbb{Z}}(mm') = \rho_{n\mathbb{Z}}(m)\rho_{n\mathbb{Z}}(m')$.

2.3.3. The $m\Theta$ Fermat-Euler theorem in $\mathbb{Z}_{n\mathbb{Z}}$

Theorem 2.4. *Let $a \in \mathbb{Z}_{n\mathbb{Z}}$ and $m \in \mathbb{N}^*_{n\mathbb{Z}}$. If $gcd(s(m), s(a)) = 1$ and n divides $s(m)$, then $a^{\rho_{n\mathbb{Z}}(m)} \equiv 1_{n\mathbb{Z}}[\frac{s(m)}{n}\mathbb{Z}_{n\mathbb{Z}}]$.*

Proof. $\gcd(s(a), s(m)) = 1 \Rightarrow s(a)^{\rho(s(m))} \equiv 1[s(m)]$ by the Fermat-Euler theorem in $\mathbb{Z}$. As n divides $s(m)$, then

$$s(a)^{\rho(s(m))} \equiv 1[n, \frac{s(m)}{n}] \Rightarrow (s(a)^{\rho(s(m))})_{n\mathbb{Z}} \equiv 1_{n\mathbb{Z}}[\frac{s(m)}{n}\mathbb{Z}_{n\mathbb{Z}}]$$

$$\Rightarrow a^{\rho_{n\mathbb{Z}}(m)} \equiv 1_{n\mathbb{Z}}[\frac{s(m)}{n}\mathbb{Z}_{n\mathbb{Z}}].$$

Corollary 2.2. *Let $a \in \mathbb{Z}_{n\mathbb{Z}}$.*

(1) *If $gcd(s(a), n) = 1$, then $s(a)^{\rho(n)} \equiv 1[n]$.*

(2) *The $m\Theta$ Fermat-Euler theorem in $\mathbb{Z}_{n\mathbb{Z}}$ implies the Fermat-Euler theorem in $\mathbb{Z}$.*

Proof. (1) As $s(n) = n$, then according to the $m\Theta$ Fermat-Euler theorem, we have:

$$a^{\rho(n)} \equiv 1_{n\mathbb{Z}}[\frac{n}{n}\mathbb{Z}_{n\mathbb{Z}}] \Rightarrow a^{\rho(n)} \equiv 1_{n\mathbb{Z}}[1\mathbb{Z}_{n\mathbb{Z}}]$$

$$\Rightarrow s(a)^{\rho(n)} \equiv 1[n].$$

(2) Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}^*$ with $\gcd(a, m) = 1$ and m a multiple of n. $a = s(a)$, $m = s(m)$. Thus,

$$a^{\rho_{n\mathbb{Z}}(m)} \equiv 1_{n\mathbb{Z}}(\frac{m}{n}\mathbb{Z}_{n\mathbb{Z}}) \Rightarrow a^{\rho(m)} \equiv 1[n.\frac{m}{n}]$$

$$\Rightarrow a^{\rho(m)} \equiv 1[m].$$

2.3.4. Small Fermat-Euler theorem in $\mathbb{Z}_{p\mathbb{Z}}$

Let p be a prime number and $a \in \mathbb{Z}_{p\mathbb{Z}}\backslash\mathbb{Z}$, $gcd(s(a), p^k) = 1$, thus by the $m\Theta$ Fermat-Euler theorem, one has : $a^{\rho_{p\mathbb{Z}}(p^k)} \equiv 1_{p\mathbb{Z}}(p^{k-1}\mathbb{Z}_{p\mathbb{Z}})$. As $p^k \in \mathbb{N}$, then $\rho_{p\mathbb{Z}}(p^k) = \rho(p^k) = (p-1)p^{k-1}$.

Theorem 2.5.

- $a^{(p-1)p^{k-1}} \equiv 1_{p\mathbb{Z}}[p^{k-1}\mathbb{Z}_{p\mathbb{Z}}]$.
- $s(a)^{(p-1)p^{k-1}} \equiv 1[p^k]$.

Proof. [1].

Corollary 2.3.

- $a^{(p-1)p^{k-1}+1} \equiv a[p^{k-1}\mathbb{Z}_{p\mathbb{Z}}]$.
- $s(a)^{(p-1)p^{k-1}+1} \equiv s(a)[p^k]$.

Corollary 2.4.

- $a^{(p-1)(p+1)} \equiv a[p\mathbb{Z}_{p\mathbb{Z}}]$.
- $s(a)^{(p-1)(p+1)} \equiv s(a)[p^2]$.

Corollary 2.5. *Let* $m \in \mathbb{Z}$ *and* $k \in \mathbb{N}$ *such that* $k \geq 2$. *If* $gcd(m, p) = 1$, *then* $m^{(p-1)p^{k-1}} \equiv 1[p^k]$.

Corollary 2.6. *In the modal p-valent quotient rings* $\frac{\mathbb{Z}_{p\mathbb{Z}}}{p\mathbb{Z}_{n\mathbb{Z}}}$ *and* $\frac{\mathbb{Z}_{p\mathbb{Z}}}{p^k\mathbb{Z}_{p\mathbb{Z}}}$, *with* $k \in \mathbb{N}\backslash\{0, 1\}$, *if one denotes for* $a \in \mathbb{Z}_{p\mathbb{Z}}\backslash\mathbb{Z}$, $\dot{a} = \frac{a}{p\mathbb{Z}_{p\mathbb{Z}}}$ *and* $\overline{a} = \frac{a}{p^k\mathbb{Z}_{p\mathbb{Z}}}$. *One has*:

- $\dot{a}^{(p-1)p} = \dot{1}_{p\mathbb{Z}}$.
- $\overline{a}^{(p-1)p^{k-1}} = \overline{1}_{p\mathbb{Z}}$.

3. A Modal Θ-Valent Approach of the RSA Cryptosystems

Let p, q and n be three prime integer numbers; let set $m = p \times q \times n$; let consider $\frac{\mathbb{Z}_{n\mathbb{Z}}}{m\mathbb{Z}_{n\mathbb{Z}}}$; let $a \in \mathbb{Z}_{n\mathbb{Z}}\backslash\mathbb{Z}$ such that $\gcd(s(a), m) = 1$ and let recall that $s(m) = m$.

According to the $m\Theta$ Fermat-Euler theorem in $\mathbb{Z}_{n\mathbb{Z}}$, we have:

$a^{\rho_{n\mathbb{Z}}(m)} \equiv 1_{n\mathbb{Z}}[\frac{s(m)}{n}\mathbb{Z}_{n\mathbb{Z}}] \Rightarrow a^{\rho(m)} \equiv 1_{n\mathbb{Z}}[pq\mathbb{Z}_{n\mathbb{Z}}]$ because $\rho_{n\mathbb{Z}}(m) = \rho(m)$.

Let $t \in \mathbb{N}$ such that $\gcd(t, \rho(m)) = 1$, then according to Bezout theorem, there exist $U, V \in \mathbb{Z}$ such that $tU + V\rho(m) = 1$. Thus $a^{tU+V\rho(m)} = a \Leftrightarrow a^{tU}a^{V\rho(m)} = a$. As $a^{\rho(m)} \equiv 1_{n\mathbb{Z}}[pq\mathbb{Z}_{n\mathbb{Z}}]$, then

$$a^{V\rho(m)} \equiv 1_{n\mathbb{Z}}[pq\mathbb{Z}_{n\mathbb{Z}}] \Rightarrow a^{tU}a^{V\rho(m)} \equiv a^{tU}1_{n\mathbb{Z}}(pq\mathbb{Z}_{n\mathbb{Z}})$$

$$\Rightarrow a^{tU} \equiv a(pq\mathbb{Z}_{n\mathbb{Z}}).$$

If x is an inversible element of $\frac{\mathbb{Z}}{m\mathbb{Z}}$, then $\gcd(x, m) = 1$ and $x^{\rho(m)} \equiv 1[m]$. Thus as above, we have $x^{tU} \equiv x[m]$.

Let $x, y \in \mathbb{Z}_{n\mathbb{Z}}$ and $U(\frac{\mathbb{Z}}{m\mathbb{Z}}) = (\frac{\mathbb{Z}}{m\mathbb{Z}})^*$ the set of inversible elements of $\frac{\mathbb{Z}}{m\mathbb{Z}}$ let set

$$C(x) \equiv \begin{cases} x^U[m], & \text{if } x \in U(\frac{\mathbb{Z}}{m\mathbb{Z}}), \\ x^U(pq\mathbb{Z}_{n\mathbb{Z}}), & \text{if } x \in \mathbb{Z}_{n\mathbb{Z}}\backslash\mathbb{Z} \text{ such that } \gcd(s(m), s(x)) = 1, \end{cases}$$

where $U(\frac{\mathbb{Z}}{m\mathbb{Z}})$ is the set of inversible elements of $\frac{\mathbb{Z}}{m\mathbb{Z}}$.

$$D(y) \equiv \begin{cases} y^t[m], & \text{if } y \in U(\frac{\mathbb{Z}}{m\mathbb{Z}}), \\ y^t(pq\mathbb{Z}_{n\mathbb{Z}}), & \text{if } y \in \mathbb{Z}_{n\mathbb{Z}}\backslash\mathbb{Z} \text{ such that } \gcd(s(m), s(y)) = 1, \end{cases}$$

Let set $U_{n\mathbb{Z},m} = \{a \in \mathbb{Z}_{n\mathbb{Z}}\backslash\mathbb{Z} : \gcd(s(a), s(m)) = 1\}$.

Proposition 3.1. *Let* $x \in U(\frac{\mathbb{Z}}{m\mathbb{Z}}) \cup U_{n\mathbb{Z},m}$.

$$D(C(x)) \equiv D(x^U) \equiv x^{Ut} \equiv x \begin{cases} modulo(m), & if\ x \in U(\frac{\mathbb{Z}}{m\mathbb{Z}}), \\ modulo(\frac{m}{n}\mathbb{Z}_{n\mathbb{Z}}), & if\ x \in U_{n\mathbb{Z},m}. \end{cases}$$

Proof. Obvious.

Remark 3.1. The functions D and C defined above will be our decoding and coding functions, respectively. To encrypt, one will need C, i.e., U and m which are of the public areas. To decrypt, one has to know t and m.

Example 3.1. Take $p = 13$, $q = 23$ and $n = 2$.

$$m = 13 \times 23 \times 2 = 598,\ \rho_{2\mathbb{Z}}(m) = \rho(s(m)) = \rho(m) = \rho(13 \times 23 \times 2) = 264.$$

An encoded message is constituted of elements $x \in U(\frac{\mathbb{Z}}{598\mathbb{Z}}) \cup U_{2\mathbb{Z},598}$, where

$$U(\frac{\mathbb{Z}}{598\mathbb{Z}}) = \{x \in \{0, 1, \cdots, 597\};\ \gcd(x, 598) = 1\},$$

$$U_{2\mathbb{Z},598} = \{x_{2\mathbb{Z}} \in \mathbb{Z}_{2\mathbb{Z}} \backslash \mathbb{Z};\ gcd(x, 598) = 1\}.$$

Let $t = 17$, we have $gcd(17, 264) = 1$.

By the Bezout theorem, there exist $U, V \in \mathbb{Z}$ such that $17U + 264V = 1$. By the method of successive Euclidian divisions, we obtain $(U, V) = (-31, 2)$.

Thus, the functions C and D are defined as follows:

$$C(x) \equiv \begin{cases} x^{-31}[598], & \text{if } x \in U(\frac{\mathbb{Z}}{598\mathbb{Z}}), \\ x^{-31}(299\mathbb{Z}_{2\mathbb{Z}}), & \text{if } x \in U_{2\mathbb{Z},598}, \end{cases}$$

$$D(y) \equiv \begin{cases} y^{17}[598], & \text{if } x \in U(\frac{\mathbb{Z}}{598\mathbb{Z}}), \\ y^{17}(299\mathbb{Z}_{2\mathbb{Z}}), & \text{if } x \in U_{2\mathbb{Z},598}. \end{cases}$$

4. Practical Application of an $m\Theta$ Approach of RSA Cryptosystems

Let consider two persons called X and Y hoping to communicate confidentially. They choose each one a pair of two great prime numbers p_X, q_X, for X and p_Y, q_Y for Y. They also choose commonly a natural integer number n.

Let set $m_X = np_Xq_X$ and $m_Y = np_Yq_Y$. Then X also chooses C_X in $\mathbb{Z}_{n\mathbb{Z}}$ such that $\gcd(s(C_X), \rho_{n\mathbb{Z}}(m_X)) = 1$ and Y chooses C_Y in $\mathbb{Z}_{n\mathbb{Z}}$ such that $\gcd(s(C_Y), \rho_{n\mathbb{Z}}(m_Y)) = 1$. The modal n-valent congruence class of C_X has an modal n-valent inverse d_X in $U(\frac{\mathbb{Z}}{m_X\mathbb{Z}}) \bigcup U_{n\mathbb{Z}, m_X}$.

As same the modal n-valent congruence class of C_Y has as modal n-valent inverse d_Y in $U(\frac{\mathbb{Z}}{m_Y\mathbb{Z}}) \bigcup U_{n\mathbb{Z}, m_Y}$.

The message is encoded as follows: one can replace k successive symbols by an another symbol element of a given set B, i.e., one defines a map from A^k to B, where A is an usual alphabet. The elements of B are on one hand identified to the inversible congruence classes modulo m_X (or modulo $\frac{m_X}{n}\mathbb{Z}_{n\mathbb{Z}}$), on the another hand are identified to the inversible congruence classes modulo m_Y (or modulo $\frac{m_X}{n}\mathbb{Z}_{n\mathbb{Z}}$).

One understands here that we have two injective maps:

$\alpha : B \to (\frac{\mathbb{Z}}{m_X\mathbb{Z}})^* \bigcup U_{n\mathbb{Z}, m_X}$ and $\beta : B \to (\frac{\mathbb{Z}}{m_Y\mathbb{Z}})^* \bigcup U_{n\mathbb{Z}, m_Y}$. These identifications are public and known by X and Y. In what follows, the messages will be considered as the sequences of symbols of $(\frac{\mathbb{Z}}{m_X\mathbb{Z}})^* \bigcup U_{n\mathbb{Z}, m_X}$ or $(\frac{\mathbb{Z}}{m_Y\mathbb{Z}})^* \bigcup U_{n\mathbb{Z}, m_Y}$.

The keys m_X, C_X and m_Y, C_Y are public. The values of p_X, q_X, d_X, n, $\rho_{n\mathbb{Z}}(m_X)$ and p_Y, q_Y, d_Y, n, $\rho_{n\mathbb{Z}}(m_Y)$ are on the other hand secret.

Let suppose that X wants to encode a message intended for Y and this message is expressed as a sequence of symbols of $(\frac{\mathbb{Z}}{m_Y\mathbb{Z}})^* \cup U_{n\mathbb{Z}, m_Y}$. X applies to this sequence of symbols, let say $(a_1, a_2, \cdots, a_k, \cdots)$ the transformation $(a_1, a_2, \cdots, a_k, \cdots) \mapsto (a_1^{C_Y}, a_2^{C_Y}, \cdots, a_k^{C_Y}, \cdots)$ and then sends the message. When Y receives the message, he applies the inverse transformation $(b_1, b_2, \cdots, b_k, \cdots) \mapsto (b_1^{d_Y}, b_2^{d_Y}, \cdots, b_k^{d_Y}, \cdots)$. This process return the message that is sent.

Remark 4.1. One can guarantee the origin of the message, i.e., Y can be sure that the message sent comes from X. For this purpose, we can suppose that $Card((\frac{\mathbb{Z}}{m_X\mathbb{Z}})^* \cup U_{n\mathbb{Z}, m_X}) < Card((\frac{\mathbb{Z}}{m_Y\mathbb{Z}})^* \cup U_{n\mathbb{Z}, m_Y})$.

To do so, i.e., to sign the message, X can proceed as follows: begin by consider his message as a sequence of elements of $(\frac{\mathbb{Z}}{m_X\mathbb{Z}})^* \cup U_{n\mathbb{Z}, m_X}$ and then applies the transformation $(a_1, a_2, \cdots, a_k, \cdots) \mapsto (a_1^{d_X}, a_2^{d_X}, \cdots, a_k^{d_X}, \cdots)$ which can only be done by him. He then consider the sequence that result from let say $(b_1, b_2, \cdots, b_k, \cdots)$ as a sequence of elements of $(\frac{\mathbb{Z}}{m_Y\mathbb{Z}})^* \cup U_{n\mathbb{Z}, m_Y}$. To do this, X uses an injective map from $(\frac{\mathbb{Z}}{m_X\mathbb{Z}})^* \cup U_{n\mathbb{Z}, m_X}$ to $(\frac{\mathbb{Z}}{m_Y\mathbb{Z}})^* \cup U_{n\mathbb{Z}, m_Y}$ that is agreed in advance with Y and so known by Y. Then X applies the transformation $(b_1, b_2, \cdots, b_k, \cdots) \mapsto (b_1^{C_Y}, b_2^{C_Y}, \cdots, b_k^{C_Y}, \cdots)$ and transmits the message.

To decrypt the message sent by X, Y proceeds as follows: he first applies the transformation $(f_1, f_2, \cdots, f_k, \cdots) \mapsto (f_1^{d_Y}, f_2^{d_Y}, \cdots, f_k^{d_Y}, \cdots)$ which can be done only by him; he then obtains a message composed of elements of $(\frac{\mathbb{Z}}{m_Y\mathbb{Z}})^* \cup U_{n\mathbb{Z}, m_Y}$ which he reinterprets as a message composed of a sequence of elements $(g_1, g_2, \cdots, g_k, \cdots)$ in $(\frac{\mathbb{Z}}{m_X\mathbb{Z}})^* \cup U_{n\mathbb{Z}, m_X}$. He then applies the transformation $(g_1, g_2, \cdots, g_k, \cdots) \mapsto (g_1^{c_X}, g_2^{c_X}, \cdots, g_k^{c_X}, \cdots)$.

If this message has not been transmitted by X but by an another person using an another key of encrypting, then the result will be incomprehensible.

5. Conclusion

In this note, we have reviewed the modal Θ-valent mathematical notions useful for our goal: $m\Theta$ Fermat-Euler's theorem; Formal $m\Theta$ Euler's function; Formal $m\Theta$ exponentiation; $m\Theta$ congruence. Then we have from these modal Θ-valent mathematical concepts defined the RSA encryption, decryption and signature. We have also propose a practical application.

References

[1] F. Ayissi Eteme, Logique et Algèbre de Structures Mathématiques Modales Θ-Valentes Chrysippiennes, Editions Hermann, Paris, 2009.

[2] F. Ayissi Eteme, A *chrm*Θ introducing Pure and Applied Mathematics, Lambert Academic Publishing Saabruken, Germany, 2015.

[3] Neal Koblitz. A Course in Number Theory and Cryptography, Springer, 1994.

[4] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21(2) (1978), 120-126.

DOI: https://doi.org/10.1145/359340.359342

[5] D. Boneh, Twenty years of attacks on the RSA cryptosystem, Notices of the American Mathematical Society 46(2) (1999), 203-213.

[6] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, Journal of Cryptology 10(4) (1997), 233-260.

DOI: https://doi.org/10.1007/s001459900030

[7] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22(6) (1976), 644-654.

DOI: https://doi.org/10.1109/TIT.1976.1055638

[8] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 1960.

[9] B. Morgan and D. Grimshaw, The Dangers of Putting too Much Trust in RSA, 2003.

■