Proyecciones Journal of Mathematics
Vol. 37, N^o 2, pp. 265-293, June 2018.
Universidad Católica del Norte
Antofagasta - Chile

A general method for to decompose modular multiplicative inverse operators over Group of units

Luis A. Cortés Vega
Antofagasta University, Chile

Received : July 2017. Accepted : October 2017

Abstract

In this article, the notion of modular multiplicative inverse operator (MMIO):

$$\mathcal{I}_\varrho : (\mathbf{Z}/\varrho\mathbf{Z})^* \longrightarrow \mathbf{Z}/\varrho\mathbf{Z},\ \mathcal{I}_\varrho(a) = a^{-1},$$

where $\varrho = b \times d > 3$ with $b, d \in \mathbf{N}$, is introduced and studied. A general method to decompose (MMIO) over group of units of the form $(\mathbf{Z}/\varrho\mathbf{Z})^*$ is also discussed through a new algorithmic functional version of Bezout's theorem. As a result, interesting decomposition laws for (MMIO)'s over $(\mathbf{Z}/\varrho\mathbf{Z})^*$ are obtained. Several numerical examples confirming the theoretical results are also reported.

Subjclass [2010] : *Primary 11P83; 11A05; 11A07; 68W10 Secondary 68U20; 68W35; 97N70; 11T55; 68R01.*

Keywords : *Descomposition laws, group of units, Bezout's theorem, modular multiplicative inverse operator, algorithmic functional technique, Chinese remainder theorem.*

1. Introduction

The modular arithmetic has become increasingly important not only in mathematics itself but also in a variety of other disciplines. It has been extremely rich in results and fertile in ideas in several areas, e.g., Number Theory, Computational Arithmetic, Public Key Cryptography, Graph Theory, Room Acoustics, Galois Theory and Digital Communications, and other areas as well.

It is useful to recall here that in modular arithmetic we encounter a valuable concept, the so-called "modular multiplicative inverse" (symbolized by MMI). In precise words, if $\mathbf{Z}/\varrho\mathbf{Z}$ denoted the residue system modulo ϱ, the (MMI) of $a \in \mathbf{Z}/\varrho\mathbf{Z}$, if it exists, is $a^{-1} \in \mathbf{Z}/\varrho\mathbf{Z}$, such that $a \times a^{-1} \equiv 1 \ mod \ \varrho$, where $p \equiv q \ mod \ \varrho$ is the usual modular representation of $q \in \mathbf{Z}/\varrho\mathbf{Z}$. This very special concept is a central element in fields of Public Key Cryptography, Cellular Automata, Computation Arithmetic, Elliptic Curves Cryptosystems and Particle Physics, as well as, in various branches of Electronic and Computer Engineering. A closer look at this concept reveals the difficulty that has its calculation in cases where $\varrho \in \mathbf{N}$ is a large number (prime or composite). In this way, the first question to be answered is: How we obtain an efficient way for to compute the (MMI)?. The seeking of an appropriate response to this question, have stimulated today the creation of innovative iterative procedures intimately connected to very efficient algorithms. For example, Wei in their original paper [33] has introduced the so-called "algorithm of sequential modular multiplication", based, inter alia, on residue signed-digit(SD). In the same context, other algorithms were obtained notably by Verkhovsky's [30], AL-Matari et.al. [1], and Hars [15], who, have been studied a modular inverse algorithm without multiplications for cryptographic applications. We also want to cite [31], where new algorithms based on table look up technique are very well structured. In addition, are also available those inspired by a fundamental idea proposed by Kaliski [17], and referred to as the inverse multiplicative modular of Kaliski-Montgomery in the early literature, we refer the interested reader to the aforementioned references, e.g., [4], [20], [22], [25] and to [26]. Finally, we also want to cite the interestig work of Dumas [11], where a systematic study of Newton-Rapshon methods over p-adic number, was specifically designed to provide a fast computation of (MMI) modulo p^m using quite different techniques.

It should be mentioned, however, that to explore the validity of other strategies, in order to reduce computational times without sacrifice memory space via parallel computing, for example, it is highly desirable; but some extra efforts may be needed. Nevertheless, this obliges among other things to put a one-second question: It is possible to find a method that can decompose the (MMI) over algebraic structures of the form $\mathbf{Z}/\varrho\mathbf{Z}$.? As can be expected, if we have an affirmative answer to this question, we could recover the (MMI) focusing all our computational efforts in each of its parts. However, and being clear that, we can we move in different directions to attempt of responding this question, to the best to the author's knowledge, the recent literature on the subject not is the sufficiently robust to try finding an appropriate response to this not obvious question.

In contrast to this scenanario, in this article we pretend, based on our recent work on the topic, to demonstrate that it is possible to give a positive response to this interesting question, when the (MMI) is considered as an operator on the group of units $(\mathbf{Z}/\varrho\mathbf{Z})^* = \{a \in \mathbf{Z}/\varrho\mathbf{Z} \, : \, \gcd(a, \varrho) = 1\}$, where we have assumed, without loss of generality, that $\varrho = b \times d \in \mathbf{N}$ with $\varrho > 3$.

To this end, we first introduce the notion of modular multiplicative inverse operator (MMIO): $\mathcal{I}_\varrho : (\mathbf{Z}/\varrho\mathbf{Z})^* \longrightarrow \mathbf{Z}/\varrho\mathbf{Z}$, such that $\mathcal{I}_\varrho(a) = a^{-1}$. In this respect, one purpose of this paper is to provide a general method for to decompose (MMIO)'s $\mathcal{I}_\varrho$ on $(\mathbf{Z}/\varrho\mathbf{Z})^*$, whom we call the "Inverse Decomposition Theorem" (IDT). After this point, we have shown that, under reasonable assumptions, the following identities, summarized in (see, Theorem 3.12, Theorem 3.26 and Theorem 3.15 of current paper):

$$\mathcal{I}_\varrho(a) := \mathcal{I}_b(a) + b \times \phi_d \, \mathcal{I}_d(d-a) \times \mathcal{I}_a(a-b)\} \, , \tag{1.1}$$

$$\mathcal{I}_\varrho(a) := \mathcal{I}_b(a) + b \times \phi_d \left\{ \frac{1}{4} \left[\mathcal{I}_{b+a}(a) - \mathcal{I}_{b-a}(a) \right] \times \left[\mathcal{I}_{a+d}(d) - \mathcal{I}_{a-d}(d) \right] \right\} \tag{1.2}$$

and

$$\mathcal{I}_\varrho(a) := \mathcal{I}_b(a) + b \times \phi_d \left\{ \mathcal{I}_d(a) \times \mathcal{I}_a(b) - 1 \right\} \tag{1.3}$$

are valid. Here, the operator $\phi_d(\cdot)$ is defined by $\phi_d : \mathbf{N}^* \to \mathbf{Z}/d\mathbf{Z}$, such that

$$\phi_d(a) = \begin{cases} a, \text{ if } 0 \leq a \leq d-1, \\ \mathbf{r}, \text{ if } a \geq d, \end{cases}$$

where $a \equiv \mathbf{r} \; mod \; d$.

In the same context, we shall also give several results relating which may become of an independent interest in the beautiful arena of the Number theory, Computer Arithmetic and related fields. In order to establish Eqs. (1.1), (1.2) and (1.3), we needs to show the following decomposition law:

$$\mathcal{I}_{\varrho}(a) := \mathcal{I}_b(a) + b \times \phi_d \left\{\mathcal{L}_d(a) \times \mathcal{L}_a(b)\right\}, \tag{1.4}$$

where, the operators $\mathcal{L}_{\beta}(\cdot)$ have the following structure:
$\gamma \in (\mathbf{Z}/\beta\mathbf{Z})^* \rightarrow \mathcal{L}_{\beta}(\gamma) \in \mathbf{Z}/\beta\mathbf{Z},$ with $\mathcal{L}_{\beta}(\gamma) = \phi_{\beta}\left[(\beta - 1) \times \mathcal{I}_{\beta}(\gamma)\right].$
This is the basic idea exploited in this paper.

An argument based on an algorithmic functional approach proposed by the author in [5] and the elegant and versatile Bezouts theorem confirms Eq. (1.4). Eqs. (1.1), (1.2) and (1.3) are extremely interesting and are naturally associated to (MMI). Furthermore, we should emphasize that, from a computational point of view, the formulae considered above offer opportunities of construct new architectures and schemes (problems that not is addressed in this work) which can complement to the different innovative algorithms mentioned in the references. It should, however, be noted that despite these recent and valuable contributions, to the author's knowledge, there is nothing in prior literature resembling Eqs. (1.1), (1.2) and (1.3).

It should be stressed that the genesis of our approach appears in two previous works [5, 6], where a new algorithmic functional technique for the Euclidean algorithm it was derived. However, being this a key ingredient in our analysis, in [5] are not study of (MMIO) has been considered.

Our work initially was motivated in part by applications of the modular inversion in RNS (Residue Number System) [3], by Chinese remainder fast algorithms for the purposes of calculating the discrete circular convolution over finite Galois fields $(\mathbf{Z}/p\mathbf{Z})^*$, where p is a prime number [27], by the seminal paper of Dumas [11], where are given different variants of Newton-Rapshon methods over p-adic numbers to compute the (MMI) a prime power, as well as, some celebrated works related to Public Key Cryptosystems (see, e.g., [21]) and the building of linear and nonlinear congruential pseudorandom number generators [12]. Knuth [18] also has an extensive and excellent discussion in these and other aspects of great interest.

Other different line of motivation of current paper this inserted in the framework of some problems associated with certain inverse states defined about finite Galois Fields $(\mathbf{Z}/p_{\alpha}\mathbf{Z})^*$, where p_{α} is a large prime number, the which are key in the computation of Higgs mass - the particle related to the mechanism thought to be responsible for giving masses to all other particles - via a p-adic metric. A general survey of this last fascinating subject may be found in [8], [9] and relevant references.

This paper is organized as follows. Section §2 deals with preliminaries and notation. In §3, we introduce an algorithmic functional setting and we present in detail the main results of this work. Section §4 we offer some numerical experiments, the which displays and captures the richness algorithmic functional of all our theoretical results.

2. Preliminaries

To state our main results we shall give a rapid survey of those parts of the Number Theory that we shall need in what follows. Details can be found for instance in [23]. First, however, we need some notation. Here, and in the rest of the paper, $\mathbf{N}$ denote the set of the natural numbers, $a \in \mathbf{N}^*$ if $a \in \mathbf{N} \cup \{0\}$. To simplify the presentation we assume that $a \in \mathbf{N}^\triangleright$ if $a \in \mathbf{N}\backslash\{1\}$. We let $(\mathbf{Z}, +, \times)$ denote the ring of integers. The operation $\times$ in $\mathbf{Z}$ is usually called the product. Let b be a fixed positive integer. Two integers a and d are said to be congruent modulo b, written $a \equiv d \ mod \ b$ if b divides $a - d$. Let $\mathbf{Z}/b\mathbf{Z}$ be the ring of residue classes modulo b, $a \in \mathbf{Z}/b\mathbf{Z}$ if $a \in \{0, 1, 2, \ldots, b-1\}$. Throughout this paper we use the convention that $(\mathbf{Z}/b\mathbf{Z})^* = \{a \in \mathbf{Z}/b\mathbf{Z} \ : \ \gcd(a, b) = 1\}$ denotes the group of unit of $\mathbf{Z}/b\mathbf{Z}$, the which under multiplication forms an abelian group. Let us emphasize that, as already mentioned above, the modular multiplicative inverse (MMI) of $a \in \mathbf{Z}/b\mathbf{Z}$, if it exists, is $a^{-1} \in \mathbf{Z}/b\mathbf{Z}$, such that $a \times a^{-1} \equiv 1 \ mod \ b$. The symbol $\gcd(b, d)$ denotes the greatest common divisor between b and d (not both zero). In this notation, if $\gcd(a, b) = 1$, we say that a and b are relatively prime. The Bézout's theorem, which states that: if a and b are positive integers, then there exist integers $\mathbf{s}$ and $\mathbf{t}$ such that $\gcd(a, b) = \mathbf{s} \times a + \mathbf{t} \times b$, is useful when a and b are relatively primes, in this case we have $\gcd(a, b) = 1$. Now following the arguments in [5], we can derive for the operators $\phi_b : \mathbf{N}^* \to \mathbf{Z}/b\mathbf{Z}$ and $C_b : \mathbf{N}^* \to \mathbf{N}^*$, defined by

$$\phi_b(a) = \begin{cases} a, \text{ if } 0 \leq a \leq b-1, \\ \mathbf{r}, \text{ if } a \geq b \end{cases} \quad \text{and} \quad C_b(a) = \tfrac{a - \phi_b(a)}{b},$$

where $a \equiv \mathbf{r} \ mod \ b$ for any $b \in \mathbf{N}^\triangleright$, the following

Theorem 2.1. *Let $b \in \mathbf{N}^{\triangleright}$. Then, the following statements are true:*

(ϕ1) $\phi_b(0) = 0$,

(ϕ2) $\phi_b(d \times b) = 0$ *for every* $d \in \mathbf{N}^*$,

(ϕ3) $\phi_b(a) = \phi_b(\phi_b(a))$ *for every* $a \in \mathbf{N}^*$,

(ϕ4) $\phi_b(a + d) = \phi_b(\phi_b(a) + \phi_b(d)) = \phi_b(a + \phi_b(d)) = \phi_b(\phi_b(a) + d)$ *for every* a, $d \in \mathbf{N}^*$,

(ϕ5) $\phi_b(a \times d) = \phi_b(\phi_b(a) \times \phi_b(d)) = \phi_b(a \times \phi_b(d)) = \phi_b(\phi_b(a) \times d)$ *for every* a, $d \in \mathbf{N}^*$,

(ϕ6) $\phi_b(a + b) = \phi_b(a)$ *for every* $a \in \mathbf{N}^*$ *("periodicity" of* ϕ_b*),*

(c1) $C_b(0) = 0$,

(c2) $C_b(b \times a) = a$ *for every* $a \in \mathbf{N}^*$*. In particular* $C_b(b) = 1$,

(c3) $C_b(\phi_b(a)) = 0$ *for every* $a \in \mathbf{N}^*$ *(*C_b *is a "annihilator" of* ϕ_b*),*

(c4) $C_b(a + d) = C_b(a) + C_b(d) + C_b(\phi_b(a) + \phi_b(d))$ *for every* a, $d \in \mathbf{N}^*$,

(c5) $C_b(a \times d) = C_b(a) \times d + \phi_b(a) \times C_b(d) + C_b(\phi_b(a) \times \phi_b(d))$ *for every* a, $d \in \mathbf{N}^*$,

(c6) $C_b(a + b) = C_b(a) + 1$ *for every* $a \in \mathbf{N}^*$ *(*C_b *is quasi-periodic),*

(c7) $C_b(a + b \times \mu) = C_b(a) + \mu$ *for every* a, $\mu \in \mathbf{N}^*$,

(e1) $a = \phi_b(a) + b \times C_b(a)$ *for every* $a \in \mathbf{N}^*$,

(e2) $a < b$ *if and only if* $C_b(a) = 0$ *for every* $a \in \mathbf{N}^*$,

(e3) $(C_b \circ C_d)(a) = C_{b \times d}(a)$ *for every* $a \in \mathbf{N}^*$ *and every* $d \in \mathbf{N}^{\triangleright}$.

Remark 2.2. *Let us remark that in the Theorem 2.1 the compositions of the operators* C_d *with* C_b*;* C_d *with* ϕ_b, ϕ_d *with* ϕ_b *and* ϕ_d *with* C_b, *are defined by one usual way, that is:*

$$\begin{aligned}
&C_d \circ C_b : \mathbf{N}^* \to \mathbf{N}^*, \text{such that } (C_d \circ C_b)(a) := C_d(C_b(a)) \text{ for all } a \in \mathbf{N}^*,\\
&C_d \circ \phi_b : \mathbf{N}^* \to \mathbf{N}^*, \text{such that } (C_d \circ \phi_b)(a) := C_d(\phi_b(a)) \text{ for all } a \in \mathbf{N}^*,\\
&\phi_d \circ \phi_b : \mathbf{N}^* \to \mathbf{N}^*, \text{such that } (\phi_d \circ \phi_b)(a) := \phi_d(\phi_b(a)) \text{ for all } a \in \mathbf{N}^*,\\
&\phi_d \circ C_b : \mathbf{N}^* \to \mathbf{N}^*, \text{such that } (\phi_d \circ C_b)(a) := \phi_d(C_b(a)) \text{ for all } a \in \mathbf{N}^*.
\end{aligned}$$

Another result coming out of Theorem 2.1, using the property ($e3$) is the following decomposition law (Theorem 4 given in [5]):

Theorem 2.3. *For any $b, d \in \mathbf{N}^{\triangleright}$ and any $a \in \mathbf{N}^*$, we have*

$$\phi_{d\times b}(a) = \phi_d(a) + d \times \phi_b(C_d(a)). \tag{2.1}$$

3. Decomposition-type theorems for modular multiplicative inverses operators in group of units: (MMIO) v/s (MMI)

In this section we shall be concerned with the construction of several laws decomposition for the (MMI) on $(\mathbf{Z}/\varrho\mathbf{Z})^*$, where $\varrho = b\times d$, and $b, d \in \mathbf{N}^{\triangleright}$. In order to investigate this, we following the approach of the previous section, we introduce the notion of modular multiplicative inverse operator (MMIO) in the following

Definition 3.1. *If $b \in \mathbf{N}^{\triangleright}$, then the modular multiplicative inverse operator (MMIO) denoted by $\mathcal{I}_b(\cdot)$ is the mapping*

$$\mathcal{I}_b : (\mathbf{Z}/b\mathbf{Z})^* \to \mathbf{Z}/b\mathbf{Z}, \textit{ defined by } \mathcal{I}_b(a) = a^{-1}, \textit{ such that}$$

$$\phi_b(a \times \mathcal{I}_b(a)) = 1 \textit{ for every } a \in (\mathbf{Z}/b\mathbf{Z})^*. \tag{3.1}$$

Note that by the definition given, for any $a \in (\mathbf{Z}/b\mathbf{Z})^*$ the (MMIO) always exist, and has the following additional property when acting on the natural numbers:

$$\mathcal{I}_b(a) = \mathcal{I}_b(\phi_b(a)),\ a \in \mathbf{N} \textit{ with } \gcd(a, b) = 1, \textit{ and } \mathcal{I}_b(1) = 1. \tag{3.2}$$

As examples, we have that $\mathcal{I}_7(5) = 3$ and $\mathcal{I}_7(13) = 6$, since

$$\phi_7(5 \times \mathcal{I}_7(5)) = \phi_7(5 \times 3) = \phi_7(15) = 1,$$

and similarly

$$\phi_7(13 \times \mathcal{I}_7(13)) = \phi_7(13 \times 6) = \phi_7(\phi_7(13) \times 6) = \phi_7(6 \times 6) = \phi_7(36) = 1.$$

In this last expression, we used property ($\phi5$) of Theorem 2.1 given above. Further noting that Eq. (3.2) yields to $\mathcal{I}_7(13) = \mathcal{I}_7(\phi_7(13)) = \mathcal{I}_7(6) = 6$.

Another specific type of operator plays an important and particular role in what follows is given in the following

Definition 3.2. *If $b \in \mathbf{N}^{\triangleright}$, the operator $\mathcal{L}_b$ given by:*

(3.3) $a \in (\mathbf{Z}/b\mathbf{Z})^* \to \mathcal{L}_b(a) \in \mathbf{Z}/b\mathbf{Z}$, *with* $\mathcal{L}_b(a) = \phi_b\left[(b-1) \times \mathcal{I}_b(a)\right]$

is well defined. $\mathcal{L}_b(a)$ will be called the "predecessor operator modulo b", since

$$\phi_b\left[a \times \mathcal{L}_b(a)\right] = b - 1 \text{ for any } a \in (\mathbf{Z}/b\mathbf{Z})^*. \tag{3.4}$$

From this definition it becomes clear that the predecessor operator $\mathcal{L}_b(a)$ also satisfies the following additionals properties:

(3.5)$\mathcal{L}_b(1) = b - 1$ and $\mathcal{L}_b(a) = \mathcal{L}_b(\phi_b(a))$ if $a \in \mathbf{N}$, with $\gcd(a, b) = 1$.

The next theorem provides the foundation of our development and contains the fundamental identity on which the analysis of the results in this section rests.

Theorem 3.3 (A algorithmic functional connection of the Bezout's). coefficients

Let be $m, n \in \mathbf{N}^{\triangleright}$ such that $gcd(m, n) = 1$. Then

$$m \times \mathcal{I}_n(m) = n \times \mathcal{L}_m(n) + 1. \tag{3.6}$$

Proof. Indeed, as $\gcd(m, n) = 1$. The Bézout's theorem, states that, there exist integers $\mathbf{x}$ and $\mathbf{y}$ such that

$$1 = m \times \mathbf{x} + n \times \mathbf{y}. \tag{3.7}$$

To prove Eq. (3.6) we assume without loss of generality that $\mathbf{x} \geq 0$ and $\mathbf{y} < 0$. If now, we multiply Eq. (3.7) by $\mathcal{I}_n(m)$, we have

$$\mathcal{I}_n(m) = m \times \mathcal{I}_n(m) \times \mathbf{x} + n \times \mathcal{I}_n(m) \times \mathbf{y}. \tag{3.8}$$

or equivalently,

$$\mathcal{I}_n(m) + n \times \mathcal{I}_n(m) \times (-\mathbf{y}) = m \times \mathcal{I}_n(m) \times \mathbf{x}.$$

(3.9)

Applying the operator $\phi_n(\cdot)$ to this identity, togheter with the Eq. (3.1) and properties (ϕ_4) and (ϕ_2) of the Theorem 2.1, we obtain

$$\phi_n(\mathbf{x}) = \mathcal{I}_n(m). \tag{3.10}$$

Now it is easy to check, using similar arguments, that:

$$\phi_m(-\mathbf{y}) = \phi_m[(m-1) \times \mathcal{I}_m(n)] = \mathcal{L}_m(n). \tag{3.11}$$

From these equations and the property $(e1)$ of the Theorem 2.1, we get

$$\mathbf{x} = \mathcal{I}_n(m) + n \times C_n(\mathbf{x}) \tag{3.12}$$

and

$$-\mathbf{y} = \mathcal{L}_m(n) + m \times C_m(-\mathbf{y}). \tag{3.13}$$

Hence, Eqs. (3.7), (3.12), (3.13) gives

$$1 = m \times \mathcal{I}_n(m) + m \times n \times C_n(\mathbf{x}) - n \times \mathcal{L}_m(n) - n \times m \times C_m(-\mathbf{y}), \tag{3.14}$$

or equivalently,

$$n \times m \times C_m(-\mathbf{y}) + (1 + n \times \mathcal{L}_m(n)) = m \times \mathcal{I}_n(m) + m \times n \times C_n(\mathbf{x}). \tag{3.15}$$

Applying the operator $\phi_{m\times n}$ to this identity, together with the properties (ϕ_4), (ϕ_2) and the definition of $\phi_\beta(\cdot)$, with $\beta = m \times n$, we obtain

$$\phi_{m\times n}[1 + n \times \mathcal{L}_m(n)] = m \times \mathcal{I}_n(m). \tag{3.16}$$

Thus, in order to prove Eq. (3.6) it is sufficient to prove that $1 + n \times \mathcal{L}_m(n) < m \times n$. In fact, by the properties $(c7)$, $(c4)$ and $(c2)$ of Theorem 2.1 we get:

$$\begin{aligned} C_n(1 + n \times \mathcal{L}_m(n)) &= C_n(1) + \mathcal{L}_m(n) \\ &= \mathcal{L}_m(n). \end{aligned}$$

Now this last identity implies that

$$C_m[C_n(1 + n \times \mathcal{L}_m(n))] = C_m(\mathcal{L}_m(n)) = 0,$$

since $\mathcal{L}_m(n) < m$. Thus by the property $(e3)$ of the Theorem 2.1, we get

$$C_{m \times n}(1 + n \times \mathcal{L}_m(n)) = 0.$$

From this identity and the property $(e2)$ of the Theorem 2.1, we deduce that

$$1 + n \times \mathcal{L}_m(n) < m \times n.$$

Finally, these last expression, the definition of $\phi_\beta(\cdot)$, with $\beta = m \times n$ and Eq. (3.16), lead to the desired result. This completes the proof of Theorem 3.3. □

Now we begin to make use of these theorem. In addition we can collect a number of important algebraic and functional properties, some of which, we shall use frequently in the current paper.

Theorem 3.4 (Fundamental identities). *If* b, $d \in \mathbf{N}^{\triangleright}$, *with* $\gcd(b, d) = 1$. *Then for every* $a \in \mathbf{N}$, *with* $\gcd(a, b) = 1$, *we have*

($\mathcal{L}1$) $\mathcal{L}_b(\mathcal{I}_b(a)) = \mathcal{I}_b(\mathcal{L}_b(a))$,

($\mathcal{L}2$) $\mathcal{L}_b(a \times d) = \phi_b(\mathcal{L}_b(a) \times \mathcal{I}_b(d))$,

($\mathcal{L}3$) For any $m, n \in \mathbf{N}$ *such that* $\gcd(m + n, b) = 1$, *we have*

$$\mathcal{L}_b(m + n) = \mathcal{L}_b(\phi_b(m) + \phi_b(n)),$$

($\mathcal{L}4$) $\mathcal{L}_b(a + b) = \mathcal{L}_b(a)$, *("periodicity" of* $\mathcal{L}_b$*),*

($\mathcal{L}5$) $\mathcal{L}_b(\mathcal{L}_b(a)) = \phi_b(a)$,

(I1) $\mathcal{I}_b(a \times d) = \phi_b(\mathcal{I}_b(a) \times \mathcal{I}_b(d))$,

(I2) For any $m, n \in \mathbf{N}$ *such that* $\gcd(m + n, b) = 1$, *we have*

$$\mathcal{I}_b(m + n) = \mathcal{I}_b(\phi_b(m) + \phi_b(n)),$$

(I3) $\mathcal{I}_b(a + b) = \mathcal{I}_b(a)$, *("periodicity" of* $\mathcal{I}_b$*),*

(I4) $\mathcal{I}_b(\mathcal{I}_b(a)) = \phi_b(a)$.

Proof. *The proof of Theorem 3.4 makes use of the properties of Theorem 2.1, the identities (3.1), (3.2), (3.4), (3.5) and the Theorem 3.3.* □

Remark 3.5. *Under the assumptions of Theorem 3.4, the compositions of the operators $\mathcal{L}_d$ with $\mathcal{I}_b$; ϕ_d with $\mathcal{L}_b$; ϕ_d with $\mathcal{I}_b$ and $\mathcal{I}_d$ with $\mathcal{L}_b$ are defined by one usual way.*

From Theorem 3.4 we can observe some potential properties of the (MMIO). The most convincing example is the following

Corollary 3.6. *Let $b \in \mathbf{N}^{\triangleright}$, then*

$$\mathcal{I}_b(b-1) = b-1. \tag{3.17}$$

Proof. In fact, using ($\mathcal{L}1$), (3.2) and (3.5), we get

$$b-1 = \mathcal{L}_b(1) = \mathcal{L}_b(\mathcal{I}_b(1)) = \mathcal{I}_b(\mathcal{L}_b(1)) = \mathcal{I}_b(b-1),$$

which completes the proof. □

Remark 3.7.

1. Other proof of this fact using (MMI) appears in [24].

2. Note that ($\mathcal{L}5$) and (3.5) implies that

$$\mathcal{L}_b(b-1) = 1.$$

We continue our study by proving the following technical lemma.

Lemma 3.8. *If m and n are natural numbers with $m \in \mathbf{N}^{\triangleright}$ and $\gcd(m,n) = 1$, then*

$$\mathcal{I}_m(n) + \mathcal{L}_m(n) = m. \tag{3.18}$$

Proof. *In fact, using Eq. (3.3) together with the properties ($\phi2$), ($\phi3$), ($\phi4$) and ($\phi5$) of Theorem 2.1 we may rewrite $\mathcal{I}_m(n) + \mathcal{L}_m(n)$ as*

$$\begin{aligned}
\mathcal{I}_m(n)+\mathcal{L}_m(n) &= \mathcal{I}_m(n)+\phi_m((m-1)\times\mathcal{I}_m(n)) \\
&= \mathcal{I}_m(n)+\phi_m((m-1)\times\mathcal{I}_m(n)+\underbrace{\phi_m(m\times(\mathcal{I}_m(n)+1))}_{0}) \\
&= \mathcal{I}_m(n)+\phi_m((m-1)\times\mathcal{I}_m(n)+m\times(\mathcal{I}_m(n)+1)) \\
&= \mathcal{I}_m(n)+\phi_m((m-\mathcal{I}_m(n))+2\times m\times\mathcal{I}_m(n)) \\
&= \mathcal{I}_m(n)+\phi_m((m-\mathcal{I}_m(n))+\underbrace{\phi_m(2\times m\times\mathcal{I}_m(n))}_{0}) \\
&= \mathcal{I}_m(n)+\phi_m(m-\mathcal{I}_m(n)) \\
&= \mathcal{I}_m(n)+m-\mathcal{I}_m(n)=m,
\end{aligned}$$

and the proof is complete. □

Thanks to this lemma and applying the properties ($\mathcal{L}1$) and ($I1$) of Theorem 3.4 the following theorem can be proved.

Theorem 3.9. *Let b be in $\mathbf{N}^{\triangleright}$, then for every $a\in\mathbf{N}$ with $\gcd(a,b)=1$ and $a<b$, we get*

$$\mathcal{I}_b(a)+\mathcal{I}_b(b-a)=b. \tag{3.19}$$

Now in this part of the work, we proved the formulas posed at the beginning, in the introduction of the paper, to do this, and illustrate the main ideas of this paper, we start with the following

Theorem 3.10 (The inverse decomposition theorem). *Let b, d be in $\mathbf{N}^{\triangleright}$. Then, for any $a\in\mathbf{N}^{\triangleright}$, with $\gcd(a,b)=1$ and $\gcd(a,d)=1$, we get*

$$\mathcal{I}_{b\times d}(a)=\mathcal{I}_b(a)+b\times\phi_d\left\{\mathcal{L}_d(a)\times\mathcal{L}_a(b)\right\}. \tag{3.20}$$

Proof. First of all, let us notice that $\gcd(a,b)=1$ and $\gcd(a,d)=1$, implies that $\gcd(a,b\times d)=1$. Thus the operator $\mathcal{I}_{b\times d}(\cdot)$ it is well defined over $(\mathbf{Z}/\varrho\mathbf{Z})^*$. Now the Theorem 3.3 implies that $a\times\mathcal{I}_b(a)-b\times\mathcal{L}_a(b)=1$. Hence, by (3.1) and the property ($e1$) of Theorem 2.1, this last equation may be written, as

$$\begin{aligned}
b\times\mathcal{L}_a(b) &= a\times\mathcal{I}_b(a)-\underbrace{\phi_b(a\times\mathcal{I}_b(a))}_{1} \\
&= b\times C_b(a\times\mathcal{I}_b(a)).
\end{aligned}$$

Thus we obtain that,

$$C_b(a \times \mathcal{I}_b(a)) = \mathcal{L}_a(b). \tag{3.21}$$

Again using the Theorem 3.3, we get

$$a \times \mathcal{I}_{b\times d}(a) - b \times d \times \mathcal{L}_a(b \times d) = 1.$$

So, if we multiply this expression by $\mathcal{I}_b(a)$, we have

$$a \times \mathcal{I}_b(a) \times \mathcal{I}_{b\times d}(a) = \mathcal{I}_b(a) + b \times d \times \mathcal{I}_b(a) \times \mathcal{L}_a(b \times d).$$

Applying the operator ϕ_b to this last identity, togheter with the Eq. (3.1) and the properties (ϕ_4), (ϕ_2), (ϕ_5) and (ϕ_3) of Theorem 2.1, we deduce that

$$\phi_b\left(\mathcal{I}_{b\times d}(a)\right) = \phi_b\left(\mathcal{I}_b(a)\right) = \mathcal{I}_b(a). \tag{3.22}$$

Hence Eq. (3.22) and the property (e1) of Theorem 2.1 gives

$$\mathcal{I}_{b\times d}(a) = \mathcal{I}_b(a) + b \times C_b(\mathcal{I}_{b\times d}(a)). \tag{3.23}$$

Now using Eq. (3.1) and Eq. (3.23),

$$\phi_{b\times d}\left(a\times\mathcal{I}_b(a) + a \times b \times \xi_d\right) = 1, \tag{3.24}$$

where $\xi_d = C_b(\mathcal{I}_{b\times d}(a))$. Furhermore, note that the properties (e3)-(e2) of Theorem 2.1, implies that $\xi_d < d$. Also, the Theorem 2.3 (see, Eq. (2.1)) converts Eq. (3.24) on

$\phi_b\left(a\times\mathcal{I}_b(a) + a \times b \times \xi_d\right) + b \times \phi_d(C_b\left(a\times\mathcal{I}_b(a) + a \times b \times \xi_d\right)) = 1.$ From there, and thanks to the properties $(\phi 4)$, $(\phi 3)$, $(\phi 2)$ and $(c7)$ of Theorem 2.1, we see that

1$= \phi_b(a \times \mathcal{I}_b(a)) + b \times \phi_d(C_b(a \times \mathcal{I}_b(a)) + a \times \xi_d)$. As $\phi_b(a \times \mathcal{I}_b(a)) = 1$ this, togheter with the equation given above, we get

$\phi_d(C_b(a \times \mathcal{I}_b(a)) + a \times \xi_d) = 0$. Now adding $(d-1) \times C_b(a \times \mathcal{I}_b(a))$ to this last equation, and later applying once again ϕ_d to obtain

$\phi_d(a \times \xi_d) = \phi_d\left((d-1) \times C_b(a \times \mathcal{I}_b(a))\right)$. Finally, multiplying this last expression by $\mathcal{I}_d(a)$, and later by applying once again ϕ_d, together with the properties $(\phi 3)$ and $(\phi 5)$ of Theorem 2.1, and the fact that $\xi_d < d$, results in

$\xi_d = \phi_d((d-1) \times \mathcal{I}_d(a) \times C_b(a \times \mathcal{I}_b(a)))$. So, the property $(\phi 5)$ of Theorem 2.1, Eq. (3.21) and the definition of $\mathcal{L}_d(a)$, yields to

$$\xi_d = \phi_d\left[\mathcal{L}_d(a) \times \mathcal{L}_a(b)\right]. \tag{3.25}$$

Finally, Eqs. (3.23) and (3.25) yields to Eq. (3.20), we obtain the desired result. □

Remark 3.11. *Note that once established the expression (3.20) of Theorem 3.10, we could prove the validity of*

$$\mathcal{I}_{b\times d}(a) = \mathcal{I}_d(a) + d \times \phi_b \left\{\mathcal{L}_b(a) \times \mathcal{L}_a(d)\right\}. \tag{3.26}$$

This has another very interesting consequence.

Theorem 3.12. *Let b, d be in $\mathbf{N}^{\triangleright}$. Then, for every $a \in (b,d) \cap \mathbf{N}^{\triangleright}$, with* $\gcd(a,b) = 1$ *and* $\gcd(a,d) = 1$, *we get*

$$\mathcal{I}_{b\times d}(a) = \mathcal{I}_b(a) + b \times \phi_d \left\{\mathcal{I}_d(d-a) \times \mathcal{I}_a(a-b)\right\}. \tag{3.27}$$

Proof. First, let us notice that $\gcd(a,b) = 1$ and $\gcd(a,d) = 1$, implies that $\gcd(a, b\times d) = 1$. Hence the operator $\mathcal{I}_{b\times d}(\cdot)$ it is well defined over $(\mathbf{Z}/\varrho\mathbf{Z})^*$, where $\varrho = b \times d$ with b, $d \in \mathbf{N}^{\triangleright}$. Now by Lemma 3.8 we have that

$$\mathcal{I}_m(n) + \mathcal{L}_m(n) = m,$$

for all positive integers $m, n > 1$ with $\gcd(m,n) = 1$. From this last expression, we derive for $m = a$ and $n = \mathcal{I}_a(b)$ the identity:

$$\mathcal{I}_a(\mathcal{I}_a(b)) + \mathcal{L}_a(\mathcal{I}_a(b)) = a. \tag{3.28}$$

Thus, by the property $(I4)$ of Theorem 3.4, we obtain of (3.28) that

$$\phi_a(b) + \mathcal{L}_a(\mathcal{I}_a(b)) = a. \tag{3.29}$$

As $a > b$, by the definition of $\phi_a(b)$ we conclude of (3.29) that

$$\mathcal{L}_a(\mathcal{I}_a(b)) = a - b. \tag{3.30}$$

Similarly, consider now that $m = d$ and $n = \mathcal{I}_d(a)$, then as $d > a$, one gets

$$\mathcal{L}_d(\mathcal{I}_d(a)) = d - a. \tag{3.31}$$

Remark 3.13. *Note that* $\gcd(a, \mathcal{I}_a(b)) = 1$ *by Bzout's theorem. Indeed, there are $x = -\mathcal{L}_b(a) \in \mathbf{Z}$ and $y = b \in \mathbf{Z}$ such that $a \times x + \mathcal{I}_a(b) \times y = 1$. In exactly the same way, we can establish that* $\gcd(d, \mathcal{I}_d(a)) = 1$.

Note now that the properties ($\mathcal{L}1$), ($\mathcal{L}4$), ($I4$) of Theorem 3.4 together with Eqs. (3.5), (3.30) and (3.31) yields to

$$\begin{aligned}\mathcal{L}_d(a) \times \mathcal{L}_a(b) &= \mathcal{L}_d(\phi_d(a)) \times \mathcal{L}_a(\phi_a(b)) \\ &= \mathcal{L}_d(\mathcal{I}_d(\mathcal{I}_d(a))) \times \mathcal{L}_a(\mathcal{I}_a(\mathcal{I}_a(b))) \\ &= \mathcal{I}_d(\mathcal{L}_d(\mathcal{I}_d(a))) \times \mathcal{I}_a(\mathcal{L}_a(\mathcal{I}_a(b))) \\ &= \mathcal{I}_d(d-a) \times \mathcal{I}_a(a-b),\end{aligned}$$

which together with the Theorem 3.10 leads to relation (3.27). This completes the proof of Theorem 3.12. □

Remark 3.14. *Another decomposition law for the (MMIO) $\mathcal{I}_{b\times d}(\cdot)$ may be obtained with the aid of the so-called reciprocity formula, the which has been exploted in the seminal papers of Arazi and Qi [2], Joye and Paillier [16] and Ko [19]. Motived in parts by this papers and our algorithmical functional technique we stablish the following theorem.*

Theorem 3.15. *Let b, d be in $\mathbf{N}^{\triangleright}$. Then, for any $a \in \mathbf{N}^{\triangleright}$, with $\gcd(a,b) = 1$ and $\gcd(a,d) = 1$, we have in terms of the (MMIO) that:*

$$\mathcal{I}_{b\times d}(a) = \mathcal{I}_b(a) + b \times \phi_d\left\{\mathcal{I}_d(a) \times \mathcal{I}_a(b) - 1\right\}. \tag{3.32}$$

Proof. First let us notice that $\gcd(a,b) = 1$ and $\gcd(a,d) = 1$, implies that $\gcd(a, b \times d) = 1$. Hence the operator $\mathcal{I}_{b\times d}(\cdot)$ it is well defined on $(\mathbf{Z}/\varrho\mathbf{Z})^*$, where $\varrho = b \times d$ with $b, d \in \mathbf{N}^{\triangleright}$. Recall that

$$\mathcal{I}_m(n) + \mathcal{L}_m(n) = m, \tag{3.33}$$

for all positive integers m, $n > 1$ with $\gcd(m,n) = 1$. Also, by Theorem 3.3 we gets

$$a \times \mathcal{I}_d(a) = 1 + d \times \mathcal{L}_a(d).$$

Now from this last identity and the Eq. (3.33) with $m = a$ and $n = d$, we have the reciprocity formula:

$$a \times \mathcal{I}_d(a) = 1 + d \times [a - \mathcal{I}_a(d)].$$

Thus

$$d \times a = a \times \mathcal{I}_d(a) + d \times \mathcal{I}_a(d) - 1. \tag{3.34}$$

Now note that $\mathcal{L}_d(a) \times \mathcal{L}_a(b)$ by Eq. (3.33) can be also rewrite as

$$\begin{aligned} \mathcal{L}_d(a) \times \mathcal{L}_a(b) &= (d - \mathcal{I}_d(a)) \times (a - \mathcal{I}_a(b)) \\ &= d \times a - d \times \mathcal{I}_a(b) - a \times \mathcal{I}_d(a) + \mathcal{I}_d(a) \times \mathcal{I}_a(b) \end{aligned}$$

Therefore, the equality (3.34) implies that

$$\mathcal{L}_d(a) \times \mathcal{L}_a(b) = d \times (\mathcal{I}_a(d) - \mathcal{I}_a(b)) + \mathcal{I}_d(a) \times \mathcal{I}_a(b) - 1.$$

So,

$$\phi_d \left\{ \mathcal{L}_d(a) \times \mathcal{L}_a(b) \right\} = \phi_d \left\{ \mathcal{I}_d(a) \times \mathcal{I}_a(b) - 1 \right\}.$$

Using the Theorem 3.10, the proposition is shown. This completes the proof of Theorem 3.15. □

Remark 3.16. *The decomposition law for the operators $\mathcal{I}_{b\times d}(\cdot)$ over group of units $(\mathbf{Z}/\varrho\mathbf{Z})^*$ established in the Theorem 3.15 facilities the understanding of how these operators depends of the (MMIO)'s $\mathcal{I}_b(\cdot)$, $\mathcal{I}_d(\cdot)$ and $\mathcal{I}_a(\cdot)$, respectively. Also, it is interesting to note that, in contrast with the Theorem 3.12, in Theorem 3.15 we does not require the assumption $a \in (b, d) \cap \mathbf{N}^{\triangleright}$.*

Corollary 3.17. *Let b, d be in $\mathbf{N}^{\triangleright}$. Then, for any $a \in \mathbf{N}^{\triangleright}$, with $\gcd(a, b) = 1$, $\gcd(a, d) = 1$ and $\phi_a(b) = 1$, we get*

$$\mathcal{I}_{b\times d}(a) = \frac{1}{a} \times (1 - b) + b \times \mathcal{I}_d(a). \tag{3.35}$$

Proof. First let us notice that $\gcd(a, b) = 1$ and $\gcd(a, d) = 1$, implies that $\gcd(a, b \times d) = 1$. Hence the operator $\mathcal{I}_{b\times d}(\cdot)$ it is well defined about $(\mathbf{Z}/\varrho\mathbf{Z})^*$, where $\varrho = b \times d$ with b, $d \in \mathbf{N}^{\triangleright}$. Now, as $\mathcal{I}_a(b) = \mathcal{I}_a(\phi_a(b)) = \mathcal{I}_a(1) = 1$ (by the hyphoteses). Using first (3.32) and after (3.34) with $d = b$, we can conclude directly the proof. □ The following Theorem that I called of "modulus change", summarize one interesting property of $\mathcal{I}_b(\cdot)$, the which plays a role in this Section.

Theorem 3.18 (Modulus change). *Let b be in $\mathbf{N}^{\triangleright}$. Then, for any $a \in \mathbf{N}^{\triangleright}$, with $\gcd(a, b) = 1$ we get*

$$\mathcal{I}_b(a) = C_a \left\{ 1 + \phi_a(b) \times \mathcal{L}_a(b) \right\} + C_a(b) \times \mathcal{L}_a(b). \tag{3.36}$$

Proof. With the aid of the Theorem 3.3, we obtain

$$a \times \mathcal{I}_b(a) = 1 + b \times \mathcal{L}_a(b).$$

Note that using the properties (ϕ_4), (ϕ_5) and ($e1$) of Theorem 2.1 we get:

$$\begin{aligned} a \times \mathcal{I}_b(a) &= 1 + b \times \mathcal{L}_a(b) - \underbrace{\phi_a\left\{1 + b \times (a-1) \times \mathcal{I}_a(b)\right\}}_{0} \\ &= 1 + b \times \mathcal{L}_a(b) - \phi_a\left\{1 + \phi_a(b) \times \phi_a((a-1) \times \mathcal{I}_a(b))\right\} \\ &= 1 + b \times \mathcal{L}_a(b) - \phi_a\left\{1 + \phi_a(b) \times \mathcal{L}_a(b)\right\} \\ &= 1 + b \times \mathcal{L}_a(b) - \left\{1 + \phi_a(b) \times \mathcal{L}_a(b) - a \times C_a(1 + \phi_a(b) \times \mathcal{L}_a(b))\right\} \\ &= (b - \phi_a(b)) \times \mathcal{L}_a(b) + a \times C_a(1 + \phi_a(b) \times \mathcal{L}_a(b)) \\ &= a \times C_a(b) \times \mathcal{L}_a(b) + a \times C_a(1 + \phi_a(b) \times \mathcal{L}_a(b)). \end{aligned}$$

This conclude the proof. □ Theorem 3.18 have some consequences which we now state.

Corollary 3.19. *If $\mu \in \mathbf{N}$ and $b \in \mathbf{N}^{\triangleright}$, then for all $a \in \mathbf{N}^{\triangleright}$, with $\gcd(a,b) = 1$ and $b - \mu \times a > 1$, we have*

$$\mathcal{I}_{b-\mu\times a}(a) = \mathcal{I}_b(a) - \mu \times \mathcal{L}_a(b). \tag{3.37}$$

Proof. First let us notice that $1 = \gcd(a,b) = \gcd(a, b - \mu \times a)$ for all $\mu \in \mathbf{N}$. So, the operator $\mathcal{I}_{b-\mu\times a}(a)$ is well defined. Now, the Theorem 3.18 implies that

$$\begin{aligned} \mathcal{I}_{b-\mu\times a}(a) &= C_a\left\{1 + \phi_a(b - \mu \times a) \times \mathcal{L}_a(b - \mu \times a)\right\} \\ &+ C_a(b - \mu \times a) \times \mathcal{L}_a(b - \mu \times a). \end{aligned} \tag{3.38}$$

Thus, in order to prove (3.37) it is sufficient to prove that

$$C_a(b) = C_a(b - \mu \times a) + \mu, \tag{3.39}$$

$$\phi_a(b) = \phi_a(b - \mu \times a) \tag{3.40}$$

and

$$\mathcal{L}_a(b) = \mathcal{L}_a(b - \mu \times a). \tag{3.41}$$

In fact, by the properties $(c5)$, $(c4)$, $(c2)$ and $(\phi 2)$ of Theorem 2.1 we get:

$$\begin{aligned} C_a(b) &= C_a(b-\mu\times a+\mu\times a) \\ &= C_a(b-\mu\times a)+C_a(\mu\times a)+C_a(\phi_a(b-\mu\times a)+\phi_a(\mu\times a)) \\ &= C_a(b-\mu\times a)+\mu+C_a(\phi_a(b-\mu\times a)) \\ &= C_a(b-\mu\times a)+\mu. \end{aligned}$$

Note also that, by the properties $(\phi 4)$, $(\phi 2)$ and $(\phi 3)$ of Theorem 2.1, we get

$$\begin{aligned} \phi_a(b) &= \phi_a(b-\mu\times a+\mu\times a) \\ &= \phi_a(\phi(b-\mu\times a)+\phi_a(\mu\times a)) \\ &= \phi_a(b-\mu\times a) \end{aligned}$$

and hence,

$$\mathcal{L}_a(b)=\mathcal{L}_a(\phi_a(b))=\mathcal{L}_a(\phi_a(b-\mu\times a))=\mathcal{L}_a(b-\mu\times a).$$

So, combining (3.39), (3.40) and (3.41) togheter with (3.38) we finally obtain (3.37). □

Corollary 3.20. *If b and μ are positive integers, then for all $a\in\mathbf{N}^{\triangleright}$, with* $\gcd(a,b)=1$, *we have*

$$\mathcal{I}_{b+\mu\times a}(a)=\mathcal{I}_b(a)+\mu\times\mathcal{L}_a(b). \tag{3.42}$$

Proof. First let us notice that $1=gcd(a,b)=gcd(a,b+\mu\times a)$ for all $\mu\in\mathbf{N}$. So, the operator $I_{b+\mu\times a}(a)$ is well defined. From Theorem 3.18 and the propeties $(\phi 4)$, $(c7)$ of Theorem 2.1 togheter with (3.5) we obtain (3.42). □

Remark 3.21. *Formulae (3.37) and (3.42) are similar to those obtained in ([19], Corollary 4.2), via the reciprocity formula for (MMI). However, in this respect our approach is methodologically of a different kind.*

Corollary 3.22. *If b and q are positive integers such that $b>2$ and $q\geq 1$, then*

$$\mathcal{I}_{b\times q-1}(b)=q. \tag{3.43}$$

Proof. By Corollary 3.20, we get

$$\begin{aligned}
\mathcal{I}_{b\times q-1}(b) &= \mathcal{I}_{(b-1)+(q-1)\times b}(b) \\
&= \mathcal{I}_{(b-1)}(b) + (q-1)\times \mathcal{L}_b(b-1) \\
&= \mathcal{I}_{(b-1)}[\phi_{b-1}(b)] + (q-1)\times 1 \\
&= \mathcal{I}_{(b-1)}(1) + (q-1) \\
&= 1 + (q-1) = q.
\end{aligned}$$

We conclude that the corollary is valid. □

Corollary 3.23. *If $b \in \mathbf{N}^{\triangleright}$, then for all $a \in \mathbf{N}^{\triangleright}$, with $\gcd(a,b) = 1$ and $b-a > 1$, we have*

$$\mathcal{I}_b(a) = \mathcal{I}_{b-a}(a) + \mathcal{L}_a(b). \tag{3.44}$$

Proof. First let us notice that the operator $\mathcal{I}_{b-a}(a)$ is well defined, from Corollary 3.19 with $\mu = 1$ follow the statment. □

Corollary 3.24. *If $b \in \mathbf{N}^{\triangleright}$, then for all $a \in \mathbf{N}^{\triangleright}$, with $\gcd(a,b) = 1$, we have*

$$\mathcal{I}_{b+a}(a) = \mathcal{I}_b(a) + \mathcal{L}_a(b). \tag{3.45}$$

Proof. One can observe that in this case the operator $I_{b+a}(a)$ is well defined. From Corollary 3.20 with $\mu = 1$ follow the statment. □

Now, as a consequence of the Corollary 3.23, Corollary 3.24 and Corollary 3.20, one easily gets

Corollary 3.25. *If $b \in \mathbf{N}^{\triangleright}$, then for all $a \in \mathbf{N}^{\triangleright}$, with $\gcd(a,b) = 1$ and $b-a > 1$, we have*

$$\mathcal{I}_{b+a}(a) = 2\times \mathcal{I}_b(a) - \mathcal{I}_{b-a}(a) \tag{3.46}$$

and

$$\mathcal{I}_{b+a}(a) = 2\times \mathcal{L}_a(b) + \mathcal{I}_{b-a}(a) \tag{3.47}$$

are valid.

We can now conbine the Theorem 3.10 with the identity (3.47) of Corollary 3.25 to conclude:

Theorem 3.26. *If* b, $d \in \mathbf{N}^{\triangleright}$ *are such that* $b > d + 3$, *then for every* $a \in (\, d+1, b-1\,) \cap \mathbf{N}^{\triangleright}$, *with* $\gcd(a,b) = 1$ *and* $\gcd(a,d) = 1$, *we have*

$$\mathcal{I}_{b\times d}(a) = \mathcal{I}_b(a) + b \times \phi_d \left\{ \frac{1}{4} \times [\mathcal{I}_{b+a}(a) - \mathcal{I}_{b-a}(a)] \times [\mathcal{I}_{a+d}(d) - \mathcal{I}_{a-d}(d)] \right\}. \tag{3.48}$$

We can now also conbine the Theorem 3.10 with the identity (3.44) of Corollary 3.23 to conclude:

Theorem 3.27. *If* b, $d \in \mathbf{N}^{\triangleright}$ *are such that* $b > d + 3$, *then for every* $a \in (\, d+1, b-1\,) \cap \mathbf{N}^{\triangleright}$, *with* $\gcd(a,b) = 1$ *and* $\gcd(a,d) = 1$, *we have*

$$\mathcal{I}_{b\times d}(a) = \mathcal{I}_b(a) + b \times \phi_d \left\{ [\mathcal{I}_b(a) - \mathcal{I}_{b-a}(a)] \times [\mathcal{I}_a(d) - \mathcal{I}_{a-d}(d)] \right\}. \tag{3.49}$$

Now it is important to observe that the Corollary 3.19 and Corollary 3.20 can be formulated in the following equivalent way.

Corollary 3.28. *If* $\mu \in \mathbf{N}$ *and* $b \in \mathbf{N}^{\triangleright}$, *then for all* $a \in (\mathbf{Z}/b\mathbf{Z})^*$, *with* $b - \mu \times a > 1$, *we have*

$$\mathcal{I}_{b-\mu\times a}(a) = (1-\mu) \times \mathcal{I}_b(a) + \mu \times \mathcal{I}_{b-a}(a), \tag{3.50}$$

Corollary 3.29. *If* $\mu \in \mathbf{N}$ *and* $b \in \mathbf{N}^{\triangleright}$, *then for all* $a \in (\mathbf{Z}/b\mathbf{Z})^*$, *we have*

$$\mathcal{I}_{b+\mu\times a}(a) = (1-\mu) \times \mathcal{I}_b(a) + \mu \times \mathcal{I}_{b+a}(a) \tag{3.51}$$

and

Corollary 3.30. *If* $\mu \in \mathbf{N}$ *and* $b \in \mathbf{N}^{\triangleright}$, *then for all* $a \in (\mathbf{Z}/b\mathbf{Z})^*$, *with* $b - \mu \times a > 1$, *we have*

$$\mathcal{I}_{b+\mu\times a}(a) = (1+\mu) \times \mathcal{I}_b(a) - \mu \times \mathcal{I}_{b-a}(a). \tag{3.52}$$

Proof. The three Corollaries given above, are a consequence direct of the Corollary 3.19, Corollary 3.20, Corollary 3.23 and Corollary 3.24, respectively. □

On the other hand, Corollaries (3.29) and (3.30) both combined, yields to

Corollary 3.31. *If $\mu \in \mathbf{N}$ and $b \in \mathbf{N}^{\triangleright}$, then for all $a \in (\mathbf{Z}/b\mathbf{Z})^{*}$, with $b - a > 1$, we have*

$$\mathcal{I}_{b+\mu\times a}(a) = \mathcal{I}_b(a) + \frac{\mu}{2} \times \left(\mathcal{I}_{b+a}(a) - \mathcal{I}_{b-a}(a)\right). \tag{3.53}$$

Finally, if we now conbine the Theorem 3.10 with the identity (3.45) of Corollary 3.24 we have the following statment:

Theorem 3.32. *If $b, d \in \mathbf{N}^{\triangleright}$, then for every $a \in \mathbf{N}^{\triangleright}$, with* $\gcd(a, b) = 1$ *and* $\gcd(a, d) = 1$, *we have*

$$\mathcal{I}_{b\times d}(a) = \mathcal{I}_b(a) + b \times \phi_d \left\{[\mathcal{I}_{b+a}(a) - \mathcal{I}_b(a)] \times [\mathcal{I}_{d+a}(d) - \mathcal{I}_a(d)]\right\}. \tag{3.54}$$

Remark 3.33. *Note that, once established the expression (3.54), we could prove under the hypotheses of Theorem 3.32 the validity of*

$$\mathcal{I}_{b\times d}(a) = \mathcal{I}_d(a) + d \times \phi_b \left\{[\mathcal{I}_{d+a}(a) - \mathcal{I}_d(a)] \times [\mathcal{I}_{b+a}(b) - \mathcal{I}_a(b)]\right\}. \tag{3.55}$$

Remark 3.34. *All our results, with suitable assumptions, can be generalized to group of units, like*

$$(\mathbf{Z}/\varrho\mathbf{Z})^{*}, \text{ with } \varrho = \prod_{l=1}^{n} d_l;\ d_l \in \mathbf{N}^{\triangleright}.$$

Theorem 3.15 is complemented by a nice identity for the (MMIO) $\mathcal{I}_{p^m}(\cdot)$. This is summarized in the following theorem.

Theorem 3.35. *Let $a \in (\mathbf{Z}/p\mathbf{Z})^{*}$, with $p > 1$ a prime number. Then for all $m \in \mathbf{N}$, we have*

$$\mathcal{I}_{p^m}(a) = a_0 + a_1 \times p + a_2 \times p^2 + a_3 \times p^3 + \ldots + a_{m-1} \times p^{m-1}, \tag{3.56}$$

where

$$\begin{array}{rcl}
a_0 & = & \mathcal{I}_p(a), \\
a_1 & = & \phi_p\left\{\mathcal{I}_p(a) \times \mathcal{I}_a(p) - 1\right\}, \\
a_2 & = & \phi_p\left\{\mathcal{I}_p(a) \times \phi_a\left({\mathcal{I}_a}^2(p)\right) - 1\right\}, \\
a_3 & = & \phi_p\left\{\mathcal{I}_p(a) \times \phi_a\left({\mathcal{I}_a}^3(p)\right) - 1\right\}, \\
\vdots & & \vdots \\
a_{m-1} & = & \phi_p\left\{\mathcal{I}_p(a) \times \phi_a\left({\mathcal{I}_a}^{m-1}(p)\right) - 1\right\}.
\end{array}$$

Here,

$${\mathcal{I}_a}^n(p) = \underbrace{\mathcal{I}_a(p) \times \mathcal{I}_a(p) \times \cdots \times \mathcal{I}_a(p)}_{n-times}.$$

Proof. This result can be shown using the Theorem 3.15 with $b = d = p$ and by using the property $(I1)$ of Theorem 3.4. □

Remark 3.36. *In addition, we see that if $p = 2$ and $a \in \mathbf{N}^{\triangleright}$ is an odd number. Then for all $m \in \mathbf{N}$, we have*

$$(3.57)\mathcal{I}_{2^m}(a) = a_0 + a_1 \times 2 + a_2 \times 2^2 + a_3 \times 2^3 + \ldots + a_{m-1} \times 2^{m-1},$$

where, now

$$\begin{array}{rcl}
a_0 & = & 1, \\
a_1 & = & \phi_2\left\{\mathcal{I}_a(2) - 1\right\}, \\
a_2 & = & \phi_2\left\{\phi_a\left({\mathcal{I}_a}^2(2)\right) - 1\right\}, \\
a_3 & = & \phi_2\left\{\phi_a\left({\mathcal{I}_a}^3(2)\right) - 1\right\}, \\
\vdots & & \vdots \\
a_{m-1} & = & \phi_2\left\{\phi_a\left({\mathcal{I}_a}^{m-1}(2)\right) - 1\right\}.
\end{array}$$

Here,

$${\mathcal{I}_a}^n(2) = \underbrace{\mathcal{I}_a(2) \times \mathcal{I}_a(2) \times \cdots \times \mathcal{I}_a(2)}_{n-times}.$$

Notice also that

$$\mathcal{I}_a(2) = \frac{1+a}{2}.$$

4. Numerical experiments

The Chinese Remainder Theorem (CRT), is actually one of the main theorems of number theory [10]. Over the year, has been playing a prominent role due to its applicability in other fields of science, engineering and engineering genetic; see, for example [28] for Photo Radar, [10, 29] for Cryptography and Theory of Code, [32] for Circuits on Systems, [14] for Matrix Theory, [5, 7] for Acoustic Diffusers and [13] for DNA Sequencing. For illustrative purposes, here we given some numerical examples. The discussion is limited only to Chinese remainder theorem in the spirit of [5]. For the sake of completeness we outline it, emphasizing some specific facts.

Theorem 4.1 (Algorithmic Functional-CRT). *Let b_1 and b_2 relatively prime in $\mathbf{N}$, with b_1, $b_2 \geq 2$ and $\varrho = b_1 \times b_2$. Let γ and β be two arbitaries numbers such that $\gamma \in \mathbf{Z}/b_1\mathbf{Z}$ and $\beta \in \mathbf{Z}/b_2\mathbf{Z}$, respectively. Then we can find in the set $\mathbf{Z}/\varrho\mathbf{Z}$ one unique element a that sastifies the system:*

$$\left\{\begin{aligned} &\phi_{b_1}(a) = \gamma, \\ &\phi_{b_2}(a) = \beta. \end{aligned}\right. \tag{4.1}$$

An explicit version of the solution of (4.1), in the case $b_2 > b_1$ have the form (for more detaild, see [5]):

$$a = \beta + b_2 \times \phi_{b_1} \left\{ \mathcal{I}_{b_1} \left(\phi_{b_1}(b_2) \right) \times \left[\gamma + \beta \times (b_1 - 1) \right] \right\}. \tag{4.2}$$

To ilustrate some of our results, we analyze the numerical form of the solution of following system:

$$\left\{\begin{aligned} &\phi_{45}(a) = 31, \\ &\phi_{52}(a) = 47. \end{aligned}\right. \tag{4.3}$$

For tested it, we first recall that all the conditions of Theorem 4.1, can be verified. Now, $\min\{45, 52\} = 45$. As we have already mentioned, the expression (4.2) yeld to:

$$a = 47 + 52 \times \phi_{45} \left\{ \mathcal{I}_{45} \left(\phi_{45}(52) \right) \times \left[31 + 47 \times (45 - 1) \right] \right\}.$$

As, $\phi_{45}(52) = 7$, we get $a = 47 + 52 \times \phi_{45} \left\{ \mathcal{I}_{45}(7) \times [31 + 47 \times 44] \right\}$. In order to recover the solution a of (4.3) and to facilitate the computation of the (MMIO) $\mathcal{I}_{45}(7)$, one may works as follows:

First, computation of $\mathcal{I}_{45}(7)$ using, for instance, the formula (3.48). In fact, if $b \times d = 45$, selecting, e.g., $b = 9$ and $d = 5$, therefore $b > d + 3$. So one finds that $a = 7 \in (d+1, b-1) \cap \mathbf{N} = (6, 8) \cap \mathbf{N}$, with $\gcd(7, 9) = 1$ and $\gcd(7, 5) = 1$. So, the Theorem 3.26 is applicable. Hence one has that

$$\begin{aligned}
\mathcal{I}_{45}(7) &= \mathcal{I}_9(7) + 9 \times \phi_5 \left\{ \frac{1}{4} \left[\mathcal{I}_{16}(7) - \mathcal{I}_2(7) \right] \times \left[\mathcal{I}_{12}(5) - \mathcal{I}_2(5) \right] \right\} \\
&= \mathcal{I}_9(7) + 9 \times \phi_5 \left\{ \frac{1}{4} \left[\mathcal{I}_{16}(7) - \mathcal{I}_2(1) \right] \times \left[\mathcal{I}_{12}(5) - \mathcal{I}_2(1) \right] \right\} \\
&= \mathcal{I}_9(7) + 9 \times \phi_5 \left\{ \frac{1}{4} \left[\mathcal{I}_{16}(7) - 1 \right] \times \left[\mathcal{I}_{12}(5) - 1 \right] \right\}.
\end{aligned}$$

For the computing of $\mathcal{I}_9(7)$, we use, for instance, the Corollary 3.24, identity (3.45). In fact:

$$\mathcal{I}_9(7) = \mathcal{I}_{2+7}(7) = \mathcal{I}_2(7) + \mathcal{L}_7(2) = 1 + \phi_7[6 \times \mathcal{I}_7(2)] = 1 + \phi_7[6 \times 4] = 4.$$

Now, for the computing of $\mathcal{I}_{16}(7)$ and $\mathcal{I}_{12}(5)$, we use, for instance, the Corollary 3.20, identity (3.42). In fact:

$$\mathcal{I}_{16}(7) = \mathcal{I}_{2+2\times 7}(7) = \mathcal{I}_2(7) + 2 \times \mathcal{L}_7(2) = 1 + 2 \times 3 = 7$$

and

$$\begin{aligned}
\mathcal{I}_{12}(5) &= \mathcal{I}_{2+2\times 5}(5) = \mathcal{I}_2(5) + 2 \times \mathcal{L}_5(2) \\
&= 1 + 2 \times \phi_5[4 \times \mathcal{I}_5(2)] = 1 + 2 \times \phi_5[4 \times 3] = 5,
\end{aligned}$$

$$\begin{aligned}
\mathcal{I}_{45}(7) &= \mathcal{I}_9(7) + 9 \times \phi_5 \left\{ \frac{1}{4} \left[\mathcal{I}_{16}(7) - 1 \right] \times \left[\mathcal{I}_{12}(5) - 1 \right] \right\} \\
&= 4 + 9 \times \phi_5 \left\{ \frac{1}{4} [7 - 1] \times [5 - 1] \right\} = 4 + 9 \times \phi_5 \left\{ \frac{1}{4} \times 6 \times 4 \right\} \\
&= 4 + 9 \times \phi_5(6) = 4 + 9 \times 1 = 13.
\end{aligned}$$

Consequently, the solution of (4.3) reduces to:

$$a = 47 + 52 \times \phi_{45} \left\{ 13 \times [31 + 47 \times 44] \right\}. \tag{4.4}$$

Now by the properties ($\phi 5$), ($\phi 4$) and ($\phi 2$) of Theorem 2.1, we get

$$\begin{aligned} \phi_{45}\left\{13 \times [31 + 47 \times 44]\right\} &= \phi_{45}\left\{13 \times [31 + 2 \times 44]\right\} \\ &= \phi_{45}\left\{13 \times 74\right\} = \phi_{45}\left\{13 \times 29\right\}. \end{aligned} \tag{4.5}$$

Now, Theorem 2.3, the properties ($\phi 5$) and ($c4$) of Theorem 2.1 yields to

$$\begin{aligned} \phi_{45}\left\{13 \times 29\right\} &= \phi_5(13 \times 29) + 5 \times \phi_9(C_5(13 \times 29)) \\ &= \phi_5(\phi_5(13) \times \phi_5(29)) + 5 \times \phi_9(C_5(13 \times 29)) = \phi_5(3 \times 4) \\ &+ 5 \times \phi_9\left[C_5(13) \times 29 + \phi_5(13) \times C_5(29) + C_5(\phi_5(13) \times \phi_5(29))\right] \\ &= \phi_5(12) + 5 \times \phi_9\left[2 \times 29 + 3 \times 5 + C_5(3 \times 4)\right] \\ &= 2 + 5 \times \phi_9\left[2 \times 2 + 3 \times 5 + 2\right] = 17. \end{aligned}$$

It then follows from (4.5) and (4.4) that $a = 931$ and $a < 2340$, like we should expect.

Remark 4.2. *Alternatively, if we apply Eq. (3.32) of Theorem 3.15 twice, we obtain the same value for the (MMIO) $\mathcal{I}_{45}(7)$. In fact,*

$$\begin{aligned} \mathcal{I}_{45}(7) &= \mathcal{I}_{9\times 5}(7) = \mathcal{I}_9(7) + 9 \times \phi_5\left\{\mathcal{I}_5(7) \times \mathcal{I}_7(9) - 1\right\} \\ &= \mathcal{I}_9(7) + 9 \times \phi_5\left\{\mathcal{I}_5(2) \times \mathcal{I}_7(2) - 1\right\} \\ &= \mathcal{I}_9(7) + 9 \times \phi_5\left\{3 \times 4 - 1\right\} \\ &= \mathcal{I}_3(7) + 3 \times \phi_3\left\{\mathcal{I}_3(7) \times \mathcal{I}_7(3) - 1\right\} + 9 \times \phi_5\left\{11\right\} \\ &= \mathcal{I}_3(1) + 3 \times \phi_3\left\{\mathcal{I}_3(1) \times \mathcal{I}_7(3) - 1\right\} + 9 \times \phi_5\left\{1\right\} \\ &= 1 + 3 \times \phi_3\left\{1 \times 5 - 1\right\} + 9 \times 1 = 13. \end{aligned}$$

Also, as $\phi_7(15) = 1$, we could use the Corollary 3.17, formula (3.35). In fact,

$$\begin{aligned} \mathcal{I}_{45}(7) &= \mathcal{I}_{15\times 3}(7) = \frac{1}{7} \times (1 - 15) + 15 \times \mathcal{I}_3(7) \\ &= -\frac{1}{7} \times 14 + 15 \times \mathcal{I}_3(1) = 13. \end{aligned}$$

Acknowledgments

I am especially indebted to professor Dr. Alvaro Restuccia, academic of Department of Physics of the Antofagasta University by their support, via fondecyt Grant #1161192, Chile. The referee made valuable comments, for which the present author is grateful. The current paper is a revised and expanded version of the original submission. I also want to thank to Professor Javier Silva Rojas for his invaluable help.

References

[1] H. M. AL-Matari, S. J. Aboud, N. F. Shilbayeh, Fast Fraction-Integer Method for Computing Multiplicative Inverse, *J. of Computing*, **1**, pp. 131–135, (2009).

[2] O. Arazi, H. Qi, On calculiting multiplicative inverses modulo 2^m, *IEEE Trans. Comput* **57**, pp. 1435–1438, (2008).

[3] J–C. Bajard, L. Imbert, A full RNS implementation of RSA, *IEEE Trans. Comput* **53**, pp. 769–774, (2004).

[4] J. W. Bos, Constant time modular inversion, *J Cryptogr Eng* **4**, pp. 275–281, (2014).

[5] L. A. Cortés–Vega, A functional technique based on the Euclidean algorithm with applications to 2-D acoustic diffractal diffusers, *J. Phys.: Conf. Ser* **633**, pp. 1–6, (2015).

[6] L. A. Cortés Vega, D. E. Rojas-Castro, Y.S. Santiago Ayala and S. C. RojasRomero, A technique based on the Euclidean algorithm and its applications to Cryptography and Nonlinear Diophantine Equations, Proyecciones. J. Math., **26**, pp. 309-333, (2007).

[7] T. J. Cox, P. D'Antonio, *Acoustic Absorbers and Diffusers: Theory, Design and Application* Spon Press, (2004).

[8] Y. Dai, A. B. Borisov, K. Boyer, C. K. Rhodes, Computation with inverse states in a Finite Field F_{P_α}: The muon neutrino mass, the Unified-Strong-Electroweak coupling constant, and the Higgs mass, *Sandia National Laboratory, Report SAND2000-2043*, pp. 1–11, (2000).

[9] Y. Dai, A.B. Borisov, K. Boyer, C.K. Rhodes, A p-Adic metric for particle mass scale organization with genetic divisors, *Sandia National Laboratory, Report SAND2001-2903*, pp. 1–12, (2001).

[10] C. Ding, D. Pey, A. Salomaa, *Chinese remainder Theorem: Applications in Computing, Coding, Cryptography*, Singapure; World Scientific, (1999).

[11] J-G. Dumas, On Newton-Rapshon iteration for multiplicative inverses modulo prime power, *IEEE Trans. Comput* **63**, pp. 2106–2109, (2014).

[12] J. Eichenauer, J. Lehn, A. Topuzoglu, A Nonlinear congruential pseudorandom numer generator with power two modulus, *Math of Compt* **51**, pp. 757–759, (1988).

[13] Y. Elrich, K. Chang, A. Gordon, R. Ronen, O. Navon, M. Rooks, G.J. Hanon, DNA Sudoku-harnessing high-throughput sequencing for multiplexed specimen analysis, *Genome Res* **19**, pp. 1243–1253, (2009).

[14] M. A. Fiol, Finite Abelian groups and the Chinese remainder theorem, *Discrete Math* **67**, pp. 101–105, (1987).

[15] L. Hars, Modular inverse algorithms without multiplications for cryptographic applications, *J Embedded Systems* **032192**, pp. 1–13, (2006).

[16] M. Joye and P. Paillier, *GCD-Free algorithms for computing modular inverses*, C.D. Walter et. al. (Eds.):CHES 2003, LNCS 2779. Springer-Verlag Berlin Heidelberg, pp. 243-253, (2003).

[17] B. S. Jr. Kaliski, The montgomery inverse and its applications, *IEEE Trans. Comput* **44**, pp. 1064–1065 (1995).

[18] D. E. Knuth, *The art of computer programming*, 2, Semi-Numerical Algorithms, 3rd Edition, Addison-Wesley, Reading, MA, (1997).

[19] W. H. Ko, Modular inverse and reciprocity formula, *arXiv:1304.6778v1*, pp. 1-7, (2013).

[20] R. Lórencz, New algorithm for classical modular inverse, in Kaliski, B.S., Jr., Koç, C.K., and Paar, C. (Eds.):CHES 2002, LNCS Springer-Verlag Berlin, pp. 57–70, (2003).

[21] D. R. Hankerson, A. J. Menezes, S. A. Vanstone, *Guide to Elliptic curve cryptography*, Springer, New York, N.Y, USA (2004).

[22] L. P. Montgomery, Modular multiplication without trial division, *Math. Comp* **44**, pp. 519–52, (1985).

[23] T. Niven, S. H. Zuckerman, H. Montgomery, *An introduction to the theory of numbers*, 5nd ed. Jhon Wiley-Sons, Inc. (1991).

[24] S. Parthasarathy, An interesting property of multiplicative inverse in mod(M), Algologic Tech. Reports, pp. 1–3, (2012).

[25] E. Savaş, C. K. Koç, The montgomery modular inverse revisited, *IEEE Trans. Comput* **49**, pp. 763–766, (2000).

[26] E. Savaş, M. Nasser, A. A-A Gutub, C. K. Koç, Efficient unified Montgomory inversion with multibit shifting, *IEEE Proc. Comput. Digit. Tech* **152**, pp. 489–498, (2005).

[27] M. R. Schroeder, *Number theory and in Science and comunication*, 3rd ed. Springer, Berlin, (1997).

[28] R. J. Sullivan, *Microwave Radar Imaging and Advanced Concepts*, 2nd ed. Scitech Pub Inc., (2004).

[29] C. E. Towers, D. P. Towers, J. D. C. Jones, Time efficient Chinese remainder theorem algorithm for full-field fringe phase analysis in multi-wavelenght interferometry, Optics Express **12**, pp. 1136–1143, (2004).

[30] S. B. Verkhovsky, Enhanced Euclid algorithm for modular multiplicative inverse and its application in Cryptographic protocols, *Int. J. Commun. Network and System Sc* **3**, pp. 901–906, (2010).

[31] S. Vollala, B.S. Degum, N. Ramasubramanian, Hardware desing for multiplicative modular inverse based on table look up technique, *IEEE Computing and Network Commun* (CoCoNet), pp. 520–523, (2015).

[32] Y. Wang, Residue to binary converters based on net Chinese remainder theorems, IEEE Trans Circuits Syst. **47**, pp. 197–204, (2000).

[33] S. Wei, Computation of modular multiplicative inverse using residue signed-digit additions, *IEEE Conf. Pub :2016 International SoC Design Conference (ISOCC)*, pp. 85–86, (2016).

Luis A. Cortés–Vega
Department of Mathematics,
Antofagasta University,
Antofagasta,
Chile
e-mail : luis.cortes@uantof.cl