A refined version of the inverse decomposition theorem for modular multiplicative inverse operators

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

Abstract. Recently, we started in the IOP Conference Series [1, 2] and in [3] the study of modular multiplicative inverse operators in an algorithmic functional context on \((\mathbb{Z}/\varrho\mathbb{Z})^*\) with \(\varrho > 3\), where it is possible to distinguish different formulas that break up these operators over \((\mathbb{Z}/\varrho\mathbb{Z})^*\), all this thanks to the so-called "inverse decomposition theorem (IDT)". In this paper, we will study these issues a little deeper. Though we mainly focus the paper on derived for these operators a refined version of the (IDT), also appear on the scene some additional contributions. Finally, in a brief overview, we compare the differences that exist among the new result here established and the old ones. However, along with this, there are still plenty of questions to be answered in this research field.

1. Introduction

Throughout the paper, unless otherwise specified, \(\mathbb{N}\) denote the set of the natural numbers, \(\mathbb{N}^> = \mathbb{N} \setminus \{1\}\), \(\mathbb{N}^0 = \mathbb{N} \cup \{0\}\). \(\mathbb{Z} =: (\mathbb{Z}, +, \times)\) denotes the ring of integers, where the operations + and \(\times\) on \(\mathbb{Z}\) are the sum and the product of integer numbers. 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 \(a - d\). Also, \(\mathbb{Z}/b\mathbb{Z}\) denote the ring of residue classes modulo \(b\), \(a \in \mathbb{Z}/b\mathbb{Z}\) if \(a \in \{0, 1, 2, \ldots, b - 1\}\). Similarly, \((\mathbb{Z}/b\mathbb{Z})^* = \{a \in \mathbb{Z}/b\mathbb{Z} : \gcd(a, b) = 1\}\) denotes the group of unit of \(\mathbb{Z}/b\mathbb{Z}\). Let us emphasize that, the modular multiplicative inverse (MMI) of \(a \in \mathbb{Z}/b\mathbb{Z}\), if it exists, is \(a^{-1} \in \mathbb{Z}/b\mathbb{Z}\), such that \(a \times a^{-1} \equiv 1 \mod b\).

The notion of modular multiplicative inverse operator (MMIO):

\[ \mathcal{S}_\varrho : (\mathbb{Z}/\varrho\mathbb{Z})^* \rightarrow \mathbb{Z}/\varrho\mathbb{Z}, \mathcal{S}_\varrho(a) = a^{-1}, \varrho > 3 \]

it was introduced and studied by the author in [2, 3]. As a result, a number of decomposition law for the (MMI) were obtained thanks to the so-called “inverse decomposition theorem”. This theorem asserts that:

**Theorem 1.1** Let \(b, d\) be in \(\mathbb{N}^>\). Then, for any \(a \in \mathbb{N}^>\), with \(\gcd(a, b) = 1\) and \(\gcd(a, d) = 1\), we get

\[ \mathcal{S}_{b \times d}(a) = \mathcal{S}_b(a) + b \times \phi_d \{\mathcal{L}_d(a) \times \mathcal{L}_a(b)\}, \]  

where, the operators \(\mathcal{L}_\beta(\cdot)\) have the following structure:

\[ \gamma \in (\mathbb{Z}/\beta\mathbb{Z})^* \rightarrow \mathcal{L}_\beta(\gamma) \in \mathbb{Z}/\beta\mathbb{Z}, \text{ with } \mathcal{L}_\beta(\gamma) = \phi_\beta [\beta - 1 \times \mathcal{S}_\beta(\gamma)] \]
and the operators \( \phi_b : \mathbb{N}^0 \to \mathbb{Z}/b\mathbb{Z} \) are defined in general by:

\[
\phi_b(a) = \begin{cases} 
a, & \text{if } 0 \leq a \leq b - 1, \\
r, & \text{if } a \geq b,
\end{cases}
\]

where \( a \equiv r \mod \beta \), for any \( \beta \in \mathbb{N}^0 \).

We will return to Theorem 1.1 later in the paper.

In this note, we derived a refined version of the Theorem 1.1. In this framework, under a new condition, the novel result here presented is sharper. Finally, we compare the similarities and differences that exist among our previous results and the new here presented.

2. Preliminaries

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. In a general context, the Bézout’s theorem states that: if \( a \) and \( b \) are positive integers, then there exist integers \( s \) and \( t \) such that \( \gcd(a, b) = s \cdot a + t \cdot b \). In order to be more precise we need to recall in this part of the article some auxiliary results taken from \([1, 2]\). Towards this goal, and for future practical computations it is convenient to introduce first the operators \( \phi_b : \mathbb{N}^0 \to \mathbb{Z}/b\mathbb{Z} \) and \( \mathcal{C}_b : \mathbb{N}^0 \to \mathbb{N}^0 \), defined by:

\[
\phi_b(a) = \begin{cases} 
a, & \text{if } 0 \leq a \leq b - 1, \\
r, & \text{if } a \geq b,
\end{cases}
\]

where \( a \equiv r \mod b \) for any \( b \in \mathbb{N}^0 \). Using this notation one may to note the naturality of the following statement.

**Theorem 2.1** Let \( b \in \mathbb{N}^0 \). Then the following mathematical expressions:

(\( \phi_1 \)) \( \phi_b(0) = 0, \)
(\( \phi_2 \)) \( \phi_b(d \times b) = 0 \) for every \( d \in \mathbb{N}^0, \)
(\( \phi_3 \)) \( \phi_b(a) = \phi_b(\phi_b(a)) \) for every \( a \in \mathbb{N}^0, \)
(\( \phi_4 \)) \( \phi_b(a + d) = \phi_b(\phi_b(a) + \phi_b(d)) = \phi_b(\phi_b(a) + d) \) for every \( a, d \in \mathbb{N}^0, \)
(\( \phi_5 \)) \( \phi_b(a \times d) = \phi_b(\phi_b(a) \times \phi_b(d)) = \phi_b(a \times \phi_b(d)) \) for every \( a, d \in \mathbb{N}^0, \)
(\( \phi_6 \)) \( \phi_b(a + b) = \phi_b(a) \) for every \( a \in \mathbb{N}^0 \) ("periodicity" of \( \phi_b \)),
(\( \phi_1 \)) \( \mathcal{C}_b(0) = 0, \)
(\( \phi_2 \)) \( \mathcal{C}_b(b \times a) = a \) for every \( a \in \mathbb{N}^0 \). In particular \( \mathcal{C}_b(b) = 1, \)
(\( \phi_3 \)) \( \mathcal{C}_b(\phi_b(a)) = 0 \) for every \( a \in \mathbb{N}^0 \) (\( \mathcal{C}_b \) is a "annihilator" of \( \phi_b \)),
(\( \phi_4 \)) \( \mathcal{C}_b(a + d) = \mathcal{C}_b(a) + \mathcal{C}_b(d) + \mathcal{C}_b(\phi_b(a) + \phi_b(d)) \) for every \( a, d \in \mathbb{N}^0, \)
(\( \phi_5 \)) \( \mathcal{C}_b(a \times d) = \mathcal{C}_b(a) \times d + \mathcal{C}_b(\phi_b(a) \times \phi_b(d)) \) for every \( a, d \in \mathbb{N}^0, \)
(\( \phi_6 \)) \( \mathcal{C}_b(a + b) = \mathcal{C}_b(a) + 1 \) for every \( a \in \mathbb{N}^0 \) (\( \mathcal{C}_b \) is quasi-periodic),
(\( \phi_7 \)) \( \mathcal{C}_b(a + b \times \mu) = \mathcal{C}_b(a) + \mu \) for every \( a, \mu \in \mathbb{N}^0, \)
(\( \phi_8 \)) \( a = \phi_b(a) + b \times \mathcal{C}_b(a) \) for every \( a \in \mathbb{N}^0, \)
(\( \phi_9 \)) \( a < b \) if and only if \( \mathcal{C}_b(a) = 0 \) for every \( a \in \mathbb{N}^0, \)
(\( \phi_{10} \)) \( (\mathcal{C}_b \circ \mathcal{C}_d)(a) = \mathcal{C}_b \times \mathcal{C}_d(a) \) for every \( a \in \mathbb{N}^0 \) and every \( d \in \mathbb{N}^0 \) are valid.
Remark 2.2 Let us remark that in the Theorem 2.1 the compositions of the operators 𝐸ₓ with 𝐸ₙ, 𝐸ₙ with 𝜙, 𝜙 with 𝜙, and 𝜙 with 𝐸ₙ, are defined by one usual way.

The Theorem 2.1 was first established by the author in [1], and will be a future reference for developing our work.

Now we need introducing as in [2, 3] the notion of modular multiplicative inverse operators (MMIO). To be precise,

Definition 2.3 If \( b \in \mathbb{N}^\ast \), then the modular multiplicative inverse operator (MMIO) denoted by \( \mathcal{I}_b(\cdot) \) is the mapping

\[
\mathcal{I}_b : (\mathbb{Z}/b\mathbb{Z})^\ast \to \mathbb{Z}/b\mathbb{Z}, \text{ defined by } \mathcal{I}_b(a) = a^{-1}, \text{ such that }
\phi_b(a \times \mathcal{I}_b(a)) = 1 \text{ for every } a \in (\mathbb{Z}/b\mathbb{Z})^\ast.
\]

Note that by the definition given, for any \( a \in (\mathbb{Z}/b\mathbb{Z})^\ast \) the (MMIO) always exist, and has the following additional property over \( \mathbb{N} \):

\[
\mathcal{I}_b(a) = \mathcal{I}_b(\phi_b(a)), \ a \in \mathbb{N} \text{ with } \gcd(a, b) = 1, \text{ and } \mathcal{I}_b(1) = 1.
\]

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

Definition 2.4 If \( b \in \mathbb{N}^\ast \), the operator \( \mathcal{L}_b \) given by:

\[
a \in (\mathbb{Z}/b\mathbb{Z})^\ast \to \mathcal{L}_b(a) \in \mathbb{Z}/b\mathbb{Z}, \text{ with } \mathcal{L}_b(a) = \phi_b[(b - 1) \times \mathcal{I}_b(a)]
\]

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

\[
\phi_b[a \times \mathcal{L}_b(a)] = b - 1 \text{ for any } a \in (\mathbb{Z}/b\mathbb{Z})^\ast.
\]

From this definition it is clear also that the predecessor operator \( \mathcal{L}_b(a) \) satisfies the following additional properties over \( \mathbb{N} \):

\[
\mathcal{L}_b(1) = b - 1 \text{ and } \mathcal{L}_b(a) = \mathcal{L}_b(\phi_b(a)) \text{ if } a \in \mathbb{N}, \text{ with } \gcd(a, b) = 1.
\]

The following theorem, recently proven in [3], is an immediate consequence of both the Bézout’s theorem and the Theorem 2.1 and will serve as a point of reference in the present paper.

Theorem 2.5 (A functional algorithmic connection of the Bézout’s coefficients) Let be \( m, n \in \mathbb{N}^\ast \) such that \( \gcd(m, n) = 1 \). Then

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

The operators \( \mathcal{I}_b(\cdot) \) and \( \mathcal{L}_b(\cdot) \) they have a number important of algebraic properties some of which will be shall use frequently.

Theorem 2.6 (Fundamental identities) For \( b, d \in \mathbb{N}^\ast \) such that \( \gcd(b, d) = 1 \), and every \( a \in \mathbb{N} \), with \( \gcd(a, b) = 1 \) we have

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

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

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

\[
\mathcal{L}_b(m + n) = \mathcal{L}_b(\phi_b(m) + \phi_b(n)),
\]
The Theorem 2.6 uses the properties of Theorem 2.1, the identities (2.1), (2.2), (2.4), (2.5) and the Theorem 2.5.

\[ \mathcal{J}_b(a + b) = \mathcal{J}_b(a), \text{ ("periodicity" of } \mathcal{J}_b) \]
\[ \mathcal{J}_b(\mathcal{L}_b(a)) = \phi_b(a), \]
\[ \mathcal{J}_b(a \times d) = \phi_b(\mathcal{J}_b(a) \times \mathcal{J}_b(d)), \]
\[ \mathcal{J}_b(m + n) = \mathcal{J}_b(\phi_b(m) + \phi_b(n)), \]
\[ \mathcal{J}_b(a + b) = \mathcal{J}_b(a), \text{ ("periodicity" of } \mathcal{J}_b) \]
\[ \mathcal{J}_b(\mathcal{J}_b(a)) = \phi_b(a), \]
\[ \mathcal{J}_b(a) + \mathcal{L}_b(a) = b. \]

**Proof.** The proof of Theorem 2.6 uses the properties of Theorem 2.1, the identities (2.1), (2.2), (2.4), (2.5) and the Theorem 2.5. ■

We will now state one of the most important theorems of this section. For a careful proof and their associated important results we refer to [3]. Here, the details of the proof have been omitted.

**Theorem 2.7 (The inverse decomposition theorem)** Let \( b, d \) be in \( \mathbb{N}^p \). Then, for any \( a \in \mathbb{N}^p, \) with \( \gcd(a, b) = 1 \) and \( \gcd(a, d) = 1 \), we get

\[ \mathcal{J}_{b \times d}(a) = \mathcal{J}_b(a) + b \times \phi_d \{ \mathcal{L}_d(a) \times \mathcal{L}_a(b) \}. \] (2.7)

Note that once established the expression (2.7) of Theorem 2.7, we could prove the validity of

\[ \mathcal{J}_{b \times d}(a) = \mathcal{J}_d(a) + d \times \phi_b \{ \mathcal{L}_b(a) \times \mathcal{L}_a(d) \}. \] (2.8)

The Theorem 2.7 has an interesting consequence which is very useful for our purposes. Even though a proof can be found in [3], one also is given here with the idea of benefiting the reading of the paper. We formulate this precisely as follows.

**Theorem 2.8** Let \( b, d \) be in \( \mathbb{N}^p \). Then, for any \( a \in \mathbb{N}^p, \) with \( \gcd(a, b) = 1 \) and \( \gcd(a, d) = 1 \), we have in terms of (MMIO)'s that:

\[ \mathcal{J}_{b \times d}(a) = \mathcal{J}_b(a) + b \times \phi_d \{ \mathcal{J}_d(a) \times \mathcal{J}_a(b) - 1 \}. \] (2.9)

**Proof.** First of all, let us notice that \( \gcd(a, b) = 1 \) and \( \gcd(a, d) = 1 \), implies that \( \gcd(a, b \times d) = 1 \). Hence the operator \( \mathcal{J}_{b \times d}(\cdot) \) it is well defined on \( \mathbb{Z}/\rho\mathbb{Z}^* \), where \( \rho = b \times d \) with \( b, d \in \mathbb{N}^p \). By virtue of property (15) of Theorem 2.6 and the assumption \( \gcd(a, d) = 1 \), we gets to

\[ \mathcal{J}_a(d) + \mathcal{L}_a(d) = a. \] (2.10)

Also, by Theorem 2.5

\[ a \times \mathcal{J}_d(a) = 1 + d \times \mathcal{L}_a(d). \]

Now from this last identity and the Eq. (2.10), we have the formula:

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

Thus

\[ d \times a = a \times \mathcal{J}_d(a) + d \times \mathcal{J}_a(d) - 1. \] (2.11)

Now note that \( \mathcal{L}_d(a) \times \mathcal{L}_a(b) \) by Eq. (2.10) can be also rewrite as

\[ \mathcal{L}_d(a) \times \mathcal{L}_a(b) = (d - \mathcal{J}_d(a)) \times (a - \mathcal{J}_a(b)) = d \times a - d \times \mathcal{J}_a(b) - a \times \mathcal{J}_d(a) + \mathcal{J}_d(a) \times \mathcal{J}_a(b) \]
Therefore, the equality (2.11) implies that
\[ \mathcal{L}_d(a) \times \mathcal{L}_a(b) = d \times (\mathcal{I}_a(d) - \mathcal{I}_a(b)) + \mathcal{I}_d(a) \times \mathcal{I}_a(b) - 1. \]

Now by applying about this last equality the operator \( \phi_d \) together the properties (\( \phi_4 \), (\( \phi_3 \) and (\( \phi_2 \) of Theorem 2.1, we find that
\[ \phi_d \{ \mathcal{L}_d(a) \times \mathcal{L}_a(b) \} = \phi_d \{ \mathcal{I}_d(a) \times \mathcal{I}_a(b) - 1 \}. \]

Using the Theorem 2.7, the proof is finished. ■

**Remark 2.9** Apply the same methods, we also can show the validity of the identity
\[ \mathcal{I}_{b \times d}(a) = \mathcal{I}_d(a) + d \times \phi_b \{ \mathcal{I}_b(d) \times \mathcal{I}_a(d) - 1 \}. \] (2.12)

**Remark 2.10** The decomposition law for the operators \( \mathcal{I}_{b \times d}(\cdot) \) over group of units \((\mathbb{Z}/\varrho\mathbb{Z})^*\) established in the Theorem 2.8 facilitates the understanding of how these operators depend of the \((\text{MMIO})'\)s \( \mathcal{I}_b(\cdot) \), \( \mathcal{I}_d(\cdot) \) and \( \mathcal{I}_a(\cdot) \), respectively. Furthermore, the arguments above presented suggests a method for treating the case of interest, i.e., that in where the additional condition \( \gcd(b, d) = 1 \) will play a special role.

### 3. A refined version of the inverse decomposition theorem for modular multiplicative inverse operators

The goal of this section is to establish the main result of the paper, in which the role of the assumption \( \gcd(b, d) = 1 \) becomes clear. In fact, based on Theorem 2.8 and the assumption \( \gcd(b, d) = 1 \), we can state the following result.

**Theorem 3.1** (A refined version of the inverse decomposition theorem) Let \( b, d \) be in \( \mathbb{N}^\ast \) such that \( \gcd(b, d) = 1 \). Then, for any \( a \in \mathbb{N}^\ast \), with \( \gcd(a, b) = 1 \) and \( \gcd(a, d) = 1 \), we obtain
\[ \mathcal{I}_{b \times d}(a) = \mathcal{I}_d(a) + d \times \phi_b \{ \mathcal{I}_b(d) \times \mathcal{I}_a(d) - 1 \}. \] (3.1)

**Proof.** To prove the theorem, we first observe that the hypothesis \( \gcd(a, b) = 1 \) 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 \((\mathbb{Z}/\varrho\mathbb{Z})^*\), where \( \varrho = b \times d \) with \( b, d \in \mathbb{N}^\ast \). Now, we only need to show the identity
\[ \phi_b \{ \mathcal{I}_b(a) \times \mathcal{I}_a(d) - 1 \} = \phi_b \{ \mathcal{I}_b(d) \times \mathcal{I}_a(d) + \mathcal{L}_b(d) \times \mathcal{I}_d(a) \}. \]

In fact, as a consequence of (2.9) and (2.12), and the hypothesis \( \gcd(a, b) = \gcd(a, d) = 1 \), we deduce that
\[ \mathcal{I}_d(a) + d \times \phi_b \{ \mathcal{I}_a(d) \times \mathcal{I}_a(d) - 1 \} = \mathcal{I}_d(a) + b \times \phi_d \{ \mathcal{I}_d(a) \times \mathcal{I}_a(b) - 1 \}. \]

Applying the operator \( \phi_b \) to this equation together with the properties (\( \phi_4 \), (\( \phi_3 \) and (\( \phi_2 \) of the Theorem 2.1, and the definition of \( \phi_b \), we have
\[ \phi_b \{ \mathcal{I}_d(a) + d \times \phi_b(\mathcal{I}_a(d) \times \mathcal{I}_a(d) - 1) \} = \phi_b \{ \mathcal{I}_d(a) + b \times \phi_d(\mathcal{I}_d(a) \times \mathcal{I}_a(b) - 1) \} \]
\[ = \phi_b \{ \mathcal{I}_b(a) \} = \mathcal{I}_b(a). \] (3.2)

Now using the Eq. (3.2) together with the properties (\( \phi_4 \), (\( \phi_5 \) of the Theorem 2.1, we conclude that
\[ \phi_b \{ \mathcal{I}_d(a) + d \times \mathcal{I}_b(a) \times \mathcal{I}_a(d) - d \} = \mathcal{I}_b(a). \] (3.3)
Hence, by multiplying both sides of the Eq.(3.3) by $\mathcal{I}_b(d)$ (which is well defined by our assumption $\gcd(b, d) = 1$), it follows that
\[
\mathcal{I}_b(d) \times \mathcal{I}_b(a) = \mathcal{I}_b(d) \times \phi_b \{ \mathcal{I}_d(a) + d \times \mathcal{I}_b(a) \times \mathcal{I}_a(d) - d \}.
\] (3.4)

Similarly, applying $\phi_b$ to this last identity, we obtain
\[
\phi_b(\mathcal{I}_b(d) \times \mathcal{I}_b(a)) = \phi_b \{ \mathcal{I}_b(d) \times \phi_b(\mathcal{I}_d(a) + d \times \mathcal{I}_b(a) \times \mathcal{I}_a(d) - d) \}.
\] (3.5)

Using the properties ($\phi_4$) and ($\phi_5$) of the Theorem 2.1 in Eq. (3.5) gives,
\[
\phi_b(\mathcal{I}_b(d) \times \mathcal{I}_b(a)) = \phi_b \{ \mathcal{I}_b(d) \times \mathcal{I}_d(a) + d \times \mathcal{I}_b(d) \times \mathcal{I}_b(a) \times \mathcal{I}_a(d) - d \times \mathcal{I}_b(d) \}.
\] (3.6)

Now add to both parts of the Eq. (3.6) the quantity $(b - 1) \times \mathcal{I}_b(d) \times \mathcal{I}_d(a) + d \times \mathcal{I}_b(d)$ we get
\[
\phi_b(\mathcal{I}_b(d) \times \mathcal{I}_b(a)) + (b - 1) \times \mathcal{I}_b(d) \times \mathcal{I}_d(a) + d \times \mathcal{I}_b(d) = \\
\phi_b \{ \mathcal{I}_b(d) \times \mathcal{I}_d(a) + d \times \mathcal{I}_b(d) \times \mathcal{I}_b(a) \times \mathcal{I}_a(d) - d \times \mathcal{I}_b(d) \} + \\
(b - 1) \times \mathcal{I}_b(d) \times \mathcal{I}_d(a) + d \times \mathcal{I}_b(d)
\]

Again applying the operator $\phi_b$ to this last identity together with the properties ($\phi_4$) and ($\phi_5$) of the Theorem 2.1, the definition of the operator $\mathcal{L}_b(d)$ and exploit the fact that $\phi_b(d \times \mathcal{I}_b(d)) = 1$ we obtain
\[
\phi_b \{ \mathcal{I}_b(d) \times \mathcal{I}_b(a) + \mathcal{L}_b(d) \times \mathcal{I}_d(a) + 1 \} = \phi_b \{ \mathcal{I}_b(a) \times \mathcal{I}_a(d) \}.
\] (3.7)

But this means that
\[
\phi_b \{ \mathcal{I}_b(d) \times \mathcal{I}_b(a) + \mathcal{L}_b(d) \times \mathcal{I}_d(a) \} = \phi_b \{ \mathcal{I}_b(a) \times \mathcal{I}_a(d) - 1 \}.
\] (3.8)

The assertion of Theorem 3.1 follows from Theorem 2.8. ■

**Remark 3.2** Apply the same methods, we also can show the validity of the following identity:
\[
\mathcal{I}_{b \times d}(a) = \mathcal{I}_b(a) + b \times \phi_d \{ \mathcal{I}_d(b) \times \mathcal{I}_a(d) + \mathcal{L}_d(b) \times \mathcal{I}_b(a) \}.
\] (3.9)

4. A brief overview

While it is true that the mathematical expressions (2.9) and (3.1) are primarily based on the (IDT), when looking at them closely, it is possible to distinguish some differences, which depend critically on the condition $\gcd(b, d) = 1$. In this sense, the mathematical structure of (3.1) is sharper from a functional algorithmic point of view. Finally, it should be emphasized that this refined version of the (IDT) will play an active role in the studies of other important structures, strongly associated with the so-called "Mixed radix systems". This, we will analyze further in the next article.

**Acknowledgments**

I express deep gratitude to Alejandro Maass for inviting him to visit el (CMM) -Center for Mathematical Modeling of the Universidad de Chile–Santiago. Some of the ideas presented here were clarified and tested during my visit to this Chilean Center.

**References**

[1] 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 (2015) 012135.

[2] L. A. Cortés–Vega, On the decomposition of modular multiplicative inverse operators via a new functional algorithm approach to Becket’s Bezout’s Lemma, *J. Phys.: Conf. Ser.*, 936 (2017) 012095.

[3] L. A. Cortés–Vega, A general method for to decompose modular multiplicative inverse operators over Group of units, *Proyecciones Journal of Mathematics*, 37 (2), 265–293, (2018).

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