A new decomposition law for inverses modular multiplicative on \((\mathbb{Z}/\varrho\mathbb{Z})^*\)

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

Abstract. In modular arithmetic, we find a valuable concept, the so-called “modular multiplicative inverse” (symbolized by MMI). In precise words, if \(\mathbb{Z}/\varrho\mathbb{Z}\) denoted the residue system modulo \(\varrho\), the (MMI) of \(a \in \mathbb{Z}/\varrho\mathbb{Z}\), if it exists, is \(a^{-1} \in \mathbb{Z}/\varrho\mathbb{Z}\), such that
\[a \times a^{-1} \equiv 1 \mod \varrho,\]
where \(p \equiv q \mod \varrho\) is the usual modular representation of \(q \in \mathbb{Z}/\varrho\mathbb{Z}\). This very special element it is one of the most wideley used mathematical concept in science, engineering and subject areas include the particle physics, the analysis and design of algorithms, data structures, databases, and computer architecture. In this paper, we establish a promising decomposition law for (MMI). In this respect, the main purpose of this paper it is shown that it is possible to express the (MMI) in terms of certain modular multiplicative inverse operators (MMIO) all, well-defined on Group of units pre-established. The main point to note here is that the result of this paper, which expands a result originally presented in [3], does not include any special conditions on the parameters involved.

1. Introduction
In what follows \(\mathbb{N}\) denote the set of the natural numbers, \(\mathbb{N}^0 = \mathbb{N} \setminus \{1\}\), \(\mathbb{N}^0 = \mathbb{N} \cup \{0\}\), \(\mathbb{Z} = (\mathbb{Z}, +, \times)\) 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 \(\mathbb{Z}/b\mathbb{Z}\). 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. 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):
\[\mathcal{I}_\varrho : (\mathbb{Z}/\varrho\mathbb{Z})^* \longrightarrow \mathbb{Z}/\varrho\mathbb{Z}, \quad \mathcal{I}(a) = a^{-1}, \quad \varrho > 3\]
it was introduced and studied by the author in [2, 3]. As a result, were obtained the so-called “inverse decomposition theorem (IDT)”\). This theorem asserts that:

**Theorem 1.1 (IDT)** Let \(b, d\) be in \(\mathbb{N}^0\). Then, for any \(a \in \mathbb{N}^0\), with \(\gcd(a, b) = 1\) and \(\gcd(a, d) = 1\), we get
\[\mathcal{I}_{b \times d}(a) = \mathcal{I}_b(a) + b \times \phi_d \{\mathcal{L}_d(a) \times \mathcal{L}_a(b)\}, \quad (1.1)\]
Let $\gamma \in (\mathbb{Z}/\beta \mathbb{Z})^* \rightarrow \mathcal{L}_\beta(\gamma) \in \mathbb{Z}/\beta \mathbb{Z}$, with $\mathcal{L}_\beta(\gamma) = \phi_\beta [(\beta - 1) \times \mathcal{I}_\beta(\gamma)]$

and the operators $\phi_b : \mathbb{N}^0 \rightarrow \mathbb{Z}/b\mathbb{Z}$ are defined in general by:

$$\phi_\beta(a) = \{ \begin{array}{ll} a, & \text{if } 0 \leq a \leq \beta - 1, \\ r, & \text{if } a \geq \beta. \end{array}$$

where $a \equiv r \mod \beta$, for any $\beta \in \mathbb{N}^\circ$.

The (IDT) that we have noted above, has a number of important implications. One of them is the following theorem.

**Theorem 1.2** Let $b, d$ be in $\mathbb{N}^\circ$. Then, for every $a \in (b, d) \cap \mathbb{N}^\circ$, with $\gcd(a, b) = 1$ and $\gcd(a, d) = 1$, we get

$$\mathcal{I}_{b \times d}(a) = \mathcal{I}_b(a) + b \times \phi_d \{ \mathcal{I}_d(d - a) \times \mathcal{I}_a(a - b) \}. \quad (1.2)$$

Unfortunately, the main limitation of these theorem is the condition $a \in (b, d) \cap \mathbb{N}^\circ$ since, play a primary role in its demonstration and significantly limits its scope. In this respect, the main aim of this paper is to extend the Theorem 1.2. In the new result, $\gcd(a, b) = 1$ and $\gcd(a, d) = 1$ will be the only assumptions considered. From now on, we will concentrate at proving the following theorem.

**Theorem 1.3** Let $b, d$ be in $\mathbb{N}^\circ$. Then, for any $a \in \mathbb{N}^\circ$, with $\gcd(a, b) = 1$ and $\gcd(a, d) = 1$, we get

$$\mathcal{I}_{b \times d}(a) = \mathcal{I}_b(a) + b \times \phi_d \{ \mathcal{I}_d(d - \phi_d(a)) \times \mathcal{I}_a(a - \phi_a(b)) \}. \quad (1.3)$$

The 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 result of this article.

2. Preliminaries

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 $\gcd(a, b) = s \times a + t \times b$. 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 $\phi_b : \mathbb{N}^0 \rightarrow \mathbb{Z}/b\mathbb{Z}$ and $\psi_b : \mathbb{N}^0 \rightarrow \mathbb{N}^0$, defined by:

$$\phi_b(a) = \{ \begin{array}{ll} a, & \text{if } 0 \leq a \leq b - 1, \\ r, & \text{if } a \geq b \end{array}, \quad \psi_b(a) = \frac{a - \phi_b(a)}{b},$$

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

**Theorem 2.1** Let $b \in \mathbb{N}^\circ$. Then the following mathematical expressions:

(φ1) $\phi_b(0) = 0$,
(φ2) $\phi_b(d \times b) = 0$ for every $d \in \mathbb{N}^0$,
(φ3) $\phi_b(a) = \phi_b(\phi_b(a))$ for every $a \in \mathbb{N}^0$,
(φ4) $\phi_b(a + d) = \phi_b(\phi_b(a) + \phi_b(d)) = \phi_b(\phi_b(a) + d)$ for every $a, d \in \mathbb{N}^0$,
(φ5) $\phi_b(a \times d) = \phi_b(\phi_b(a) \times \phi_b(d)) = \phi_b(\phi_b(a) \times d)$ for every $a, d \in \mathbb{N}^0$,
(φ6) $\phi_b(a + b) = \phi_b(a)$ for every $a \in \mathbb{N}^0$ ("periodicity" of $\phi_b$),
(c1) $\mathcal{C}_b(0) = 0$,
(c2) $\mathcal{C}_b(b \times a) = a$ for every $a \in \mathbb{N}_0$. In particular $\mathcal{C}_b(b) = 1$,
(c3) $\mathcal{C}_b(\phi_b(a)) = 0$ for every $a \in \mathbb{N}_0$ ($\mathcal{C}_b$ is a “annihilator” of $\phi_b$),
(c4) $\mathcal{C}_b(a + d) = \mathcal{C}_b(a) + \mathcal{C}_b(d) + \mathcal{C}_b(\phi_b(a) + \phi_b(d))$ for every $a, d \in \mathbb{N}_0$,
(c5) $\mathcal{C}_b(a \times d) = \mathcal{C}_b(a) \times d + \phi_b(a) \times \mathcal{C}_b(d) + \mathcal{C}_b(\phi_b(a) \times \phi_b(d))$ for every $a, d \in \mathbb{N}_0$,
(c6) $\mathcal{C}_b(a + b) = \mathcal{C}_b(a) + 1$ for every $a \in \mathbb{N}_0$ ($\mathcal{C}_b$ is quasi-periodic),
(c7) $\mathcal{C}_b(a + b \times \mu) = \mathcal{C}_b(a) + \mu$ for every $a, \mu \in \mathbb{N}_0$,
(e1) $a = \phi_b(a) + b \times \mathcal{C}_b(a)$ for every $a \in \mathbb{N}_0$,
(e2) $a < b$ if and only if $\mathcal{C}_b(a) = 0$ for every $a \in \mathbb{N}_0$,
(e3) $(\mathcal{C}_b \circ \mathcal{C}_d)(a) = \mathcal{C}_{b \times d}(a)$ 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 $\mathcal{C}_d$ with
$\mathcal{C}_b; \mathcal{C}_d$ with $\phi_b, \phi_d$ with $\phi_b$ and $\phi_d$ with $\mathcal{C}_b$, 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)’s. To be precise,

**Definition 2.3** If $b \in \mathbb{N}_0$, then the modular multiplicative inverse operator (MMIO) denoted by
$\mathcal{J}_b(\cdot)$ is the mapping

$$\mathcal{J}_b : (\mathbb{Z}/b\mathbb{Z})^* \rightarrow \mathbb{Z}/b\mathbb{Z}, \text{ defined by } \mathcal{J}_b(a) = a^{-1}, \text{ such that}$$

$$\phi_b(a \times \mathcal{J}_b(a)) = 1 \text{ for every } a \in (\mathbb{Z}/b\mathbb{Z})^*. \quad (2.1)$$

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

$$\mathcal{J}_b(a) = \mathcal{J}_b(\phi_b(a)), a \in \mathbb{N} \text{ with } \gcd(a, b) = 1, \text{ and } \mathcal{J}_b(1) = 1. \quad (2.2)$$

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

**Definition 2.4** If $b \in \mathbb{N}_0$, the operator $\mathcal{L}_b$ given by:

$$a \in (\mathbb{Z}/b\mathbb{Z})^* \rightarrow \mathcal{L}_b(a) \in \mathbb{Z}/b\mathbb{Z}, \text{ with } \mathcal{L}_b(a) = \phi_b \left[(b - 1) \times \mathcal{J}_b(a)\right] \quad (2.3)$$

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

$$\phi_b \left[a \times \mathcal{L}_b(a)\right] = b - 1 \text{ for any } a \in (\mathbb{Z}/b\mathbb{Z})^*. \quad (2.4)$$

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

$$\mathcal{L}_b(1) = b - 1 \text{ and } \mathcal{L}_b(a) = \mathcal{L}_b(\phi_b(a)) \text{ if } a \in \mathbb{N}, \text{ with } \gcd(a, b) = 1. \quad (2.5)$$

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 $m, n \in \mathbb{N}^*$ such that $\gcd(m, n) = 1$. Then

$$m \times \mathcal{I}_n(m) = n \times \mathcal{L}_m(n) + 1. \quad (2.6)$$

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 $b, d \in \mathbb{N}^*$ such that $\gcd(b, d) = 1$, and every $a \in \mathbb{N}$, with $\gcd(a, b) = 1$ we have

(L1) $\mathcal{L}_b(\mathcal{I}_b(a)) = \mathcal{I}_b(\mathcal{L}_b(a))$,  
(L2) $\mathcal{L}_b(a \times d) = \phi_b(\mathcal{L}_b(a) \times \mathcal{I}_b(d)) = \phi_b(\mathcal{I}_b(a) \times \mathcal{L}_b(d))$,  
(L3) For any $m, n \in \mathbb{N}$ such that $\gcd(m + n, b) = 1$, we have

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

(L4) $\mathcal{L}_b(a + b) = \mathcal{L}_b(a)$, (“periodicity” of $\mathcal{L}_b$),  
(L5) $\mathcal{L}_b(\mathcal{L}_b(a)) = \phi_b(a)$,  
(I1) $\mathcal{I}_b(a \times d) = \phi_b(\mathcal{I}_b(a) \times \mathcal{I}_b(d))$,  
(I2) For any $m, n \in \mathbb{N}$ 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) $\mathcal{I}_b(\mathcal{I}_b(a)) = \phi_b(a)$,  
(I5) $\mathcal{I}_b(a) + \mathcal{L}_b(a) = b$.

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

$$\mathcal{I}_{b \times d}(a) = \mathcal{I}_b(a) + b \times \phi_d \{\mathcal{L}_d(a) \times \mathcal{L}_a(b)\}. \quad (2.7)$$

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

$$\mathcal{I}_{b \times d}(a) = \mathcal{I}_d(a) + d \times \phi_b \{\mathcal{L}_b(a) \times \mathcal{L}_a(d)\}. \quad (2.8)$$

The Theorem 2.7 has an interesting consequence, which expands a recent result presented in [3]. This is the main result of the paper, which we formulate precisely as follows.

Theorem 2.8 Let $b, d \in \mathbb{N}^*$. Then, for any $a \in \mathbb{N}^*$, with $\gcd(a, b) = 1$ and $\gcd(a, d) = 1$, we get

$$\mathcal{I}_{b \times d}(a) = \mathcal{I}_b(a) + b \times \phi_d \{\mathcal{I}_d(d - \phi_d(a)) \times \mathcal{I}_a(a - \phi_a(b))\}. \quad (2.9)$$
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 \( \mathbb{Z}/\varrho \mathbb{Z}\), where \( \varrho = b \times d \) with \( b, d \in \mathbb{N}^e \). Now by the property \((I5)\) of the Theorem 2.6, 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:
\[
\mathcal{I}_{a}(\mathcal{I}_{a}(b)) + \mathcal{L}_{a}(\mathcal{I}_{a}(b)) = a. \tag{2.10}
\]
Thus, by the property \((I4)\) of Theorem 2.6, we obtain of (2.10) that
\[
\phi_{a}(b) + \mathcal{L}_{a}(\mathcal{I}_{a}(b)) = a. \tag{2.11}
\]
Thus,
\[
\mathcal{L}_{a}(\mathcal{I}_{a}(b)) = a - \phi_{a}(b). \tag{2.12}
\]
Similarly, consider now that \( m = d \) and \( n = \mathcal{I}_{d}(a) \), then, one gets
\[
\mathcal{L}_{d}(\mathcal{I}_{d}(a)) = d - \phi_{d}(a). \tag{2.13}
\]

Remark 2.9 Note that \( \gcd(a, \mathcal{I}_{a}(b)) = 1 \) by Bézout’s theorem. Indeed, there are \( x = -\mathcal{L}_{b}(a) \in \mathbb{Z} \) and \( y = b \in \mathbb{Z} \) 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 \((L1), (L4), (I4)\) of Theorem 2.6 together with Eqs. \((2.5), (2.12)\) and \((2.13)\) yields to
\[
\mathcal{L}_{d}(a) \times \mathcal{L}_{b}(b) = \mathcal{L}_{d}(\phi_{d}(a)) \times \mathcal{L}_{a}(\phi_{a}(b)) = \mathcal{L}_{d} \left( \mathcal{L}_{d}(\mathcal{I}_{d}(a)) \times \mathcal{L}_{a}(\mathcal{I}_{a}(b)) \right) = \mathcal{I}_{d} \left( \mathcal{L}_{d}(\mathcal{I}_{d}(a)) \times \mathcal{L}_{a}(\mathcal{I}_{a}(b)) \right) = \mathcal{I}_{d} \left( \mathcal{I}_{d}(a) \times \mathcal{I}_{a}(b) \right),
\]
which together with the Theorem 2.7 leads to relation \((2.9)\). This completes the proof of Theorem 2.8. ■

Remark 2.10 It is interesting to note that, in contrast with the Theorem 1.2, the Theorem 2.8 not uses the assumption \( a \in (b, d) \cap \mathbb{N}^e \), but it is obvious that \( \gcd(a, b) = 1 \) and \( \gcd(a, d) = 1 \) are needed. In this context, the Theorem 2.8 is a generalization of the Theorem 1.2 given in [3].

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 Bachet’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).