On the decomposition of modular multiplicative inverse operators via a new functional algorithm approach to Bachet’s-Bezout’s Lemma

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

Abstract. In this paper, we consider modular multiplicative inverse operators (MMIO)’s of the form:

\[ I_{(m+n)} : \mathbb{Z}/(m+n)\mathbb{Z}^* \rightarrow \mathbb{Z}/(m+n)\mathbb{Z}, \quad I_{(m+n)}(a) = a^{-1}. \]

A general method to decompose \( I_{(m+n)}(\cdot) \) over group of units \((\mathbb{Z}/(m+n)\mathbb{Z})^*\) is derived. As a result, an interesting decomposition law for these operators over \((\mathbb{Z}/(m+n)\mathbb{Z})^*\) is established. Numerical examples illustrating the new results are given. This, complement some recent results obtained by the author for \((\text{MMIO})’s\) defined over group of units of the form \((\mathbb{Z}/\varrho\mathbb{Z})^*\), with \(\varrho = m \times n > 2\).

1. Introduction

In a general context, if \(\mathbb{Z}/\varrho\mathbb{Z}\) denoted the residue system modulo \(\varrho\), the modular multiplicative inverse (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 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, see, for instance, \([1, 2, 6, 7, 11, 13, 14, 17, 18]\).

Previously, the author in \([4]\) introduce the notion of modular multiplicative inverse operator (MMIO): \(I_{\varrho} : (\mathbb{Z}/\varrho\mathbb{Z})^* \rightarrow \mathbb{Z}/\varrho\mathbb{Z}\), such that \(I_{\varrho}(a) = a^{-1}\). and provide a general method for to decompose \((\text{MMIO})’s\) \(I_{\varrho}\) over \((\mathbb{Z}/\varrho\mathbb{Z})^*\), where \(\varrho = m \times n \in \mathbb{N}\), \(\varrho > 2\), which is closely related to the work in this paper. In this article, using a similar approach we extend and completed these results to a class of modular multiplicative inverse operator defined in group of units of the form \((\mathbb{Z}/(m+n)\mathbb{Z})^*\). In particular, under reasonable assumptions, we showed that:

\[ I_{m+n}(a) := I_{m+n}(a) + I_{n} - I_{a} \quad (1.1) \]

is still valid, where \(\phi_{a}(m) = \alpha\) and \(\phi_{a}(n) = \beta\). Here, the operator \(\phi_{d}(\cdot)\) have the following structure: \(\phi_{d} : \mathbb{N}^* \rightarrow \mathbb{Z}/d\mathbb{Z}\), such that

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

where \(a \equiv r \mod d\). 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

Published under licence by IOP Publishing Ltd

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Arithmetic and applicable in other fields as well. In order to establish Eq.(1.1), we need to show the following generalized algorithmic functional version of Bachet’s-Bezout’s Lemma:

\[ a \times \mathcal{A}_\beta(a) = b \times \mathcal{L}_\beta(b) + 1, \]

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

\[ \gamma \in (\mathbb{Z}/\beta \mathbb{Z})^* \to \mathcal{L}_\beta(\gamma) \in \mathbb{Z}/\beta \mathbb{Z}, \text{ with } \mathcal{L}_\beta(\gamma) = \phi_\beta[(\beta - 1) \times \mathcal{A}_\beta(\gamma)]. \]

An argument based on an algorithmic functional approach proposed by the author in [3, 4] confirms Eq. (1.2). From a mathematical point of view Eq. (1.1) is extremely interesting and naturally, this associated to (MMI). Furthermore, we should emphasize that from a computational point of view, the Eq. (1.1) 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 Eq. (1.1).

Our work initially was motivated in part by some problems associated with certain inverse states defined about finite Galois Fields \((\mathbb{Z}/p_n \mathbb{Z})^*\), where \(p_n\) is a large prime number, the which is 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 on the state of the art of this last fascinating subject may be found in [6], [7] 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 result 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 [15]. First, however, we need some notation. Here, and in the rest of the paper, \(\mathbb{N}\) denote the set of the natural numbers, \(a \in \mathbb{N}^*\) if \(a \in \mathbb{N} \cup \{0\}\). To simplify the presentation we assume that \(a \in \mathbb{N}^o\) if \(a \in \mathbb{N}\setminus\{1\}\). We let \((\mathbb{Z}, +, \times)\) denote the ring of integers. The operation \(\times\) in \(\mathbb{Z}\) 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 \(\mathbb{Z}/b\mathbb{Z}\) be the ring of residue classes modulo \(b\), \(a \in \mathbb{Z}/b\mathbb{Z}\) if \(a \in \{0, 1, 2, \ldots, b-1\}\). Throughout this paper we use the convention that \((\mathbb{Z}/b\mathbb{Z})^* = \{a \in \mathbb{Z}/b\mathbb{Z} : \gcd(a, b) = 1\}\) denotes the group of unit of \(\mathbb{Z}/b\mathbb{Z}\), the which under multiplication forms an abelian group. Let us emphasize that, as already mentioned above, 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 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 Bachet’s-Bezout’s Lemma, which states that: if \(a\) and \(b\) are positive integers, then there exist integers \(s\) and \(t\) such that \(\gcd(a, b) = s \times a + t \times b\), is useful when \(a\) and \(b\) are relatively primes, in this case we have \(\gcd(a, b) = 1\). Now following the arguments in [3], we can derive for the operators \(\phi_b : \mathbb{N}^* \to \mathbb{Z}/b\mathbb{Z}\) and \(\mathcal{C}_b : \mathbb{N}^* \to \mathbb{N}^*\), defined by

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

where \(a \equiv r \mod b\) for any \(b \in \mathbb{N}^o\), the following

**Theorem 2.1** Let \(b \in \mathbb{N}^o\). Then, the following statements are true:
(1) \( \phi_b(0) = 0 \),
(2) \( \phi_b(d \times b) = 0 \) for every \( d \in \mathbb{N}^* \),
(3) \( \phi_b(a) = \phi_b(\phi_b(a)) \) for every \( a \in \mathbb{N}^* \),
(4) \( \phi_b(a + d) = \phi_b(\phi_b(a) + \phi_b(d)) = \phi_b(a + \phi_b(d)) = \phi_b(a) + \phi_b(d) \) for every \( a, d \in \mathbb{N}^* \),
(5) \( \phi_b(a \times d) = \phi_b(\phi_b(a) \times \phi_b(d)) = \phi_b(a \times \phi_b(d)) = \phi_b(\phi_b(a) \times d) \) for every \( a, d \in \mathbb{N}^* \),
(6) \( \phi_b(a + b) = \phi_b(a) \) for every \( a \in \mathbb{N}^* \) ("periodicity" of \( \phi_b \)),
(1) \( C_b(0) = 0 \),
(2) \( C_b(b \times a) = a \) for every \( a \in \mathbb{N}^* \). In particular \( C_b(b) = 1 \),
(3) \( C_b(\phi_b(a)) = 0 \) for every \( a \in \mathbb{N}^* \) (\( C_b \) is a "annihilator" of \( \phi_b \)),
(4) \( C_b(a + d) = C_b(a) + C_b(d) + C_b(\phi_b(a) + \phi_b(d)) \) for every \( a, d \in \mathbb{N}^* \),
(5) \( C_b(a \times d) = C_b(a) \times d + \phi_b(a) \times C_b(d) + C_b(\phi_b(a) \times \phi_b(d)) \) for every \( a, d \in \mathbb{N}^* \),
(6) \( C_b(a + b) = C_b(a) + 1 \) for every \( a \in \mathbb{N}^* \) (\( C_b \) is quasi-periodic),
(7) \( C_b(a + b \times \mu) = C_b(a) + \mu \) for every \( a, \mu \in \mathbb{N}^* \),
(8) \( a = \phi_b(a) + b \times C_b(a) \) for every \( a \in \mathbb{N}^* \),
(9) \( a < b \) if and only if \( C_b(a) = 0 \) for every \( a \in \mathbb{N}^* \),
(10) \( (C_b \circ C_d)(a) = C_b \times d(a) \) for every \( a \in \mathbb{N}^* \) and every \( d \in \mathbb{N}^* \).

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 \( \phi_b \), \( \phi_d \) with \( \phi_b \) and \( \phi_d \) with \( C_b \), are defined by one usual way. We shall not prove this theorem here but assume its validity. A proof appear in [3].

Another result coming out of Theorem 2.1, using the property (e3) is the following decomposition law (Theorem 4 given in [3]):

**Theorem 2.3** For any \( b, d \in \mathbb{N}^* \) and any \( a \in \mathbb{N}^* \), we have

\[
\phi_{d \times b}(a) = \phi_d(a) + d \times \phi_b(\mathcal{C}_d(a)).
\]  

**3. Decomposition-type theorems for modular multiplicative inverses operators in group of units of the form \((\mathbb{Z}/(m + n)\mathbb{Z})^*\)**

As already pointed out in the introduction, in this section we shall be concerned with the construction of a specific law of decomposition for the (MMI) over \((\mathbb{Z}/\varrho\mathbb{Z})^*\), with \( \varrho = m + n \), and \( m, n \in \mathbb{N}^* \). In order to investigate this, in the spirit of [4] we introduce first, the notion of modular multiplicative inverse operators (MMIO)'s. To be precise,

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

\[ \mathcal{I}_b : (\mathbb{Z}/b\mathbb{Z})^* \to \mathbb{Z}/b\mathbb{Z}, \text{ defined by } \mathcal{I}_b(a) = a^{-1}, \text{ such that } \]

\[
\phi_b(a \times \mathcal{I}_b(a)) = 1 \text{ for every } a \in (\mathbb{Z}/b\mathbb{Z})^*.
\]  

**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 when acting on the natural numbers:

\[
\mathcal{I}_b(a) = \mathcal{I}_b(\phi_b(a)), a \in \mathbb{N} \text{ with } \gcd(a, b) = 1, \text{ and } \mathcal{I}_b(1) = 1.
\]
As examples, we have that $I_7(5) = 3$ and $I_7(13) = 6$, since 
\[ \phi_7(5 \times I_7(5)) = \phi_7(5 \times 3) = \phi_7(15) = 1, \]
and similarly
\[ \phi_7(13 \times I_7(13)) = \phi_7(13 \times 6) = \phi_7(\phi_7(13) \times 6) = \phi_7(6 \times 6) = \phi_7(36) = 1. \]
In this last expression, we used property (\phi 5) of Theorem 2.1 given above. Further noting that Eq. (3.2) yields to $I_7(13) = I_7(\phi_7(13)) = I_7(6) = 6$.

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

**Definition 3.2** If $b \in \mathbb{N}$, the operator $L_b$ given by:
\[ a \in (\mathbb{Z}/b\mathbb{Z})^* \rightarrow L_b(a) \in \mathbb{Z}/b\mathbb{Z}, \text{ with } L_b(a) = \phi_b[(b - 1) \times I_b(a)] \quad (3.3) \]
is well defined. $L_b(a)$ will be called the “predecessor operator modulo $b$”, since
\[ \phi_b[a \times L_b(a)] = b - 1 \text{ for any } a \in (\mathbb{Z}/b\mathbb{Z})^*. \quad (3.4) \]
From this definition it is clear also that the predecessor operator $L_b(a)$ satisfies the following additional properties:
\[ L_b(1) = b - 1 \text{ and } L_b(a) = L_b(\phi_b(a)) \text{ if } a \in \mathbb{N}, \text{ with } \gcd(a, b) = 1. \quad (3.5) \]

Equipped with these operators, we can collect a number of important algebraic and functional properties, some of which, we shall use frequently in the current paper.

**Theorem 3.3 (A algorithmic functional version of Bachet’s-Bezout’s Lemma)** Let be $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$. Then
\[ m \times I_n(m) = n \times L_m(n) + 1. \quad (3.6) \]

**Proof.** Indeed, as $\gcd(m, n) = 1$. The Bachet’s-Bezout’s Lemma, states that there exist integers $x$ and $y$ such that
\[ 1 = m \times x + n \times y. \quad (3.7) \]
To prove Eq. (3.6) we assume without loss of generality that $x \geq 0$ and $y < 0$. In this case, we obtain from Eq. (3.7) that:
\[ \phi_n(x) = I_n(m) \quad (3.8) \]
and
\[ \phi_m(-y) = \phi_m[(m - 1) \times I_m(n)] = L_m(n). \quad (3.9) \]
On the other hand, from the property (e1) of the Theorem 2.1, Eqs. (3.8) and (3.9) it follows that:
\[ x = I_n(m) + n \times e_n(x) \quad (3.10) \]
and
\[ -y = L_m(n) + m \times e_m(-y). \quad (3.11) \]
Now from Eqs. (3.7), (3.10), (3.11) together with the properties (e2) and (e3) of the Theorem 2.1 we obtain Eq. (3.6) as desired. ■

The following Theorem that I called of “modulus change”, summarize one interesting property of $I_b(\cdot)$, the which plays a role in this Section.
Theorem 3.4 (Modulus change) Let \( b \) be in \( \mathbb{N}^\circ \). Then, for any \( a \in \mathbb{N}^\circ \), with \( \gcd(a, b) = 1 \) we get
\[
\mathcal{S}_b(a) = \mathcal{C}_a \{ 1 + \phi_a(b) \times \mathcal{L}_a(b) \} + \mathcal{C}_a(b) \times \mathcal{L}_a(b).
\] (3.12)

Proof. With the aid of Theorem 3.3, we obtain that
\[
a \times \mathcal{S}_b(a) = 1 + b \times \mathcal{L}_a(b).
\]
Note that using the properties \((\phi_4), (\phi_5)\) and \((c1)\) of Theorem 2.1 we get:
\[
a \times \mathcal{S}_b(a) = 1 + b \times \mathcal{L}_a(b) - \phi_a \{ 1 + \phi_a(b) \times (a - 1) \times \mathcal{S}_b(b) \}
\]
\[
= 1 + b \times \mathcal{L}_a(b) - \phi_a \{ 1 + \phi_a(b) \times \phi_a((a - 1) \times \mathcal{S}_b(b)) \}
\]
\[
= 1 + b \times \mathcal{L}_a(b) - \phi_a \{ 1 + \phi_a(b) \times \mathcal{L}_a(b) \}
\]
\[
= 1 + b \times \mathcal{L}_a(b) - \{ 1 + \phi_a(b) \times \mathcal{L}_a(b) - a \times \mathcal{C}_a(1 + \phi_a(b) \times \mathcal{L}_a(b)) \}
\]
\[
= (b - \phi_a(b)) \times \mathcal{L}_a(b) + a \times \mathcal{C}_a(1 + \phi_a(b) \times \mathcal{L}_a(b))
\]
\[
= a \times \mathcal{C}_a(b) \times \mathcal{L}_a(b) + a \times \mathcal{C}_a(1 + \phi_a(b) \times \mathcal{L}_a(b)).
\]
This conclude the proof. □

Theorem 3.4 have a important consequence which we now state.

Theorem 3.5 (A law of decomposition for (MMIO)'s over \((\mathbb{Z}/(m+n)\mathbb{Z})^\star\))

Let \( m, n \in \mathbb{N}^\circ \). Then for any \( a \in (\mathbb{Z}/(m+n)\mathbb{Z})^\star \cap \mathbb{N}^\circ \) we have
\[
\mathcal{S}_{m+n}(a) = \mathcal{S}_{a+n}(a) + \mathcal{S}_{m+\beta}(a) - \mathcal{S}_{a+\beta}(a),
\] (3.13)

where \( \alpha = \phi_a(m) \) and \( \beta = \phi_a(n) \).

Proof. To prove this theorem we first of all note that for \( a \in (\mathbb{Z}/(m+n)\mathbb{Z})^\star \cap \mathbb{N}^\circ \), the identity
\[
\mathcal{C}_a(n) \times \mathcal{L}_a(m+n) = \mathcal{S}_{a+n}(a) - \mathcal{S}_{a+\beta}(a)
\]
follows from Theorem 3.4 and the properties \((\phi_4), (c4)\) of the Theorem 2.1, respectively. Now as before, using Theorem 3.4 and the properties \((\phi_4), (c4)\) of the Theorem 2.1 it is easy to check, repeating the previous argument, that if \( a \in (\mathbb{Z}/(m+n)\mathbb{Z})^\star \cap \mathbb{N}^\circ \), then
\[
\mathcal{C}_a(n) \times \mathcal{L}_a(m+n) = \mathcal{S}_{m+n}(a) - \mathcal{S}_{m+\beta}(a).
\]
These two last identities show the theorem, the proof is complete. □

Remark 3.6 We assume also that \( \mathcal{S}_1(a) = 1 \), for any \( a \in (\mathbb{Z}/(m+n)\mathbb{Z})^\star \cap \mathbb{N}^\circ \).

4. Numerical experiments

The Chinese Remainder Theorem (CRT), is actually one of the main theorems of number theory [8]. 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 [16] for Photo Radar, [15, 12] for Cryptography and Theory of Code, [10] for Matrix Theory, [3, 5, 15] for Acoustic Diffusers and [9] for DNA Sequencing.

We shall use some numerical results to illustrate most of the ideas and results of our approach. The discussion is limited only to Chinese remainder theorem in the spirit of [3], 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 $\mathbb{N}$, with $b_1, b_2 \geq 2$ and $\varrho = b_1 \times b_2$. Let $\gamma$ and $\beta$ be two arbitrary numbers such that $\gamma \in \mathbb{Z}/b_1\mathbb{Z}$ and $\beta \in \mathbb{Z}/b_2\mathbb{Z}$, respectively. Then we can find in the set $\mathbb{Z}/\varrho\mathbb{Z}$ one unique element $a$ that satisfied the system:

$$
\begin{align*}
\phi_{b_1}(a) &= \gamma, \\
\phi_{b_2}(a) &= \beta.
\end{align*}
$$

A explicit version of the solution of (4.1), in the case $b_2 > b_1$ have the form (for more detaild, see [3]):

$$
a = \beta + b_2 \times \phi_{b_1} \{ \mathcal{J}_{b_1}(\phi_{b_1}(b_2)) \times [\gamma + \beta \times (b_1 - 1)] \}.
$$

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

$$
\begin{align*}
\phi_{45}(a) &= 31, \\
\phi_{52}(a) &= 47.
\end{align*}
$$

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:

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

As, $\phi_{45}(52) = 7$, we get $a = 47 + 52 \times \phi_{45} \{ \mathcal{J}_{45}(7) \times [31 + 47 \times 44] \}$. In order to recover the solution $a$ of (4.3) and to facilitate the computation of the (MMIO) $\mathcal{J}_{45}(7)$, one may works as follows: Using Eq. (3.13), we find that

$$
\mathcal{J}_{45}(7) = \mathcal{J}_{24+21}(7) = \mathcal{J}_{3+21}(7) + \mathcal{J}_{24}(7) - \mathcal{J}_{3}(7).
$$

Here, $m = 24$ and $n = 21$. So

$$
\mathcal{J}_{45}(7) = 2 \times \mathcal{J}_{24}(7) - \mathcal{J}_{3}(\phi_{3}(7)).
$$

It follows immediately from equation above that

$$
\mathcal{J}_{45}(7) = 2 \times \mathcal{J}_{24}(7) - \mathcal{J}_{3}(1) = 2 \times \mathcal{J}_{24}(7) - 1.
$$

Similarly, for $\mathcal{J}_{24}(7)$ we have that

$$
\mathcal{J}_{24}(7) = \mathcal{J}_{12+12}(7) = \mathcal{J}_{3+12}(7) + \mathcal{J}_{12+5}(7) - \mathcal{J}_{10}(7).
$$

So,

$$
\mathcal{J}_{24}(7) = 2 \times \mathcal{J}_{17}(7) - \mathcal{J}_{10}(7).
$$

Following this process for $\mathcal{J}_{17}(7)$ we find

$$
\mathcal{J}_{17}(7) = \mathcal{J}_{10+7}(7) = \mathcal{J}_{3+7}(7) + \mathcal{J}_{10}(7) - \mathcal{J}_{3}(7) = 2 \times \mathcal{J}_{10}(7) - 1.
$$

Now as $\mathcal{J}_{10}(7) = 3$ a simple computation yields

$$
\mathcal{J}_{24}(7) = 3 \times \mathcal{J}_{10}(7) - 2 = 3 \times 3 - 2 = 7.
$$

Finally, it follows immediately from Eq. (4.4) that

$$
\mathcal{J}_{45}(7) = 2 \times \mathcal{J}_{24}(7) - 1 = 2 \times 7 - 1 = 13.
Consequently, the solution of (4.3) reduces to:

\[ a = 47 + 52 \times \phi_{45} \{13 \times [31 + 47 \times 44]\}. \quad (4.5) \]

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

\[
\phi_{45} \{13 \times [31 + 47 \times 44]\} = \phi_{45} \{13 \times [31 + 2 \times 44]\} = \phi_{45} \{13 \times 74\} = \phi_{45} \{13 \times 29\}. \quad (4.6)
\]

Also, Theorem 2.3, the properties \((\phi 5)\) and \((\phi 4)\) of Theorem 2.1 yields to

\[
\phi_{45} \{13 \times 29\} = \phi_{5}(13 \times 29) + 5 \times \phi_{9}(\phi_{5}(13 \times 29)) = \phi_{5}(13 \times 29) + 5 \times \phi_{9}(\phi_{5}(13 \times 29)) = \phi_{5}(3 \times 4) + 5 \times \phi_{9}(\phi_{5}(13 \times 29)) = \phi_{5}(12) + 5 \times \phi_{9}(2 \times 29 + 3 \times 5 + \phi_{5}(3 \times 4)) = 2 + 5 \times \phi_{9}(2 \times 2 + 3 \times 5 + 2) = 17.
\]

It then follows from (4.6) and (4.5) that \(a = 931\) and \(a < 2340\), like we should expect.

Acknowledgments

I am especially indebted to profesor Dr. Alvaro Restuccia, academic of Departament of Physics of the Antofagasta University by their support, via fondecyt Grant #1161192, Chile.

References

[1] H. M. AL-Matari, S. J. Aboud, N. F. Shilbayeh, Fast Fraction-Integer Method for Computing Multiplicative Inverse, *J. of Computing*, 1 (2009) 131–135.
[2] O. Arazi, H. Qi, On calculating multiplicative inverses modulo \(2^n\), *IEEE Trans. Comput* 57 1435–1438 (2008).
[3] 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 1–6 (2015).
[4] L. A. Cortés-Vega, About the decomposition of modular multiplicative inverse operators over group of units, *Submitted for publication* (2017).
[5] T. J. Cox, P. D’Antonio, *Acoustic Absorbers and Diffusers: Theory, Design and Application* Spon Press, 2004.
[6] Y. Dai, A. B. Borisov, K. Boyer, C. K. Rhodes, Computation with inverse states in a Finite Field \(\mathbb{F}_p\); The muon neutrino mass, the Unified-Strong-Electroweak coupling constant, and the Higgs mass, *Sania National Laboratory, Report SAND2000-2043* 1–11 (2000).
[7] Y. Dai, A.B. Borisov, K. Boyer, C.K. Rhodes, A p-Adic metric for particle mass scale organization with genetic divisors, *Sania National Laboratory, Report SAND2001-2903* 1–12 (2001).
[8] C. Ding, D. Pey, A. Saloma, *Chinese remainder Theorem: Applications in Computing, Coding, Cryptography, Singapore: World Scientific*, (1999).
[9] 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 1243–1253 (2009).
[10] M.A. Fiol, Finite Abelian groups and the Chinese remainder theorem, *Discrete Math* 67 101–105 (1987).
[11] L. Hars, Modular inverse algorithms without multiplications for cryptographic applications, *J Embedded Systems* 052192 1–13 (2006).
[12] D. E. Knuth, *The art of computer programming*, 2, Semi-Numerical Algorithms, 3rd Edition, Addison-Wesley, Reading, MA, (1997).
[13] W. H. Ko, Modular inverse and reciprocity formula, *arXiv:1304.6778v1* 1–7 (2013).
[14] R. Lôrencz, New algorithm for classical modular inverse, in Kaliski, B.S., Jr., Koç, C.K., and Paar, C. (Eds.):CHES 2002, LNCS Springer-Verlag Berlin 2003, 57–70.
[15] M. R. Schroeder, *Number theory and in Science and communication*, 3rd ed. Springer, Berlin (1997).
[16] R. J. Sullivan, *Microwave Radar Imaging and Advanced Concepts*, 2nd ed. Scitech Pub Inc. (2004).
[17] S. B. Verkhovsky, Enhanced Euclid algorithm for modular multiplicative inverse and its application in Cryptographic protocols, *Int. J. Communications, Network and System Sciences*, 3, p.p., 901–906 (2010).
[18] S. Wei, Computation of modular multiplicative inverse using residue signed-digit additions, *IEEE Conf. Pub :2016 International SoC Design Conference (ISOCC)* 85–86 (2016).