A TYPE OF A MAXIMUM COMMON FACTOR

By

Roxana M. Barrios-Rosales

A thesis submitted in partial fulfillment of the requirements for the degree of:

MASTER OF SCIENCES

in

PURE MATHEMATICS

UNIVERSITY OF PUERTO RICO
MAYAGÜEZ CAMPUS

2016

Approved by:

Gabriele Castellini, Ph.D Member, Graduate Committee	Date
Wieslaw Dziobiak, Ph.D Member, Graduate Committee	Date
Reyes M. Ortiz-Albino, Ph.D President, Graduate Committee	Date
Henrick M. Ierkic, Ph.D Representative of Graduate Studies	Date
Olgamary Rivera-Marrero, Ph.D Chairperson Department	Date

Resumen de Disertation Presentado a Escuela Graduada
de la Universidad de Puerto Rico como requisito parcial de los
Requerimientos para el grado de MASTER OF SCIENCES

A TYPE OF A MAXIMUM COMMON FACTOR

Por

Roxana M. Barrios-Rosales

2016

Consejero: Reyes M. Ortiz-Albino. Phd.
Departamento: Ciencias Matemáticas

Motivados por las factorizaciones en elementos comaximales Anderson y Frazier crearon el concepto de factorizaciones generalizadas o teoría de τ-factorizaciones sobre dominios integrales. Sea D un dominio integral, $U(D)$ es el conjunto de las unidades y τ una relación simétrica sobre el conjunto $D^{\#}$, el conjunto que consiste de los elementos distintos de cero que no son unidades en D. Un elemento $x \in D^{\#}$ tiene una τ-factorizacion, si $x = \lambda x_1 * * * x_n$, donde $\lambda \in U(D)$ y $x_i \tau x_j$ para todo $i \neq j$. También se dice que, x es un τ-producto de los $x_i's$, cada x_i es un τ-factor de x o x_i τ-divide a x. Un ejemplo que Frazier consideró fue la relación $\tau_{(n)}$ sobre $\mathbb{Z}^{\#}$ definida por $x_i \tau_{(n)} x_j$ si y solo si $x_i - x_j \in (n)$. Es importante reconocer que cuando $n \geq 2$, la relación $\tau_{(n)}$ coincide con la relación de equivalencia módulo n en $\mathbb{Z}^{\#}$. Con esta relación ella solo permitió que dos enteros se pudieran multiplicar si ambos estaban en la misma clase de equivalencia. Este nuevo producto resultó con nuevas interrogantes de teoría de números.

En 2008, Ortiz generalizó el concepto algebraico de máximo común divisor. En caso de que se considere la relación $\tau_{(n)}$, definimos d como el máximo $\tau_{(n)}$-factor en común de x y y, $\tau_{(n)}$-$GCD(x, y)$ si y solo si (1) d es un $\tau_{(n)}$-factor en común de x y y, y (2) si c es $\tau_{(n)}$-factor en común de x y y, c tiene que ser un $\tau_{(n)}$-factor de d. Resulta que la condición (2) es muy fuerte, la misma evitó que se garantizara la existencia del $\tau_{(n)}$-GCD. Ortiz en su tesis de doctorado dió varias ideas acerca de como debilitar la segunda condición. Una de ellas consistió en reemplazar la condición (2) por "si c es un $\tau_{(n)}$-factor en común de x y y, entonces $c \leq d$". Esta nueva versión Ortiz la denotó el $\tau_{(n)}$-MCD. La misma fue estudiada en el 2011 con Luna como parte de un proyecto de investigación subgraduada bajo la supervision de Ortiz. Ellos encontraron fórmulas para calcular el $\tau_{(n)}$-MCD, cuando $n \in \{0, 1, 2, 3, 4\}$. Este trabajo presenta una caracterización del $\tau_{(n)}$-MCD, cuando $n \in \{5, 6, 8, 10, 12\}$ y un algoritmo para calcular el $\tau_{(7)}$-MCD. Además, presenta algunas generalizaciones y algunas ideas de como continuar en los casos cuando $n \in \{9, 11, 13, 14, 15, \ldots\}$.

Abstract of Dissertation Presented to the Graduate School
of the University of Puerto Rico in Partial Fulfillment of the
Requirements for the Degree of Master of Sciences

A TYPE OF A MAXIMUM COMMON FACTOR

By

Roxana M. Barrios-Rosales

2016

Chair: Reyes M. Ortiz-Albino. Phd.
Major Department: Mathematical Sciences

Motivated by the comaximal factorizations Anderson and Frazier created the concept of generalized factorizations or the theory of τ-factorizations on integral domains. Let D be an integral domain and τ be a symmetric relation on the set $D^{\#}$, the set of nonzero nonunits elements in D. An element $x \in D^{\#}$ has a τ-factorization, if $x = \lambda x_1 * * * x_n$, where $\lambda \in U(D)$ and $x_i \tau x_j$ for any $i \neq j$. Also, x is called a τ-product of $x_i' s$, and each x_i is called a τ-factor of x (is to say that x_i τ-divide x). As an example, Frazier considered the relation $\tau_{(n)}$ on $\mathbb{Z}^{\#}$ defined by $x_i \tau_{(n)} x_j$ if and only if $x_i - x_j \in (n)$. It is important to recognize that the relation $\tau_{(n)}$ coincides with the equivalence relation modulo n, when $n \geq 2$. With this relation Frazier allowed to multiply two integers only when both of them are in the same equivalence class. The new product defined opened the doors to many number theory questions.

In 2008, Ortiz generalized the algebraic concept of the greatest common divisor in the theory of τ-factorizations. In case when considering the relation $\tau_{(n)}$, define d to be the greatest common $\tau_{(n)}$-factor ($\tau_{(n)}$-GCD) of x and y, if and only if (1) d is a common $\tau_{(n)}$-factor of x and y and (2) if c is a common $\tau_{(n)}$-factor of x and y, c

must be a $\tau_{(n)}$-factor of d. The condition (2) is very strong, the $\tau_{(n)}$-GCD does not exist in general. Ortiz in his dissertation gave several ideas about how to weaken the second condition. One of them, consisted in replacing (2) with "if c is a common $\tau_{(n)}$-factor of x and y, then $c \leq d$". This new version was denoted by $\tau_{(n)}$-MCD. It was studied in 2011 by Luna as an undergraduate research under Ortiz's supervision. They found formulas to compute the $\tau_{(n)}$-MCD, when $n \in \{0, 1, 2, 3, 4\}$. This work presents a characterization of $\tau_{(n)}$-MCD, when $n \in \{5, 6, 8, 10, 12\}$ and an algorithm to compute the $\tau_{(7)}$-MCD. Also, presents some generalizations and some ideas about how to continue in the cases when $n \in \{9, 11, 13, 14, 15, \ldots\}$.

To you, who I can not longer say goodbye.

To my parents and my brother, because they have taugth me the value of the sacrifice.

To you my Mor.

ACKNOWLEDGMENTS

First at all, I like thank God for allowed me to fulfill this dream. I like to thank a lot my parents Evangelina Rosales and Carlos Barrios-Leon; my brother Carlos Barrios-Rosales; and all my family in general for being there when I needed the most, for their support and for believing in me. Also, I like to thank my lovely husband Einstein Morales for his unconditional support, guidance, motivation and advices all this time.

I like to thank my advisor, Matiel, for accepting me as his master student. Thank you for his patience, dedication and support along this time in my career.

In a very special way, I like to thank all my friends. I will never forget all these memories that I share with all of you. You all make this way a very nice experience and full of joy. I will not mention any one in particular, because you know who I am talking about.

Contents

page

RESUMEN EN ESPAÑOL iii

ABSTRACT ENGLISH v

ACKNOWLEDGMENTS ix

LIST OF TABLES xi

LIST OF SYMBOLS xii

1 Introduction 1

1.1 Chapters summary 6

2 Theorical concepts 7

2.1 Notions in number theory 7

2.2 The $\tau_{(n)}$-factorizations 13

2.2.2 On common $\tau_{(n)}$-factors 15

2.2.5 Associated-preserving extension of $\tau_{(n)}$. 18

2.2.6 The $\tau_{(n)}$-$MCD(x, y)$ for $n \in \{0, 1, 2, 3, 4\}$ 19

3 The $\tau_{(n)}$-MCD when $n \in \{5, 6, 8, 10, 12\}$ 21

3.1 The $\tau_{(6)}$-MCD 21

3.2 The $\tau_{(n)}$-MCD when $\phi(n) = 4$ 25

3.2.1 The $\tau_{(5)}$-MCD 25

3.2.2 The $\tau_{(8)}$-MCD 30

3.2.3 The $\tau_{(10)}$-MCD 36

3.2.4 The $\tau_{(12)}$-MCD 46

4 About $\tau_{(n)}$-MCD when $\phi(n) = 6$ and some generalizations 54

4.1 On the $\tau_{(7)}$-MCD 54

4.2 Some generalizations 68

4.3 About the $\tau_{(n)}$-MCD when $\phi(n) = 6$. 74

5 Conclusions and future works 76

5.1 Conclusions 76

5.2 Future works 78

LIST OF TABLES

Table | Page

2–1 The form of the non-irreducible $\tau_{(n)}$-atoms for $n \in \{0, 2, 3, 4, 5, 6\}$ . . . 15

2–2 The $\tau_{(n)}$-$MCD(x, y)$, for $n \in \{0, 1, 2, 3, 4\}$. 20

3–1 The $\tau_{(6)}$-MCD 24

3–2 The $\tau_{(5)}$-$MCD(x, y)$. 29

3–3 Class options for $2 \cdot d_1$ and $2 \cdot x''$ 31

3–4 Class options for $2^2 \cdot d_1$ and $2^2 \cdot x''$ 32

3–5 The $\tau_{(8)}$-MCD for numbers in $[0]_{(8)}$ 35

3–6 The $\tau_{(8)}$-MCD for numbers in $[\pm b]_{(8)}$ where $b \in \{1, 3\}$ 35

3–7 The $\tau_{(10)}$-MCD for numbers in $[0]_{(10)}$ and $[\pm 5]_{(10)}$ 44

3–8 The $\tau_{(10)}$-MCD when $(x, y) \in [\pm 2]_{(10)} \times ([\pm 2]_{(10)} \cup [\pm 4]_{(10)})$ 45

3–9 The $\tau_{(12)}$-MCD for numbers in $[0]_{(12)}$ 53

3–10 The $\tau_{(12)}$-MCD when $(x, y) \in [\pm b]_{(10)}$ for $b \in \{4, 3\}$ 53

LIST OF SYMBOLS

R	Commutative ring.
D	Integral domain.
D^*	The set of nonzero elements of D.
$D^{\#}$	Set of the nonunit nonzero elemens of D.
$U(D)$	Set of units of D.
λ	Unit on D.
τ	Symetric relation.
$a\tau b$	a is τ related with b.
$a\|_{\tau}b$	a τ-divides b.
$\mathbb{N}$	Natural numbers.
$\mathbb{Z}$	The set of integers.
$\mathbb{Z}^+$	The set of positive integers.
GCD	Greatest common divisor.
MCD	Maximum common divisor.
ϕ	The Euler's function ϕ.
$\equiv$	The Congruence relation $mod\, n$.
$*$	The τ-product symbol.
$\cdot$	The usual multiplication symbol.
$a_1 \cdots a_n$	The usual product of the indexed set $a_1, a_2, \ldots, a_n$.
$a_1 * * * a_n$	The τ-product of the indexed set $a_1, a_2, \ldots, a_n$.
(n)	The principal ideal generated by n.
$[a]_{(n)}$	The equivalence class of the integer a under the relation $(mod\, n)$.
$[a]_{\tau_{(n)}}$	The equivalence class of the integer a under the relation $\tau_{(n)}$.
$[\pm a]_{(n)}$	The equivalence class of the integer a under the relation $\tau'_{(n)}$.

Chapter 1
Introduction

The concept of the greatest common divisor (GCD) is also known as the greatest common factor (GCF). During the ancient greek's times, it was called greatest common measure (GCM), because it was used to find the length of a segment of greatest common measure between two line segments. This concept has been important due to the theoretical applications like the Bezout identity, the existence of Diophantine equations among others. To compute the GCD between two integers there are several ways but the most known is the Euclidean algorithm.

Let a and b be integers with $a \neq 0$. It is said that a divides b (denoted by $a|b$), if there exist an integer c such that $b = ac$. In such cases, a is called a divisor of b and b divisible by a. If no such c exists, then a does not divide b and denoted by $a \nmid b$. Let $x, y \in \mathbb{Z}^*$ (the set nonzero integers). Then there are two equivalent statement that define the GCD.

1. We say that $d \in \mathbb{Z}^*$ is the GCD of x and y, if d is a common divisor of x and y and for any other common divisor c of x and y, $c \leq d$.

2. We say that $d \in \mathbb{N}$ is the GCD of x and y if d is a common divisor of x and y and for any common divisor c of x and y, $c|d$.

The assumption of d being a natural number is necessary in the second definition in order to both definitions be equivalent. Otherwise, the opposite of d is a potential integer to be a GCD in the second statement and the staments will not be equivalent.

Abstract algebra came as a reaction of number theory. It generalized the concept of divisibility and the GCD on an integral domain D. For the definition of divisibility, just replace the word "integer" with "element" and "$d \in \mathbb{N}$" with "$d \in D^*$" (the set of nonzero elements) in the second statement of the definition of the GCD. The algebraic definition of the GCD obtained in this way is not unique, due to the previous observation, that any associate of d (λd, where $\lambda \in U(D)$, the set of multiplicative invertible elements of the integral domain D) satisfies the GCD definition. Hence, it is unique up to associates or in the quotient structure $D^*/U(D)$. Since our work is based on an unusual multiplication let us introduced basics concepts on factorizations and this new product.

The theory of factorizations of nonzero nonunit elements of an integral domain D into a product of irreducible elements has been widely studied. Lately, there is a great interest of the study of factorizations into elements that need not to be irreducible. For example, Mcadam and Swan [8] studied factorizations in terms of comaximal elements, that is, elements that their respective principal ideals are pairwise comaximal. Such definition motivated Anderson and Frazier [1] to create the concept of the theory of τ-factorizations. Let D be an integral domain D and τ be a symmetric relation on $D^{\#}$ (the set of nonzero nonunit elements of D). An $x \in D^{\#}$ has a τ-factorization, if $x = \lambda x_1 * * * x_n$, where $\lambda \in U(D)$ and $x_i \tau x_j$ for all $i \neq j$. We also say that x is the τ-product of x_i and each x_i is a τ-factor of x. Here $x * y$ means the product of x and y in D which emphasizes the fact that x and y are

τ-related, i.e. $x\tau y$; and $x \cdot y$ means the usual product of x and y in D. We also consider $x = x$ and $x = \lambda(\lambda^{-1}x)$ both to be (vacuously) τ-factorizations. These two τ-factorizations are known as the trivial ones.

This type of factorization generalized all the known factorizations. To see this, let $S \subset D^{\#}$ a desire set of elements. Define $\tau = S \times S$, then the τ-factorizations are the product of elements in S. As an example Anderson and Frazier [1] consider the integral domain $\mathbb{Z}$ and the equivalence relation $\tau_{(n)}$ defined by $x_i\tau_{(n)}x_j$ if and only if $n|x_i - x_j$. Formally, an $x \in \mathbb{Z}^{\#}(= \mathbb{Z} - \{0, \pm 1\})$ has a $\tau_{(n)}$-factorization, if $x = \pm x_1 * x_2 * * * x_n$, where $x_i\tau_{(n)}x_j$ for all $i \neq j$. Since $U(\mathbb{Z}) = \{\pm 1\}$, instead λ, we will use the "±" sign in the front of the definition of $\tau_{(n)}$-factorization.

Hamon in [4] characterized the $\tau_{(n)}$-products or the $\tau_{(n)}$-factorizations as special case of the τ_J-factorizations where τ_J is defined by $x\tau_J y$ if and only if $x - y \in J$ and J is a proper ideal of D. That is, Hamon considered J to be the principal ideal (n) on the integer domain $\mathbb{Z}$. Hamon identified the $\tau_{(n)}$-atoms (integers with no non-trivial $\tau_{(n)}$-factorizations) for $n \in \{0, 1, 2, 3, 4, 5, 6\}$. The work done by Hamon [4] and Juett [5] showed that every nonzero nonunit integer can be written as a $\tau_{(n)}$-product of $\tau_{(n)}$-atoms, when $n \in \{0, 1, 2, 3, 4, 5, 6, 8, 10\}$. The reader must notice that, the existence of such type of $\tau_{(n)}$-factorizations does not guarantee that such $\tau_{(n)}$-factorizations are unique. In fact, they are not unique. Hence, the theory of $\tau_{(n)}$-factorizations is a little bit more complicated than it seems.

In 2008, Ortiz [9] generalized the definition of the greatest common divisor using the concept of $\tau_{(n)}$-divisibility, defined as follows: x $\tau_{(n)}$-divides y if and only if x is a $\tau_{(n)}$-factor of y. In such case, we write "$x|_{(\tau_{(n)})}y$", otherwise we write "$x \nmid_{(\tau_{(n)})} y$" (meaning x is not a $\tau_{(n)}$-factor of y or x does not $\tau_{(n)}$-divide y). He gave different definitions of GCD with respect to the theory of $\tau_{(n)}$-factorizations. First let see what he called the algebraic definition of the $\tau_{(n)}$-GCD. A positive number is called the greatest common $\tau_{(n)}$-factor of x and y (denoted by $\tau_{(n)}$-$GCD(x, y)$) if d satisfies two conditions: (1) d is a common $\tau_{(n)}$-factor of x and y, and (2) if c is a common $\tau_{(n)}$-factor of x and y, then $c|_{\tau_{(n)}}d$. However, the second condition turns out to be very strong. In general the $\tau_{(n)}$-GCD of two elements does not necessarily exist. Ortiz in his dissertation [9], presented different ideas to weaken the second condition. One of them is to compute the largest common $\tau_{(n)}$-factor. This is done by replacing the second condition on the definition of the $\tau_{(n)}$-GCD with "for any common $\tau_{(n)}$-factor c, of x and y, $c \leq d$". Since the set of integers $\mathbb{Z}$ is a total by ordered set, this definition makes sense and this will guarantee the existence of it. In 2011, Ortiz and Luna [7] studied this new definition and they called it the maximum common $\tau_{(n)}$-factor and was denoted by $\tau_{(n)}$-MCD. They found formulas of the $\tau_{(n)}$-MCD for $n \in \{0, 1, 2, 3, 4\}$. They also tried the case $n = 5$, but the techniques used in the previous cases did not work for the case $n = 5$. New methods were necessary to find the formulas of the $\tau_{(5)}$-MCD. They also gave an algorithm for finding the $\tau_{(n)}$-MCD, which consists in listing all the common factors, which are bound by the GCD. Then checking for the largest $\tau_{(n)}$-factor such $\tau_{(n)}$-factor will be the $\tau_{(n)}$-MCD. The process gave the existence of maximum common factor $\tau_{(n)}$-MCD for any n, but no other formulas were given.

This work presents a characterization of the maximum common $\tau_{(n)}$-factor when $n \in \{5, 6, 7, 8, 10, 12\}$ and some generalizations. One of the techniques used in this study is the work done by Serna [10] about the relation $\tau'_{(n)} = \{(\pm x, \pm y) : x\tau_{(n)}y\}$, that is an associative preserving extension of $\tau_{(n)}$. At the beginning, we use a code written in Sagemath to find the patterns. The patterns showed that the complexity of the computation depends on the known Euler's ϕ-function or Euler's number.

Since the Euler's number gives the number of relative prime elements, which determine how the primes of the prime factorization of an integer are distributed. Serna's technique helps us to reduce the amount of sets in which the primes are distributed. In the case when $n = 7$ we do not give a formula, but we present a procedure of logical steps or algorithms which help us to compute the $\tau_{(n)}$-MCD in an easier way than the way of looking for common $\tau_{(n)}$-factors.

1.1 Chapters summary

This work is about finding formulas of the $\tau_{(n)}$-MCD. In the second chapter, the reader can find some notions in number theory, which are useful for our work. Also, there is an introduction to the $\tau_{(n)}$-factorizations theory, the characterizations done for the $\tau_{(n)}$-atoms when $n \in \{0, \ldots, 6\}$. Also, the results of a study of the $\tau_{(n)}$-GCD and $\tau_{(n)}$-MCD. The notion and details of the associate-preserving extension $\tau'_{(n)}$ of the relation $\tau_{(n)}$ presented in [10] and its relevance in this work.

The third chapter gives a characterization of formulas for the $\tau_{(n)}$-MCD, when $n \in \{5, 6, 8, 10, 12\}$. First we present the case of $n = 6$, because most of the primes are in two sets. Then the rest of the cases in order, which coincide with the order of the complexity of the formulas and calculations.

The fourth chapter presents other contributions. The first one is the study of the $\tau_{(7)}$-MCD. This case is more difficult than the cases in Chapter 4, because $\phi(7) = 6$. This means that all the primes, except 7, are distributed in 6 distinct set (or 3 distinct set if using Serna's work). We provide some algorithms to find the $\tau_{(7)}$-MCD. Also, there are some generalizations found to compute the $\tau_{(n)}$-MCD for elements in $[0]_{(n)}$, in $[\pm 1]_{(n)}$ and the classes $[\pm m]_{(qm)}$, where q is a divisor of 6. There is a suggestion of how to use the results of the $\tau_{(7)}$-MCD to find the $\tau_{(n)}$-MCD when $n \in \{9, 14, 18\}$.

Finally in Chapter 5, the reader can find our conclusions and future works.

Chapter 2
Theorical concepts

Number theory has been very important for the development of mathematics, topics like divisibility and factorization of an integer. This chapter introduces a few definitions, the fundamental theorem of arithmetic and other important properties needed for our work. We divide this chapter in two sections, the first one talks properties of the integers and the second about $\tau_{(n)}$-factorizations.

2.1 Notions in number theory

In this section we summarized the definitions of divisibility, GCD and theorems that are needed in this work. First let us formalize the definition of a factor in $\mathbb{Z}$.

Definition 2.1.1. *[6] Let a and b are integers, with $a \neq 0$. It is said that a divides b (denoted by $a|b$), if there exist an integer c such that $b = ac$. If no such c exists, then it is said that a does not divide b (denoted by $a \nmid b$). If a divides b, then a is called a divisor or a factor of b, and b is divisible by a.*

It is well known that "$|$" is a partial ordered relation on $\mathbb{N}$. But on $\mathbb{Z}$ we loose the antisymmetric property. That is, if $a|b$ and $b|a$, then $a = \pm b$ (not exactly b). In abstract algebra this happens when a and b are associates (equivalently the principal ideals generated by a and b are equal).

A positive integer whose only positive divisors are 1 and itself is called a positive prime. On $\mathbb{Z}$, a prime p is a nonzero nonunit integer that is divisible by ± 1, $\pm p$. For this reason, we will always write positive prime to refer the usual natural primes. The following theorem is called the Fundamental Theorem of Arithmetic which says that any nonzero nonunit positive integer is either a positive prime or a product of positive primes. As atoms in chemistry, the positive primes are known as the building blocks of the natural numbers and hence the integers.

Theorem 1. *[6]* **Fundamental Theorem of Arithmetic.** *Every positive integer greater than 1 can be factored uniquely (up to order) as a product of positive primes.*

A consequence of the fundamental theorem of arithmetic is the canonical factorization of a natural (integer) number x. Since x can be written uniquely as the product of positive primes, $x = p_1 \cdots p_k$ (respectively, $x = \pm p_1 \cdots p_k$), by putting together the primes that are equal (respectively, that have the same absolute value) we could rewrite x as $\prod\limits_{i=1}^{r} p_i^{a_i}$ (respectively $\pm \prod\limits_{i=1}^{r} p_i^{a_i}$), where a_i is the number of times p_i appears in the prime factorization. This form or expression is more known as the product of power primes or the canonical factorization.

The fundamental theorem of arithmetic and the canonical factorization gives a way to find all divisors of a natural (integer) number. For example if we consider the number $30 = 2 \cdot 3 \cdot 5$, then $1, 2, 3, 5, 6, 10, 15, 30$ are all the divisors of 30. In general, if $x = p_1^{a_1} \cdots p_k^{a_k}$, the divisors of x are of the form $p_1^{b_1} \cdots p_k^{b_k}$ where each $0 \leq b_k \leq a_k$. Several algebraist have studied many type of factors. Among them, the maximum or greatest common factor (or divisor) of any two integers (not both zero).

Definition 2.1.2. Greatest common divisor *[6] The greatest common divisor (GCD) of two numbers a and b, not both zero, is the largest integer dividing both a and b. It will be denoted by $GCD(a, b)$.*

When the GCD between two integers is equal to 1, the numbers are called coprime or relatively primes. A way for computing their GCD between two nonzero integers is using their canonical factorizations, by taking the product of the common prime factors to the minimum exponent that appears in the cannonical factorizations of the integers of interest. That is, if $x = p_1^{n_1} \cdots p_k^{n_k}$ and $y = p_1^{m_1} \cdots p_k^{m_k}$, then any common factor c of x and y, must have the form $c = p_1^{l_1} \cdots p_k^{l_k}$ where we have that $0 \leq l_i \leq min\{n_i, m_i\}$ for $1 \leq i \leq k$. For example, let $x = 720$ and $y = 945$. Their canonical factorizations are $x = 2^4 \cdot 3^2 \cdot 5$, $y = 3^3 \cdot 5 \cdot 7$. The common prime factors are 3 and 5 (the minimum exponent are 2 and 1, respectively). Obtain $3^2 \cdot 5 = 45$ is the greatest common divisor between 720 and 945.

If very large numbers without their canonical factorizations are considered last technique is not appropriated. For these cases, it is better to use the Euclidean algorithm, which can be found in [6]. Now we introduce the definition of congruence modulo m.

Definition 2.1.3. *[6] If a, b and m are integers, we say that a is congruent to b modulo m (denoted by $a \equiv b \,(mod\, m)$) if $m|a-b$. If $m \nmid a-b$, we write $a \not\equiv b \,(mod\, m)$ and say that a is not congruent, or incongruent to b modulo m.*

The reader can notice that, the relation modulo m is an equivalence relation on $\mathbb{Z}$. The relation modulo m partitions the set of integers into m equivalence classes, the set of equivalence classes is denoted by $\mathbb{Z}/m\mathbb{Z} = \{[a]_{(m)} : 0 \leq a \leq m-1\}$, where $a \in \mathbb{Z}$ and $[a]_{(m)} = \{r \in \mathbb{Z} : r \equiv a \, (mod \, m)\}$.

Algebraically, $\mathbb{Z}/m\mathbb{Z}$ is a commutative ring with identity, with the operations defined by $[a]_{(m)} + [b]_{(m)} = [a+b]_{(m)}$ and $[a]_{(m)} \cdot [b]_{(m)} = [ab]_{(m)}$. The set $\mathbb{Z}/m\mathbb{Z}$, also known as the set of residues modulo m, have many other properties. In this document, we will cite several results, some with their respective proofs, needed for our purpose.

Proposition 1. *[6] Let a, b, c, m integers where $m \geq 2$ and $k > 0$. If $GCD(c, m)$ is different of m, then the following holds.*

i. If $a \cdot c \equiv b \cdot c \, (mod \, m)$ implies that $a \equiv b \left(mod \, \frac{m}{GCD(c,m)} \right)$.

ii. If $a \equiv b \, (mod \, m)$, then $a^k \equiv b^k \, (mod \, m)$, for any $k \in \mathbb{N}$.

Proof. For part $(i.)$, assume $d = GCD(c, m)$. Then $c = dc'$ and $m = dm'$. Notice that it holds $dm'|c(a-b) = dc'(a-b)$, thus $m'|c'(a-b)$. Since m' and c' have no factors in common, $m'|a-b$, that is, $a \equiv b \left(mod \, \frac{m}{GCD(c,m)} \right)$. The proof for $(ii.)$ follows using that $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1})$, hence $(a-b)|(a^k - b^k)$ and by transitivity $m|(a^k - b^k)$, then $a^k \equiv b^k \, (mod \, m)$. □

Theorem 2. (Fermat's Little Theorem.) *[6] Let p be a positive prime. Then $a^p \equiv a \, (mod \, p)$ for all integers a. In particular, if $p \nmid a$, then $a^{p-1} \equiv 1 \, (mod \, p)$.*

Theorem (2) was proposed by Fermat 1640. In a letter from Fermat to his friend Frenicle, but Fermat admitted that he could not write the demonstration, because there was not enough space on the paper to write the proof. However, in 1736, Euler did the proof of the "Fermat's Little Theorem" using the notation of modular congruence. The proof of the theorem follows by induction and the Binomial theorem. We recommend [6] for more details about the proof.

Definition 2.1.4. *[6] A number a' is called the multiplicative inverse of a modulo m if $aa' \equiv 1 (mod\, m)$. And, we say a is invertible modulo m if it has an inverse. The inverse of a will be denoted by $a^{-1} (mod\, m)$.*

By Theorem (2) and Proposition (2.1), if $p \nmid a$, then the inverse of $a\, (mod\, p)$ exists. In fact, an integer a is invertible modulo m if and only if $GCD(a, m) = 1$. Moreover, if a has an inverse, then it is unique modulo m. As an example, the inverse of 3 modulo 10 is 7, because $3 \cdot 7 \equiv 21 \equiv 1\, (mod\, 10)$.

Definition 2.1.5. *[6] The cardinality of the set of invertible elements in $\mathbb{Z}/m\mathbb{Z}$ is denoted by $\phi(m)$, where ϕ is called Euler's Totient function or ϕ-function, and $\phi(m)$ the Euler number of m.*

The Euler's Totient function ϕ function is a multiplicative function that is, if $GCD(n, m) = 1$, then $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$. This property allows us to compute the Euler number for any positive integer. First, notice that if p is a positive prime $n \geq 1$, then $\phi(p^n) = p^n - p^{n-1} = p^n \left(1 - \frac{1}{p}\right)$. First suppose $n = 1$. Since p is prime, if a is a number such that $1 \leq a \leq p - 1$, then $GCD(a, p) = 1$. Hence, $\phi(p) = p - 1$. Now, if $n \neq 1$, it is necessary to consider the number of multiples of p which are less than p^n, it is $\lfloor \frac{p^n}{p} \rfloor = \lfloor p^{n-1} \rfloor$. Thus, $\phi(p^n) = p^n - p^{n-1} = p^n \left(1 - \frac{1}{p}\right)$. Now, if $m = p_1^{a_1} \cdots p_k^{a_k}$ is the canonical factorization of m, then we have that $\phi(m)$ is $\prod_{i=1}^{k} \phi(p_i^{a_i}) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$. Euler theorem and its consequences will help in the calculations. Hence we include Euler Theorem as Theorem (2.1.5).

Theorem 3. *(Euler) [6] If a and m are integers such that $GCD(a, m) = 1$, then $a^{\phi(m)} \equiv 1\,(mod\,m)$.*

Proof. Let $(a, m) = 1$, and let $r_1, \ldots, r_{\phi(m)}$ be the invertible elements in the residue system $mod\,m$. Then $ar_1, \ldots, ar_{\phi(m)}$ are all invertible, no two of which are congruent modulo m. Therefore, $(ar_1)(ar_2)\cdots(ar_{\phi(m)}) \equiv r_1 r_2 \cdots r_{\phi(m)}\,(mod\,m)$ or, by rearranging the terms is obtained $a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)}\,(mod\,m)$ which, by Proposition (i), implies that $a^{\phi(m)} \equiv 1\,(mod\,m)$.

□

This theorems summarize the basic concepts and tools needed to do most of the calculations of the $\tau_{(n)}$-factors and $\tau_{(n)}$-MCD which will be formally define in the following sections.

2.2 The $\tau_{(n)}$-factorizations

In this section we introduce the notion of $\tau_{(n)}$-factorizations studied in [1, 4] and some properties with respect to the relation $\tau_{(n)}$ on $\mathbb{Z}^{\#}$. Formally, we defined (as in [1, 4]) $\tau_{(n)}$ by $x\tau_{(n)}y$ if and only if $x - y \in (n)$; where (n) is the principal ideal generated by (n) on $\mathbb{Z}$. We assume that $\tau_{(n)}$ is a relation on $\mathbb{Z}^{\#}$ and not on $\mathbb{Z}$. Such assumption was made in [1]. Notice that $\tau_{(n)}$ expanded on $\mathbb{Z}$ coincides with the relation modulo n (for any $n \geq 2$).

Let us recall the fact $\tau_{(n)}$ is an equivalence relation on $\mathbb{Z}^{\#}$, hence it partitions $\mathbb{Z}^{\#}$. We denote the equivalence class of $a \in \mathbb{Z}^{\#}$ by $[a]_{\tau_{(n)}} = \{b \in \mathbb{Z}^{\#} : a\tau_{(n)}b\}$. Notice that $\{\pm 1, 0\} \nsubseteq \mathbb{Z}^{\#}$, hence formally $[0]_{\tau_{(n)}}$, $[1]_{\tau_{(n)}}$ and $[-1]_{\tau_{(n)}}$ do not exist. For simplicity, $[0]_{\tau_{(n)}}$ (respectively $[1]_{\tau_{(n)}}$ and $[-1]_{\tau_{(n)}}$) will represent the formal equivalence class of $[n]_{\tau_{(n)}}$ (respectively $[n+1]_{\tau_{(n)}}$ and $[n-1]_{\tau_{(n)}}$). And must be clear that $0 \notin [0]_{\tau_{(n)}}$ (respectively $1 \notin [1]_{\tau_{(n)}}$ and $-1 \notin [-1]_{\tau_{(n)}}$), because $0 \notin \mathbb{Z}^{\#}$ (respectively $\pm 1 \notin \mathbb{Z}^{\#}$).

Definition 2.2.1. *($\tau_{(n)}$-factorization.) An element $x \in \mathbb{Z}^{\#}$ has a $\tau_{(n)}$-factorization if $x = \pm x_1 * * * x_m$ and $x_i \tau_{(n)} x_j$ for all $i \neq j$.*

The product $\pm x_1 * * * x_m$ in Definition (2.2.1) is also called a $\tau_{(n)}$-product of the $x_i's$. Each x_i is called a $\tau_{(n)}$-factor of x, and we say that x_i τ-divides x and write $x_i|_{\tau_{(n)}}x$. The expressions of the form $x = x$ or $x = -(-x)$ are $\tau_{(n)}$-factorizations vacuous. They are called as the trivial $\tau_{(n)}$-factorizations of x. Notice that, if $\tau_{(n)}$ was defined on $\mathbb{Z}$, then the definition of a $\tau_{(n)}$-factorization needs the assumption that each x_i is in $\mathbb{Z}^{\#}$. Otherwise the $\tau_{(n)}$-factorization will not make sense, because one could write an infinitive product of 1 and -1.

For $n = 0$, $a\tau_{(0)}b$, if and only if $a - b \in (0)$, which implies that $a = b$. If $x = x_1 * * * x_k$, is a $\tau_{(0)}$-product of x, then each $x_i = x_j$. Thus the $\tau_{(0)}$-factorizations of x are of the form $\pm c^m$. If $x = 144 = 2^4 \cdot 3^2$, then $x = (2^2 \cdot 3) * (2^2 \cdot 3) = (2^2 \cdot 3)^2$ is a $\tau_{(0)}$-factorization of x. If $n = 1$, and $a\tau_{(1)}b$, then $a - b \in (1)$, thus $1|a - b$. Hence, the $\tau_{(1)}$-factorizations coincide with the usual factorizations. For $n = 2$, $a * b$ is a $\tau_{(2)}$-product if and only if a and b both are even or both are odd (that is $a, b \in [0]_{(2)}$ or $a, b \in [1]_{(2)}$). The $\tau_{(n)}$-products for $n \geq 3$ do not have another friendly and equivalent definition, other than its formal definition.

If an integer does not have any nontrivial $\tau_{(n)}$-factorizations, then such integer acts as a prime integer with respect to the $\tau_{(n)}$-products. Those integer are called $\tau_{(n)}$-atoms. In [4], the author characterized the $\tau_{(n)}$-atoms when $n \in \{0, 2, 4, 5, 6\}$. The main results of Hamon's work includes a characterization of when every nonzero nonunit integer can be written as a $\tau_{(n)}$-product of $\tau_{(n)}$-atoms. Hamon ruled out most of the integers n (for which $\mathbb{Z}$ is not $\tau_{(n)}$-atomic) by using Dirichelt's Theorem of infinite sequence of primes. Later, Hamon eliminated case by case until the list of integers was reduced to $n \in \{0, 1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Several years later, Juett [5] (Example 4.1.4), gave a counterexample showing that $\mathbb{Z}$ is not $\tau_{(12)}$-atomic. Hence it is very reasonable to first focus on studying the concepts of $\tau_{(n)}$-factors, when $\mathbb{Z}$ is $\tau_{(n)}$-atomic, that is, $n \in \{0, 1, 2, 3, 4, 5, 6, 8, 10\}$.

Table (2–1) contains a summary or characterizations, done by Hamon [4] of the nonprime (which are of course $\tau_{(n)}$-atoms) $\tau_{(n)}$-atoms when $n \in \{0, 2, 4, 5, 6\}$. Observe that the usual primes $p_1, \cdots p_k$ are $\tau_{(n)}$-atoms.

Table 2–1: The form of the non-irreducible $\tau_{(n)}$-atoms for $n \in \{0, 2, 3, 4, 5, 6\}$

n	$\tau_{(n)}$-atom
0	$\pm p_1^{a_1} \cdots p_k^{a_k}$, $a_i \geq 1$ and $GCD(a_1, \ldots, a_k) = 1$
2	$x = 2t$, where $2 \nmid t$
3	$x = 3t$, where $3 \nmid t$
4	$x = 2t$, where $2 \nmid t$
5	$x = 5t$, where $5 \nmid t$, $\pm p_1 p_2 \cdots p_m$, $p_i \neq 5$,$p_1 \equiv \pm 2\,(mod\,5)$ and $p_1 \equiv \pm 1\,(mod\,5)$ for all $j > 1$.
6	$x = at$, where $a \in \{2, 3\}$ and $a \nmid t$.

In Table (2–1), each p_i denotes a positive prime, $a_i \in \mathbb{N}$, and $t \in \mathbb{Z}^{\#}$. Hamon also gave sufficient conditions for an integer to be a $\tau_{(n)}$-atom for n in general.

Lemma 1. *[2] Let $a \in \mathbb{Z}^{\#}$ and $p_1, \ldots, p_m$ be positive primes, then:*

i. If a is a $\tau_{(n)}$-atom where $a \not\equiv \pm 1\,(mod\,n)$, then $ap_1 \cdots p_m$ is also a $\tau_{(n)}$-atom where p_i are not necessarily distinct positive primes satisfying $p_i \equiv \pm 1\,(mod\,n)$.

ii. If $p_i \not\equiv \pm p_j\,(mod\,n)$, then $\pm p_i p_j$ is a $\tau_{(n)}$-atom.

iii. Numbers of the form $ap_1 \cdots p_m q$ with $p_i \equiv \pm 1\,(mod\,n)$, $a \not\equiv p_i\,(mod\,n)$, and $\pm ap_1 \cdots p_t \not\equiv q\,(mod\,n)$ are $\tau_{(n)}$-atoms.

2.2.2 On common $\tau_{(n)}$-factors

From the point of view of number theory there are a lot of questions of which results can be extended to this theory of the $\tau_{(n)}$-products. One of them is the concept of $\tau_{(n)}$-common factors. It is clear that any common $\tau_{(n)}$-factor is a factor, hence the canonical factorization helps to recognized the form of the common $\tau_{(n)}$-factors (by looking the form as a factor). That is, if c is a common $\tau_{(n)}$-factor of $x = p_1^{n_1} \cdots p_k^{n_k}$ and $y = p_1^{m_1} \cdots p_k^{m_k}$, then c must have the form $c = p_1^{l_1} \cdots p_k^{l_k}$ with $0 \leq l_i \leq min\{n_i, m_i\}$ for $1 \leq k$ (but not all zeros). This does not imply that $p_1^{l_1} \cdots p_k^{l_k}$ is a $\tau_{(n)}$-factorization, but it does it inherites the form as a factor.

Motivated by the common $\tau_{(n)}$-factors Ortiz [9] developed the greatest common $\tau_{(n)}$-divisor.

Definition 2.2.3. *[9] Let $d \in \mathbb{Z}^{\#}$. Then d is called the greatest common $\tau_{(n)}$-factor of x and y (denoted by $\tau_{(n)}$-$GCD(x,y)$), if* (1) *$d|_{\tau_{(n)}}x$, $d|_{\tau_{(n)}}y$ and* (2) *if there is a c such that $c|_{\tau_{(n)}}x$ and $c|_{\tau_{(n)}}y$, then $c|_{\tau_{(n)}}d$. If x and y do not have a common $\tau_{(n)}$-factor, as a convention, we denote the $\tau_{(n)}$-$GCD(x,y) = 1$.*

For example, let $x = 16$ and $y = 48$. Then, $x = 16 = 8 * 2 = 4 * 4 = 2 * 2 * 2 * 2$ and $y = 8 * 6 = 12 * 4 = 12 * 2 * 2$ are the $\tau_{(2)}$-factorizations of x and y, respectively. Observe that 8, 4 and 2 are $\tau_{(2)}$-factors of x and y, and $8 = 4 * 2$ (therefore $4|_{\tau_{(2)}}8$ and $2|_{\tau_{(2)}}8$) which forces 8 to be the $\tau_{(n)}$-$GCD(16, 48)$. Unfortunately, in [9], Ortiz proved that the $\tau_{(n)}$-GCD of any two nonzero nonunit integers does not always exist. For example, let $x = 24 = 2^3 \cdot 3$ and $y = 36 = 3^2 \cdot 2^2$. Notice that, $x = 6 * 4 = 2 * 12$ and $y = 36 = 6 * 6 = 2 * 18$. The set of common $\tau_{(2)}$-factors is $\{6, 2\}$. But $6 \nmid_{\tau_{(2)}} 2$ and $2 \nmid_{\tau_{(2)}} 6$, then $\tau_{(2)}$-$GCD(x,y)$ does not exist. This says that the second condition in Definition (2.2.3) is very strong. Ortiz in [9] in his dissertation suggested to weaken it. The new definition considers to select the largest common $\tau_{(n)}$-factor, by using an order relation as in the following definition.

Definition 2.2.4. *[9] Let $d \in \mathbb{Z}^{\#}$, d is the $\tau_{(n)}$-$MCD(x,y)$ if* (1) *$d|_{\tau_{(n)}}x$, $d|_{\tau_{(n)}}y$ and* (2) *if $c|_{\tau_{(n)}}x$ and $c|_{\tau_{(n)}}y$, then $c \leq d$. If there is no common $\tau_{(n)}$-factor of x and y, as a convention we will denote the $\tau_{(n)}$-$MCD(x,y) = 1$.*

With this definition he obtained the existence of the $\tau_{(n)}$-$MCD(x,y)$ in $\mathbb{Z}^{\#}$ for all n. Luna and Ortiz [7] gave a proof of it, but we formalize their idea in the following theorem.

Theorem 4. *If $x, y \in \mathbb{Z}^{\#}$, $\tau_{(n)}$-$MCD(x,y)$ exist for all n.*

Proof. Let $D(x,y) = \{d_i : d_i|x \text{ and } d_i|y\}$ be, the set of the common divisor of x and y and denote $D_{(n)}(x,y) = \{d_i \in \mathbb{Z}^* : d_i|_{\tau_{(n)}}x \text{ and } d_i|_{\tau_{(n)}}y\}$ the set of common $\tau_{(n)}$-factors of x and y. If $D_{(n)}(x,y) = \emptyset$, then is denoted the $\tau_{(n)}$-$MCD(x,y) = 1$. If $D_{(n)}(x,y) \neq \emptyset$, $|D_{(n)}(x,y)| \leq |D(x,y)| < \infty$. Since $\mathbb{Z}$ is well ordered and $D_{(n)}(x,y)$ is finite, $D_{(n)}(x,y)$ has a maximum element. □

In the previous example, the reader may notice that the $\tau_{(2)}$-$MCD(24,36) = 6$, because $D_{(2)}(24,36) = \{1,2,6\}$ and 6 is the maximum in the set of the common $\tau_{(2)}$-factors of 24 and 36. Until now, we have used the canonical factorization of integers to provide examples of common $\tau_{(n)}$-product. Unfortunately to figure out a formula for the $\tau_{(n)}$-factors, we require to understand the behavior of the $\tau_{(n)}$-factors and look for patterns. For this, we wrote a program in sage (computer package for symbolic computation), to helps us to analyze the patterns. An observation from this patterns is that most of the positive primes are distributed in exactly $\phi(n)$ sets. These sets are the equivalence classes represented by an integer which is relatively prime to n. Hence the Euler's number determines the complexity of the behavior of the $\tau_{(n)}$-products, because the elements are allowed to be $\tau_{(n)}$-multiplied if and only if they are in the same equivalence class with respect to $\tau_{(n)}$. The following Lemma gives a tool to know the form of the $\tau_{(n)}$-factor for some special cases.

Lemma 2. *Let $n = p_1^{n_1} \cdot p_2^{n_2}$ with p_1 and p_2 positive primes and $n_1, n_2 \in \mathbb{N}$. Suppose $x = p_1^{m_1} \cdot p_2^{m_2} x'$ where m_1 and m_2 are no-negative integers (no both zero) and $GCD(p_1 p_2, x') = 1$. If a positive integer c $\tau_{(n)}$-divides x, then $c = p_1^{l_1} \cdot p_2^{l_2} \cdot c'$ with $1 \leq l_i < m_i$ for $i \in \{1,2\}$ and $c' \leq x'$.*

Proof. Suppose that $c|_{\tau_{(n)}}x$, then there are nonzero nonunit integers $c_1, c_2, \ldots, c_k$ with $x = \pm c{*}c_1{*}{*}{*}c_k$. Since $c|x$, $c = p_1^{l_1}p_2^{l_2}c'$ with $c'|x'$ and $0 \leq l_i \leq m_i$ for $i \in \{1, 2\}$. In order to finish the proof, we need to show that $l_i \neq 0$ and $l_i \neq m_i$. Suppose by contradiction that $l_i = 0$, then $c = p_2^{l_2} \cdot c'$. Since $x = p_1^{m_1} \cdot p_2^{m_2}x' = c * c_1 * c_2 * * * c_k$ and $p_1 \nmid c$, then $p_1|c_i$ for some $i \in \{1, \ldots, k\}$. Now $c_i\tau_{(n)}c$, so $n|c - c_i$. By transitivity of division $p_1|c - c_i$. Therefore p_1 must divide c, a contradiction. If $l_1 = m_1$, then $c = p_1^{m_1} \cdot p_2^{l_2} \cdot c'$. Again $c\tau_{(n)}c_i$ for all $i \in \{1, \ldots, k\}$, that means $p_1|c - c_i$ for all $i \in \{1, \ldots, k\}$. Clearly $p_1|c$, hence $p_1|c_i$. This is not possible, because $p_1^{m_1}|c$. In conclusion, $l_1 \neq 0$ and $l_1 \neq m_1$. Similarly, $l_2 \neq 0$ and $l_2 \neq m_2$.

□

Before we give a summary of the known maximum common $\tau_{(n)}$-factor formulas when $n \leq 5$, we pause to introduce an useful tool.

2.2.5 Associated-preserving extension of $\tau_{(n)}$.

Serna [10] gave an extension of the relation, $\tau_{(n)}$, denoted by $\tau'_{(n)} = \{(\pm x, \pm y) : x\tau_{(n)}y\}$ such relation is called an associated-preserving relation, because if $x\tau'_{(n)}y$, then $-x\tau'_{(n)}y$, $x\tau'_{(n)} - y$ and $-x\tau'_{(n)} - y$. It is also known that in fact, it is an equivalence relation on $\mathbb{Z}^{\#}$. The equivalence class of an integer $a \in \mathbb{Z}^{\#}$ under the relation $\tau'_{(n)}$ is defined by $[a]_{\tau'_{(n)}} = \{b \in \mathbb{Z}^{\#} : b\tau'_{(n)}a\}$. In fact, $[a]_{\tau'_{(n)}} = [a]_{\tau_{(n)}} \cup [-a]_{\tau_{(n)}}$. Since $[a]_{\tau_{(n)}} \subseteq [a]_{\tau'_{(n)}}$ and $[-a]_{\tau_{(n)}} \subseteq [a]_{\tau'_{(n)}}$, then $[a]_{\tau_{(n)}} \cup [-a]_{\tau_{(n)}} \subseteq [a]_{\tau'_{(n)}}$. Now, if there exist $b \in [a]_{\tau'_{(n)}}$, then either $a\tau_{(n)}b$ or $-a\tau_{(n)}b$. In the first case, $b \in [a]_{\tau_{(n)}}$ and in the second case $b \equiv -a \,(mod\, n)$ and $b \in [-a]_{\tau_{(n)}}$. Therefore $b \in [a]_{\tau_{(n)}} \cup [-a]_{\tau_{(n)}}$. For simplicity, we will write $[\pm a]_{(n)}$ to mean $[a]_{\tau'_{(n)}} = [a]_{\tau_{(n)}} \cup [-a]_{\tau_{(n)}}$. We write $[\pm 1]_{(n)}$ (and $[0]_{(n)}$) to represent $[n+1]_{\tau'_{(n)}}$ (respectively $[n]_{\tau'_{(n)}}$); $\pm 1 \notin [\pm 1]_{(n)}$ (respectively $0 \notin [0]_{(n)}$), because $\pm 1 \notin \mathbb{Z}^{\#}$ (respectively $0 \notin \mathbb{Z}^{\#}$). The main reason of defining this concept is contained in the following corollary.

Corollary 1. *(Serna [10]) If $x, y \in \mathbb{Z}^{\#}$, then*

i. $x|_{\tau_{(n)}} y$ if and only if $x|_{\tau'_{(n)}} y$.

ii. x in an $\tau_{(n)}$-atom if and only if x in an $\tau'_{(n)}$-atom.

Remark 1. *The Corollary (1) is an important tool for our work, because m is the $\tau_{(n)}$-$MCD(x, y)$ if and only if m is the $\tau'_{(n)}$-$MCD(x, y)$. Therefore, the problem of computing $\tau_{(n)}$-$MCD(x, y)$ is equivalent to the problem of computing the $\tau'_{(n)}$-$MCD(x, y)$; which should be easier to find due to the number of equivalence classes with respect to $\tau'_{(n)}$ are basically half than with $\tau_{(n)}$.*

2.2.6 The $\tau_{(n)}$-$MCD(x, y)$ for $n \in \{0, 1, 2, 3, 4\}$

The authors in [7] gave a characterization of the $\tau_{(n)}$-MCD for $n \in \{0, 1, 2, 3, 4\}$. In this section those the reader can see characterizations. For the case $n = 0$, let $x, y \in \mathbb{Z}^{\#}$, if $x = p_1^{a_1} \cdots p_k^{a_k}$ and $y = p_1^{b_1} \cdots p_k^{b_k}$, where p_i are distinct usual positive primes. Suppose $x = \alpha^s$ and $y = \beta^t$, where α and β are (the only) $\tau_{(0)}$-atoms dividing x and y, respectively. Also, $s = GCD(a_1, \ldots, a_k)$ and $t = GCD(b_1, \ldots, b_k)$. Hence, in [7] the authors demonstrate that if $x = \alpha^s$ and $y = \beta^t$, with $|\alpha| = |\beta|$, then $\tau_{(0)}$-$MCD(x, y) = \alpha^{GCD(s,t)}$. Otherwise $\tau_{(0)}$-$MCD(x, y) = 1$. This result coincide with the $\tau_{(0)}$-$GCD(x, y)$, a result of [9]. When $n = 1$, the $\tau_{(1)}$-factorizations are the usual factorizations. Hence, if $x, y \in \mathbb{Z}^{\#}$, $\tau_{(1)}$-$MCD(x, y) = GCD(x, y)$. For $n = 2$, notice that a $\tau_{(n)}$-factor of an odd integer must be odd integer. Hence the $\tau_{(2)}$-$MCD(x, y) = GCD(x, y)$, when both x and y are odd. On the other hand, if $x = 2^n x'$ and $y = 2^m y'$ (where x' and y' are odd) are both even integers, then by Lemma (2) the $\tau_{(2)}$-$MCD(x, y)$ is 2 to the $min\{n, m\} - 1$ times the $GCD(x', y')$. If x is odd and y is even, then there is no common $\tau_{(2)}$-factor. When $n = 3$, the formula for the $\tau_{(3)}$-$MCD(x, y)$ turned out to have a great similarity to the formula of the $\tau_{(2)}$-MCD. If $x = 3^n x'$ and $y = 3^m y'$ are both divisible by 3 (x' and y' are not divisible by 3), then the $\tau_{(3)}$-$MCD(x,y) = 3^{min\{n,m\}-1} \cdot GCD(x',y')$. If x and y are not divisible by 3, then $\tau_{(3)}$-$MCD(x,y) = GCD(x,y)$. If x and y are not divisible by 3 and y is not, then they de not have any common $\tau_{(3)}$-factor. If $n=4$, then there are several cases but the two main cases arose again. We summarize this case, together to the previous ones in Table (2–2).

Table (2–2) summarized the work done in [7] for computing the $\tau_{(n)}$-MCD, when $n \in \{0,1,2,3,4\}$.

Table 2–2: The $\tau_{(n)}$-$MCD(x,y)$, for $n \in \{0,1,2,3,4\}$.

$\tau_{(n)}$	(x,y)	$\tau_{(n)}$-$MCD(x,y)$
$\tau_{(0)}$	(α^s, β^t)	$\lvert\alpha\rvert = \lvert\beta\rvert$: $\alpha^{GCD(s,t)}$
		$\lvert\alpha\rvert \neq \lvert\beta\rvert$: 1
$\tau_{(1)}$	(x,y)	$GCD(x,y)$
$\tau_{(2)}$	$(2^t x', 2^s y')$	$2^{min\{s,t\}-1}GCD(x',y')$
	$(2^t x', 2k+1)$	1
	$(2l+1, 2k+1)$	$GCD(x,y)$
$\tau_{(3)}$	$(3^t x', 3^s y')$	$3^{min\{s,t\}-1}GCD(x',y')$
	$(3^t x', 3k+1)$	1
	$(3l+1, 3k+1)$	$GCD(x,y)$
$\tau_{(4)}$	$(2^t x', 2^s y')$ $t \in \{2,3\}$	$2GCD(x',y')$
	$(2^t x', 2^s y')$ $t, s \geq 4$	$2^{min\{s,t\}-2}GCD(x',y')$
	$(2^t x', 4k+1)$	1
	$(2^t x', 4k+2)$	1
	$(4l+1, 4k+1)$	$GCD(x,y)$
	$(4l+2, 4k+2)$	1
	$(4l+1, 4k+2)$	1

Summary of $\tau_{(n)}$-MCD for any $x, y \in \mathbb{Z}^{\#}$, when $n \in \{0, \ldots, 4\}$

As a summary, the concepts of $\tau_{(n)}$-factorization seems to be a very naive and easy concept, but at the same time the level of technicalities and the behavior of the $\tau_{(n)}$-product become more complicated to put on a formula. The next chapter will present the formulas of the $\tau_{(n)}$-$MCD(x,y)$ for $n \in \{5,6,8,10,12\}$ and when x and y have a common $\tau_{(n)}$-factor.

Chapter 3
The $\tau_{(n)}$-MCD when $n \in \{5, 6, 8, 10, 12\}$

In [7], Luna and Ortiz found formulas for the $\tau_{(n)}$-MCD when $n \in \{0, 1, 2, 3, 4\}$. Through the brainstorming of this work, we realized that the difficulty of $\tau_{(5)}$-MCD was based on how the prime factors are distributed in the equivalence classes of $\tau'_{(n)}$. Hence, there is the need of understanding how the equivalence classes of $\tau'_{(n)}$ behave among themselves.

In this chapter, we present the formulas of $\tau_{(n)}$-MCD when $n \in \{5, 6, 8, 10, 12\}$. Since the primes distinct to 2 and 3 are located in basically two classes modulo 6, first we present the case when $n = 6$. Later, we present the cases when n belongs to $\{5, 8, 10, 12\}$, because the $\tau'_{(n)}$ has the same number of equivalence classes that contain almost all the primes.

3.1 The $\tau_{(6)}$-MCD

In this section the reader will find our result obtained for the case $n = 6$. The case was split into several subcases. Most (if not all) of the subcases will give a characterization for the $\tau'_{(n)}$-MCD, and so the $\tau_{(n)}$-MCD is obtained through Remark (1). Before we give the formulas of the $\tau_{(6)}$-MCD, let us explain how does the $\tau'_{(6)}$-products behave.

Proposition 2. *Let $x = \prod_{i=1}^{m} x_i$ be a $\tau'_{(6)}$-product. Then each $x_i \in [0]_{(6)}$ if and only if $x \in [0]_{(6)}$. If each $x_i \in [\pm 1]_{(6)}$, then $x \in [\pm 1]_{(6)}$.*

Proof. If each $x_i \equiv 0\,(mod\,6)$, then $x \equiv \prod_{i=1}^{m} x_i \equiv 0\,(mod\,6)$. For the converse, notice that since $x = \prod_{i=1}^{m} x_i$ is a $\tau'_{(6)}$-product and $x \in [0]_{(6)}$, there is at least one of the $x_i's$ must being in $[0]_{(6)}$. Hence all of them are in $[0]_{(6)}$. Similarly if each $x_i \equiv \pm 1\,(mod\,6)$, then $\prod_{i=1}^{m} x_i \equiv (\pm 1)^m\,(mod\,6)$ and so $x \equiv (\pm 1)^m\,(mod\,6) \equiv \pm 1\,(mod\,6)$. □

Proposition 3. *Let $x = \prod_{i=1}^{m} x_i$ be a $\tau'_{(6)}$-product, where for $b \in \{2, 3\}$ each x_i is in $[\pm b]_{(6)}$, then $x \in [\pm b]_{(6)}$.*

Proof. Suppose that for all $i \in \{1, \ldots, m\}$, $x_i \equiv 2\,(mod\,6)$. If m is odd, then $\prod_{i=1}^{m} x_i \equiv 2^m\,(mod\,6)$ and so $x \equiv 2^m(mod\,6) \equiv 2\,(mod\,6)$. If m is even, $2^m \equiv 4\,(mod\,6)$. Hence, $x \equiv \pm\,2\,(mod\,6)$. Now if each $x_i \equiv 3\,(mod\,6)$, then $x \equiv x_1 \cdots x_m\,(mod\,6)$, so $x \equiv 3^m(mod\,6)$. Since $3^m \equiv 3\,(mod\,6)$, then $x \equiv \pm\,3\,(mod\,6)$. □

Now we are ready to present the formulas of the $\tau_{(6)}$-MCD. For it, we split the result in several cases.

Theorem 5. *Let $x = 2^{n_1}3^{n_2}x'$ and $y = 2^{m_1}3^{m_2}y'$ where $n_1, n_2, m_1, m_2 > 1$. If $GCD(x' \cdot y', 6) = 1$, then $\tau_{(6)}$-$MCD(x, y) = 2^{min\{n_1,m_1\}-1} \cdot 3^{min\{n_2,m_2\}-1} GCD(x', y')$.*

Proof. Let $d_1 = GCD(x', y')$. Without loss of generality, suppose $n_1 = min\{n_1, m_1\}$ and $m_2 = min\{n_2, m_2\}$. We need to prove that $2^{n_1-1} \cdot 3^{m_2-1}d_1$ is the maximum common $\tau_{(6)}$-factor of x and y. Since $d_1 = GCD(x', y')$, there are x'' and y'' such that $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. Since $m_2 = min\{n_2, m_2\}$ and $n_1 = min\{n_1, m_1\}$, there are t and l non-negative integers such that $n_2 = t + m_2$ and $m_1 = l + n_1$. Then by Proposition (2)

$$x = \underbrace{(2^{n_1-1} \cdot 3^{m_2-1}d_1)}_{[0]_{(6)}} * \underbrace{(2 \cdot 3^{t+1}x'')}_{[0]_{(6)}}$$

and

$$y = \underbrace{(2^{n_1-1} \cdot 3^{m_2-1} d_1)}_{[0]_{(6)}} * \underbrace{(2^{l+1} \cdot 3y'')}_{[0]_{(6)}}$$

are $\tau_{(6)}$-products. Thus $2^{n_1-1} \cdot 3^{m_2-1} d_1|_{\tau_6} x, y$. Now suppose that there exists a common $\tau_{(6)}$-factor c of x and y, then by Lemma (2) $c = 2^n \cdot 3^m \cdot c_1$, $n < n_1$, $m < m_2$ and $c_1|x', y'$. Since $d_1 = GCD(x', y')$, $c_1|d_1$ and $c_1 \leq d_1$. Therefore, $c = 2^n \cdot 3^m \cdot c_1 \leq 2^{n_1-1} \cdot 3^{m_2-1} \cdot d_1$. Hence, the maximum common $\tau_{(6)}$-factor is $2^{n_1-1} \cdot 3^{m_2-1} \cdot d_1$. □

Proposition 4. *If $x, y \in [\pm 1]_{(6)}$, then $\tau_{(6)}$-$MCD(x, y) = GCD(x, y)$.*

Proof. Let $d = GCD(x, y)$, then there exist x' and y' such that $x = dx'$ and $y = dy'$. Since $x, y \in [\pm 1]_{(6)}$, $d \in [\pm 1]_{(6)}$, and $x', y' \in [\pm 1]_{(6)}$. By Proposition (2) with suitable signs, $x = (\pm 1)\, d * (\pm x')$ and $y = (\pm 1)\, d * (\pm y')$ are $\tau'_{(6)}$-factorizations of x and y, respectively. By Remark (1), we have that $\tau_{(6)}$-$MCD(x, y) = GCD(x, y)$. □

Theorem 6. *Let $x = a^n x'$ and $y = a^m y'$, with $n, m > 1$, $a \nmid x'$ and $a \nmid y'$, where $a \in \{2, 3\}$, then $\tau_{(6)}$-$MCD(x, y) = a^{min\{n,m\}-1} GCD(x', y')$.*

Proof. Without loss of generality suppose that $n = min\{n, m\}$, and $d_1 = GCD(x', y')$. First, one needs to prove that $a^{n-1} d_1$ is a common $\tau'_{(6)}$-factor of x and y. Since $d_1 = GCD(x', y')$ there exist x' and y' such that $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. Note that d_1, x'' and $y'' \in [\pm 1]_{(6)}$ (because d_1 is not divisible by 2 and 3). By Proposition (2) $x = (\pm 1)\ \underbrace{(a^{n-1} \cdot d_1)}_{[\pm a]_{(6)}} * \underbrace{(\pm a \cdot x'')}_{[\pm a]_{(6)}}$, with suitable choice of signs $a^{n-1} \cdot d_1|_{\tau'_{(6)}} x$. Analogously, $d_1|_{\tau'_{(6)}} y$. If c is a common $\tau'_{(6)}$-factor of x and y, then by Lemma (2) $c = a^t c'$, with $t < n$ and $c'|d_1$. Therefore $c = a^t c' \leq 2^{n-1} d_1$, and the $\tau'_{(6)}$-$MCD(x, y) = a^{n-1} d_1$. By Remark (1), $\tau_{(6)}$-$MCD(x, y) = a^{n-1} d_1$. □

The last theorem can be included as part of Theorem (5), but splitting it in this way is clearer to prove without getting involve in many detailed cases. If there exists x such that $GCD(x, 6) = 1$, then $d \in [\pm 1]_{(6)}$. It implies that for $x \in [\pm 1]_{(6)}$ and $y \notin [\pm 1]_{(6)}$, then $y \in [a]_{(6)}$ where $a \in \{0, \pm 2, \pm 3\}$ there is no common $\tau_{(6)}$-factors. Hence, $\tau_{(6)}$-$MCD(x, y) = 1$. If $x \in [\pm 2]_{(6)}$ and $y \in [\pm 3]_{(6)}$, then x and y have no common $\tau'_{(6)}$-factors. Because by Proposition (3), the $\tau'_{(6)}$-factors of x are in $[\pm 2]_{(6)}$ and the $\tau'_{(6)}$-factors of y are in $[\pm 3]_{(6)}$. Hence $\tau'_{(6)}$-$MCD(x, y)$ must be 1. As a consequence of Hammon's result [4] we have that the $\tau_{(6)}$-atoms, are either primes or integers of the form: $x = 2^{n_1} \cdot 3^{n_2} \cdot x'$ with $n_1, n_2 \in \{0, 1\}$ where $GCD(6, x') = 1$. If x is a $\tau_{(6)}$-atom and $x \nmid_{\tau_{(6)}} y$, then x and y do not have common $\tau_{(6)}$-factor. Hence, $\tau_{(6)}$-$MCD(x, y) = 1$.

Observe that an element in $[\pm 1]_{(6)}$ can be written as $6k \pm 1$. In Table (3–1), the results for the $\tau_{(6)}$-MCD are summarized.

Table 3–1: The $\tau_{(6)}$-MCD

(x, y)	$\tau_{(6)}$-$MCD(x, y)$
$(2^n 3^u x', 2^m 3^v y')$	$2^{min\{n,m\}-1} 3^{min\{u,v\}-1} GCD(x', y')$
$(2^n 3^m x', 6k \pm 1)$	1
$(2^n 3^m x', 2^r y')$	1
$(2^n 3^m x', 3^r y')$	1
$(6l \pm 1, 6k \pm 1)$	$GCD(x, y)$
$(6l \pm 1, 6k \pm 2)$	1
$(6l \pm 1, 6k + 3)$	1
$(2^n x', 2^r y')$	$2^{min\{n,m\}-1} GCD(x', y')$
$(2^n x', 3^r y')$	1
$(3^n x', 3^m y')$	$3^{min\{n,m\}-1} GCD(x', y')$

The table summarizes the formulas for $\tau_{(6)}$-MCD for elements in $[0]_{(6)}$, $[3]_{(6)}$ and $[\pm a]_{(6)}$ where $a \in \{1, 2\}$.

3.2 The $\tau_{(n)}$-MCD when $\phi(n) = 4$

The solutions for the equation $\phi(n) = 4$, are $n \in \{5, 8, 10, 12\}$. In this section, we present results about the characterization of the $\tau_{(n)}$-MCD for these cases. Observe that there are 2 classes $[\pm a]_{(n)}$ with respect to the equivalence relation $\tau'_{(n)}$, with $GCD(a, n) = 1$.

3.2.1 The $\tau_{(5)}$-MCD

In this section the reader can find a formula to compute the $\tau_{(5)}$-MCD between integers in $[0]_{(5)}$. Also, there is a method for finding the $\tau'_{(n)}$-MCD with the elements that are relative primes to 5. These elements are in the equivalence classes $[\pm 1]_{(5)}$ and $[\pm 2]_{(5)}$. First, we need to see the behavior of the $\tau'_{(5)}$-products.

Proposition 5. *Let $x = \prod_{i=1}^{m} x_i$ be a $\tau_{(5)}$-product. Then each $x_i \equiv\ 0\,(mod\,5)$ if and only if $x \equiv\ 0\,(mod\,5)$. If each $x_i \equiv\ \pm 1(mod\,5)$, then $x \equiv\ \pm 1\,(mod\,5)$.*

Proof. If each $x_i \equiv 0\,(mod\,5)$, $x_i = 5x'_i$ for some $x'_i \in \mathbb{Z}^*$. Therefore we have that $x = \prod_{i=1}^{m} x_i = 5^m \prod_{i=1}^{m} x'_i \equiv\ 0\,(mod\,5)$. For the converse, notice that since $x = \prod_{i=1}^{m} x_i$ is a $\tau'_{(5)}$-product, one of the x_i must be a multiple of 5 and hence all of them. If each $x_i \equiv \pm 1\,(mod\,5)$, then $x_1 \cdots x_k \equiv\ \pm 1(mod\,5)$, that is $x \equiv\ \pm 1\,(mod\,5)$. □

Proposition 6. *Let $x = \prod_{i=1}^{m} x_i^{a_i}$ be a $\tau'_{(5)}$-product, where each $x_i \in [\pm 2]_{(5)}$.*

i. Then, $\sum_{i=1}^{m} a_i = 2k$ if and only if $x \in [\pm 1]_{(5)}$.

ii. Then, $\sum_{i=1}^{m} a_i = 2k + 1$ if and only if $x \in [\pm 2]_{(5)}$.

Proof. ($\Rightarrow$) Since $GCD(2, 5) = 1$, $2^2 \equiv -1\,(mod\,5)$. Hence $2^{2m} \equiv \pm 1\,(mod\,5)$, for any $m \in \mathbb{Z}$, so (i) follows. For $(ii.)$, write $x = \left(\prod_{i=1}^{m-1} x_i^{a_i}\right) x_m$, notice that $\left(\prod_{i=1}^{m-1} x_i^{a_i}\right) \in [\pm 1]_{(5)}$ and $x_m \in [\pm 2]_{(5)}$, then $x \in [\pm 2]_{(5)}$.

($\Leftarrow$) Note that $\sum\limits_{i=1}^{m} a_i$ is either even or odd. Hence, by the previous part the theorem holds. □

Theorem 7. *Let $x = 5^s x'$ and $y = 5^t y'$, where $5 \nmid x'$, $5 \nmid y'$ and $s, t > 1$. Then, $\tau_{(5)}$-$MCD(x, y) = 5^{min\{s,t\}-1} GCD(x', y')$.*

Proof. Let $d_1 = GCD(x', y')$ and without loss of generality, suppose that $s \leq t$. First need to prove that $5^{s-1}d_1$ is a common $\tau_{(5)}$-factor of x and y. Since d_1 is $GCD(x', y')$, there exist x'' and y'' such that, $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. By Proposition (5), $x = 5^s d_1 x'' = \pm \underbrace{(5^{s-1}d_1)}_{[0]_{(5)}} * \underbrace{(\pm 5x'')}_{[0]_{(5)}}$ and hence $5^{s-1}d_1|_{\tau_{(5)}} x$. Since $s \leq t$, there exist $l \in \mathbb{Z}^+$ such that $t = l + s$. By Proposition (5), we have that x is equal to $5^t d_1 x'' = 5^{s+l} d_1 x'' = \pm \underbrace{(5^{s-1}d_1)}_{[0]_{(5)}} * \underbrace{(\pm 5^{l+1} x'')}_{[0]_{(5)}}$ and $5^{s-1}d_1|_{\tau_{(5)}} y$. Therefore $5^{min\{s,t-1\}} \cdot GCD(x', y')$ is a common $\tau_{(5)}$-factor of x and y. If there exist a common $\tau_{(5)}$-factor c of x and y, by Lemma (2) $c = 5^r c'$, where $1 \leq r \leq s - 1$ with $c'|x'$ and $c'|y'$. Then we have that $5^r \leq 5^{min\{s,t\}-1}$ and $c'|d_1$. Therefore $c = 5^r c' \leq 5^{s-1}d_1$ and $5^{s-1}d_1 = \tau_{(5)}$-$MCD(x, y)$. □

When $n = 6$, if $x \in [\pm 1]_{(6)}$ and $d|x$, we had $d \in [\pm 1]_{(6)}$. In $\tau'_{(5)}$, this fact does not hold. Now, if $x \in [\pm 1]_{(5)}$ and $d|x$, then $GCD(d, 5) = 1$, which implies that $d \in [\pm 1]_{(5)}$ or $d \in [\pm 2]_{(5)}$. This fact helps to prove the following theorem.

Theorem 8. *If $x, y \in [\pm 1]_{(5)}$, then $\tau_{(5)}$-$MCD(x, y) = GCD(x, y)$.*

Proof. Let $d = GCD(x, y)$, then $x = dx'$ and $y = dy'$ for some x' and y'. Since $x, y \in [\pm 1]_{(5)}$, then we have $GCD(d, 5) = 1$, and either $d \in [\pm 1]_{(5)}$ or $d \in [\pm 2]_{(5)}$. If $d \in [\pm 1]_{(5)}$, then both $x' \in [\pm 1]_{(5)}$ and $y' \in [\pm 1]_{(5)}$ (because, by hypothesis, x, y are in $[\pm 1]_{(5)}$). In this case with an appropriate choice of signs, $x = (\pm 1) \underbrace{(d)}_{[\pm 1]_{(5)}} * \underbrace{(\pm x')}_{[\pm 1]_{(5)}}$

and $y = (\pm 1)\underbrace{(d)}_{[\pm 1]_{(5)}} * \underbrace{(\pm\, y')}_{[\pm 1]_{(5)}}$ are both $\tau'_{(5)}$-factorizations of x and y, respectively. If $d \in [\pm 2]_{(5)}$ by Proposition (6), $x' \in [\pm 2]_{(5)}$ and $y' \in [\pm 2]_{(5)}$. Hence we have that $x = (\pm 1)\underbrace{(d)}_{[\pm 2]_{(5)}} * \underbrace{(\pm\, x')}_{[\pm 2]_{(5)}}$ and $y = (\pm 1)\underbrace{(d)}_{[\pm 2]_{(5)}} * \underbrace{(\pm\, y')}_{[\pm 2]_{(5)}}$ are both $\tau_{(5)}$-factorizations of x and y, respectively. Notice that d is the maximum common $\tau'_{(5)}$-factor of x and y. Because for any c common $\tau'_{(5)}$-factor of x and y, $c|d$, which implies that $c \leq d$. By Remark (1), the $GCD(x, y)$ coincides with $\tau'_{(5)}$-$MCD(x, y)$. □

Let $x \in [\pm 2]_{(5)}$ and $x_1 \in \mathbb{Z}^{\#}$. If $x_1|_{\tau_{(5)}} x$, then $x_1 \in [\pm 2]_{(5)}$. Otherwise if $x_1 \in [\pm 1]_{(5)}$, then $x = \pm x_1 * * * x_k$, where each $x_i \in [\pm 1]_{(5)}$ and by Proposition (5), $x \in [\pm 1]_{(5)}$. A contradiction, then each $\tau'_{(5)}$-factor of x must be in $[\pm 2]_{(5)}$. If p is a prime number different from ± 5, then either $p \in [\pm 1]_{(5)}$ or $p \in [\pm 2]_{(5)}$ (the 2 equivalence classes determined by $\phi(5)$ with respect to $\tau'_{(5)}$). Recall $\Pi_b(x) = \prod_{i=1}^{\alpha_b} p_{ib}^{a_{ib}}$ the product of primes factors p_{ib} of x where each $p_{ib} \in [\pm b]_{(5)}$ and $b \in \{1, 2\}$. As a consequence, the factorization of a number $x \notin [0]_{(5)}$ can be rewritten as $x = \Pi_1(x) \cdot \Pi_2(x) = \prod_{i=1}^{\alpha_1} p_{i1}^{a_{i1}} \cdot \prod_{i=1}^{\alpha_2} p_{i2}^{a_{i2}}$ (by reordering the primes, if it is necessary).

Proposition 7. *Let $x \in [\pm b]_{(5)}$ and $d \in [\pm 2]_{(5)}$, where $b \in \{1, 2\}$. Suppose there exist x', such that $x = d \cdot x'$. If $\Pi_2(x') \neq 1$, $d|_{\tau_{(5)}} x$.*

Proof. Since $x = d \cdot x'$ and $d \in [\pm 2]_{(5)}$. If $x \in [\pm 1]_{(5)}$, by Proposition (6) then $x' \in [\pm 2]_{(5)}$. Hence $x = (\pm 1)d * x'$ is a $\tau'_{(5)}$-factorization of x; so $d|_{\tau_{(5)}} x$. If $x \in [\pm 2]_{(5)}$, by Proposition (6) $x' \in [\pm 1]_{(5)}$. Notice that x' can be rewritten as $x' = \Pi_1(x') \cdot \Pi_2(x')$. By Proposition (5), $\Pi_1(x') \in [\pm 1]_{(5)}$. Therefore $\Pi_2(x') \in [\pm 1]_{(5)}$; and by Proposition

(6), the amount of prime factors in $[\pm 2]_{(5)}$ is even. For a suitable choice of signs:

$$\begin{aligned} x &= d \cdot \Pi_1(x') \cdot \Pi_2(x') \\ &= d \cdot \Pi_1(x') \cdot \prod_{i=1}^{\alpha_2} p_{i2}^{a_{i2}} \\ &= (\pm 1) \underbrace{d}_{[\pm 2]_{(5)}} * \underbrace{(\pm \Pi_1(x') p_{12})}_{[\pm 2]_{(5)}} * \underbrace{(\pm p_{12})}_{[\pm 2]_{(5)}} *** \underbrace{(\pm p_{\alpha_2 2})}_{[\pm 2]_{(5)}} \end{aligned}$$

therefore $d|_{\tau_{(5)}} x$. □

Proposition 8. *Let $x \in [\pm b]_{(5)}$ and $y, c \in [\pm 2]_{(5)}$, where $b \in \{1, 2\}$. Suppose $d = GCD(x, y)$. If there exist $c' \in \mathbb{Z}^{\#}$ such that $d = c \cdot c'$ and $\Pi_2(c') \neq 1$, then $c|_{\tau'_{(5)}} x, y$ if and only if $c|_{\tau'_{(5)}} d$.*

Proof. (⇒) If $d \in [\pm 1]_{(5)}$, by Proposition (6) $c' \in [\pm 2]_{(5)}$, because $c \in [\pm 2]_{(5)}$. Hence $d = (\pm 1) \underbrace{(c)}_{[\pm 2]_{(5)}} * \underbrace{(c')}_{[\pm 2]_{(5)}}$, is a $\tau'_{(5)}$-factorization of d and $c|_{\tau'_{(5)}} d$. If $d \in [\pm 2]_{(5)}$, $c' \in [\pm 1]_{(5)}$. Since $\Pi_2(c') \neq 1$, by the Proposition (7), $c|_{\tau'_{(5)}} d$.

(⇐) Suppose $c|_{\tau'_{(5)}} d$, hence $c|d$ and by transitivity $c|x$ and $c|y$. By Pproposition (7), $c|_{\tau'_{(5)}} x, y$. (Because $c \in [\pm 2]_{(5)}$ and $\Pi_2(c') \neq 1$). □

The last proposition shows that the set of common $\tau_{(5)}$-factors of $x \in [\pm 2]_{(5)}$ and $y \in [\pm b]_{(5)}$, where $b \in \{1, 2\}$, is equal to the set of the $\tau_{(5)}$-factors of $GCD(x, y)$, which are in $[\pm 2]_{(5)}$. Hence, the following theorem gives a simpler way to compute the $\tau_{(5)}$-$MCD(x, y)$, because we only need to look at the list of the $\tau'_{(5)}$-factors of the $GCD(x, y)$.

Theorem 9. *If $y \in [\pm 2]_{(5)}$ and $x \in [\pm b]_{(5)}$, $y \in [\pm 2]_{(5)}$ where $b \in \{1, 2\}$, then $\tau_{(5)}$-$MCD(x, y) = m$, where $m = max\{c \in [\pm 2]_{(5)} : c|_{\tau'_{(5)}} GCD(x, y)\}$.*

Proof. By the Proposition (8), we have that the set of common $\tau'_{(5)}$-factors of x and y is $A = \{d \in [\pm 2]_{(5)} : d|_{\tau_{(5)}} x, y\}$. Also, by Proposition (8), it holds that $A = \{c \in [\pm 2]_{(5)} : c|_{\tau'_{(5)}} GCD(x, y)\}$. Since $\tau_{(5)}$-$MCD(x, y) = max\,\{d : d|_{\tau'_{(5)}} x, y\}$ which is equal to $max\{d : d \in A\}$. Then the maximum common $\tau_{(5)}$-factor of x and y is m. □

Observe that if $x = 5x'$ where $5 \nmid x'$, x is a $\tau_{(5)}$-atom. Hence if $x = 5x'$, where $5 \nmid x'$, $y \in \mathbb{Z}^{\#}$ and $x \nmid_{\tau_{(5)}} y$, then x and y have no common $\tau_{(5)}$-factors and $\tau_{(5)}$-$MCD(x, y) = 1$. In the case of $x|_{\tau_{(5)}} y$, then $\tau_{(5)}$-$MCD(x, y) = x$. If $x \in [0]_{(5)}$ and $y \notin [0]_{(5)}$, then x and y do not have $\tau_{(5)}$-common factors. Hence, the $\tau_{(5)}$-$MCD(x, y)$ is 1. Table (3–2) summarizes the formulas for the $\tau_{(5)}$-MCD. Note that if an element $x \in [\pm 1]_{(5)}$ or $x \in [\pm 2]_{(5)}$, then x can be written as $x = 5k \pm 1$ or $5k \pm 2$, respectively. In Table (3–2), for $x, y \in \mathbb{Z}^{\#}$, m denotes the $max\,\{x_i \in [\pm 2]_{(5)} : x_i|_{\tau_{(5)}} GCD(x, y)\}$.

Table 3–2: The $\tau_{(5)}$-$MCD(x, y)$.

(x, y)	$\tau_{(5)}$-$MCD(x, y)$
$(5^s x', 5^t y')$	$5^{min\{s,t\}-1} GCD(x', y')$
$(5^s x', 5k \pm 1)$	1
$(5^s x', 5k \pm 2)$	1
$(5l \pm 1, 5k \pm 1)$	$GCD(x, y)$
$(5l \pm 1, 5k \pm 2)$	m
$(5l \pm 2, 5k \pm 2)$	m

A summary of the formulas for the $\tau_{(5)}$-MCD for elements of the form $5^k \cdot x'$, $5k \pm 1$ and $5k \pm 2$.

3.2.2 The $\tau_{(8)}$-MCD

For $n = 8$, we have five equivalence classes, $[0]_{(8)}$, $[\pm 1]_{(8)}$, $[\pm 2]_{(8)}$, $[\pm 3]_{(8)}$. The equivalence classes $[\pm 1]_{(8)}$ and $[\pm 3]_{(8)}$ behaves as it happened for the equivalence classes $[\pm 1]_{(5)}$ and $[\pm 2]_{(5)}$. So, we could use the results in Proposition (5) and (6) to approach this cases. The other 3 equivalence classes have elements of the form $2^n x'$ where $2 \nmid x'$. If $n = 1$ (respectively $n = 2$ and $n = 3$), then $x \in [\pm 2]_{(8)}$ (respectively $x \in [\pm 4]_{(8)}$ and $x \in [\pm 0]_{(8)}$). If $2 \nmid x$, then either $x \in [\pm 1]_{(8)}$ or $x \in [\pm 3]_{(8)}$ and so its factors.

Theorem 10. *Let $x = 2^n x'$ and $y = 2^m y'$, where $2 \nmid x', y'$ and $n, m \geq 6$. Then $\tau_{(8)}$-$MCD(x, y) = 2^{min\{n,m\}-3} GCD(x', y')$.*

Proof. Let $d_1 = GCD(x', y')$, then $x' = d_1 x''$ and $y' = d_1 y''$ where $x'', y'' \in \mathbb{Z}^*$. Without loss of generality, suppose $n = min\{n, m\}$ and $m = n + l$ for some $l \geq 0$. Then for a suitable choice of signs, $x = \pm \underbrace{(2^{n-3} \cdot d_1)}_{[0]_{(8)}} * \underbrace{(\pm 2^3 \cdot x'')}_{[0]_{(8)}}$ and $y = \pm \underbrace{(2^{n-3} \cdot d_1)}_{[0]_{(8)}} * \underbrace{(\pm 2^{m+3} \cdot y'')}_{[0]_{(8)}}$ are $\tau_{(8)}$-factorizations of x and y, respectively. If there exist $c = 2^t \cdot c'$ with $c|_{\tau_{(8)}} x, y$, then $t \leq n - 1$ and $c'|x', y'$, which implies, $c' \leq d_1$. Therefore, $c \leq (2^{n-1} \cdot d_1)$ and $\tau'_{(8)}$-$MCD(x, y) = 2^{min\{n,m\}-3} GCD(x', y')$ and it is the $\tau_{(8)}$-$MCD(x, y)$. □

Now, we will address the cases when at least the power of x and y is strictly less than 6.

Proposition 9. *Let $x = 2^n x'$, where $n \geq 2$ and $GCD(2, x') = 1$. If there exists $d_1 | x'$, then $2d_1 |_{\tau_{(8)}} x$.*

Proof. If $d_1 | x'$, there exist $x'' \in \mathbb{Z}^*$ such that $x' = d_1 \cdot x''$. Since $2 \nmid x'$ either $x' \in [\pm 1]_{(8)}$ or $x' \in [\pm 3]_{(8)}$. So either $d_1 \in [\pm 1]_{(8)}$ or $d_1 \in [\pm 3]_{(8)}$ and either

$x'' \in [\pm 1]_{(8)}$ or $x'' \in [\pm 3]_{(8)}$. If $x' \in [\pm 1]_{(8)}$, then by the results (applied on $\tau'_{(8)}$) of Proposition (5) and Proposition (6) d_1 and x'' are in a same equivalence class, in order for $x' \in [\pm 1]_{(8)}$. That is, $d_1, x'' \in [\pm a]_{(8)}$ for $a \in \{1, 3\}$, in both cases we obtain that $(2 \cdot d_1)$ and $(2 \cdot x'') \in [\pm 2]_{(8)}$. If $x' \in [\pm 3]_{(8)}$, then by the results (applied on $\tau'_{(8)}$) of Proposition (6) d_1 and x'' are in different classes, in order for $x' \in [\pm 3]_{(8)}$. That is, $d_1 \in [\pm a]_{(8)}$ and $x'' \in [\pm b]_{(8)}$ with $a \neq b \in \{1, 3\}$. See Table (3–3) where there is a summary about these results.

Table 3–3: Class options for $2 \cdot d_1$ and $2 \cdot x''$

x'	d_1	x''	$2 \cdot d_1$	$2 \cdot x''$
$[\pm 1]_{(8)}$	$[\pm 1]_{(8)}$	$[\pm 1]_{(8)}$	$[\pm 2]_{(8)}$	$[\pm 2]_{(8)}$
$[\pm 1]_{(8)}$	$[\pm 3]_{(8)}$	$[\pm 3]_{(8)}$	$[\pm 2]_{(8)}$	$[\pm 2]_{(8)}$
$[\pm 3]_{(8)}$	$[\pm 1]_{(8)}$	$[\pm 3]_{(8)}$	$[\pm 2]_{(8)}$	$[\pm 2]_{(8)}$
$[\pm 3]_{(8)}$	$[\pm 3]_{(8)}$	$[\pm 1]_{(8)}$	$[\pm 2]_{(8)}$	$[\pm 2]_{(8)}$

By a suitable choice of signs,

$$x = 2^n \cdot d_1 \cdot x'' = (\pm 1)\, \underbrace{(2 \cdot d_1)}_{[\pm 2]_{(8)}} * \underbrace{(\pm\, 2 \cdot x'')}_{[\pm 2]_{(8)}} * \underbrace{(\pm\, 2)}_{[\pm 2]_{(8)}} *** \underbrace{(\pm\, 2)}_{[\pm 2]_{(8)}}$$

Then $(2 \cdot d_1)|_{\tau'_{(8)}} x$ and by Remark (1), $(2 \cdot d_1)|_{\tau_{(8)}} x$. □

As a consequence of Proposition (9), if $x = 2^2 x'$ and $y = 2^m y'$, where $GCD(2, x'y')$ is 1 and $m > 1$, then we have that $\tau_{(8)}$-$MCD(x, y) = 2 \cdot GCD(x', y')$.

Theorem 11. *Let $x, y \in [0]_{(8)}$. Suppose $x = 2^n x'$ and $y = 2^m y'$, where $2 \nmid x', y'$, $n \in \{3, 4, 5\}$ and $m \in \{3, 5\}$. Then $\tau_{(8)}$-$MCD(x, y) = 2 \cdot GCD(x', y')$.*

Proof. For simplicity denote $d_1 = GCD(x', y')$, then there are x'', y'' such that $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. By the Proposition (9) $2d_1|_{\tau_{(8)}} x$ and $2d_1|_{\tau_{(8)}} y$. Need to prove that $2d_1$ is the maximum common $\tau_{(8)}$-factor between x and y. If there exist c, such that $c|_{\tau_{(8)}} x, y$, then by Lemma (2) $c = 2^t \cdot c_1$ with $0 < t < min\{n, m\}$

and $c_1 | x', y'$. Then there exist $c', c'' \in \mathbb{Z}^*$ such that $x' = c_1 \cdot c'$ and $y' = c_1 \cdot c''$. By definition of d_1, $c_1 | d_1$, and hence $c_1 \leq d_1$. Then $c_1, c'' \in [\pm 1]_{(8)} \cup [\pm 3]_{(8)}$.

i. If $m = 3$, then $t \in \{1, 2\}$. In the case of $t = 1$, by the inequality $c_1 \leq d_1$, we have $c \leq (2 \cdot d_1)$. Now, we may assume $t = 2$. Since $y = 2^3 \cdot c_1 \cdot c''$, note that $(2^2 \cdot c_1) \in [\pm 4]_{(8)}$, but $(2 \cdot c'') \in [\pm 2]_{(8)}$. Then $c \nmid_{\tau_{(8)}} y$, a contradiction. Hence $t = 1$.

ii. If $m = 5$, $t \in \{1, 2, 3, 4\}$. Suppose $t = 1$, since $c_1 \leq d_1$, $c \leq 2 \cdot d_1$. If $t \geq 2$, $c \nmid_{\tau_{(8)}} y$ as in the above case.

For any common $\tau_{(8)}$-$factor$ c of x and y, $c \leq (2 \cdot d_1)$. Hence the $\tau_{(8)}$-$MCD(x, y)$ is $2 \cdot GCD(x', y')$. □

Theorem 12. *Let $x = 2^4 x'$ and $y = 2^n y'$, where $2 \nmid x', y'$ and n is even, $n \geq 4$. Then $\tau_{(8)}$-$MCD(x, y) = 2^2 GCD(x', y')$.*

Proof. Let $d_1 = GCD(x', y')$, then there exist $x'', y'' \in \mathbb{Z}^*$, such that $x' = d_1 x''$ and $y' = d_1 y''$. Since $GCD(x', 8) = 1$, then either $d_1, x' \in [\pm 1]_{(8)} \cup [\pm 3]_{(8)}$. The Table (3–4) gives all the posibilities for x', d_1, x'', $2^2 x'$ and $2^2 d_1$.

Table 3–4: Class options for $2^2 \cdot d_1$ and $2^2 \cdot x''$

x'	d_1	x''	$2^2 \cdot d_1$	$2^2 \cdot x''$
$[\pm 1]_{(8)}$	$[\pm 1]_{(8)}$	$[\pm 1]_{(8)}$	$[\pm 4]_{(8)}$	$[\pm 4]_{(8)}$
$[\pm 1]_{(8)}$	$[\pm 3]_{(8)}$	$[\pm 3]_{(8)}$	$[\pm 4]_{(8)}$	$[\pm 4]_{(8)}$
$[\pm 3]_{(8)}$	$[\pm 1]_{(8)}$	$[\pm 3]_{(8)}$	$[\pm 4]_{(8)}$	$[\pm 4]_{(8)}$
$[\pm 3]_{(8)}$	$[\pm 3]_{(8)}$	$[\pm 1]_{(8)}$	$[\pm 4]_{(8)}$	$[\pm 4]_{(8)}$

With a suitable choice of signs $x = (\pm 1)\,(2^2 \cdot d_1) * (\pm 2^2 \cdot x'')$ is a $\tau'_{(8)}$-factorization of x. Since n is even and $n \geq 4$, then $y = (\pm 1)(2^2 d_1) * (\pm 2^2 \cdot y'') * (\pm 2^2) * * * (\pm 2^2)$ is a $\tau'_{(8)}$-factorization of y (for a suitable choice of signs). If there is a common $\tau_{(8)}$-factor c, of x and y, then then by Lemma (2) $c = 2^t c'$ where $c' | x', y'$ and $1 \leq t \leq 3$. By definition of d_1, $c' \leq d_1$. If $t \in \{1, 2\}$, $c \leq 2^2 \cdot d_1$. For $t = 3$, notice that $x' = c' \cdot c''$ for some $c'' \in [\pm 1]_{(8)} \cup [\pm 3]_{(8)}$. Then $2^3 \cdot c' \in [0]_{(8)}$ and $2 \cdot c'' \in [\pm 2]_{(8)}$.

Hence $c \nmid_{\tau_8} x$. In conclusion, $\tau'_{(8)}$-$MCD(x,y) = 2^2 GCD(x',y')$. By Remark (1), $2^2 GCD(x',y') = \tau_{(8)}$-$MCD(x,y)$. □

Theorem 13. *Let $x = 2^4 x'$, $y = 2^n y'$, with $2 \nmid x', y'$, and n an odd integer with $n \geq 3$. Then $\tau_{(8)}$-$MCD(x,y) = 2 \cdot GCD(x',y')$.*

Proof. The proof is analogous to the proof of the Theorem (12). □

Theorem 14. *If $x, y \in [\pm 1]_{(8)}$, then $\tau_{(8)}$-$MCD(x,y) = GCD(x,y)$.*

Proof. Let $d = GCD(x,y)$. Then there are $x', y' \in \mathbb{Z}^*$, such that $x = dx'$ and $y = dy'$. If $d \in [\pm 1]_{(8)}$, then $x', y' \in [\pm 1]_{(8)}$, in order for $x \in [\pm 1]_{(8)}$. On other hand, if $d \in [\pm 3]_{(8)}$, then by the result in Proposition (6) $x', y' \in [\pm 3]_{(8)}$. In both cases, $x = (\pm 1)\, d * (\pm x')$, $y = (\pm 1)\, d * (\pm y')$ are $\tau'_{(8)}$-factorizations of x and y, respectively. By Remark (1), $\tau_{(8)}$-$MCD(x,y) = GCD(x,y)$. □

Observe that, if p is a positive odd prime, $p \in [\pm 1]_{(8)}$ or $p \in [\pm 3]_{(8)}$. Let us recall $\Pi_b(x) = \prod_{i=1}^{\alpha_b} p_{ib}^{a_{ib}}$ denotes the product of positive primes that divides x, with the property, $p_{ib} \in [\pm b]_{(8)}$, for $b \in \{1,3\}$.

Lemma 3. *Let $x \in [\pm b]_{(8)}$, where $b \in \{1,3\}$. Suppose $d \in [\pm 3]_{(8)}$ such that $d | x$. If $\Pi_3(\frac{x}{d}) \neq 1$, then $d|_{\tau_{(8)}} x$.*

Proof. Since $d|x$, then $x = d \cdot x'$ for $x' \in \mathbb{Z}^*$. Let us rewrite $x' = \frac{x}{d}$ into a product of primes in $[\pm 1]_{(8)}$ and primes in $[\pm 3]_{(8)}$. So the canonical factorization of x' is $x' = \Pi_1(x') \cdot \Pi_3(x') = \prod_{i=1}^{\alpha_1} p_{i1}^{a_{i1}} \cdot \prod_{i=1}^{\alpha_3} p_{i3}^{a_{i3}}$, then $x = d \cdot x' = d \cdot \prod_{i=1}^{\alpha_1} p_{i1}^{a_{i1}} \cdot \prod_{i=1}^{\alpha_3} p_{i3}^{a_{i3}}$. Since $\Pi_3(x') \neq 1$, $x = (\pm 1) \underbrace{(d)}_{[\pm 3]_{(8)}} * \underbrace{(\pm \Pi_1\, p_{13})}_{[\pm 3]_{(8)}} *** \underbrace{(\pm p_{k3})}_{[\pm 3]_{(8)}} *** \underbrace{(\pm p_{\alpha_3 3})}_{[\pm 3]_{(8)}}$. Hence, $d|_{\tau'_{(8)}} x$ and by Remark (1) $d|_{\tau_{(8)}} x$. □

Lemma (3) showed that given any divisor $d \in [\pm 3]_{(8)}$ of x with $GCD(x, 2) = 1$, with some positive prime factors equivalent to $[\pm 3]_{(8)}$ is a $\tau_{(8)}$-factor of x; similar as in Proposition (7). The next result is very similar to Proposition (8) and Theorem (9).

Theorem 15. *Let x be a relative prime integer with respect to 2 and $y \in [\pm 3]_{(8)}$. Suppose $d = GCD(x, y)$ and $c|d$ where $c \in [\pm 3]_{(8)}$ and $\Pi_3\left(\frac{x}{d}\right) \neq 1$. Then $c|_{\tau_{(8)}} x, y$ if and only if $c|_{\tau_{(8)}} GCD(x, y)$. Moreover the maximum common $\tau_{(8)}$-factor of x and y is the $max\{c \in [\pm 3]_{(8)} : c|_{\tau_{(8)}} GCD(x, y)\}$.*

Proof. Since $c|d$, there exist $c' \in \mathbb{Z}^*$ such that $d = c \cdot c'$.
$(\Rightarrow)$ If $d \in [\pm 1]_{(8)}$, $c' \in [\pm 3]_{(8)}$ (because $c \in [\pm 3]_{(8)}$). Therefore $c|_{\tau_{(8)}} d$ because $d = (\pm 1)\underbrace{(c)}_{[\pm 3]_{(8)}} * \underbrace{(\pm c')}_{[\pm 3]_{(8)}}$, is a $\tau_{(8)}$-factorization of d. If $d \in [\pm 3]_{(8)}$, $c' \in [\pm 1]_{(8)}$. Since $\Pi_3(c') \neq 1$, by Lemma (3), $c|_{\tau_{(8)}} d$.
$(\Leftarrow)$ Now suppose that $c|_{\tau_{(8)}} d$, hence c divides d. By transitivity $c|x$ and $c|y$. Since $c \in [\pm 3]_{(8)}$, then by Lemma (3), $c|_{\tau_{(8)}} x, y$. For the second statement notice by Lemma (3) that, $\{d : d|_{\tau_{(8)}} x, y\} = \{d \in [\pm 3]_{(8)} : d|_{\tau_{(8)}} x, y\}$ and by the first statement $\{d : d|_{\tau_{(8)}} x, y\} = \{c \in [\pm 3]_{(8)} : c|_{\tau_{(8)}} GCD(x, y)\}$. Since $\tau_{(8)}$-$MCD(x, y)$ is the maximum of the common $\tau_{(8)}$-factors of x and y, then

$$\tau_{(8)}\text{-}MCD(x, y) = max\{c \in [\pm 3]_{(8)} : c|_{\tau_{(8)}} GCD(x, y)\}.$$

□

Note that if $x \in [\pm 2]_{(8)}$, $x = 2x'$ where $2 \nmid x'$, then x is a $\tau_{(8)}$-atom. In the case of $y \in \mathbb{Z}^{\#}$ and $x|_{\tau_{(8)}} y$, then $\tau_{(8)}$-$MCD(x, y) = x$, otherwise the $\tau_{(8)}$-$MCD(x, y) = 1$. If $y \in [\pm b]_{(8)}$ where $b \in \{1, 3\}$, the $\tau_{(8)}$-factors of y are in $[\pm b]_{(8)}$. Hence, if $x \notin [\pm b]_{(8)}$, then $\tau_{(8)}$-$MCD(x, y) = 1$.

The following summarize the formulas found for the $\tau_{(8)}$-MCD of elements in $\mathbb{Z}^{\#}$ when the $\tau_{(8)}$-$MCD \neq 1$. The tables (3–5) and (3–6) show the results found for elements in $[0]_{(8)}$, $[\pm 4]_{(8)}$ and $[\pm b]_{(8)}$ for $b \in \{1, 3\}$, respectively. If a number $x \in [0]_{(8)}$, then $x = 2^n \cdot x'$ where $n \geq 3$ and $2 \nmid x'$.

Table 3–5: The $\tau_{(8)}$-MCD for numbers in $[0]_{(8)}$

$(2^n x', 2^m y')$	$\tau_{(8)}$-$MCD(x, y)$
$n, m \geq 3$	$2^{min\{n,m\}-3} \cdot GCD(x', y')$
$n \in \{3, 5\}$ and $m \in \{3, 5\}$	$2 \cdot GCD(x', y')$
$n = 4$ and $m = 2k$ for $k \geq 2$	$2^2 \cdot GCD(x', y')$
$n = 4$ and $m > 1$ an odd number	$2 \cdot GCD(x', y')$

If a number $x \in [\pm 4]_{(8)}$, then $x = 2^2 x'$ where $2 \nmid x'$. Hence, when a number $x \in [\pm 4]_{(8)}$ and other number y is of the form $2^m y'$ for $m \geq 2$ and $2 \nmid y'$. Then the maximum common $\tau_{(8)}$-factor of x and y is $2 \cdot GCD(x', y')$.

Note that if a number $x \in [\pm 1]_{(8)}$ or $x \in [\pm 3]_{(8)}$, then x can be written as $8k \pm 1$ or $8k \pm 3$, respectively. Table (3–6) summarizes the formulas found for the $\tau_{(8)}$-MCD between numbers that are in classes whose representatives are relative primes to 8, that are the classes $[\pm 1]_{(8)}$ or $[\pm 3]_{(8)}$.

Table 3–6: The $\tau_{(8)}$-MCD for numbers in $[\pm b]_{(8)}$ where $b \in \{1, 3\}$

(x, y)	$\tau_{(8)}$-$MCD(x, y)$
$(8k \pm 1, 8l \pm 1)$	$GCD(8k \pm 1, 8l \pm 1)$
$(8k \pm 1, 8l \pm 3)$	m
$(8k \pm 3, 8l \pm 3)$	m

Where m denotes the the $max\,\{x_i \in [\pm 3]_{(8)} : x_i|_{\tau_{(8)}} GCD(x, y)\}$.

3.2.3 The $\tau_{(10)}$-MCD

In the previous section, we developed a pattern of the $\tau_{(8)}$-MCD. The approach used to study the $\tau_{(10)}$-MCD is very similar. The main differences is the number of equivalences classes with respect to τ_{10}. But as for $n = 8$, there is two clases that are very similar to $[\pm 1]_{(5)}$ and $[\pm 2]_{(5)}$ and they are $[\pm 1]_{(10)}$ and $[\pm 3]_{(10)}$ respectively. First, we find pattern when $x, y \in [\pm a]_{(10)}$ and $GCD(a, 10) \neq 1$. In these cases, the patterns are divided into 4 distinct cases to be analyze individually. Finally the cases, when $GCD(a, 10) = 1$, should be very similar to the results in Lemma (3) and Theorem (15) from previous section or Propositions (7), (8). But first let us study, how the equivalence classes of $\tau'_{(10)}$ behave and the connection with the $\tau'_{(10)}$-products.

Proposition 10. *Let* $x = \prod_{i=1}^{m} x_i$ *be a* $\tau_{(10)}$*-product, where each* $x_i \in [\pm b]_{(10)}$ *and* $b \in \{2, 3, 4, 5\}$. *Then:*

i. If $b = 2$ *and* m *is odd,* $x \in [\pm 2]_{(10)}$,

ii. If $b = 2$ *and* m *is even* $x \in [\pm 4]_{(10)}$,

iii. If $b = 3$ *and* m *is even* $x \in [\pm 1]_{(10)}$,

iv. If $b = 3$ *and* m *is odd,* $x \in [\pm 3]_{(10)}$,

v. If $b = 5$, $x \in [\pm 5]_{(10)}$, *and*

vi. If $b = 4$, $x \in [\pm 4]_{(10)}$.

Proof. First note that $3^2 \equiv -1\,(mod\,10)$ and $3^4 \equiv 1\,(mod\,10)$. Hence $3^{2n} \equiv \pm 1\,(mod\,10)$ for any n. If $m = 2l$ for some $l \in \mathbb{N}$, $x \equiv \prod_{i=1}^{m} x_i \equiv 3^{2l} \equiv \pm 1\,(mod\,10)$ and in the case of $m = 2l + 1$, then $x \equiv \prod_{i=1}^{m} x_i \equiv 3^{2l+1} \equiv \pm 3\,(mod\,10)$. Hence (iii) and (iv) follows. Also, observe that $2^{2l} \equiv \pm 4(mod\,10)$. So if $m = 2l$ and each $x_i \in [\pm 2]_{(10)}$, $x \equiv 2^{2l} \equiv \pm 4\,(mod\,10)$. On other hand if $m = 2l + 1$, then $x \equiv 2^{2l+1} \equiv 2^{2l} \cdot 2 \equiv \pm 4 \cdot 2 \equiv \pm 2\,(mod\,10)$. Therefore, (i) and (ii) follows. For (v) and (vi), note that $a^n \equiv \pm a\,(mod\,10)$, where $a \in \{4, 5\}$, for any $n \in \mathbb{Z}^+$. □

According to Proposition (10), if $x = 2^n x'$ where $GCD(x', 10) = 1$ and n is an even number, then $x \in [\pm 4]_{(10)}$. As a consequence, x' must be in $[\pm 1]_{(10)}$.

Corollary 2. *Let $x \in [\pm 4]_{(10)}$ and $x = c_1 * * * c_k$ be a $\tau_{(10)}$-factorization of x.*

- *Then, k is odd if and only if $c_i \in [\pm 4]_{(10)}$.*
- *Then, k is even if and only if $c_i \in [\pm 2]_{(10)}$.*

Proof. By Proposition (10), each c_i must be either in $[\pm 2]_{(10)}$ or $[\pm 4]_{(10)}$. Now if k is even and $c \in [\pm 4]_{(10)}$, then x is not in $[\pm 4]_{(10)}$. So if k is even, then each c_i must be in $[\pm 4]_{(10)}$. Similarly, if k is odd, thne each c_i must be in $[\pm 2]_{(10)}$. □

If x is an integer in $[0]_{(10)}$ and c is a $\tau_{(10)}$-factor of x, then by Lemma (2) $c \in [0]_{(10)}$. Suppose $x = 2^{n_1} \cdot 5^{n_2} x'$ with $n_1, n_2 > 1$, and $GCD(x', 10) = 1$. Then as a result of Lemma (2) $c = 2^{m_1} \cdot 5^{m_2} x''$, $m_1 < n_1$, $m_2 < n_2$ and $x'' | x'$. The following Theorem is similar to Theorem (5).

Theorem 16. *Let $x, y \in [0]_{(10)}$, where $x = 2^{n_1} 5^{n_2} x'$ and $y = 2^{m_1} 5^{m_2} y'$ with $n_1, n_2, m_1, m_2 > 1$. Then $\tau_{(10)}$-$MCD(x, y) = 2^{min\{n_1, m_1\}-1} . 5^{min\{n_2, m_2\}-1} GCD(x', y')$.*

Proof. Let $d_1 = GCD(x', y')$, and without loss of generality we suppose that $n_1 = min\{n_1, m_1\}$ and $m_2 = min\{n_2, m_2\}$. We claim that $2^{n_1-1} \cdot 5^{m_2-1} d_1$ is the maximum common $\tau_{(10)}$-factor of x and y. Since $d_1 = GCD(x', y')$, there are integers x'' and y'' such that, $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. Notice that $x = \underbrace{(2^{n_1-1} \cdot 5^{m_2-1} d_1)}_{[0]_{(10)}} * \underbrace{(2 \cdot 5^{t_2+1} x'')}_{[0]_{(10)}}$ and $y = \underbrace{(2^{n_1-1} \cdot 5^{m_2-1} d_1)}_{[0]_{(10)}} * \underbrace{(2^{t_1+1} \cdot 5y'')}_{[0]_{(10)}}$. Thus $2^{n_1-1} \cdot 5^{m_2-1} d_1 |_{\tau_{(10)}} x, y$. Now suppose that there exists c, a common $\tau_{(10)}$-factor of x and y, then by Lemma (2) $c = 2^n \cdot 5^m c_1$ where $1 \leq n < n_1$, $1 \leq m < m_2$ and $c_1 | x', y'$. Since $d_1 = GCD(x', y')$, by definition of d_1, $c_1 \leq d_1$ and $c \leq 2^{n_1-1} . 5^{m_2-1} . d_1$. Hence $2^{n_1-1} . 5^{m_2-1} . d_1 = \tau_{(10)}$-$MCD(x, y)$. □

Under the assumption that $x \in [\pm a]_{(10)}$, where $a \in \{2,5\}$, x can be written as $x = a^n x'$ with $n \geq 1$ and x' not divisible by 2 and 5. If there exist $c|_{\tau_{(10)}} x$, then by Lemma (2) $c = a^m c'$ with $1 \leq m < n$ and $c'|x'$.

Theorem 17. *Let* $x = 5^n x'$, $y = 5^m y'$, *where* $n, m > 1$, $GCD(5, x'y') = 1$, *then* $\tau_{(10)}$*-*$MCD(x,y) = 5^{min\{n,m\}-1} GCD(x', y')$*.*

Proof. Without loss of generality suppose that $n = min\{n,m\}$, let $d_1 = GCD(x', y')$. Then there are integers x'' and y'' such that $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. Note that by Proposition (10) x', d_1, x'' and y'' belong to either $[\pm 1]_{(10)}$ or $[\pm 3]_{(10)}$ (because d_1 is not divisible by 5 nor 2). Since $d_1 \in [\pm 1]_{(10)}$ or $d_1 \in [\pm 3]_{(10)}$, $5 \cdot d_1 \in [\pm 5]_{(10)}$. Therefore, $x = (\pm 1) \underbrace{(5^{n-1} \cdot d_1)}_{[\pm 5]_{(10)}} * \underbrace{(\pm 5 \cdot x'')}_{[\pm 5]_{(10)}}$ for a suitable signs and $d_1|_{\tau_{(10)}} x$. Analogously, $d_1|_{\tau_{(10)}} y$. If there exist a common $\tau_{(10)}$-factor c of x and y, then by Lemma (2) $c = 5^t c'$ where $0 < m < n$ and $c'|d_1$. Hence, $c = 5^t c' \leq 5^{n-1} d_1$. So $\tau'_{(10)}$-$MCD(x,y) = 5^{n-1} d_1$. By Remark (1), $\tau_{(10)}$-$MCD(x,y) = 5^{n-1} d_1$. □

Proposition 11. *Suppose that* $x = 2^n x'$ *and* $2 \nmid x'$*. If* $x \in [\pm 2]_{(10)}$*, then the following holds.*

i. If n *is even,* $x' \in [\pm 3]_{(10)}$*.*

ii. If n *is odd,* $x' \in [\pm 1]_{(10)}$*.*

Proof. Since $x \in [\pm 2]_{(10)}$ and $2 \nmid x'$, then $GCD(x', 10) = 1$. So either $x' \in [\pm 1]_{(10)}$ or $x' \in [\pm 3]_{(10)}$. By Proposition (10), if n is odd, then $2^n \in [\pm 2]_{(10)}$ and $x' \in [\pm 1]_{(10)}$. Otherwise, if $x' \in [\pm 3]_{(10)}$, then $x \in [\pm 4]_{(10)}$. A contradiction to the assumption of $x \in [\pm 2]_{(10)}$. Now, by Proposition (10), $2^n \in [\pm 4]_{(10)}$ only when n is even. In order for $x \in [\pm 2]_{(10)}$, x' must be in $[\pm 3]_{(10)}$. □

Suppose $x \in [\pm 2]_{(10)}$, $x = 2^n x'$ where $2 \nmid x'$. If there exists $c|_{\tau_{(10)}} x$, then by Lemma (2) $c = 2^l \cdot c'$, where $0 < l < n$ and $c'|x'$.

Proposition 12. *Let $x \in [\pm 2]_{(10)}$. Suppose that $x = 2^n x'$ where $2 \nmid x'$, $c|_{\tau_{(10)}} x$, that is $x = (\pm 1)\, c * c_1 * * * c_k$. Then $c \in [\pm 2]_{(10)}$ and k is even.*

Proof. First note that by Lemma (2) $c = 2^l \cdot c'$, where $l < n$ and $c'|x'$. If c is not in $[\pm 2]_{(10)}$. Then c must be in $[\pm 4]_{(10)}$. But Proposition (10) implies that $x \in [\pm 4]_{(10)}$, a contradiction to the assumption of $x \in [\pm 2]_{(10)}$. Therefore $c \in [\pm 2]_{(10)}$. On the other hand, if k is even, there is an odd number of $\tau_{(10)}$-factors of x and by Proposition (10), $x \in [\pm 2]_{(10)}$. Otherwise, if k is odd there is an even number of $\tau_{(10)}$-factors of x and by Proposition (10), $x \in [\pm 4]_{(10)}$. □

Theorem 18. *Let $x, y \in [\pm 2]_{(10)}$. Suppose that $x = 2^n x'$, $y = 2^m y'$, with $2 \nmid x', y'$ and $min\{n, m\}$ is an odd number . If $d_1 = GCD(x', y')$, then $\tau_{(10)}$-$MCD(x, y)$ is*

i. $2^{min\{n,m\}-2} d_1$, *when* $d_1 \in [\pm 1]_{(10)}$, *or*

ii. $2^{min\{n,m\}-3} d_1$, *when* $d_1 \in [\pm 3]_{(10)}$.

Proof. Without loss of generality, assume that $n \leq m$, then n is odd. There exist $t \in \mathbb{Z}^+$, such that, $m = n + t$. Suppose m is odd, then t is even. By Proposition (10) $2^t \equiv \pm 4\,(mod\, 10)$ and by Proposition (11) $x', y' \in [\pm 1]_{(10)}$. Since $d_1 = GCD(x', y')$, there are x'' and y'' such that $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. For the first statement, suppose $d_1 \in [\pm 1]_{(10)}$, and Proposition (10) forces both x'' and y'' belong to $[\pm 1]_{(10)}$. Hence, $x = 2^{n-2+2} \cdot d_1 \cdot x'' = (\pm 1) \underbrace{(2^{n-2} \cdot d_1)}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2 \cdot d_1)}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2)}_{[\pm 2]_{(10)}}$ and $(2^{n-2} \cdot d_1)|_{\tau_{(10)}} x$. Since $t + 1$ is odd, $2^{t+1} \in [\pm 2]_{(10)}$. Therefore, we have $y = 2^{n+t-2+2} \cdot d_1 \cdot y''$ and $y = (\pm 1) \underbrace{(2^{n-2} \cdot d_1)}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2^{t+1} \cdot y'')}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2)}_{[\pm 2]_{(10)}}$.

If m is even, $y' \in [\pm 3]_{(10)}$. Since $d_1 \in [\pm 1]_{(10)}$, then $y'' \in [\pm 3]_{(10)}$. Note that t is odd.

By Proposition (10) $2^t \equiv \pm 2\,(mod\,10)$, so $y = (\pm 1)\underbrace{(2^{n-2}\cdot d_1)}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2^{t+1}\cdot y'')}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2)}_{[\pm 2]_{(10)}}$.
With a suitable choice of signs $(2^{n-2}\cdot d_1)|_{\tau_{(10)}} x, y$.
Suppose there exists a common $\tau_{(10)}$-factor c of x and y. By contradiction suppose $c > (2^{n-2}\cdot d_1)$. By Lemma (2) $c = 2^l c'$, where $0 < l < n$, by the definition of d_1, $c'|d_1$, then $c' \leq d_1$. By the assumption of $c > (2^{n-2}\cdot d_1)$ and $c' \leq d_1$, $2^l > 2^{n-2}$. Therefore, $n-2 < l < n$. The only possible integer is $l = n-1$, which l is even. By Propositions (12) and (11), $c \in [\pm 2]_{(10)}$ and $c' \in [\pm 3]_{(10)}$. Since $c'|x'$, there is $c'' \in [\pm 3]_{(10)}$ (because $x' \in [\pm 1]_{(10)}$) such that, $x' = c''\cdot c'$. Then $x = (2^{n-1}c')\cdot(2\cdot c'') = c\cdot(2\cdot c'')$, but $(2\cdot c'') \in [\pm 4]_{(10)}$, a contradiction because c is a $\tau_{(10)}$-factor of x. Therefore, $2^{n-2}\cdot d_1 = \tau_{(10)}\text{-}MCD(x,y)$.
In the case $d_1 \in [\pm 3]_{(10)}$, $x'', y'' \in [\pm 3]_{(10)}$. Suppose m is an odd integer. Observe that $2^{n-3} \in [\pm 4]_{(10)}$, because $n-3$ is an even number.
So $x = (\pm 1)\underbrace{(2^{n-3}\cdot d_1)}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2^2\cdot x'')}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2)}_{[\pm 2]_{(10)}}$ and $2^{n-3}\cdot d_1|_{\tau_{(10)}} x$. We can observe that $2^{t+2} \equiv \pm 4\,(mod\,10)$, hence, $y = (\pm 1)\underbrace{(2^{n-3}\cdot d_1)}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2^{t+2}\cdot y'')}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2)}_{[\pm 2]_{(10)}}$ and $2^{n-3}\cdot d_1|_{\tau_{(10)}} y$. If m is even, $y'' \in [\pm 1]_{(10)}$ and t is odd. Hence this is a $\tau_{(10)}$-factorization of y, $y = (\pm 1)\underbrace{(2^{n-3}\cdot d_1)}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2^{t+2}\cdot y'')}_{[\pm 2]_{(10)}} * \underbrace{(\pm 2)}_{[\pm 2]_{(10)}}$ and $2^{n-3}\cdot d_1|_{\tau_{(10)}} y$. Therefore $2^{n-3}\cdot d_1$ is a common $\tau_{(10)}$-factor of x and y. If there exist c another common $\tau_{(10)}$-factor of x and y. Suppose by contradiction $c > (2^{n-3}\cdot d_1)$, then by Lemma (2) $c = 2^{n-2}\cdot c_1$ or $c = 2^{n-1}\cdot c_1$.

By proposition (12), $c \in [\pm 2]_{(10)}$ and $c_1|x', y'$, hence $c_1|d_1$ and $d_1 = c_1 k$. In the case $c = 2^{n-1}c_1$, we observe that $n-1$ is an even integer, hence $c_1 \in [\pm 3]_{(10)}$. As a consequence, $x' = c_1\cdot c''$ and $x = (2^{n-1}\cdot c_1)\cdot(2\cdot c'')$. Since $2^{n-1}\cdot c_1 \in [\pm 2]_{(10)}$ and $2\cdot c'' \in [\pm 4]_{(10)}$, $c = 2^{n-1}\cdot c_1 \nmid x$. Now assume $c = 2^{n-2}\cdot c_1$, $n-2$ is odd and $c_1 \in [\pm 1]_{(10)}$. Since $d_1 = c_1 k$ and $d_1 \in [\pm 3]_{(10)}$, then $k \in [\pm 3]_{(10)}$ and $2^{n-3}d_1$ is $2^{n-2}c_1 + 2^{n-3}kc_1 - 2^{n-2}c_1 = 2^{n-2}c_1\left(1 + \frac{1}{2}(k-2)\right)$. Notice that $\left(1 + \frac{1}{2}(k-2)\right) > 0$, because $k \geq 3$. Therefore $2^{n-3}d_1 = 2^{n-2}c_1 \cdot l > 2^{n-2}c_1$, where $l = \big(1 + \frac{1}{2}(k-2)\big)$. This concludes the proof. □

Theorem 19. *Let $x, y \in [\pm 2]_{(10)}$, with $x = 2^n x'$, $y = 2^m y'$, $2 \nmid x', y'$ and $min\{n, m\}$ an even number. If $d_1 = GCD(x', y')$, then $\tau_{(10)}$-$MCD(x, y)$ is*

i. $2^{min\{n,m\}-3}d_1$, when $d_1 \in [\pm 1]_{(10)}$, or

ii. $2^{min\{n,m\}-2}d_1$, when $d_1 \in [\pm 3]_{(10)}$.

Proof. Without loss of generality, suppose that $n = min\{n, m\}$. Then n is an even number. Hence, there exist $t \in \mathbb{Z}^+$, such that $m = n + t$. In the case of m to be an even number, then t is even and, $2^t \equiv \pm 4\,(mod\,10)$, if m is odd, then t is odd and $2^t \equiv \pm 2(mod\,10)$. By hypothesis $d_1 = GCD(x', y')$, then $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. By the proof of Proposition (11), $x', y' \in [\pm 3]_{(10)}$ when both n and m are even. And $y' \in [\pm 1]_{(10)}$, if m is odd.

For (i), suppose that $d_1 \in [\pm 1]_{(10)}$, then either both $x'', y'' \in [\pm 3]_{(10)}$, or $x'' \in [\pm 3]_{(10)}$ and $y'' \in [\pm 1]_{(10)}$. Since $2^{n-3} \in [\pm 2]_{(10)}$, an analogous proof of (ii) in the previous theorem gives the proof for this case.

Similarly for (ii), if $d_1 \in [\pm 3]_{(10)}$, $x'', y'' \in [\pm 1]_{(10)} \cup [\pm 3]_{(10)}$. Since $2^{n-2} \in [\pm 4]_{(10)}$, an analogous proof of (i) in the previous theorem does the work. □

Theorem 20. *Let $x, y \in [\pm 4]_{(10)}$, where $x = 2^n x'$, $y = 2^m y'$. If $GCD(x' \cdot y', 10) = 1$. Then $\tau_{(10)}$-$MCD(x, y) = 2^{min\{n,m\}-1}GCD(x', y')$.*

Proof. Suppose that $n = min\{n, m\}$ is an odd number (respectively, an even number), and $m = n + t$ for some positive integer t. By proposition (10), $x' \in [\pm 3]_{(10)}$ (respectively $x' \in [\pm 1]_{(10)}$). Let $d_1 = GCD(x', y')$, then $x' = d_1 x''$ and $y' = d_1 y''$, note that, either $d_1 \in [\pm 1]_{(10)}$ or $d_1 \in [\pm 3]_{(10)}$. So, we split the proof into two cases:

Case 1. If $d_1 \in [\pm1]_{(10)}$, $x'' \in [\pm3]_{(10)}$ (respectively $x'' \in [\pm1]_{(10)}$). Then $2^{n-1} \cdot d_1 \in [\pm4]_{(10)}$ (respectively, $2^{n-1} \cdot d_1 \in [\pm2]_{(10)}$) and $x = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm4]_{(10)}} * \underbrace{(2 \cdot x'')}_{[\pm4]_{(10)}}$, (respectively $x = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm2]_{(10)}} * \underbrace{(2 \cdot x'')}_{[\pm2]_{(10)}}$), thus $(2^{n-1} \cdot d_1)|_{\tau_{(10)}} x$. Observe that m could be either an odd or an even integer. If m is odd, then $y' \in [\pm3]_{(10)}$ and $y'' \in [\pm3]_{(10)}$. Therefore t is an even number (respectively, odd number), then $2^t \in [\pm4]_{(10)}$ (respectively, $2^t \in [\pm2]_{(10)}$) and $y = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm4]_{(10)}} * \underbrace{(2^{t+1} \cdot y'')}_{[\pm4]_{(10)}}$, (respectively $y = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm2]_{(10)}} * \underbrace{(2^{t+1} \cdot y'')}_{[\pm2]_{(10)}}$). If m is an even number, then we have that $y' \in [\pm1]_{(10)}$ and $y'' \in [\pm1]_{(10)}$ therefore t is odd (respectively, even), $2^t \in [\pm2]_{(10)}$ (respectively, $2^t \in [\pm4]_{(10)}$) and $y = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm4]_{(10)}} * \underbrace{(2^{t+1} \cdot y'')}_{[\pm4]_{(10)}}$ (respectively, ($y = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm2]_{(10)}} * \underbrace{(2^{t+1} \cdot y'')}_{[\pm2]_{(10)}}$)). Hence, in both cases $2^{n-1} \cdot d_1$ is a common $\tau_{(10)}$-factor of x and y.

Case 2. If $d_1 \in [\pm3]_{(10)}$, then $x'' \in [\pm1]_{(10)}$ (respectively, $x'' \in [\pm3]_{(10)}$). Therefore we have $2^{n-1} \cdot d_1 \in [\pm2]_{(10)}$ (respectively, $2^{n-1} \cdot d_1 \in [\pm4]_{(10)}$), obtaining $x = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm2]_{(10)}} * \underbrace{(2 \cdot x'')}_{[\pm2]_{(10)}}$ (respectively, $x = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm4]_{(10)}} * \underbrace{(2 \cdot x'')}_{[\pm4]_{(10)}}$) , and we have that $(2^{n-1} \cdot d_1)|_{\tau_{(10)}} x$.

If m is odd, then $y' \in [\pm3]_{(10)}$, $y'' \in [\pm1]_{(10)}$ and t is an even number (respectively, odd number). Hence $2^t \in [\pm4]_{(10)}$ (respectively, $2^t \in [\pm2]_{(10)}$) and $y = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm2]_{(10)}} * \underbrace{(2^{t+1} \cdot y'')}_{[\pm2]_{(10)}}$, (respectively, $y = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm4]_{(10)}} * \underbrace{(2^{t+1} \cdot y'')}_{[\pm4]_{(10)}}$).

If m is an even number, then $y' \in [\pm1]_{(10)}$, $y'' \in [\pm3]_{(10)}$ and t is odd (respectively, an even) integer. Therefore, $2^t \in [\pm2]_{(10)}$ (respectively, $2^t \in [\pm4]_{(10)}$) and $y = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm2]_{(10)}} * \underbrace{(2^{t+1} \cdot y'')}_{[\pm2]_{(10)}}$, (respectively, $y = (\pm1)\ \underbrace{(2^{n-1} \cdot d_1)}_{[\pm4]_{(10)}} * \underbrace{(2^{t+1} \cdot y'')}_{[\pm4]_{(10)}}$).

So, $(2^{n-1} \cdot d_1)|_{\tau_{(10)}} x, y$.

If c is another common $\tau_{(10)}$-factor of x and y, by Lemma (2) $c = 2^l c'$, where $c'|x', y'$ and $1 \leq l \leq n-1$. Therefore, $c' \leq d_1$ by the definition of d_1. So $c \leq 2^{n-1} \cdot d_1$. This shows that that $\tau'_{(10)}$-$MCD(x,y) = 2^{n-1} \cdot d_1$. By remark $\tau_{(10)}$-$MCD(x,y) = 2^{n-1} \cdot d_1$ (1). □

Corollary 3. *Let $x \in [\pm 2]_{(10)}$ and $y \in [\pm 4]_{(10)}$, with $x = 2^n x'$, $y = 2^m y'$, with $2 \nmid x', y'$. If $d_1 = GCD(x', y')$, then $\tau_{(10)}$-$MCD(x,y)$ is given by one of the following formulas.*

i. $2^{min\{n,m\}-2} d_1$, *when $d_1 \in [\pm 1]_{(10)}$ and $min\{n,m\}$ is odd.*

ii. $2^{min\{n,m\}-3} d_1$, *when $d_1 \in [\pm 3]_{(10)}$ and $min\{n,m\}$ is odd.*

iii. $2^{min\{n,m\}-3} d_1$, *when $d_1 \in [\pm 1]_{(10)}$ and $min\{n,m\}$ is even.*

iv. $2^{min\{n,m\}-2} d_1$, *when $d_1 \in [\pm 3]_{(10)}$ and $min\{n,m\}$ is even.*

Proof. The proof is analogous to the proof of the Theorems (18), (19) and (20). □

Proposition 13. *If $x, y \in [\pm 1]_{(10)}$, then $\tau_{(10)}$-$MCD(x,y) = GCD(x,y)$.*

Proof. Let $d = GCD(x,y)$, then there are integers x' and y' such that $x = dx'$ and $y = dy'$. Since $x, y \in [\pm 1]_{(6)}$, $d \in [\pm a]_{(10)}$ with $a \in \{1, 3\}$. If $d \in [\pm 1]_{(10)}$, then $x' \in [\pm 1]_{(10)}$. If $d \in [\pm 3]_{(10)}$, then $x' \in [\pm 3]_{(10)}$. In both cases, for a suitable choice of the signs $x = (\pm 1)\, d * (\pm x')$ is a $\tau'_{(10)}$-factorizations of x. Analogously, $d|_{\tau_{(10)}} y$. Therefore, $\tau_{(10)}$-$MCD(x,y) = GCD(x,y)$. □

Lemma 4. *Let $x \in [\pm b]_{(10)}$, where $b \in \{1, 3\}$. Suppose $d \in [\pm 3]_{(10)}$ such that $d|x$. If $\Pi_3(\frac{x}{d}) \neq 1$, then $d|_{\tau_{(10)}} x$.*

Proof. Since $d|x$, then $x = d \cdot x'$ for $x' \in \mathbb{Z}^*$. Let us rewrite $x' = \frac{x}{d}$ into a product of primes in $[\pm 1]_{(10)}$ and primes in $[\pm 3]_{(10)}$. So the canonical factorization of x' is $x' = \Pi_1(x') \cdot \Pi_3(x') = \prod_{i=1}^{\alpha_1} p_{i1}^{a_{i1}} \cdot \prod_{i=1}^{\alpha_3} p_{i3}^{a_{i3}}$, then $x = d \cdot x' = d \cdot \prod_{i=1}^{\alpha_1} p_{i1}^{a_{i1}} \cdot \prod_{i=1}^{\alpha_3} p_{i3}^{a_{i3}}$. Since

$\Pi_3(x') \neq 1$, $x = (\pm 1) \underbrace{(d)}_{[\pm 3]_{(10)}} * \underbrace{(\pm \Pi_1 \, p_{13})}_{[\pm 3]_{(10)}} *** \underbrace{(\pm p_{k3})}_{[\pm 3]_{(10)}} *** \underbrace{(\pm p_{\alpha 33})}_{[\pm 3]_{(10)}}$. Hence, $d|_{\tau'_{(10)}} x$ and by Remark (1) $d|_{\tau_{(10)}} x$. □

Lemma (4) showed that given any divisor $d \in [\pm 3]_{(8)}$ of x with $GCD(x, 2) = 1$, with some positive prime factors equivalent to $[\pm 3]_{(10)}$ is a $\tau_{(10)}$-factor of x; similar as in Proposition (7). The next result is very similar to Proposition (8) and Theorem (9).

Theorem 21. *Let x be a relatively prime integer with respect to 2 and $y \in [\pm 3]_{(10)}$. Suppose $d = GCD(x, y)$ and $c|d$ where $c \in [\pm 3]_{(10)}$ and $\Pi_3\left(\frac{x}{d}\right) \neq 1$. Then $c|_{\tau_{(10)}} x, y$ if and only if $c|_{\tau_{(10)}} GCD(x, y)$. Moreover, the maximum common $\tau_{(10)}$-factor between x and y is the max$\{c \in [\pm 3]_{(10)} : c|_{\tau_{(10)}} GCD(x, y)\}$.*

Proof. The proof is analogous to the proof in Theorem (15). □

Now, we present a summary of the formulas for the $\tau_{(10)}$-MCD of elements in $\mathbb{Z}^{\#}$ when they have a common $\tau_{(10)}$-factor. The Tables (3–7) and (3–8) show the results found for numbers that are in classes whose representatives are not relative prime to 10, that are $[0]_{(10)}$, $[\pm 5]_{(10)}$, $[\pm 2]_{(10)}$ and $[\pm 4]_{(10)}$. Suppose $x = 2^n \cdot 5^m x'$, where $GCD(10, x') = 1$. If $n, m > 1$, then $x \in [0]_{(10)}$. Notice that for $n = 0$, $x \in [\pm 5]_{(10)}$ and in the case of $m = 0$, $x \in [\pm 2]_{(10)}$ or $x \in [\pm 4]_{(10)}$. The first table summarizes the formulas for the $\tau_{(10)}$-MCD when the elements are in $[0]_{(10)}$ and $[\pm 5]_{(10)}$.

Table 3–7: The $\tau_{(10)}$-MCD for numbers in $[0]_{(10)}$ and $[\pm 5]_{(10)}$

(x, y)	$\tau_{(10)}$-$MCD(x, y)$
$(2^n 5^u x', 2^m 5^v y')$	$2^{min\{n,m\}-1} 5^{min\{u,v\}-1} GCD(x', y')$
$(5^u x', 5^v y')$	$5^{min\{u,v\}-1} GCD(x', y')$

If both numbers are in $[\pm 2]_{(10)}$, notice that these formulas depended of the parity of the least power of 2 and in which equivalence class is $d_1 = GCD(x', y')$. Moreover, if a number is in $[\pm 2]_{(10)}$ and the other number is in $[\pm 4]_{(10)}$, then the results are summarized in Table (3–8).

Table 3–8: The $\tau_{(10)}$-MCD when $(x, y) \in [\pm 2]_{(10)} \times ([\pm 2]_{(10)} \cup [\pm 4]_{(10)})$

(x, y)	$\tau_{(10)}$-$MCD(x, y)$
$(2^n x', 2^m y')$ n is even and $n < m$	$2^{n-3}d_1$, when $d_1 \in [\pm 1]_{(10)}$ $2^{n-2}d_1$, when $d_1 \in [\pm 3]_{(10)}$
$(2^n x', 2^m y')$ n is odd and $n < m$	$2^{n-2}d_1$, when $d_1 \in [\pm 1]_{(10)}$ $2^{n-3}d_1$, when $d_1 \in [\pm 3]_{(10)}$

Here $d_1 = GCD(x', y')$

When both elements are in $[\pm 4]_{(10)}$, then

$$\tau_{(10)}\text{-}MCD(2^n x', 2^m y') = 2^{min\{n,m\}-1} GCD(x', y').$$

Since the behavior of $[\pm 1]_{(10)}$ and $[\pm 3]_{(10)}$ is similar to the behavior of $[\pm 1]_{(8)}$ and $[\pm 3]_{(8)}$, the results for the $\tau_{(10)}$-$MCD(x, y)$ and the $\tau_{(10)}$-$MCD(x, y)$ are also similar. Then the results found between elements of $[\pm 1]_{(8)}$ and $[\pm 3]_{(10)}$ can be observed in Table (3–6), and does not need for another table. The reader must notice that the cases left out are the ones of pair of integers such that they do not have common τ_{10}-factors. With this case we have found all the formulas of the $\tau_{(n)}$-MCD for each n that makes $\mathbb{Z}$ $\tau_{(n)}$-atomic.

3.2.4 The $\tau_{(12)}$-MCD

As seen in the cases of $n \in \{5, 8, 10\}$, when $n = 12$, there two equivalence classes that will follow the same behavior as $[\pm 1]_{(5)}$ and $[\pm 2]_{(5)}$. This classes are $[\pm 1]_{(12)}$ and $[\pm 5]_{(12)}$, respectively. For the other equivalence classes of $\tau'_{(12)}$ need to be study case by case, hence we develope several propositions and theorem to address those cases and to see the behavior of $\tau'_{(12)}$-factors on such equivalence classes.

If $x = \prod_{i=1}^{m} x_i$ be a $\tau_{(12)}$-product and $x_i \in [\pm 1]_{(12)}$, then $x \in [\pm 1]_{(12)}$. The converse is not true in general, because the product of two integers in the equivalence class of $[\pm 5]_{(10)}$ will give an element in the equivalence class of $[\pm 1]_{(10)}$. This result is very similar to what happen with $[\pm 2]_{(10)}$ and we formalize in the following proposition.

Proposition 14. *Let $x = \prod_{i=1}^{m} x_i$ be a $\tau_{(12)}$-product, where each $x_i \in [\pm 5]_{(12)}$, then*

i. m is even if and only if $x \in [\pm 1]_{(12)}$, and

ii. m is odd if and only if $x \in [\pm 5]_{(12)}$.

Proof. ($\Rightarrow$) Since $(\pm 5)^2 \equiv 1\,(mod\,12)$, hence if $m = 2k$, $5^m \equiv \pm 1\,(mod\,12)$, for any $m \in \mathbb{Z}$, so (i) follows. For $(ii.)$, write $x = \left(\prod_{i=1}^{m-1} x_i\right) x_m$, and notice that $\left(\prod_{i=1}^{m-1} x_i\right) \in [\pm 1]_{(12)}$ and $x_m \in [\pm 5]_{(12)}$. Therefore $x \in [\pm 5]_{(12)}$.
($\Leftarrow$) Recall that each $x_i \in [\pm 5]_{(12)}$ and note that m is either an even or an odd integer. We have that $5^{2k} \equiv \pm 1\,(mod\,12)$, and $5^{2k+1} \equiv \pm 5 \cdot 5^{2k}\,(mod\,12)$. □

Proposition 15. *Let $x, y \in [\pm 1]_{(12)}$, $\tau_{(12)}$-$MCD(x, y) = GCD(x, y)$.*

Proof. Let $d = GCD(x, y)$, then $x = dx'$ and $y = dy'$ for some $x', y' \in \mathbb{Z}^*$. Since $x, y \in [\pm 1]_{(12)}$, either $d \in [\pm 1]_{(12)}$ or $d \in [\pm 5]_{(12)}$. If $d \in [\pm 1]_{(12)}$, then $x' \in [\pm 1]_{(12)}$ and $y' \in [\pm 1]_{(12)}$ (because $x, y \in [\pm 1]_{(12)}$). In this case, with an appropiate choice of signs, $x = (\pm 1)\underbrace{(d)}_{[\pm 1]_{(12)}} * \underbrace{(\pm\, x')}_{[\pm 1]_{(12)}}$ and $y = (\pm 1)\underbrace{(d)}_{[\pm 1]_{(12)}} * \underbrace{(\pm\, y')}_{[\pm 1]_{(12)}}$ are $\tau_{(12)}$-factorizations of x and y, respectively. If $d \in [\pm 5]_{(12)}$, by Proposition (14), $x' \in [\pm 5]_{(12)}$ and $y' \in [\pm 5]_{(12)}$ which implies $x = (\pm 1)\underbrace{(d)}_{[\pm 5]_{(12)}} * \underbrace{(\pm\, x')}_{[\pm 5]_{(12)}}$ and $y = (\pm 1)\underbrace{(d)}_{[\pm 5]_{(12)}} * \underbrace{(\pm\, y')}_{[\pm 5]_{(12)}}$ are $\tau_{(12)}$-factorizations of x and y, respectively. If there is a $\tau_{(12)}$-factor c of x and y. So it is a factor and therefore $c \leq d$. This shows $d = \tau_{(12)}\text{-}MCD(x, y)$, in both cases. □

Proposition 16. *Let $x \in [\pm b]_{(12)}$ and $d \in [\pm 5]_{(12)}$, where $b \in \{1, 5\}$ and $d|x$. If $\Pi_5\left(\frac{x}{d}\right) \neq 1$, $d|_{\tau_{(12)}} x$.*

Proof. Since $d|x$, $x = d \cdot x'$. If $x \in [\pm 1]_{(12)}$, $x' \in [\pm 5]_{(12)}$, (because $d \in [\pm 5]_{(12)}$). Hence $x = (\pm 1)\, d * (\pm x')$ is a $\tau_{(12)}$-factorization of x. If $x \in [\pm 5]_{(12)}$, hence we have $x' \in [\pm 1]_{(12)}$. Now rewrite $x' = \Pi_1(x') \cdot \Pi_5(x')$. Notice that, $\Pi_1(x') \in [\pm 1]_{(12)}$, this forces $\Pi_5(x') = \prod_{i=1}^{\alpha_5} p_{i5}^{a_{i5}} \in [\pm 1]_{(12)}$. By Proposition (14), $\sum_{i=1}^{\alpha_5} a_{i5} = 2k$. Since $\Pi_5(x') \neq 1$, then

$$x = (\pm 1)\underbrace{(d)}_{[\pm 5]_{(12)}} * \underbrace{(\pm \Pi_1 \cdot p_{15})}_{[\pm 5]_{(12)}} * \underbrace{(\pm p_{15})}_{[\pm 5]_{(12)}} * * * \underbrace{(\pm p_{\alpha_5 5})}_{[\pm 5]_{(12)}}$$

is a $\tau_{(12)}$-factorization and $d|_{\tau_{(12)}} x$. □

Proposition 17. *Let $x \in [\pm b]_{(12)}$ where $y, c \in [\pm 5]_{(12)}$ and $b \in \{1, 5\}$. Denote the $GCD(x, y)$ as d. If $c|d$, and $\Pi_5\left(\frac{d}{c}\right) \neq 1$, then $c|_{\tau_{(12)}} x$ if and only if $c|_{\tau_{(12)}} d$.*

Proof. Let $d = c \cdot c'$, for some $c' \in \mathbb{Z}^{\#}$. By hypothesis $\Pi_5(c') \neq 1$.

($\Leftarrow$) Suppose that $c|_{\tau_{(12)}} d$. Hence c divides d and by transitivity $c|x$ and $c|y$. Since $c \in [\pm 5]_{(12)}$, by Proposition (16), $c|_{\tau_{(12)}} x$.

($\Rightarrow$) If $d \in [\pm 1]_{(12)}$, $c' \in [\pm 5]_{(12)}$. So $d = (\pm 1)\underbrace{(c)}_{[\pm 5]_{(12)}} * \underbrace{(\pm c')}_{[\pm 5]_{(12)}}$ is a $\tau_{(12)}$-factorization of d and $c|_{\tau_{(12)}}d$. If $d \in [\pm 5]_{(12)}$, $c' \in [\pm 1]_{(12)}$. Since $\Pi_5(c') \neq 1$, by Proposition (16), $c|_{\tau_{(12)}}d$. □

Theorem 22. *If $x \in [\pm b]_{(12)}$ where $b \in \{1,5\}$ and $y \in [\pm 2]_{(12)}$, then the maximum common $\tau_{(12)}$-factor of x and y is m, where $m = max\{c \in [\pm 5]_{(12)} : c|_{\tau_{(12)}}GCD(x,y)\}$.*

Proof. The proof follows by the fact that $\{c \in [\pm 5]_{(12)} : c|_{\tau_{(12)}}GCD(x,y)\}$ is the set given by $\{c \in: c|_{\tau_{(12)}}x, y\}$. □

Observe that, if $x \in [\pm 4]_{(10)}$, x can be written as $x = 2^n x'$ where $n > 1$, $GCD(a, x') = 1$ and $a \in \{2,3\}$, then by Proposition (14), either $x' \in [\pm 1]_{(12)}$ or $x' \in [\pm 5]_{(12)}$. Hence, if there exist c such that $c|_{\tau_{(12)}}x$, then by Lemma (2) $c = 2^t c' \in [\pm 2]_{(12)}$ (if $t = 1$) or $c \in [\pm 4]_{(12)}$(if $t > 1$).

Proposition 18. *Let $x = 2^n x'$ and $y = 2^m y'$. Then the following holds.*

i. If $n = 2$ or $n = 3$, $\tau_{(12)}$-$MCD(x,y) = 2 \cdot GCD(x', y')$.

ii. If $n, m \geq 4$, $\tau_{(12)}$-$MCD(x,y) = 2^{min\{n,m\}-2}GCD(x', y')$.

Proof. Without loss of generality, assume that $n = min\{n,m\}$ and we denote d_1 as the $GCD(x', y')$. So $d_1 \in [\pm b]_{(12)}$, where $b \in \{1,5\}$. For the first statement, suppose that $n = 2$. Observe that $(2 \cdot d_1) \in [\pm 2]_{(12)})$. Therefore $x = (\pm 1)\underbrace{(2 \cdot d_1)}_{[\pm 2]_{(12)}} * \underbrace{(\pm 2x'')}_{[\pm 2]_{(12)}}$ and $(2 \cdot d_1)|_{\tau_{(12)}}x$. Now, $y = (\pm 1)\underbrace{(2 \cdot d_1)}_{[\pm 2]_{(12)}} * \underbrace{(\pm 2y'')}_{[\pm 2]_{(12)}} * \underbrace{(\pm 2)}_{[\pm 2]_{(12)}} *** \underbrace{(\pm 2)}_{[\pm 2]_{(12)}}$, then $(2 \cdot d_1)$ is the maximum common $\tau_{(12)}$-factor of x and y. Similarly, if $n = 3$, $(2 \cdot d_1)|_{\tau_{(12)}}x$. It is the maximum common $\tau_{(12)}$-factor of x and y. Otherwise, there exist c such that $c > 2 \cdot d_1$, with the form $c = 2^2 c'$. But such integer is not a $\tau_{(12)}$-factor of x. Thus, $2 \cdot d_1 = \tau_{(12)}$-$MCD(x,y)$ if $n = 2$ or $n = 3$. For $(ii.)$ we need to show that $2^{n-2}d_1$ is a common $\tau_{(12)}$-factor of x and y. Since $d_1 = GCD(x', y')$, there exist x'' and y'' such that $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. Note that by Proposition (14) d_1, x'' and $y'' \in [\pm a]_{(12)}$ where $a \in \{1, 5\}$ (because d_1 is not divisible by 2 nor by 3). Then $x = (\pm 1)\, \underbrace{(2^{n-2} \cdot d_1)}_{[\pm 4]_{(12)}} * \underbrace{(\pm 2^2 \cdot x'')}_{[\pm 4]_{(12)}}$ for a suitable choice of signs $d_1|_{\tau_{(12)}} x$. Analogously, $d_1|_{\tau_{(12)}} y$. If there exist a common $\tau_{(12)}$-factor c of x and y, then by Lemma (2) $c = 2^t c'$, with $1 \leq t \leq n$ and $c'|d_1$. By contradiction suppose $c > 2^{n-2} \cdot d_1$, then $t = n - 1$, because $c'|x'$, (due to $c'|d_1$ and $d_1|x'$) $x' = c' \cdot c''$. Now, $x = (2^{n-1} \cdot c')(2 \cdot c'')$ where $(2 \cdot c'') \in [\pm 2]_{(12)}$ and $2^{n-1} \cdot c' \in [\pm 4]_{(12)}$. A contradiction, because such decomposition must be a $\tau_{(12)}$-factorization. This prove that $\tau_{(12)}$-$MCD(x, y) = 2^{n-2} d_1$. □

Now, we study the case when x, y are both in $[\pm 3]_{(12)}$. These numbers are of the form $3^n x'$, where x' is relative prime to 12. Notice that $3^n \equiv \pm 3\, (mod\, 12)$ for all n. Hence, if there exist a $\tau_{(12)}$-factor of an integer of the form $3^n x'$, such $\tau_{(12)}$-factor must be in $[\pm 3]_{(12)}$.

Proposition 19. *Let $x = 3^n x'$ and $y = 3^m y'$, where $GCD(12, x'y') = 1$. Then $\tau_{(12)}$-$MCD(x, y) = 3^{min\{n,m\}-1} GCD(x', y')$. In other words, if $x, y \in [\pm 3]_{(12)}$ of such form, then $\tau_{(12)}$-$MCD(x, y) = 3^{min\{n,m\}-1} GCD(x', y')$.*

Proof. Without loss of generality suppose that $n = min\{n, m\}$, and $d_1 = GCD(x', y')$. Since $d_1 = GCD(x', y')$, there are integers x'' and y'' such that $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. Note that d_1, x'' and $y'' \in [\pm a]_{(12)}$, where $a \in \{1, 5\}$ (because d_1 is not divisible by 2 nor by 3). Thus $d_1|_{\tau_{(12)}} x$, because $x = (\pm 1)\, \underbrace{(3^{n-1} \cdot d_1)}_{[\pm 3]_{(12)}} * \underbrace{(\pm 3 \cdot x'')}_{[\pm 3]_{(12)}}$ is a $\tau'_{(12)}$-factorization for a suitable choice of signs. Analogously, $d_1|_{\tau_{(12)}} y$. If there exist a common $\tau_{(12)}$-factor c of x and y, then by Lemma (2) $c = 3^t c'$, where $t < n$ and $c'|d_1$. Then $c = 3^t c' \leq 3^{n-1} d_1$. Hence, $\tau_{(12)}$-$MCD(x, y) = 3^{n-1} d_1$. □

If $x \in [\pm 4]_{(12)}$ and $y \in [\pm 3]_{(12)}$, then $\tau_{(12)}$-$MCD(x, y) = 1$, because due to Lemma (2) the $\tau_{(12)}$-factors of x are in $[\pm 2]_{(12)}$ or $[\pm 4]_{(12)}$ and the $\tau_{(12)}$-factors of y are in $[\pm 3]_{(12)}$.

Proposition 20. *Let $x = 2^n \cdot 3^m \cdot x'$, where $GCD(12, x') = 1$, $n \geq 2$ and $m \geq 1$. If $d|x'$ and $n \leq m$, then $(2 \cdot 3 \cdot d)|_{\tau_{(12)}} x$.*

Proof. Suppose that $d|x'$, then there exist x'' such that $x' = d \cdot x''$, and we have $x = (\pm 1)\underbrace{(2 \cdot 3 \cdot d)}_{[\pm 6]_{(12)}} * \underbrace{(2 \cdot 3 \cdot x'')}_{[\pm 6]_{(12)}} * \underbrace{(2 \cdot 3)}_{[\pm 6]_{(12)}} * * * \underbrace{(2 \cdot 3)}_{[\pm 6]_{(12)}} * \underbrace{(2 \cdot 3^{m-(n-2)})}_{[\pm 6]_{(12)}}$. This shows that $(2 \cdot 3 \cdot d)$ is a $\tau_{(12)}$-factor of x. □

Proposition 21. *Suppose that $x = 2^{n_1} \cdot 3^{n_2} \cdot x'$ and $y = 2^{m_1} \cdot 3^{m_2} \cdot y'$, where $GCD(12, x' \cdot y') = 1$ and $x \nmid_{\tau_{(12)}} y$. If $n_1 \in \{2, 3\}$, then $n_1 \leq n_2$ and $m_1 \leq m_2$ if and only if $\tau_{(12)}$-$MCD(x, y) \neq 1$. Moreover, the following holds.*

i. If $n_1 = 2$, $\tau'_{(12)}$-$MCD(x, y) = 2 \cdot 3^{min\{n_2-1, m_2-(m_1-1)\}} \cdot GCD(x', y')$.

ii. If $n_1 = 3$, $\tau'_{(12)}$-$MCD(x, y) = 2 \cdot 3^{min\{n_2-2, m_2-(m_1-1)\}} \cdot GCD(x', y')$.

Proof. ($\Leftarrow$) Suppose by contradiction that $n_1 > n_2$ or $m_1 > m_2$. If $n_1 > n_2$, we have that $x \in \{2^2 3x', 2^3 3^2 x', 2^3 3x'\}$. Therefore x is a $\tau_{(12)}$-atom. Since $x \nmid_{\tau_{(12)}} y$, hence $\tau_{(12)}$-$MCD(x, y) = 1$, a contradiction to the hypothesis. If $m_1 > m_2$, then y can not have $\tau_{(12)}$-factors in $[\pm 6]_{(12)}$, because the amount of $2's$ is greater than the amount of $3's$ in y. But all the $\tau_{(12)}$-factors of x are in $[\pm 6]_{(12)}$. Therefore the $\tau_{(12)}$-$MCD(x, y)$ must be 1, a contradiction.

($\Rightarrow$) Suppose that $d_1 = GCD(x', y')$, then exists x'' and y'' such that $x' = d_1 x''$ and $y' = d_1 y''$. For (i), we claim that $2 \cdot 3^{min\{n_2-1, m_2-(m_1-1)\}} \cdot d_1$ is a common $\tau_{(12)}$-factor of x and y. If $min\{n_2 - 1, m_2 - (m_1 - 1)\} = n_2 - 1$, so $x = \underbrace{(2 \cdot 3^{n_2-1} \cdot d_1)}_{[\pm 6]_{(12)}} * \underbrace{(2 \cdot 3 \cdot x'')}_{[\pm 6]_{(12)}}$ is a $\tau_{(12)}$-factorization of x, so $(2 \cdot 3^{n_2-1} \cdot d_1)|_{\tau_{(12)}} x$. Since $n_2 - 1 \leq m_2 - (m_1 - 1)$, there is a nonnegative integer t such that $m_2 - (m_1 - 1) = (n_2 - 1) + t$. Observe that $m_1 - 1 \leq m_1 - 1 + t = m_2 - (n_2 - 1)$, so the amount of $2's$ is less or equal than the amount of $3's$ in $2^{m_1-1} \cdot 3^{m_2-(n_2-1)}$. Hence $(2 \cdot 3^{n_2-1} \cdot d_1)|_{\tau_{(12)}} y$, because

$$\begin{aligned} y &= (2 \cdot 3^{n_2-1}) \cdot (2^{m_1-1} \cdot 3^{m_2-(n_2-1)}) \\ &= \underbrace{(2 \cdot 3^{n_2-1} \cdot d_1)}_{[\pm 6]_{(12)}} * \underbrace{(2 \cdot 3 \cdot y'')}_{[\pm 6]_{(12)}} * \underbrace{(2 \cdot 3)}_{[\pm 6]_{(12)}} *** \underbrace{(2 \cdot 3)}_{[\pm 6]_{(12)}} * \underbrace{(2 \cdot 3^{m_2-(n_2-1)-(m_1-2)})}_{[\pm 6]_{(12)}}. \end{aligned}$$

In the case of the $min\{n_2 - 1, m_2 - (m_1 - 1)\} = m_2 - (m_1 - 1)$, then we have that $x = \underbrace{(2 \cdot 3^{m_2-(m_1-1)} \cdot d_1)}_{[\pm 6]_{(12)}} * \underbrace{(2 \cdot 3^l \cdot x'')}_{[\pm 6]_{(12)}}$. Notice that $n_2 = m_2 - (m_1 - 1) + l$ where l is a nonnegative integer. And

$$\begin{aligned} y &= (2 \cdot 3^{m_2-(m_1-1)}) \cdot (2^{m_1-1} \cdot 3^{m_1-1}) \\ &= \underbrace{(2 \cdot 3^{m_2-(m_1-1)} \cdot d_1)}_{[\pm 6]_{(12)}} * \underbrace{(2 \cdot 3 \cdot y'')}_{[\pm 6]_{(12)}} *** \underbrace{(2 \cdot 3)}_{[\pm 6]_{(12)}}. \end{aligned}$$

In both cases we have that $2 \cdot 3^{m_2-(m_1-1)} \cdot d_1$ is a common $\tau_{(12)}$-factor of x and y. If there exists c a common $\tau_{(12)}$-factor of x and y, then by Lemma (2), c is $2 \cdot 3^k c_1$ (because the common $\tau_{(12)}$-factors of x and y must be in $[\pm 6]_{(12)}$), where c_1 divides to x' and y'. Therefore $c_1 \leq d_1$ and $k \leq min\{n_2 - 1, m_2 - 1\}$. If $min\{n_2 - 1, m_2 - (m_1 - 1)\} = n_2 - 1$, then $c \leq 2 \cdot 3^{n_2-1} d_1$. Otherwise if the $min\{n_2 - 1, m_2 - (m_1 - 1)\} = m_2 - (m_1 - 1)$ and $c = 2 \cdot 3^k c_1 > 2 \cdot 3^{m_2-(m_1-1)} d_1$, then $k > m_2 - (m_1 - 1)$. But $y = (2 \cdot 3^k c_1)(2^{m_1-1} \cdot 3^{m_2-k} c_1')$ and $m_2 - k < m_1 - 1$, which implies that the amount of $2's$ is greater than the amount of $3's$, and c can not be a $\tau_{(12)}$-factor of y. For (ii), $n_1 = 3$, then we need to split the $2's$ otherwise would obtain a factor in $[\pm 6]_{(12)}$ and the other in the equivalence class of $[0]_{(12)}$. Therefore when considering the minimum of the powers of 2, we must choose among $n_2 - 2$ (to assume that the $\tau_{(12)}$-MCD only has 2 and it is not divisible by 4) and $m_2 - (m_1 - 1)$. The rest would follows as in the previous case. □

Theorem 23. *Let* $x = 2^{n_1}3^{n_2}x'$ *and* $y = 2^{m_1}3^{m_2}y'$ *with* $n_1, m_1 \geq 4$ *and* $m_2, n_2 > 1$. *Then* $\tau_{(12)}$*-*$MCD(x, y) = 2^{min\{n_1,m_1\}-2} \cdot 3^{min\{n_2,m_2\}-1}GCD(x', y')$

Proof. Without loss of generality let $d_1 = GCD(x', y')$, $n_1 = min\{n_1, m_1\}$ and $m_2 = min\{n_2, m_2\}$. Claim: $2^{n_1-2} \cdot 3^{m_2-2}d_1$ is the maximum common $\tau_{(12)}$-factor of x and y. Since $d_1 = GCD(x', y')$, there exist x'' and y'' such that, $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. Since $m_2 = min\{n_2, m_2\}$ and $n_1 = min\{n_1, m_1\}$, there are $t, l \in \mathbb{Z}^+$ such that $n_2 = t+n_1$ and $m_1 = l+n_1$. Now we can rewrite x and y as follows $x = 2^{n_1-2+2} \cdot 3^{t+m_2}d_1 \cdot x''$ and $y = 2^{t_1+n_1} \cdot 3^{m_2}d_1 \cdot y''$. Hence $x = \underbrace{(2^{n_1-2} \cdot 3^{m_2-1}d_1)}_{[0]_{(12)}} * \underbrace{(2 \cdot 3^{t_2+2}x'')}_{[0]_{(12)}}$ and $y = \underbrace{(2^{n_1-2} \cdot 3^{m_2-1}d_1)}_{[0]_{(12)}} * \underbrace{(2^{t_1+2} \cdot 3y'')}_{[0]_{(12)}}$ are $\tau_{(12)}$-factorizations of x and y respectively. Thus $2^{n_1-2} \cdot 3^{m_2-1}d_1|_{\tau_{(12)}}x, y$. Now suppose $c = 2^n \cdot 3^m c_1$ is a common $\tau_{(12)}$-factor of x and y. Then by Lemma (2) $n < n_1$, $m < m_2$ and $c_1|x', y'$, which forces c_1 to be less or equal than d_1. Hence $2^{n_1-2} \cdot 3^{m_2-1} \cdot d_1 = \tau_{(12)}$-$MCD(x, y)$. □

An element $x \in [\pm 2]_{(12)}$ is of the form $x = 2x'$ where $2 \nmid x'$ and $3 \nmid x'$, hence the elements in $[\pm 2]_{(12)}$ are $\tau_{(12)}$-atoms. On the other hand, if $x \in [\pm 6]_{(12)}$, then $x = 2 \cdot 3^n x'$ with $GCD(x', 12) = 1$, then x is a $\tau_{(12)}$-atom. If $x \in [\pm a]_{(12)}$, where $a \in \{2, 6\}$ and $y \in \mathbb{Z}^{\#}$, with $x \nmid_{\tau_{(12)}} y$. Then $\tau_{(12)}MCD(x, y) = 1$.

As a summary are presented the tables (3–9) and (3–10), where are the formulas found for the $\tau_{(12)}$-$MCD(x, y)$ when $\tau_{(12)}$-$MCD(x, y) \neq 1$. Since the numbers in $[\pm 1]_{(12)}$ and $[\pm 5]_{(12)}$ are relative prime to 12 and these classes have the same behavior than the $[\pm 1]_{(8)}$ and $[\pm 3]_{(8)}$. And the formulas found also are similar, the reader can observe the Table (3–6) for a summary of these formulas. On other hand, suppose $x = 2^n 3^m x'$ where $GCD(12, x'y') = 1$. If $x \in [0]_{(12)}$, then $n \geq 2$ and $m > 1$. In the case of $x \in [\pm 4]_{(12)}$, $m = 0$ and if $x \in [\pm 3]_{(12)}$, then $n = 0$. Table (3–9) summarizes the results found for the $\tau_{(12)}$-MCD for elements in $[0]_{(10)}$.

Table 3–9: The $\tau_{(12)}$-MCD for numbers in $[0]_{(12)}$

$(2^{n_1}3^{n_2}x', 2^{m_1}3^{m_2}y')$	$\tau_{(12)}$-$MCD(x,y)$
$n_1 = 2$	$2 \cdot 3^{min\{n_2-1, m_2-(m_1-1)\}}GCD(x',y')$
$n_1 = 3$	$2 \cdot 3^{min\{n_2-2, m_2-(m_1-1)\}}GCD(x',y')$
$n_1, m_1 \geq 4$	$2^{min\{n_1,m_1\}-2} \cdot 3^{min\{n_2,m_2\}-1}GCD(x',y')$

In Table (3–10) there are the formulas for the $\tau_{(12)}$-$MCD(x,y)$, when both $x, y \in [\pm b]_{(12)}$ for $b \in \{4,3\}$.

Table 3–10: The $\tau_{(12)}$-MCD when $(x,y) \in [\pm b]_{(10)}$ for $b \in \{4,3\}$

(x,y)	$\tau_{(12)}$-$MCD(x,y)$
$(2^n x', 2^m y')$ $n \in \{2,3\}$	$2 \cdot GCD(x',y')$
$(2^n x', 2^m y')$ $n, m \geq 4$	$2^{min\{n,m\}-2} \cdot GCD(x',y')$
$(3^n x', 3^m y')$ $n, m \geq 2$	$3^{min\{n,m\}-1} \cdot GCD(x',y')$

In this section we had address the formula of the $\tau_{(n)}$-MCD for an n for which $\mathbb{Z}$ is not $\tau_{(n)}$-atomic. But it turns out that it behaved very similar as the case when $n \in \{5, 8, 10\}$. This is because as expected they have the same level of difficulty, determined by the Euler Number of 12 (respectively, 5,8, and 10) which is 4. The main difference appears on the equivalence class of $[0]_{(12)}$, which needed more attention, because the element of in such equivalence classes are the ones that makes $\mathbb{Z}$ not $\tau_{(12)}$-atomic. The next non-$\tau_{(n)}$-atomic case happens when $n = 7$. This case is studied in the next chapter.

Chapter 4
About $\tau_{(n)}$-MCD when $\phi(n) = 6$ and some generalizations

In this chapter there are three sections. The first section is about the study of the $\tau_{(7)}$-MCD of the numbers that are not divisible by 7. The second section is about some generalizations done, which help us to find the $\tau_{(7)}$-MCD, for any n. For the last section the reader can find some results when n satisfies the equation $\phi(n) = 6$, that is $n \in \{9, 14, 18\}$.

4.1 On the $\tau_{(7)}$-MCD

In this section, we present a characterization of the $\tau_{(7)}$-MCD between two integers in $\mathbb{Z}^{\#}$. The complexity of the case $n = 7$ is higher than when $n \in \{5, 8, 10, 12\}$, which is given when $\mathbb{Z}$ is not $\tau_{(12)}$-atomic. The complexity arise because the technique used depends on the distribution of the prime integers distinct from 7. In this case, the positive primes are distributed in the other six equivalence classes modulo 7. Using $\tau'_{(7)}$, they are reduced to 3 distinct equivalence classes, given by $[\pm 1]_{(7)}$, $[\pm 2]_{(7)}$ and $[\pm 3]_{(7)}$. The cases analyzed before only deal with at most two distinct equivalence classes with respect to $\tau'_{(7)}$. Hence the need to understand, how the elements of these three equivalence classes interact among them.

Proposition 22. *Let $x = \prod_{k=1}^{\alpha} x_k$, where each x_k are in the same equivalence class $[\pm a]_{(7)}$ for $a \in \{1,2,3\}$, then the following holds.*

1. *If $\alpha = 3m$, $x \in [\pm 1]_{(7)}$.*
2. *If $\alpha = 3m+1$ and $x_k \in [\pm a]_{(7)}$, then $x \in [\pm a]_{(7)}$, where $a \in \{2,3\}$.*
3. *If $\alpha = 3m+2$ and $x_k \in [\pm a]_{(7)}$, then $x \in [\pm b]_{(7)}$, where $a \neq b \in \{2,3\}$.*

Proof. Let $a \in \mathbb{Z}^{\#}$. By the Euler's Theorem $a^{\phi(n)/2} \equiv \pm 1 \,(mod\, n)$. This says $a^{3m} \equiv a^{6m/2} \equiv \pm 1 \,(mod\, 7)$ for any $m \in \mathbb{Z}$, so (1) follows. For (2), let us re-write $x = \left(\prod_{k=1}^{\alpha-1} x_k\right) x_\alpha$, then $\prod_{k=1}^{\alpha-1} x_k \cdot x_\alpha^{\alpha-1} \in [\pm 1]_{(7)}$. Then $x_\alpha \in [\pm a]_{(7)}$ if and only if $x \in [\pm a]_{(7)}$. Similarly for (3), let $\alpha_1, \alpha_2 \in \{1, \ldots, \alpha\}$, then $x = \left(\prod_{k=1}^{\alpha} x_k/(x_{\alpha_1} \cdot x_{\alpha_2})\right)(x_{\alpha_1} x_{\alpha_2})$. Notice that, if $x_{\alpha_1}, x_{\alpha_2} \in [\pm a]_{(7)}$, then $(x_{\alpha_1} x_{\alpha_2}) \in [\pm b]_{(7)}$. Hence $x \in [\pm b]_{(7)}$, because $\prod_{k=1}^{\alpha} x_k/(x_{\alpha_1} \cdot x_{\alpha_2}) \in [\pm 1]_{(7)}$. □

We recall the previously used notation $\Pi_b(x) = \prod_{k=1}^{\alpha_b} p_{kb}^{a_{kb}}$, where each p_{kb} is a positive prime factor of x and $p_{kb} \in [\pm b]_{(7)}$, with $b \in \{1,2,3\}$. With this notation, the canonical factorization of a number x that is not divisible by 7 can be rewritten as, $x = \Pi_1(x) \cdot \Pi_2(x) \cdot \Pi_3(x)$, and note that $\Pi_1(x) \in [\pm 1]_{(7)}$. But the product of primes in $[\pm 2]_{(7)}$ and $[\pm 3]_{(7)}$ have other patterns and we study how this affects the $\tau_{(7)}$-factors of x. The following propositions addresses this situation.

Proposition 23. *Let $x \in \mathbb{Z}^{\#}$. Suppose that $x = \Pi_1(x) \cdot \Pi_2(x) \cdot \Pi_3(x)$ (as in the notation in the previous paragraph) and $\sum_{k=1}^{\alpha_2} a_{k2} = 3m+j$ and $\sum_{k=1}^{\alpha_3} a_{k3} = 3n+i$. Then $j \equiv (i+t)\,(mod\, 3)$ if and only if $x \in [\pm(1+t)]_{(7)}$ for $t \in \{0,1,2\}$.*

Proof. ($\Rightarrow$) Assume $j \equiv (i+t)\,(mod\, 3)$. The proof follows by dividing it into several cases. First, let us split into 3 cases (based on whether $t \in \{0,1,2\}$).

First case $t = 0$ or $j \equiv i \,(mod\, 3)$. We need to show that $x \in [\pm 1]_{(7)}$. For this, let us show it again by exhausting all the possible cases.

- Case 1.1 Suppose $j \equiv 0\,(mod\,3)$. Since $i \equiv j\,(mod\,3)$, then $i \equiv 0\,(mod\,3)$. Therefore the number of primes in the classes $[\pm 2]_{(7)}$ and $[\pm 3]_{(7)}$, is a multiple of 3. By Proposition (22), $\Pi_2(x) \in [\pm 1]_{(7)}$ and $\Pi_3(x) \in [\pm 1]_{(7)}$, so $x \in [\pm 1]_{(7)}$.
- Case 1.2 Assume $j \equiv e \equiv i\,(mod\,3)$, where $e \in \{1, 2\}$. Then this forces $\Pi_2(x) \in [\pm b]_{(7)}$ and $\Pi_3(x) \in [\pm a]_{(7)}$, for $a \neq b \in \{2, 3\}$. Since $\Pi_2(x) \cdot \Pi_3(x)$ is in $[\pm 1]_{(7)}$, then $x \in [\pm 1]_{(7)}$.

If $t = 0$, $x \in [\pm 1]_{(7)}$, in all the cases .

For the second case assume $t = 1$, $j \equiv (i + 1)\,(mod\,3)$. The proof follows similarly as in the previous case.

- Case 2.1 Suppose, $j \equiv 0\,(mod\,3)$, then $i \equiv 2\,(mod\,3)$. So $\sum\limits_{k=1}^{\alpha_2} a_{k2} = 3m$ and $\sum\limits_{k=1}^{\alpha_3} a_{k3} = 3n + 2$. By Proposition (22) $\Pi_2(x) \in [\pm 1]_{(7)}$ and $\Pi_3(x) \in [\pm 2]_{(7)}$. Therefore, $x \in [\pm 2]_{(7)}$.
- Case 2.2 Now let us assume, $j \equiv 1\,(mod\,3)$, then $i \equiv 0\,(mod\,3)$. Hence $\Pi_2(x) \in [\pm 2]_{(7)}$ and $\Pi_3(x) \in [\pm 1]_{(7)}$. As a consequence, $x \in [\pm 2]_{(7)}$.
- Case 2.3 For the lasta case let $j \equiv 2\,(mod\,3)$. Then $i \equiv 1\,(mod\,3)$. So $\sum_{k=1}^{\alpha_2} a_{(k2)} = 3m + 2$ and $\sum_{k=1}^{\alpha_3} a_{(k3)} = 3n + 1$. Since $\Pi_2(x)$ and $\Pi_3(x)$ are in $[\pm 3]_{(7)}$, $x \in [\pm 2]_{(7)}$.

Therefore, if $j \equiv (i + 1)\,(mod\,3)$, then $x \in [\pm 2]_{(7)}$.

For the case 3, $t = 2$ or $j \equiv (i + 2)\,(mod\,3)$. A similar technique is used.

- Case 3.1 If $j \equiv 0\,(mod\,3)$, $i \equiv 1\,(mod\,3)$. Therefore, $\Pi_2(x) \in [\pm 1]_{(7)}$ and $\Pi_3(x) \in [\pm 3]_{(7)}$, and hence $x \in [\pm 3]_{(7)}$.
- Case 3.2 Now, suppose $j \equiv 1\,(mod\,3)$, then $i \equiv 2\,(mod\,3)$. This conditions force $\Pi_2 \in [\pm 2]_{(7)}$ and $\Pi_3 \in [\pm 2]_{(7)}$, and hence $x \in [\pm 3]_{(7)}$.
- Case 3.3 Finally assume, $j \equiv 2\,(mod\,3)$ and $i \equiv 0\,mod\,3$. By Proposition (22), $x \in [\pm 3]_{(7)}$.

Therefore, if $j \equiv (i + 2)\,(mod\,3)$, then $x \in [\pm 3]_{(7)}$. These cases concludes this direction.

($\Leftarrow$) The converse follows by the previous construction. Suppose $x \in [\pm 1]_{(7)}$. Now, there are three options for j. The possibilities are $j \equiv i \,(mod\, 3)$ $j \equiv (i+1)\,(mod\, 3)$ or $j \equiv (i+2)\,(mod\, 3)$. The last two options force $x \in [\pm 2]_{(7)}$ and $x \in [\pm 3]_{(7)}$, respectively. Therefore, the only possible choice is $j \equiv i\,(mod\, 3)$. Similarly, if $x \in [\pm 2]_{(7)}$, then the only one possible option is $j \equiv (i+1)\,(mod\, 3)$; and for $x \in [\pm 3]_{(7)}$, the only one option is $j \equiv (i+2)\,(mod\, 3)$. □

Proposition 24. *Let $x \in [\pm 1]_{(7)}$. If $d_1|x$ and $d_1 \in [\pm 1]_{(7)}$, then $d_1|_{\tau_{(7)}}x$.*

Proof. By hypothesis $x = d_1 x'$, for some x'. Since $x \in [\pm 1]_{(7)}$ and $d \in [\pm 1]_{(7)}$, this forces $x' \in [\pm 1]_{(7)}$, then with an appropriate choice of signs, $(\pm 1)d_1 * (\pm x')$ is a $\tau_{(7)}$-factorization of x and $d_1|_{\tau_{(7)}}x$. □

If $x \in [\pm b]_{(7)}$ where $b \in \{1,2,3\}$ and $d_1|x$ with $d_1 \in [\pm c]_{(7)}$, $c \in \{2,3\}$. We denote $u_c(\frac{x}{d_1}) = \sum_{k=1}^{\alpha_c} a_{kc}$, the sum of the power of the prime positive numbers in the factorization of $\frac{x}{d_1}$, which are in $[\pm c]_{(7)}$. We said that $\frac{x}{d_1}$ satisfies the condition C_1 : if $u_2\left(\frac{x}{d_1}\right) + u_3\left(\frac{x}{d_1}\right) \neq 1$.

Proposition 25. *Let $x \in [\pm 1]_{(7)}$ and $d_1 \notin [\pm 1]_{(7)}$. If $\frac{x}{d_1}$ satisfies the condition C_1, then $d_1|_{\tau_{(7)}}x$.*

Proof. By hypothesis $x = d_1 x'$, for some $x' = \frac{x}{d_1}$. Since $x \in [\pm 1]_{(7)}$, is necessary to consider two cases for d_1. First case, $d_1 \in [\pm 2]_{(7)}$. A priori $x' \in [\pm 3]_{(7)}$. Notice that $\frac{x}{d_1} = \Pi_1\left(\frac{x}{d_1}\right) \cdot \Pi_2\left(\frac{x}{d_1}\right) \cdot \Pi_3\left(\frac{x}{d_1}\right)$. By Proposition (23) on x', if $\sum_{k=1}^{\alpha_2} a_{k2} = 3m_0 + j$ and $\sum_{k=1}^{\alpha_3} a_{k3} = 3n_0 + i$, then $j \equiv (i+2)\,(mod\, 3)$. First subcase, $j \equiv 0\,(mod\, 3)$. Consequently $i \equiv 1\,(mod\, 3)$, and hence $\sum_{k=1}^{\alpha_2} a_{k2} = 3m$ and $\sum_{k=1}^{\alpha_3} a_{k3} = 3n + 1$. By hypothesis $\sum_{k=1}^{\alpha_2} a_{k2} + \sum_{k=1}^{\alpha_3} a_{k3} = 3m + (3n+1) \neq 1$, hence $m \neq 0$ or $n \neq 0$. Now, Suppose $m = 0$, then $n \neq 0$. Let p and q two prime factors of $\Pi_3\left(\frac{x}{d_1}\right)$. Then we have that $\prod_{k=1}^{\alpha_3} p_{k3}^{a_{k3}} = \underbrace{(p \cdot q)}_{[\pm 2]_{(7)}} \underbrace{\left(\prod_{k=1}^{\alpha_3} p_{k3}^{a_{k3}}/p \cdot q\right)}_{[\pm 2]_{(7)}}$. Therefore,

$$\begin{aligned} x &= d_1 \cdot x' \\ &= d_1 \cdot (\Pi_1(x') \cdot \Pi_2(x')) \cdot (\Pi_3(x')) \\ &= d_1 \cdot (\Pi_1(x') \cdot \Pi_2(x')) \cdot \left(\prod_{k=1}^{\alpha_3} p_{k3}^{a_{k3}}/pq\right) \cdot (pq) \\ &= (\pm 1)\ \underbrace{d_1}_{[\pm 2]_{(7)}} * \underbrace{\left(\Pi_1(x') \cdot \Pi_2(x') \prod_{k=1}^{\alpha_3} p_{k3}^{a_{k3}}/pq\right)}_{[\pm 2]_{(7)}} * \underbrace{(pq).}_{[\pm 2]_7} \end{aligned}$$

Note that this method also works whether $m = 0$. Now, if $n = 0$, by hypothesis $m \neq 0$, then the following gives a $\tau_{(7)}$-factorization of x.

$$\begin{aligned} x &= d_1 \cdot x' \\ &= d_1 \cdot (\Pi_1(x') \cdot \Pi_2(x') \cdot p_{13}) \\ &= d_1 \cdot (\Pi_1(x') \cdot p_{13} \cdot (p_{12} \cdot p_{22})) \cdot p_{32} \cdots p_{\alpha_2 2} \\ &= (\pm 1)\ \underbrace{(d_1)}_{[\pm 2]_{(7)}} * \underbrace{(\pm \Pi_1(x') \cdot p_{13} \cdot (p_{12} \cdot p_{22}))}_{[\pm 2]_{(7)}} * \underbrace{(\pm p_{32})}_{[\pm 2]_{(7)}} * * * \underbrace{(\pm p_{\alpha_2 2}).}_{[\pm 2]_{(7)}} \end{aligned}$$

For the second subcase, suppose $j \equiv 1\,(mod\,3)$ and $i \equiv 2\,(mod\,3)$. By Proposition (22), $\Pi_2(x') \in [\pm 2]_{(7)}$ and $\Pi_3(x') \in [\pm 2]_{(7)}$. Hence $d_1|_{\tau_{(7)}} x$, because

$$\begin{aligned} x &= d_1 \cdot x' \\ &= d_1 \cdot (\Pi_1(x') \cdot \Pi_2(x') \cdot \Pi_3(x')) \\ &= (\pm 1) * \underbrace{(d_1)}_{[\pm 2]_{(7)}} * \underbrace{(\pm \Pi_1(x') \cdot \Pi_2(x'))}_{[\pm 2]_{(7)}} * \underbrace{(\pm \Pi_3(x'))}_{[\pm 2]_{(7)}}. \end{aligned}$$

For the last subcase, assume that $j \equiv 2\,(mod\,3)$ and $i \equiv 0\,(mod\,3)$. By Proposition (24) $\Pi_2(x') \in [\pm 3]_{(7)}$ and $\Pi_3(x') \in [\pm 1]_{(7)}$, thus

$$\begin{aligned} x &= d_1 \cdot x' \\ &= d_1 \cdot (\Pi_1(x') \cdot \Pi_2(x') \cdot \Pi_3(x')) \\ &= d_1 \cdot (\Pi_1(x') \cdot \Pi_2(x') \cdot p_{13}) \cdot \prod_{k=1}^{\alpha_3} \frac{p_{k3}^{a_{k3}}}{p_{13}} \\ &= (\pm 1) \underbrace{(d_1)}_{[\pm 2]_{(7)}} * \underbrace{(\Pi_1(x') \cdot \Pi_2(x') \cdot p_{13})}_{[\pm 2]_{(7)}} * \underbrace{\left(\prod_{k=1}^{\alpha_3} \frac{p_{k3}^{a_{k3}}}{p_{13}} \right)}_{[\pm 2]_{(7)}}. \end{aligned}$$

Note that $\prod_{k=1}^{\alpha_3} \frac{p_{k3}^{a_{k3}}}{p_13} \in [\pm 2]_{(7)}$, because the amount of primes in this product is of the form $3n - 1 = 3(n-1) + 2$, with a suitable choice of signs, $d_1|_{\tau_{(7)}} x$.

Finally suppose $d_1 \in [\pm 3]_{(7)}$, hence $x' \in [\pm 2]_{(7)}$. As a consequence we can rewrite x' as $x' = \Pi_1(x') \cdot \Pi_2(x') \cdot \Pi_3(x')$ where $\sum_{k=1}^{\alpha_2} a_{k2} = 3m_0 + j$, $\sum_{k=1}^{\alpha_3} a_{k3} = 3n_0 + i$, and $j \equiv (i+1)\,(mod\,3)$. Once one again we need to consider three cases when $j \in \{0, 1, 2\}$.

If $j \equiv 0\,(mod\,3)$, $i \equiv 2\,(mod\,3)$. Now $\left(\sum_{k=1}^{\alpha_3} a_{k3} \right) - 1 = (3n+2) - 1 = 3n+1$. By Proposition (24) $\Pi_2(x') \in [\pm 1]_{(7)}$, $\Pi_3(x') \in [\pm 2]_{(7)}$ and $\left(\prod_{k=1}^{\alpha_3} \frac{p_{k3}^{a_{k3}}}{p_{13}} \right) \in [\pm 3]_{(7)}$. Hence, we have d_1 is a $\tau_{(7)}$-factor of x, with a suitable choice of signs:

$$x = (\pm 1) \underbrace{(d_1)}_{[\pm 3]_{(7)}} * \underbrace{(\pm \Pi_1(x') \Pi_2(x') p_{13})}_{[\pm 3]_{(7)}} * \underbrace{\left(\pm \prod_{k=1}^{\alpha_3} \frac{p_{k3}^{a_{k3}}}{p_{13}} \right)}_{[\pm 3]_{(7)}}.$$

If we suppose $j \equiv 1\,(mod\,3)$, $i \equiv 0\,(mod\,3)$. By hypothesis the condition C_1 says that: $\sum_{k=1}^{\alpha_2} a_{k2} + \sum_{k=1}^{\alpha_3} a_{k3} = (3m+1) + 3n \neq 1$, then $m \neq 0$ or $n \neq 0$. First, we suppose that $m \neq 0$ and let p and q are prime factors of $\Pi_2(x')$. And notice that $(3m+1) - 2 = 3(m-1) + 2$. By Proposition (22) $\Pi_2(x')/pq \in [\pm 3]_{(7)}$. So we get,

$$x = (\pm 1)\ \underbrace{(d_1)}_{[\pm 3]_{(7)}} * \underbrace{(\pm \Pi_1(x') \cdot \Pi_3(x') \cdot \Pi_2(x')/pq)}_{[\pm 3]_{(7)}} * \underbrace{(\pm p \cdot q)}_{[\pm 3]_{(7)}}.$$

Suppose $n \neq 0$. As in the proof of the previous cases, if $m > 0$, $d_1|_{\tau_{(7)}} x$. If $m = 0$, then $\Pi_2(x') = p_{12}$. Let p and q prime factors of $\Pi_3(x')$. Note that $3n - 2 = 3(n-1) + 1$, so $\prod_{k=1}^{\alpha_3} p_{k3}/pq \in [\pm 3]_{(7)}$.

$$x = (\pm 1)\ \underbrace{(d_1)}_{[\pm 3]_{(7)}} * \underbrace{(\pm \Pi_1(x') \cdot p \cdot q \cdot p_{12})}_{[\pm 3]_{(7)}} * \underbrace{\left(\pm \prod_{k=1}^{\alpha_3} p_{k3}^{a_{k3}}/pq \right)}_{[\pm 3]_{(7)}}$$

and $d_1|_{\tau_{(7)}} x$.

If $j \equiv 2\,(mod\,3)$, $i \equiv 1\,(mod\,3)$. Therefore $\Pi_2(x') \in [\pm 3]_{(7)}$ and $\Pi_3(x') \in [\pm 3]_{(7)}$. So $x = (\pm 1)\ \underbrace{(d_1)}_{[\pm 3]_{(7)}} * \underbrace{(\pm \Pi_1(x') \cdot \Pi_2(x'))}_{[\pm 3]_{(7)}} * \underbrace{(\pm \Pi_3(x'))}_{[\pm 3]_{(7)}}$, thus $d_1|_{\tau_{(7)}} x$. In conclusion, if $d_1 \in [\pm 3]_{(7)}$, d_1 is a common $\tau_{(7)}$-factor of x. □

Proposition 26. *Let $x \in [\pm 1]_{(7)}$ and $d_1 \notin [\pm 1]_{(7)}$. If $d_1|_{\tau_{(7)}} x$, then $\frac{x}{d_1}$ satisfies the condition $C_1 : u_2\left(\frac{x}{d_1}\right) + u_3\left(\frac{x}{d_1}\right) \neq 1$.*

Proof. Since $d_1|_{\tau_{(7)}} x$, there exist $d_2, \ldots, d_s$ such that $x = \lambda\, d_1 * d_2 * * * d_s$, where $\lambda \in \{1, -1\}$. If $d_1 \in [\pm a]_{(7)}$, then each $d_i \in [\pm a]_{(7)}$. Now, $\frac{x}{d_1} = d_2 * \cdots * d_s \in [\pm b]_{(7)}$, where $a \neq b \in \{2, 3\}$. Note that $u_a\left(\frac{x}{d_1}\right) = u_a(d_2) + \cdots + u_a(d_s)$. Suppose by contradiction that $u_a\left(\frac{x}{d_1}\right) + u_b\left(\frac{x}{d_1}\right) = 1$. That is, $u_a\left(\frac{x}{d_1}\right) = 0$ or $u_b\left(\frac{x}{d_1}\right) = 0$. If $u_a\left(\frac{x}{d_1}\right) = 0$, then $u_b\left(\frac{x}{d_1}\right) = 1$. Hence, there are no primes factor of $\frac{x}{d_1}$ in $[\pm a]_{(7)}$ and there is only one prime factor of $\frac{x}{d_1}$ in $[\pm b]_{(7)}$. Thus for all $i \in \{2, \ldots, s\}$, $u_b(d_i) = 0$, except for one of them. Suppose $u_b(d_k) \neq 0$ and rewrite $d_k = \Pi_1(d_k) \cdot p_{kb}$. Since $d_k \in [\pm b]_{(7)}$, $d_1 \nmid_{\tau_{(7)}} x$ a contradiction to the assumption of the hypothesis of $d_1|_{\tau_{(7)}} x$. Now, if $u_b\left(\frac{x}{d_1}\right) = 0$ and $u_a\left(\frac{x}{d_1}\right) = 1$, then there is no primes factors of $\frac{x}{d_1}$ in $[\pm b]_{(7)}$

and only one prime $p_{ka} \in [\pm a]_{(7)}$. So $\frac{x}{d_1} = \Pi_1\left(\frac{x}{d}\right) \cdot p_{ka} \in [\pm a]_{(7)}$. Hence $x \in [\pm b]_{(7)}$, that is a contradiction, because $x \in [\pm 1]_{(7)}$. □

Corollary 4. *Let $x \in [\pm 1]_{(7)}$ and $d_1 \notin [\pm 1]_{(7)}$, with $d_1|x$. Then $d_1|_{\tau_{(7)}} x$, if and only if $\frac{x}{d_1}$ satisfies the condition $C_1 :\ u_2\left(\frac{x}{d_1}\right) + u_3\left(\frac{x}{d_1}\right) \neq 1$.*

Notice that if $x \in [\pm 1]_{(7)}$, $d_1|x$ (with $d_1 \notin [\pm 1]_{(7)}$) and $\frac{x}{d_1}$ does not satisfies the condition C_1, $p_{i1} \cdot \frac{x}{d_1}$ satisfies the condition C_1, where $p_{i1} \in [\pm 1]_{(7)}$ and $p_{i1}|d_1$. The condition C_1 will help us to compute the $\tau_{(7)}$-MCD between two numbers in $\mathbb{Z}^{\#}$. We did not find a formula to compute the maximum common $\tau_{(7)}$-factor between two integers in $[\pm 1]_{(7)}$, but found a procedure of logical steps is presented, or an algorithm to compute the $\tau_{(7)}$-MCD.

Algorithm 1 $\tau_{(7)}$-MCD for elements in $[\pm 1]_{(7)}$

```
Input: $x, y \in [\pm 1]_{(7)}$
Output: $\tau_{(7)}$-$MCD(x, y)$
 1: $d_1 \leftarrow GCD(x, y)$
 2: if $d_1 \in [\pm 1]_{(7)}$ then
 3:     return $d_1$
 4: else
 5:     while $d_1 \neq 1$ do
 6:         $x' \leftarrow \frac{x}{d_1}$ and $y' \leftarrow \frac{y}{d_1}$
 7:         if $x'$ and $y'$ satisfies condition $C_1$ or $d_1 \in [\pm 1]_{(7)}$ then
 8:             return $d_1$
 9:         else
10:             $d_1 \leftarrow d_1/p_{d_1}$
11:         end if
12:     end while
13: end if
```

The Algorithm (1) takes as entry two integers $x, y \in [\pm 1]_{(7)}$ and returns the $\tau_{(7)}$-$MCD(x, y)$. From lines 1 to 3, the algorithm verifies whether $GCD(x, y)$ is in $[\pm 1]_{(7)}$. In case it is affirmative, then $GCD(x, y)$ coincides with the $\tau_{(7)}$-$MCD(x, y)$, (which was predicted by Proposition (24)). From lines 6 to 12, the algorithm asks if d_1 satisfies the condition C_1 or d_1 is in $[\pm 1]_{(7)}$. If d_1 satisfies the condition then C_1 or $d_1 \in [\pm 1]_{(7)}$, immediatly $d_1|_{\tau_{(7)}} x$ and $d_1|_{\tau_{(7)}} y$, (proved in Corollary (4) and Proposition (24)) : and d_1 is the maximum common $\tau_{(7)}$-factor, of x and y. If d_1 does not satisfies C_1, then d_1 is divided by p_{d_1}, where p_{d_1} is the smallest positive prime factor of d_1 that is not in $[\pm 1]_{(7)}$, (p_{d_1} exists because otherwise all prime factors belong to $[\pm 1]_{(7)}$). While $d_1 \neq 1$, the process from line 6 to 12 is repeated. For example if we have $x = 3^2 \cdot 2^2 \cdot 17^2 \cdot 19^2 \in [\pm 1]_{(7)}$ and $y = 2^3 \cdot 3 \cdot 17^2 \in [\pm 1]_{(7)}$, so $GCD(x, y) = d_1 = 2^2 \cdot 3 \cdot 17^2 \in [\pm 3]_{(7)}$. Hence $\frac{x}{d_1} = 3 \cdot 19^2$ and $\frac{y}{d_1} = 2$. And $u_2\left(\frac{x}{d_1}\right) + u_3\left(\frac{x}{d_1}\right) = 2 + 1 = 3$ and $\frac{x}{d_1}$ satisfies C_1. But, $u_2\left(\frac{y}{d_1}\right) + u_3\left(\frac{y}{d_1}\right) = 1$ and $\frac{x}{d_1}$ does not satisfies C_1. Now, taking $p_{d_1} = 2$, let $d_1 \leftarrow \frac{d_1}{p_{d_1}} = 2 \cdot 3 \cdot 17^2$. Then $\frac{x}{d_1} = 3 \cdot 19^2 \cdot 2$ and $\frac{x}{d_1}$ satisfies C_1. And $\frac{y}{d_1} = 2^2$, so $u_2\left(\frac{y}{d_1}\right) + u_3\left(\frac{y}{d_1}\right) = 2$ and $\frac{y}{d_1}$ satisfies C_1. Therefore, $d_1 = 2 \cdot 3 \cdot 17^2 = \tau_{(7)}\text{-}MCD(x, y)$.

Proposition 27. *Let $x \in [\pm c]_{(7)}$ and $d_1|x$ if $d_1 \in [\pm a]_{(7)}$ where $a \neq c \in \{2, 3\}$. Then $d_1|_{\tau_{(7)}} x$.*

Proof. Suppose $x = d_1 \cdot x'$, for some x'. If $x \in [\pm 2]_{(7)}$, $d_1 \in [\pm 3]_{(7)}$. This forces $x' \in [\pm 3]_{(7)}$ which implies that $(\pm 1)\, d_1 * (\pm x')$ with an appropriate choice of signs is a $\tau_{(7)}$-factorization of x. Now, If $x \in [\pm 3]_{(7)}$, $d_1 \in [\pm 2]_{(7)}$. Hence, $x' \in [\pm 3]_{(7)}$. Therefore $(\pm 1)\, d_1 * (\pm x')$ with an appropriate choice of signs is a $\tau_{(7)}$-factorization of x. In conclusion, $d_1|_{\tau_{(7)}} x$. □

Suppose $x \in [\pm b]_{(7)}$ and $d_1 \in [\pm c]_{(7)}$, where $c, b \in \{2, 3\}$. If $b \neq c$, by Proposition (27), $d_1|_{\tau_{(7)}} x$. In the case of $b = c$, we say that $\frac{x}{d_1}$ satisfies the following condition $C_{2,3}$: (1.) $u_b\left(\frac{x}{d_1}\right) \neq 0$ or $u_{5-b} \notin \{0, 3\}$ and (2.) $u_b\left(\frac{x}{d_1}\right) \notin \{0, 1\}$ or $u_{5-b}\left(\frac{x}{d_1}\right) \neq 1$.

Note that the choice of the subindex $5-c$ was made so that if $c=2$ (or 3) then $u-5=3$ (respectively 2).

Theorem 24. *Let $x \in [\pm b]_{(7)}$ where $b \neq c \in \{2,3\}$. Suppose $d_1|x$ and $d_1 \notin [\pm 1]_{(3)}$. Recall $\frac{x}{d_1} = \Pi_1\left(\frac{x}{d_1}\right)\Pi_b\left(\frac{x}{d_1}\right)\Pi_c\left(\frac{x}{d_1}\right) = \left(\prod_{k=1}^{\alpha_1} p_{k1}^{a_{k1}}\right)\cdot\left(\prod_{k=1}^{\alpha_b} p_{kb}^{a_{kb}}\right)\cdot\left(\prod_{k=1}^{\alpha_c} p_{kc}^{a_{kc}}\right)$. If $\frac{x}{d_1}$ satisfies the condition $C_{2,3}$. Then, $d_1|_{\tau(7)}x$.*

Proof. Suppose $x = d_1 \cdot x'$, that is $x' = \frac{x}{d_1}$ and $d_1 \in [\pm b]_{(7)}$ or $d_1 \notin [\pm c]_{(7)}$. Notice that by Proposition (27), $d_1|_{\tau(7)}x$, because $d_1 \in [\pm c]_{(7)}$. If $d_1 \in [\pm b]_{(7)}$, then $x' \in [\pm 1]_{(7)}$. So $\sum_{k=1}^{\alpha_b} a_{kb} = 3m_0 + j$ and $\sum_{k=1}^{\alpha_c} a_{kc} = 3n_0 + i$, where $j \equiv i\,(mod\,3)$. Hence, there are 3 cases:

- Case 1.1 If $j \equiv 0\,(mod\,3)$, $i \equiv 0\,mod\,3$, hence $\sum_{k=1}^{\alpha_b} a_{kb} = 3m$ and $\sum_{k=1}^{\alpha_c} a_{kc} = 3n$ then if $m \neq 0$, $d_1|_{\tau(7)}x$, because

$$\begin{aligned} x &= (\pm 1)\, d_1 \cdot \left(\Pi_1(x') \cdot \prod_{k=1}^{\alpha_b} p_{kb}^{a_{kb}} \prod_{k=1}^{\alpha_c} p_{kc}^{a_{kc}}\right) \\ &= (\pm 1)\, d_1 \cdot \left(\Pi_1(x') \cdot \prod_{k=1}^{\alpha_c} p_{kc}^{a_{kc}} p_{1b}\right)\left(\prod_{k=1}^{\alpha_b} \frac{p_{kb}^{a_{kb}}}{p_{1b}}\right) \\ &= (\pm 1)\, \underbrace{(d_1)}_{[\pm b]_{(7)}} \cdot \underbrace{(\Pi_1(x') \cdot \Pi_c(x') \cdot p_{1b})}_{[\pm b]_{(7)}} * \underbrace{(\pm p_{1b})}_{[\pm b]_{(7)}} *** \underbrace{(\pm p_{\alpha_b b})}_{[\pm b]_{(7)}}. \end{aligned}$$

If $m = 0$ and $n > 1$. Suppose $n = 2t$, for some $t \in \mathbb{Z}^+$ $\sum_{k=1}^{\alpha_c} a_{kc} = 3(2t) = 6t$. Take primes in $[\pm c]_{(7)}$ and put them in pairs, that is of the form $(p_{l_1 c} p_{l_j c})$, which are in $[\pm b]_{(7)}$. Then,

$$\begin{aligned} x &= d_1 \cdot \left(\Pi_1(x') \cdot \prod_{k=1}^{\alpha_c} p_{kc}^{a_{kc}}\right) \\ &= (\pm 1)\, \underbrace{(d_1)}_{[\pm b]_{(7)}} * \underbrace{(\pm \Pi_1(x') \cdot\, (p_{l_1 c} \cdot p_{l_2 c}))}_{[\pm b]_{(7)}} * \underbrace{(\pm p_{l_3 c} \cdot p_{l_4 c})}_{[\pm b]_{(7)}} *** \underbrace{\left(\pm p_{l_{i'} c} \cdot p_{l_{j'} c}\right)}_{[\pm b]_{(7)}} \end{aligned}$$

with a suitable choice of signs, $d_1|_{\tau(7)}x$. If $n = 2n_1 + 1$, for some n_1, and $n > 1$ then $n_1 \neq 0$. And $3n$ can be rewritten as follows

$$\begin{aligned} 3n &= 3(2n_1+1)-5+5 \\ &= (6n_1+3-5)+5 \\ &= (6n_1-2)+5 \\ &= 2(3n_1-1)+5 \\ &= (3n_1-1)+(3n_1-1)+5. \end{aligned}$$

Therefore, there are γ_1, γ_2, such that $\sum_{k=1}^{\gamma_1} a_{kc} = 3n_1 - 1$, $\sum_{k=\gamma_1+1}^{\gamma_2} a_{kc} = 3n_1 - 1$ and $\sum_{k=\gamma_2+1}^{\alpha_3} a_{kc} = 5$. These arrangements force all $\prod_{k=1}^{\gamma_1} p_{kc}^{a_{kc}}$, $\prod_{k=\gamma_1+1}^{\gamma_2} p_{kc}^{a_{kc}}$ and $\prod_{k=\gamma_2+1}^{\alpha_c} p_{kc}^{a_{kc}}$ to belong in $[\pm b]_{(7)}$. This gives a $\tau_{(7)}$-factorization of x

$$x = (\pm 1)\ \underbrace{(d_1)}_{[\pm b]_{(7)}} * \underbrace{\left(\pm\Pi_1(x')\cdot\prod_{k=1}^{\gamma_1} p_{kc}^{a_{kc}}\right)}_{[\pm b]_{(7)}} * \underbrace{\left(\pm\prod_{k=\gamma_1+1}^{\gamma_2} p_{kc}^{a_{kc}}\right)}_{[\pm b]_{(7)}} * \underbrace{\left(\pm\prod_{k=\gamma_2+1}^{\alpha_c} p_{kc}^{a_{kc}}\right)}_{[\pm b]_{(7)}}.$$

Therefore, $d_1|_{\tau_{(7)}} x$. Note that $n = 0$ and $m = 0$ is not possible, because $\frac{x}{d_1}$ satisfies the condition $C_{2,3}$.

- Case 1.2 If $j \equiv 1\,(mod\,3)$, then $i \equiv 1\,(mod\,3)$. Hence, $\sum_{k=1}^{\alpha_b} a_{kb} = 3m+1$ and $\sum_{k=1}^{\alpha_c} a_{kc} = 3n+1$. Observe that $\Pi_b(x') \in [\pm b]_{(7)}$ and $\Pi_c(x') \in [\pm c]_{(7)}$. Now, if $m \neq 0$,

$$x = (\pm 1)\ \underbrace{d_1}_{[\pm b]_{(7)}} * \underbrace{(\pm\Pi_1(x')\cdot\Pi_c(x')\cdot(p_{1b}\cdot p_{2b}))}_{[\pm b]_{(7)}} * \underbrace{(\pm p_{3b})}_{[\pm b]_{(7)}} ** * \underbrace{(\pm p_{\alpha_b b})}_{[\pm b]_{(7)}}.$$

then $d_1|_{\tau_{(7)}} x$. If $m = 0$, there is only one prime in $[\pm b]_{(7)}$, without loss of generality suppose that this prime is p_{1b}. On the other hand, $n > 0$ and we have that $3(n)+1 = (3(n-1)+2)+2$. Then there exist γ_1 a nonnegative integer such that the following holds $\sum\limits_{k=1}^{\alpha_c} a_{kc} = \left(\sum\limits_{k=1}^{\gamma_1} a_{kc}\right) + \left(\sum\limits_{k=\gamma_1+1}^{\alpha_c} a_{kc}\right) = (3(n-1)+2)+2$, then

$$x \;=\; (\pm 1)\ \underbrace{(d_1)}_{[\pm b]_{(7)}} * \underbrace{(\pm \Pi_1(x') \cdot p_{1b})}_{[\pm b]_{(7)}} * \underbrace{\left(\pm \prod_{k=1}^{\gamma_1} p_{kc}^{a_{kc}}\right)}_{[\pm b]_{(7)}} * \underbrace{\left(\pm \prod_{k=\gamma_1+1}^{\alpha_c} p_{kc}^{a_{kc}}\right)}_{[\pm b]_{(7)}}.$$

Hence, $d_1|_{\tau_{(7)}} x$. Note that, $m = 0$ and $n = 0$ is not possible, because $\frac{x}{d_1}$ satisfies $C_{2,3}$.

- Case 1.3 If $j \equiv 2\,(mod\,3)$, $i \equiv (2\,mod\,3)$ and $d_1|_{\tau_{(7)}} x$, because:

$$x \;=\; (\pm 1)\ \underbrace{(d_1)}_{[\pm b]_{(7)}} * \underbrace{(\pm \Pi_1(x') \cdot \Pi_c(x'))}_{[\pm b]_{(7)}} * \underbrace{\left(\pm \prod_{k=1}^{\alpha_b} \frac{p_{kb}^{a_{kb}}}{p_{1b}}\right)}_{[\pm b]_{(7)}} * \underbrace{(\pm p_{1b})}_{[\pm b]_{(7)}}.$$

In conclusion, $d_1|_{\tau_{(7)}} x$. □

Proposition 28. *Let $x, d_1 \in [\pm b]_{(7)}$, where $b \neq c \in \{2,3\}$. If $d_1|_{\tau_{(7)}} x$, then $\frac{x}{d_1}$ satisfies the conditions $C_{2,3}$:*

(1). $u_b\left(\frac{x}{d_1}\right) \neq 0$ or $u_c\left(\frac{x}{d_1}\right) \notin \{0,3\}$, and

(2). $u_b\left(\frac{x}{d_1}\right) \notin \{0,1\}$ or $u_c\left(\frac{x}{d_1}\right) \neq 1$.

Proof. Suppose $x, d_1 \in [\pm b]_{(7)}$, where $b \in \{2,3\}$. Since $d_1|_{\tau_{(7)}} x$, there is a $\tau_{(7)}$-factorization $x = \lambda d_1 * * * d_s$, where each $d_k \in [\pm b]_{(7)}$ and $\frac{x}{d_1} = d_2 \cdots d_s \in [\pm 1]_{(7)}$. By contradiction suppose that $\frac{x}{d_1}$ does not satisfies the condition $C_{2,3}$, that is: (1) $u_b\left(\frac{x}{d_1}\right) = 0$ and $(u_c\left(\frac{x}{d_1}\right) = 0$ or $u_c\left(\frac{x}{d_1}\right) = 3$ or (2) $\left(u_b\left(\frac{x}{d_1}\right) = 0 \text{ or } u_b\left(\frac{x}{d_1}\right) = 1\right)$ and $u_c\left(\frac{x}{d_1}\right) = 1$. If $u_b\left(\frac{x}{d_1}\right) = 0$ and $u_c\left(\frac{x}{d_1}\right) = 0$, then for all k, $u_b(d_k) = 0$ and $u_c(d_k) = 0$. This implies that $d_1 \in [\pm 1]_{(7)}$, a contradiction. If $u_b\left(\frac{x}{d_1}\right) = 0$ and $u_c\left(\frac{x}{d_1}\right) = 3$, there are no primes in $[\pm b]_{(7)}$, (for all k, $u_b(d_k) = 0$) and there are 3 primes in $[\pm c]_{(7)}$. Without loss of generality, let us call these prime factors of $\frac{x}{d_1}$, p_{1c}, p_{2c}, p_{3c}. So, $\frac{x}{d_1} = \Pi_1\left(\frac{x}{d_1}\right) \cdot p_{1c} \cdot p_{2c} \cdot p_{3c}$. Since $\frac{x}{d_1} = d_2 \cdots d_k$, then $p_{1c}, p_{2c}, p_{3c} | d_j$, for some $j < s$. If $d_j = \Pi_1(d_j)p_{lc}$, for some $l \in \{1, 2, 3\}$, then $d_j \in [\pm c]_{(7)}$, a contradiction to the fact that $d_j \in [\pm b]_{(7)}$. In the case of $d_j = \Pi_1(d_j)p_{1c}p_{2c}$, $d_j \in [\pm b]_{(7)}$. But there exists $d_l = \Pi_1(d_l) \cdot p_{3c} \in [\pm c]_{(7)}$ a contradiction. Hence $p_{1c}p_{2c}p_{3c}|d_j$, but this says $d_j = \Pi_1(d_j)p_{1c}p_{2c}p_{3c} \in [\pm 1]_{(7)}$, a contradiction. Now, if $u_b\left(\frac{x}{d_1}\right) = 1$, (that is $\Pi_b\left(\frac{x}{d_1}\right) = p_{1b}$) and $u_c\left(\frac{x}{d_1}\right) = 1$, (that is $\Pi_c\left(\frac{x}{d_1}\right) = p_{1c}$). For some $j < k$, $d_j = \Pi_1(d_j)p_{1c} \in [\pm c]_{(7)}$, or $d_j = \Pi_1(d_j)p_{1b}p_{1c} \in [\pm 1]_{(7)}$. If $u_b\left(\frac{x}{d_1}\right) = 0$ and $u_c\left(\frac{x}{d_1}\right) = 1$ (that is, $\Pi_c\left(\frac{x}{d_1}\right) = p_{1c}$). For some $j < k$, $d_j = \Pi_1(d_j)p_{1c} \in [\pm c]_{(7)}$, a contradiction. Both leads to the hypothesis of $d_1|_{\tau(7)}x$. □

Corollary 5. *Let $x, d_1 \in [\pm c]_{(7)}$, where $c \in \{2, 3\}$. Then $d_1|_{\tau(7)}x$ if and only if $\frac{x}{d_1}$ satisfies the condition $C_{2,3}$:*

(1). $u_b\left(\frac{x}{d_1}\right) \neq 0$ or $u_c\left(\frac{x}{d_1}\right) \notin \{0, 3\}$ and

(2). $u_b\left(\frac{x}{d_1}\right) \notin \{0, 1\}$ or $u_c\left(\frac{x}{d_1}\right) \neq 1$

Algorithm 2 $\tau_{(7)}$-MCD for elements in $[\pm b]_{(7)}$

```
Input: $x, y \in [\pm b]_{(7)}$
Output: $\tau_{(7)}$-$MCD(x, y)$
 1: $d_1 \leftarrow GCD(x, y)$
 2: if $d_1 \in [\pm c]_{(7)}$ with $b \neq c \in \{2, 3\}$ then
 3:     return $d_1$
 4: else
 5:     while $d_1 \neq 1$ do
 6:         $x' \leftarrow \frac{x}{d_1}$ and $y' \leftarrow \frac{y}{d_1}$
 7:         if $x'$ and $y'$ satisfies the condition $C_{2,3}$ or $d_1 \in [\pm c]_{(7)}$ then
 8:             return $d_1$
 9:         else
10:             $d_1 \leftarrow d_1/p_d$
11:         end if
12:     end while
13:     return $d_1$
14: end if
```

The Algorithm (2) takes as entries two integers $x, y \in [\pm b]_{(7)}$, where $b \in \{2, 3\}$, and returns the $\tau_{(7)}$-$MCD(x, y)$. From lines 1 to 4, the algorithm verifies whether

$GCD(x,y) \in [\pm c]_{(7)}$ where $b \neq c \in \{2,3\}$. In case it is affirmative, then $GCD(x,y)$ coincides with the $\tau_{(7)}$-$MCD(x,y)$. This is true by Proposition (27). From lines 6 to 12, the algorithm asks whether d_1 satisfies the condition $C_{2,3}$ or $d_1 \in [\pm c]_{(7)}$. If d_1 satisfies the condition $C_{2,3}$ or $d_1 \in [\pm c]_{(7)}$, immediately $d_1|_{\tau_{(7)}}x$ and $d_1|_{\tau_{(7)}}y$, (proven in Corollary (5) and Proposition (27)), and d_1 is the maximum common $\tau_{(7)}$-factor of x and y. If d_1 does not satisfies $C_{2,3}$, then d_1 is divided by p_{d_1}, where p_{d_1} is the smallest positive prime factor of d_1 that is not in $[\pm 1]_{(7)}$. While $d_1 \neq 1$, the process from line 6 to 12 is repeated. For example if is considered, $x = 3^2 \cdot 2^2 \cdot 17^2 \cdot 19^2 \cdot 11 \in [\pm 3]_{(7)}$ and $y = 2^3 \cdot 3 \cdot 17^2 \cdot 31 \in [\pm 3]_{(7)}$, $GCD(x,y) = d_1 = 2^2 \cdot 3 \cdot 17^2 \in [\pm 3]_{(7)}$. Hence $\frac{x}{d_1} = 3 \cdot 19^2 \cdot 11$ and $\frac{y}{d_1} = 2 \cdot 31$. And $u_2\left(\frac{x}{d_1}\right) + u_3\left(\frac{x}{d_1}\right) = 2 + 2 = 4$ and $\frac{x}{d_1}$ satisfies $C_{2,3}$. But, $u_2\left(\frac{y}{d_1}\right) = 1$ and $u_3\left(\frac{y}{d_1}\right) = 1$ and $\frac{y}{d_1}$ does not satisfies $C_{2,3}$. Now, let $d_1 \leftarrow \frac{d_1}{p_d} = 2 \cdot 3 \cdot 17^2$. Then $\frac{x}{d_1} = 3 \cdot 19^2 \cdot 2 \cdot 11$ and $\frac{x}{d_1}$ satisfies $C_{2,3}$. And $\frac{y}{d_1} = 2^2 \cdot 31$, so $u_2\left(\frac{y}{d_1}\right) = 2$ and $u_3\left(\frac{y}{d_1}\right) = 1$ and $\frac{y}{d_1}$ = satisfies $C_{2,3}$. Therefore, $d_1 = 2 \cdot 3 \cdot 17^2 = \tau_{(7)}$-$MCD(x,y)$.

4.2 Some generalizations

In this section, the reader can find some generalizations of propositions and theorems. With these generalizations is possible to compute the $\tau_{(n)}$-MCD between two integers, for any n. We also consider other cases when both numbers either in $[0]_{(n)}$, $[\pm 1]_{(n)}$ or $[\pm q]_{(n)}$, where $n = rq$ and $r|6$. First, we consider elements in $[0]_n$, $k \geq 1$, $n = p^k$, and p a positive prime integer.

Theorem 25. *Let $x = p^n x'$ and $y = p^m y'$, where p is a positive prime integer and $p \nmid x', y'$. If $n, m \geq 2k$, then $\tau_{(p^k)}$-$MCD(x,y) = p^{min\{n,m\}-k} GCD(x', y')$, for any k.*

Proof. Let $d_1 = GCD(x', y')$. Then $x' = d_1 x''$ and $y' = d_1 y''$ for some $x'', y'' \in \mathbb{Z}^*$. Without loss of generality suppose $n = min\{n, m\}$, $m = n + l$ for some integer $l \geq 0$. The following $x = \underbrace{(p^{n-k} \cdot d_1)}_{[0]_{(p^k)}} * \underbrace{(p^k \cdot x'')}_{[0]_{(p^k)}}$ and $y = \underbrace{(p^{n-k} \cdot d_1)}_{[0]_{(p^k)}} * \underbrace{(p^{l+k} \cdot y'')}_{[0]_{(p^k)}}$ are $\tau_{(n)}$-factorizations, of x and y, respectively. If $c|_{\tau_{(p^k)}} x, y$, then by Lemma (2) $c = p^t \cdot c'$, where $0 < t \leq n-1$, and c' must divide x' and y'. Hence $c' \leq d_1$. So, $c \leq (p^{n-1} \cdot d_1)$ and $\tau'_{(p^k)}$-$MCD(x,y) = p^{min\{n,m\}-k} GCD(x', y') = \tau_{(p^k)}$-$MCD(x,y)$. □

In Theorem (25), elements $x = p^n x'$, in $[0]_{(p^k)}$, such that $n \geq 2k$ were considered. But, the theorem does not consider all the cases when both x and y are in $[0]_{p^k}$, for example when $k \leq n < 2k$. The formula for the $\tau_{(n)}$-MCD of these elements is different from the one given in the above theorem. On other hand, if are considered p^a and p^b, such that $0 < a < b < k$, then p^a and p^b are in different equivalence classes with respect to the relation $\tau'_{(p^k)}$. Such case is addressed in the following lemmas.

Lemma 5. *Let $x \in [0]_{(p^k)}$, where $x = p^m x'$ and $GCD(x', p) = 1$. If $c = p^t c_1$ with $c_1 \equiv \pm \frac{x'}{c_1} \equiv \pm 1 \, (mod \, p^{k-t})$ and t a proper divisor of m, then $c|_{\tau_{(p^k)}} x$.*

Proof. Since $t|m$, then $m = ta$. Also, $x' = c_1 \cdot c''$. Hence $x = p^m x' = p^{ta} \cdot c_1 \cdot c''$. Thus, $x = (p^t \cdot c_1) \cdot (p^t \cdot c'') \underbrace{(p^t) \cdots (p^t)}_{(a-2)-times}$. By hypothesis, $c_1 \equiv \pm c'' \equiv \pm 1 \, (mod \, p^{k-t})$, then $p^t \cdot c_1 \equiv \pm p^t \cdot c'' \equiv \pm p^t \, (mod \, p^k)$. Then, $x = (p^t \cdot c_1) * (\pm p^t \cdot c'') * (\pm p^t) * * * (\pm p^t)$ is a $\tau'_{(p^k)}$-factorization of x. By Remark (1), $c|_{\tau_{(p^k)}} x$. □

Lemma 6. *Let $x = p^m x'$, where $k \leq m < 2k$ and $p \nmid x'$. If $c = p^t c_1$ and $c|_{\tau_{p^k}} x$, then t is a proper divisor of m.*

Proof. Suppose by contradiction that t is not a proper divisor of m. Note that $x' = c_1 \cdot c''$ and note that $t < m$. So either $k > t$ or $k \leq t$. First assume, $k \leq t$. Since $t < m$, $m = t + r_0$, where $r_0 < k$ (because $k \leq t < m < 2k$). Therefore, $x = p^{t+r_0} \cdot c_1 \cdot c''$, and $x = (p^t \cdot c_1) \cdot (p^{r_0} \cdot c'')$, note that $p^t \cdot c_1 \in [0]_{(p^k)}$, but $p^{r_0} \cdot c'' \notin [0]_{(p^k)}$. Hence, a $\tau_{(p^k)}$-factorization is not possible, with $c = p^t \cdot c_1$ as a $\tau_{(p^k)}$-factor. Now, suppose $k > t$. By the division theorem, there exist q and $0 \leq r < t$, with $m = qt + r$. If assumme $r \neq 0$, then

$$\begin{aligned} x &= p^{qt+r} \cdot c_1 \cdot c'' \\ &= (p^{qt} \cdot c_1)(p^r \cdot c'') \\ &= (p^t \cdot c_1) \cdot \underbrace{(p^t) \cdots (p^t)}_{(q-1)-times} \cdot (p^r \cdot c'') \\ &= (c) \cdot \underbrace{(p^t) \cdots (p^t)}_{(q-1)-times} \cdot (p^r \cdot c''). \end{aligned}$$

Note that for any integer a, $t(q-1) + r > t$ (because $r > 0$), and we have that $p^{at+r} c'' \notin [\pm p^t \cdot c_1]_{(p^k)}$, and c can not be a $\tau_{(p^k)}$-factor of x. Hence, $r = 0$ and $m = qt$. □

Definition 4.2.1. *Let $x, y \in \mathbb{Z}^{\#}$, we define the greatest common proper factor of x and y (denoted by $GCPD(x, y)$) as the greatest common factor strictly less than x and y.*

Notice that this definition was motivated by Lemma 5. Such result was used in several results and in (25): in which it is assumed that $t \leq n-1$ instead $t \leq n$. At the moment it was important to recognize that if $x \nmid_{\tau_{(n)}} y$, then the proper powers naturally arise. This concept is used to prove the following theorem.

Theorem 26. *Let $x = p^{n_1} \cdot x'$ and $y = p^{n_2} \cdot y'$, where $2 \leq k \leq n_1 < 2k$ and $GCD(x'y', p) = 1$. If $GCD(x', y') \equiv \frac{x'}{GCD(x',y')} \equiv \frac{y'}{GCD(x',y')} \equiv 1\, (mod\, p^{k-GCPD(n_1,m_1)})$. Then $\tau_{(p^k)}$-$MCD(x, y) = p^{GCPD(n_1,m_1)} GCD(x', y')$, where $GCD(n_1, m_1)$, is as in Definition (4.2.1).*

Proof. Let $d_1 = GCD(x', y')$, then there are x'' and y'', such that $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. For simmplicity denote $GCPD(n_1, m_1) = m$. By Lemma (5), $p^m \cdot d_1|_{\tau_{(p^k)}} x$ and $p^m \cdot d_1|_{\tau_{(p^k)}} y$. If there exist c, such that $c|_{\tau_{(p^k)}} x, y$, then $c = p^t c_1$, where c_1 is a common divisor of x', y'. By definition of d_1, $c_1 \leq d_1$. By Lemma (6), t is a proper divisor of n_1 and m_1, thus $t \leq m$. Therefore, $c = p^t \cdot c_1 \leq p^m \cdot d_1$. Hence $\tau_{(p^k)}$-$MCD(x, y) = p^{GCPD(n_1,m_1)} GCD(x', y')$. □

If $n = 2^2$, that was a case studied in [7], the results for elements $x = 2^a x'$ in $[0]_{(4)}$, where $a \in \{2, 3\}$, coincide with the result of Theorem (26), because $x' \equiv \pm 1\, (mod\, 4)$, and satisfies the condition of the Theorem. Also, if $n = 2^3$, the Theorem (11), studied in Chapter 3, coincides with the above theorem.

Theorem 27. *Let $x, y \in [0]_{(n)}$, where $n = p_1^{a_1} \cdots p_k^{a_k}$. If $x = p_1^{n_1} \cdots p_k^{n_k} x'$ and $y = p_1^{m_1} \cdots p_k^{m_k}$ with $n_i, m_i \geq 2a_i$ and $GCD(p_i, x' \cdot y') = 1$. Then, the maximum common $\tau_{(n)}$-factor of x and y is $p_1^{min\{n_1,m_1\}-a_1} \cdots p_k^{min\{n_k,m_k\}-a_k}$.*

Proof. Let $d_1 = GCD(x', y')$. Since $d_1 = GCD(x', y')$, there exist x'' and y'' such that, $x' = d_1 \cdot x''$ and $y' = d_1 \cdot y''$. Notice that,

$$x = \underbrace{(p_1^{min\{n_1,m_1\}-a_1} \cdots p_k^{min\{n_k,m_k\}-a_k} \cdot d_1)}_{[0]_{(n)}} * \underbrace{(p_1^{t_1+a_1} * p_k^{t_k+a_k} x'')}_{[0]_{(n)}}$$

and

$$y = \underbrace{(p_1^{min\{n_1,m_1\}-a_1} \cdots p_k^{min\{n_k,m_k\}-a_k} \cdot d_1)}_{[0]_{(n)}} * \underbrace{(p_1^{t_1+a_1} \cdots p_k^{t_k+a_k} y'')}_{[0]_{(n)}}$$

are $\tau_{(n)}$-factorizations of x and y. Hence, if $m = (p_1^{min\{n_1,m_1\}-a_1} \cdots p_k^{min\{n_k,m_k\}-a_k} \cdot d_1)$, then m is a $\tau_{(n)}$-factor of x and y. Now suppose that there exists $c = p_1^{s_1} \cdots p_k^{s_k} c_1$, a common $\tau_{(n)}$-factor of x and y, then $s_i \leq min\{n_i, m_i\}$, and $c_1 \leq d_1$, because $c_1 | x', y'$ and $d_1 = GCD(x', y')$. Since $c|x$, there is $l_i \geq 0$ for $i \in \{1, \ldots, k\}$, such that $n_i = s_i + l_i$, and $x = (p_1^{s_1} \cdots p_k^{s_k} c_1) \cdot (p_1^{l_1} \cdots p_k^{l_k} c'')$. Suppose by contradiction that $c \geq m$, then $p_1^{s_1} \cdots p_k^{s_k} c_1 \geq p_1^{min\{n_1,m_1\}-a_1} \cdots p_k^{min\{n_k,m_k\}-a_k} \cdot d_1$ holds. Since $c_1 \leq d_1$, then $\prod_{i=1}^{k} p_i^{s_i} \geq \prod_{i=1}^{k} p_i^{min\{n_i,m_i\}-a_i}$. Then there is at least some $s_t \geq min\{n_t, m_t\} - a_t$. Without loss of generality, suppose $n_t = min\{n_t, m_t\}$. Now, $n_t - a_t \leq s_t \leq n_t$, and so $s_t = (n_t - a_t) + r$ for some $r \geq 0$. On other hand, if $s_t + l_t = n_t$, then $l_t = a_t - r$. This mean that $l_t \leq a_t$. Since $c|_{\tau_{(n)}} x$, then $x = c * c_2 * * * c_w$, where each $c_i \in [0]_{(n)}$. Therefore, $c_2 * \cdots * c_w = p_1^{l_1} \cdots p_k^{l_k} c''$, but $c_2 * \cdots * c_w \in [0]_{(n)}$, and $p_1^{l_1} \cdots p_k^{l_k} c'' \notin [0]_{(n)}$, a contradiction. Hence, $\tau_{(n)}$-$MCD(x, y) = \prod_{i=1}^{k} p_i^{min\{n_1,m_1\}-a_i} \cdot GCD(x', y')$. □

Theorem (27) generalized because Theorems (5), (7), (16) and (23) presented in Chapter 3. Note that the proof of Theorem (27) also generalized Lemma (2), for any $n = p_1^{a_1} \cdots p_k^{a_k}$.

Lemma 7. *Let $x, d \in \mathbb{Z}^{\#}$, where $x \in [\pm 1]_{(n)}$ and $d^2 \equiv \pm 1\,(mod\, n)$, then $d|_{\tau_{(n)}} x$.*

Proof. Since $d|x$, there exist x' such that $x = d{\cdot}x'$. Since $x \in [\pm 1]_{(n)}$, d and n are relatively prime and $d^{-1}(mod\, n)$ exist. By hypothesis $d^2 \equiv \pm 1\,(mod\, n)$, which implies $d \equiv \pm\, d^{-1}(mod\, n)$. Since $d \cdot x' \equiv \pm 1 (mod\, n)$, $d^{-1} \equiv x'\,(mod\, n)$. And transitivity, we obtain that $d \equiv \pm\, x'\,(mod\, n)$. Therefore, $x = d * (\pm x')$ is a $\tau_{(n)}$-factorization of x and $d|_{\tau'_{(n)}} x$. By Remark (1), $d|_{\tau_{(n)}} x$. □

As consequence of Lemma (7), if $x, y \in [\pm 1]_{(n)}$ and $GCD(x, y) \in [\pm 1]_{(n)}$, then $GCD(x, y) = \tau_{(n)}\text{-}MCD(x, y)$.

Corollary 6. *Let $x, y \in [\pm 1]_{(n)}$, and $d = GCD(x, y)$. If $d^2 \equiv \pm 1 (mod\, n)$, then $d = \tau_{(n)}\text{-}MCD(x, y)$.*

Proof. By Theorem (7), $d|_{\tau_{(n)}} x$ and $d|_{\tau_{(n)}} y$. Hence $d = \tau_{(n)}\text{-}MCD(x, y)$. □

By Euler's theorem if $\phi(n) = 4$, then for all a, with $GCD(a, n) = 1$, $a^2 \equiv \pm 1\,(mod\, n)$. In particular if $x, y \in [\pm 1]_{(n)}$, and $d = GCD(x, y)$, then $GCD(d, n) = 1$. Hence $d^2 \equiv \pm 1\,(mod\, n)$, as consequence of Corollary (6), we have that $d = \tau_{(n)}\text{-}MCD(x, y)$. This is the reason why in the cases $n \in \{5, 8, 10, 12\}$, the $GCD(x, y)$ coincides with the $\tau_{(n)}\text{-}MCD(x, y)$.

Lemma 8. *Consider $2m$, with $GCD(m, 2) = 1$. Then $m^k \equiv m\,(mod\, 2m)$ for all $k \in \mathbb{Z}^+$.*

Proof. Since $GCD(m, 2) = 1$, for all nonnegative integer k, $m^{k-1} \equiv m\,(mod\, 2)$. Thus, $m^k \equiv m\,(mod\, 2m)$. □

Lemma 9. *Consider with $GCD(m,3) = 1$. Then $m^k \equiv \pm m \,(mod\, 3m)$ for all $k \in \mathbb{Z}^+$.*

Proof. Since $GCD(m,3) = 1$, for all nonnegative integer k, $m^{k-1} \equiv \pm m \,(mod\, 3)$. Thus, $m^k \equiv m \,(mod\, 3m)$. □

Lemma 10. *Consider with $GCD(m,6) = 1$. Then for all nonnegative integer k, $m^k \equiv \pm m \,(mod\, 6m)$.*

Proof. The proof follows from Lemmas (8, 9). □

Theorem 28. *Let $n = qt$ where $q \nmid t$ for $q|6$. If $x, y \in [t]_{(n)}$ with $x = t^{n_1}x'$, $y = t^{m_1}y'$. If $GCD(x',y') \equiv \pm\frac{x'}{GCD(x',y')} \equiv \pm\frac{y'}{GCD(x',y')} \,(mod\, q)$. Then the maximum common $\tau_{(n)}$-factor of x and y is $t^{min\{n_1,m_1\}-1}GCD(x',y')$.*

Proof. Without loss of generality, suppose $n_1 = min\{n_1, m_1\}$. Let $d_1 = GCD(x',y')$, then $x' = d_1x''$ and $y' = d_1y''$. We claim that $t^{n_1-1} \cdot d_1|_{\tau_{(n)}} x, y$.
Since, $x = (t^{n_1-1}d_1) \cdot (t \cdot x'')$, by Lemma (10) and $t^{n_1-1} \equiv t \,(mod\, n)$. By hypothesis $d_1 \equiv x'' \,(mod\, q)$, hence $td_1 \equiv tx'' \,(mod\, n)$, and $t^{n_1-1}d_1 \equiv tx'' \,(mod\, n)$. Hence, we have that $x = (\pm 1)(t^{n_1-1}d_1) * (t \cdot x'')$ a $\tau_{(n)}$-factorization of x. Analogously, $t^{n_1-1} \cdot d_1|_{\tau_{(n)}} y$. If there exist c a common $\tau_{(n)}$-factor by Lemma (2) $c = p^r c'$, with $c|_{\tau_{(n)}} x, y$, then $c' \leq d_1$ and $r \leq min\{n_1, m_1\}$. So, $c \leq t^{min\{n_1,m_1\}-1}GCD(x',y')$. Therefore, $t^{min\{n_1,m_1\}-1}GCD(x',y') = \tau_{(n)}\text{-}MCD(x,y)$. □

The above theorem, is the reason why, Theorem (28) and the Theorem (17) work well. If any other prime q, satisfies $q^k \equiv \pm q \,(mod\, qt)$, for all k, it is possible to find the $\tau_{(qt)}MCD$ as in the Theorem (28).

Remark 2. *Let $n = p^k$, with p a prime number. Then the elements in $[\pm p]_{(n)}$, are $\tau_{(n)}$-atoms. Because, $x = p \cdot (p_1 \cdots p_k)$, where $p_i \notin [\pm p]_{(n)}$. If $x \in [\pm p]_{(n)}$, hence is not possible to find any $\tau_{(n)}$-factorization for x. Now, if $y \in \mathbb{Z}^{\#}$ in the case of $x|_{\tau_{(n)}} y$, then $\tau_{(n)}$-$MCD(x, y) = x$. Otherwise, $\tau_{(n)}$-$MCD(x, y) = 1$.*

4.3 About the $\tau_{(n)}$-MCD when $\phi(n) = 6$.

Notice that $\phi(n) = 6$, when $n \in \{7, 9, 14, 18\}$. In the first section of this chapter, was studied the $\tau_{(n)}$-MCD, when $n = 7$. With the above section it is possible to find a characterization of $\tau_{(n)}$-MCD, for some cases when $n \in \{9, 14, 18\}$.

For elements in $[0]_{(n)}$ when $n = 9$, with Theorems (25) and (26), it is possible to find the $\tau_{(9)}$-MCD. If $n = 14$ and $n = 18$, the $\tau_{(n)}$-MCD, can be computed with Theorem (27).

For elements in $[\pm 1]_{(n)}$ we provide a method to find the $\tau_{(n)}$-MCD. If an element $d^2 \equiv \pm 1 \,(mod\, n)$, immediately by Theorem (7), $d|_{\tau_{(n)}} x$. As a consequence of Euler Theorem, $d^3 \equiv \pm 1 \,(mod\, n)$. So, at least 3 $\tau_{(n)}$-factors are necessary, to having d as a $\tau_{(n)}$-factor. The other $\tau_{(n)}$-factors depend on $\frac{x}{d}$. One needs some conditions for $\frac{x}{d}$, to guarantee the existence of $d_2, \ldots, d_k$, such that d_i are in the same equivalence class of d, with respect to the relation $\tau'_{(n)}$. For $\phi(n) = 6$, if $u_a\left(\frac{x}{d}\right) + u_b\left(\frac{x}{d}\right) \neq 0$, then the $\tau_{(n)}$-factors d_i exist, where $a \equiv b^{-1} \,(mod\, n)$. The algorithm (1), can be modified for these computations.

By Remark (2), the elements in $[\pm 3]_{(9)}$ are $\tau_{(9)}$-atoms. With elements in $[3^2]_{(18)}$ and $[7]_{(14)}$ is possible to apply Theorem (28) for finding a formula for the $\tau_{(n)}$-MCD.

In the case of the classes $[\pm a]_{(n)}$, where $GCD(a, n) = 1$, since $\frac{\phi(n)}{2} = 3$, then there are 3 equivalence classes which elements are relative prime to n. Let $\{1, a_1, a_2\}$ be the set that represents the equivalence classes with respect to $\tau'_{(n)}$ (where $GCD(a_i, n) = 1$). Then $a_1^2 \equiv a_2 \,(mod\, n)$ and $a^3 \equiv \pm 1 \,(mod\, n)$. The behavior of the elements of these classes is like the behavior of the elements in the classes $[\pm 1]_{(7)}$, $[\pm 2]_{(7)}$ and $[\pm 3]_{(7)}$. Therefore, the theorems and algorithms of the first section of this chapter, can be modified and can work for finding the $\tau_{(n)}$-MCD.

Chapter 5
Conclusions and future works

In the first section of this chapter, the reader can find a summary of the main results of our work. In the second section, there are some advices for future works about the maximum common $\tau_{(n)}$-factor.

5.1 Conclusions

After reviewing Ortiz and Luna [7] preliminary report on the cases when the Euler's number $\phi(n)$ is 4 and $n \in \{0, 1, 2, 3, 4\}$, there are two general conclusions: the $\tau_{(n)}$-MCD of two nonzero nonunit integers is not easy to compute and its complexity depends on the Euler's number $\phi(n)$. Finding the $\tau_{(n)}$-$MCD(x, y)$ formula, for integers with the same Euler's numbers (as $\phi(n)$), required similar techniques. When x, y lies on an equivalence classes represented by a relative prime integer to n.

This work confirms and coincides with the results of Ortiz and Luna [7] for the cases when $\phi(n) = 2$. Also, it uses a similar technique to find the formula of $\tau_{(6)}$-MCD, with the exception that it requieres more individual cases.

One of our main results, is the formula of the $\tau_{(n)}$-MCD when $\phi(n) = 4$. The case when $n = 5$, basically served as the background to develop the techniques to analyze the $\tau_{(n)}$-MCD when $\phi(n) = 4$. That is when $n \in \{5, 8, 10, 12\}$. One must note that by finding the formulas for $n = 5, 8$ and 10, the characterization of formulas of $\tau_{(n)}$-MCD for which n makes $\mathbb{Z}$ $\tau_{(n)}$-atomic (every nonzero nonunit can be written as a $\tau_{(n)}$-product of $\tau_{(n)}$-irreducible elements) is complete. This was one of the item goals of Ortiz and Luna [7] in 2011. Juett [5] proved that $\mathbb{Z}$ is not $\tau_{(12)}$-atomic. The problem arose in the equivalence class of $[0]_{(12)}$, which difficulty was studied by splitting it into several cases.

Another result was the identification of the following patterns summarized in the following 3 theorems:

- Let $x \in [\pm b]_{(n)}$, where $b \in \{1, a\}$, with $a \not\equiv \pm 1\,(mod\, n)$ and $a^2 \equiv \pm 1\,(mod\, n)$. If there exist $d|x$ and $\Pi_a\left(\frac{x}{d}\right) \neq 1$, then $d|_{\tau_{(n)}} x$.
- Let $x \in [\pm b]_{(n)}$ and $y \in [\pm a]_{(n)}$, where $b \in \{1, a\}$, with $a \not\equiv \pm 1\,(mod\, n)$ and $a^2 \equiv \pm 1\,(mod\, n)$. Suppose $d = GCD(x, y)$ and there exist c, such that $c|d$. If $\Pi_a\left(\frac{x}{d}\right) \neq 1$, then $c|_{\tau'_{(n)}} x, y$ if and only if $c|_{\tau'_{(n)}} d$.
- Let $x \in [\pm b]_{(n)}$ and $y \in [\pm a]_{(n)}$, where $b \in \{1, a\}$, with $a \not\equiv \pm 1\,(mod\, n)$ and $a^2 \equiv \pm 1\,(mod\, n)$. Then $\tau_{(n)}$-$MCD(x, y) = max\{d_i \in [\pm a]_{(n)} : d_i|_{\tau_{(n)}} GCD(x, y)\}$.

Such patterns can be applied in future cases. As for example, it happens when $n = 3$, $\tau_{(3)}$-$MCD(x, y)$ when $x, y \in [3]_{(6)}$. In other words, this will always work with multiplicative closed equivalence classes. In this case the theorems just address when $x \in [\pm a]_{(n)}$ and $y \in [\pm b]_{(n)}$ where a^2 or b^2 are equivalent to ± 1 modulo n.

Finally, there are some results when $n = 7$. Including two algorithms to find the $\tau_{(7)}$-$MCD(x, y)$ when x and y can not be both in $[\pm 1]_{(7)}$. Both algorithms are based in conditions C_1 and $C_{2,3}$. This conditions can be used to apply a similar algorithm when $n = 9, 14$ and 18, by identifying who is playing the roles of the equivalences classes of $[\pm 2]_{(7)}$ and $[\pm 3]_{(7)}$. For example, when $n = 9$, the roles are given by $[\pm 2]_{(9)}$ and $[\pm 4]_9$, respectively. When $n = 14$, the equivalence classes are $[\pm 3]_{(14)}$ and $[\pm 5]_{14}$.

5.2 Future works

As a future work, the idea is to continue to find a formula or a general algorithm to find the $\tau_{(n)}$-MCD. To accomplish this, it will be necessary to spent more time studying case by case for each n. Try to find a pattern between classes for the cases when $\phi(n) \geq 6$.

One must recognized that the study of the behavior between equivalence classes requires more mathematical machinery. Some suggestion are results in additive partitions of an integer and Lagrange polynomials. It seems that both theories will give some other options or point of views to further analyze the cases when $\phi(n)$ is greater than 6.

Bibliography

[1] D.D. Anderson and A.M. Frazier. "*On a general theory of factorization in integral domains*". Rocky Mountain J. Math, Volume 41, Number 3(2011), 663-705, 2011.

[2] A. Florescu. "*Reduced τ_n-factorizations in $\mathbb{Z}$ and τ_n-factorizations in* $\mathbb{N}$". Phd thesis, The University of Iowa, 2013.

[3] A. M. Frazier. "*Generalized factorizations in integral domains.*" Phd thesis, The University of Iowa, 2006.

[4] S. M. Hamon. "*Some topics in τ-factorizations*". Phd thesis, The University of Iowa, 2007.

[5] J. R. Juett. "*Some topics in abstract factorization*". Phd thesis, The University of Iowa, 2013.

[6] R. Kumanduri and C. Romero. "*Number theory with computer applications*" Prentice Hall, 1998.

[7] N. Luna and R.M. Ortiz-Albino. "*Sobre máximo común $\tau_{(n)}$-factor, para $n = 0, 1, 2, 3, 4$*". Preliminary report, 2012.

[8] S. McAdam and R. Swan. "*Unique comaximal factorization*". J. Algebra, 276(1):180-192, 2004.

[9] R. M. Ortiz-Albino. "*On Generalized nonatomic factorizations* ". Phd thesis, The University of Iowa, 2008.

[10] C. A. Serna. "*Factorizaciones sobre particiones de un dominio integral*". Master thesis, University of Puerto Rico at Mayaguez, 2014.