ALGEBRAIC ARITHMETIC OF THE REMAINDER (AAR) OR NON-MODULAR ARITHMETIC OF THE REMAINDER (NMAR)

1. Odirley Willians Miranda Saraiva
Regional University of the Northwest of the State of Rio Grande do Sul, Unijuí, Brazil.
https://orcid.org/0000-0001-9090-3788
williamatematica32@gmail.com
2. Cássio Pinho dos Reis
Federal University of Mato Grosso of South (UFMS)
https://orcid.org/0000-0002-2211-2295
cassio.reis@ufms.br
3. Antônio Thiago Madeira Beirão
Federal Rural University of Amazônia, Belém, Pará, Brazil.
https://orcid.org/0000-0003-1366-5995
Thiago.madeira@ufra.edu.br
4. Katiane Pereira da Silva
Federal Rural University of Amazônia, Belém, Pará, Brasil.
https://orcid.org/0000-0001-7864-6467
Katiane.silva@ufra.edu.br
5. Herson Oliveira da Rocha
Federal Rural University of Amazônia, Belém, Pará, Brazil.
https://orcid.org/0000-0002-2494-6277
herson@ufra.edu.br
6. Fabrício da Silva Lobato
State University of Pará, Belém, Pará, Brazil
https://orcid.org/0000-0002-4250-4763
fabriciolobatomat15@hotmail.com
7. Daniele Cristina de Brito Soares
Federal Rural University of Amazônia, Belém, Pará, Brazil.
https://orcid.org/0000-0002-2684-9171
daneiele.soares@ufra.edu.br
8. Adonai do Socorro da Cruz Gonçalves
Federal University of Para, Brazil
https://orcid.org/0000-0001-8319-9788
adogon3@hotmail.com
9. Angélica Bittencourt da Cruz Galiza
Federal University of Para, Brazil.
https://orcid.org/0000-0002-1553-8511
angelicagaliza@yahoo.com.br
10. Inocêncio Renato Gasparim
Associação Internacional de Educação Continuada - AIEC
https://orcid.org/0000-0001-8063-1176
inocencio.gasparim@gmail.com

ABSTRACT

The Algebraic Arithmetic of Remainder or The Non-Modular Arithmetic of Remainder has the purpose of describing the demonstrations of Modular Arithmetic in a different language, providing its theorems and axioms in a totally new and different way, with no necessity of the use of modulus anyway, from what has been done until now. This article is not about which language is better or not to express this topic of Pure Mathematics, but about a new language that was developed to give a different approach to the Arithmetic developed at present, and to get equal results in a different form and with new propositions of the theorems developed by many mathematicians who created this branch of Pure Mathematics over the last three hundred years.

INTRODUCTION

The Non-Modular Arithmetic of the Remainder (NMAR) or Algebraic Arithmetic of the Remainder (AAR) emerged as an alternative to the so-called Arithmetic of Remainder or Modular Arithmetics with the notion of congruence by the present author. This area is so important for Pure and Applied Mathematics, much needed for Cryptography. And in this new language presented by the author known as AAR or NMAR, the notion and use of the term congruence is required no more.

About that, it should be noticed that the term congruence, for this case, was used for the first time by Gauss himself in his work entitled ***Disquisitiones Arithmaticae*** (Arithmetic Investigation) in 1801. Such a book is considered the initial milestone of modern Number Theory. “In it, [Gauss] compiled the work of his predecessors and gave the field a new life, developing the thoeries of quadratic congruences, forms and residues” (Mol, 2003, p.125).

In many Discrete Mathematics textbooks, the symbology "mod", can be presented as laid out in Schienerman (2017), book below: Let $\boldsymbol{a} \; and \; \boldsymbol{b} \in \mathbb{Z}$**,** with $\boldsymbol{b > 0}$ there exist a unique pair of numbers $\boldsymbol{q} \; and \; \boldsymbol{r}$**,** so that $\boldsymbol{a = qb + r}$ and $\boldsymbol{0 \leq r < b}$**.** Hence the expression,

$$\boldsymbol{a \; mod \; b = r}.$$

This means, this operation describes, and taking any number $\boldsymbol{a} \in \mathbb{Z}$ divide it by $\boldsymbol{b}$, and take the remainder $\boldsymbol{r}$**.**

Therefore, when making $a = 10$, $b = 13 \; and \; r = 1$, we have:

$$\boldsymbol{10 \; mod \; 3 = 1}$$

For, when dividing the integer $\boldsymbol{a = 10}$ by $\boldsymbol{b = 3}$, it leaves remainder $\boldsymbol{r = 1}$. Since $\boldsymbol{10}$ can be described arithmetically by $\boldsymbol{10 = 3 \cdot 3 + 1}$.

As the symbology of the operation "$\boldsymbol{mod}$" appears distinctly and employed in Modular Mathematics, as shown in the book by Hefez (2008), which defines congruence and application of the symbology "$\boldsymbol{mod}$", as:

Let m be a nonzero number. We will say that two natural numbers $a \; and \; b$ are congruent modulo m if the remainders of Euclidean division by m are equal. When the integers $a \; and \; b$ are congruent modulo m, we write

$$\boldsymbol{a \equiv b \; mod \; m}$$

For example, when $\boldsymbol{a = 21}$, $\boldsymbol{b = 13}$, and $\boldsymbol{m = 2}$ you have $\boldsymbol{21 \equiv 13\, mod\, 2}$, where the remainders of the division of $\mathbf{21}$ and $\mathbf{13}$ divided by $\mathbf{2}$ leave the same remainder **1.** As we can easily conclude that, according to the definition denoted above to "mod", now is denoted as a congruence relation. So, we have:

$$\boldsymbol{a \ \equiv b\, mod\, m \rightarrow a\, mod\, m = r}\ and\ \boldsymbol{b\, mod\, m = r}$$

So,

$$\boldsymbol{a \ \equiv b\, mod\, m \rightarrow a\, mod\, m = b\, mod\, m}$$

As $\boldsymbol{a \equiv b\, mod\, m}$ is a language used to express the division $\boldsymbol{a}\ and\ \boldsymbol{b}$ by $\boldsymbol{m}$ leave the same remainder $\boldsymbol{r}$. And, if it leave the same remainder, than $\boldsymbol{a = ma' + r}$, $\boldsymbol{b = mb' + r}$**,** such that $\boldsymbol{a - b = m(a' - b')}\ since\ \boldsymbol{a'}\, e\, \boldsymbol{b'} \in \mathbb{Z}$.

Topics of the Non-Modular Arithmetic of the Remeinder

Therefore, the following properties of Modular Arithmetic use the Symbol "mod" to express several properties to the Theory that support Modular Mathematics. And, this paper will be addressed the Language of Non-Modular Arithmetic, not only to present this new Language but to prove properties as: Algebraic Arithmetic of the Remainder's Definitions, Axiom of Algebraic Arithmetic of the Remainder, Property of the Neutral Element of Addition.

Proof by Reduction to absurdity or Contradiction of the Neutral element of Addition, Algebraic Formalism Arithmetic Property of the Remainder, Commutative Property of Addition, Proof of Commutative Property, Neutral Element Property of Multiplication, Product Prorperty, Power Property, Commutative property of multiplication, Inverse Element of Multiplication.

As well as, Consequences of the Existence of the Neutral Element of Multiplication, Conditions of Existence of the Remainder $\mathrm{w(ax)_n}$, A Unique Property of the Product of Remainders. Demonstration of Fermat's Little Theorem by Operator W, Proof of Fermat's Little Theorem, Direct Proof of Fermat Little Theorem, Property of the Sum of the Remainder with Diferent Bases.

And finally, Proof of Catalan Conjecture, Function for Finding All the Numbers $\mathrm{p^k}$ divisible by p, Function that Enumerate all values of $\mathrm{p^k}$ with respect to a given $\mathrm{q} \in \mathbb{N}$, $0 < \mathrm{q} < \mathrm{p^k}$, where $\mathrm{gdc}(\mathrm{p^k}, \mathrm{q}) = 1$; The sum of Equal Bases with Different Kernel and A Relation of the Sum of Different Kernel and Congruence.

It should be noted that, once the axiom of the Algebraic Arithmetic of the Remainder is exposed, all the rest will be a consequence of this axiom, and from which all others follow. And, its development will lead to a New Language that can be used for this Theory of Pure Mathematics.

Algebraic Arithmetic of the Remainder's Definitions

The first axiom (a basic property took as evidente) of the Non-Modular Arithmetic is designed to replace (in this text) the usual Arithmetic. Let's look the property of multiplication like that $\boldsymbol{a = nk + r}$. And extract some new terms.

Where : $\boldsymbol{a}$: $Dividend\ or\ Kernel$, $\boldsymbol{n}$: $Base$, $\boldsymbol{k}$: $Quotient$ $\boldsymbol{r}$: $Remainder$.

Axiom of Algebraic Arithmetic of the Remainder

Definition: $\boldsymbol{a\ mod\ n = w(a-nk)_n = r, if\ and\ only\ if, a \neq kn\ e\ 1 \leq r < n\ and\ k \in \mathbb{Z}}$.

So, $\boldsymbol{w(a \pm nk) = r, if\ and\ only\ if, a \neq kn\ e\ 1 \leq r < n\ e\ k \in \mathbb{Z}}$.

An immediate consequence of the definition of the Non-Modular Arithmetic of the Remainder's Operation, which will be called $\boldsymbol{w}\ Operation$, and it will be precisely that: $\boldsymbol{w(kn)_n = 0}, to\ a\ number\ \boldsymbol{k} \in \mathbb{Z}\ that, \boldsymbol{w(a)_n = r}\ for\ all\ \boldsymbol{a \neq kn}\ e\ \boldsymbol{1 \leq r < n\ e\ k} \in \mathbb{Z}$. It's easy to prove this proposition, since: $\boldsymbol{w(a-nk)_n = 0}$. If $\boldsymbol{a = nk}$, so $\boldsymbol{w(nk-nk) = w(0)_n = 0}$. Therefore, we can state the following property of the Non-Modular Arithmetic of the Remainder, such as:

Lemma 1.1

If, $\boldsymbol{w(a-nk)_n = w(nk)_n.\ So, w(nk)_n = 0, to\ any\ k} \in \mathbb{Z}$.

I. Property of the Neutral Element of Addition

$$\boldsymbol{w(na)_n = na, to\ any\ \ n} \in \mathbb{Z}$$

The proof is immediate, therefore, by the definition of the Algebraic Arithmetic of the Remainder, since, if $\boldsymbol{n/na}\ and\ \boldsymbol{n/na - nk}$. Therefore, this division of $\boldsymbol{(na \div n) = a\ or\ (na - nk) \div n = a - k}$, leaves no remainder. For,$\boldsymbol{(na-nk) = n(a-k)}$, which makes it a multiple of $\boldsymbol{n}$. Hence, $\boldsymbol{w(nk)_n = 0\ e\ w(na-na)_n}$ can be rewritten by $\boldsymbol{w(n(a-a)_n = w(a * 0)_n = w(0)_n = 0}$. Therefore, it is proved that $\boldsymbol{w(na)_n = r = 0}$.

Proof by Reduction to the Absurd of the Neutral Element of Addition.

Let, $\boldsymbol{w(na)_n = r}$, mean that $\boldsymbol{w(na)_n = na}$. Hence, $\boldsymbol{an = r}$. However, $\boldsymbol{r = na}$ means that $\boldsymbol{n}$ is a multiple of $\boldsymbol{r}$, resulting in $\boldsymbol{r > n}$. Because, $\boldsymbol{w(a)_n}$ exists, by the very definition of the Algebraic Arithmetic of the Remainder, if and only if, $\boldsymbol{r \neq na}\ and\ \boldsymbol{1 \leq r < n}$.

Theorem 2. Sum of the Terms of Non-Modular Arithmetic.

The sum of the remainder´s terms is equal to the sum of the terms separated.

$$\boldsymbol{w(a+b)_n = w(a)_n + w(b)_n}$$

Proof of Theorem 2.

Let $\boldsymbol{w(a)_n = r_1\ and\ w(b)_n = r_2}$. So, $\boldsymbol{w(a-nk)_n + w(b-nk)_n = r_1 + r_2}$. Because, $\boldsymbol{a - nk_1 = r_1\ and\ b - nk_2 = r_2}$. Therefore, applying the operation of the remainder, we have that $\boldsymbol{w(a - nk_1)_n + w(b - nk_2)_n = r_1 + r_2}$. And, the sum of the values of $\boldsymbol{r_1 + r_2 > n}$, has the remainder operation applied again. Hence, $\boldsymbol{w(a)_n + w(b)_n = w(r_1 + r_2)_n = w(r)_n = r}$.

Now we can calculate the value of $\boldsymbol{w(a+b)_n}$. Since, $\boldsymbol{w(a+b)_n = w(a - kn + b - nk)_n}\ w$. And, as $\boldsymbol{a - kn = r_1\ e\ b - nk = r_2}$, it implies that, $\boldsymbol{w(a - nk_1 + b - nk_2)_n = w(r_1 + r_1 + n(k_1 - k_2))_n = r}$. Therefore, it is proven that, $\boldsymbol{w(a+b)_n = w(a)_n + w(b)_n}$.

II. Commutative Property of Addition.

$$w(a)_n + w(b)_n = w(b)_n + w(a)_n$$

Proof of Commutative property

As $w(a)_n = a'$ and $w(b)_n = b$ that is, their respective remainders. There is if, $w(a)_n + w(b)_n = a' + b'$. Applying the remainder property of the AAR, again we have: $w(\ w(a)_n + w(b)_n = w(a' + b')_n$. Now, let's do, $w(b + a)_n$. So, as $w(b + a)_n = w(b' + a')$. And, by the property of addition of remainder, we have that: $w(a')_n + w(b')_n = w(b' + a')_n = w(b') + w(a)'$. And, as $w(a')_n + w(b')_n = w(b')_n + w(a')$, then replacing $a' = a - nk_1 \text{ and } b' = b - nk_2$, we have: $w(a - nk_1)_n + w(b - nk_2)_n = w(a - nk_1 + b - nk_2)$. Therefore, applying the property of the sum of the remainder, there is, $w(a)_n - w(nk_1)_n + w(b)_n - w(nk_2)_n = w(a)_n + w(b)_n - w(n(k_1 + k_2)_n$. Canceling the portions of the remainder where we have multiples of n, it follows that:

$$w(a)_n + w(b)_n = w(b)_n + w(a)_n$$

The generalization of the property above for more terms, is up to the reader

Commutative Property Generalized.

$$(\mathrm{w}(\mathrm{a})_\mathrm{n} + \mathrm{w}(\mathrm{b})_\mathrm{n}) + \mathrm{w}(\mathrm{c})_\mathrm{n} = \mathrm{w}(\mathrm{a})_\mathrm{n} + (\mathrm{w}(\mathrm{b})_\mathrm{n} + \mathrm{w}(\mathrm{c})_\mathrm{n})$$

Proof of Commutative Property

Let $(\mathrm{w}(\mathrm{a})_\mathrm{n} + \mathrm{w}(\mathrm{b})_\mathrm{n}) = w(a + b)_n = (r_1 + r_2)_n$ and $w(c)_n = r_3$. So, $(\mathrm{w}(\mathrm{a})_\mathrm{n} + \mathrm{w}(\mathrm{b})_\mathrm{n}) + \mathrm{w}(\mathrm{c})_\mathrm{n} = w(r_1 + r_2)_n + w(r_1)_n = w(r_1 + r_2 + r_3)$. When doing $r_2 + r_3 = r$ and, applying the property of sum of remainders in $(\mathrm{w}(\mathrm{a})_\mathrm{n} + \mathrm{w}(\mathrm{b})_\mathrm{n}) + \mathrm{w}(\mathrm{c})_\mathrm{n}$, we have: $w(r_1 + (r_2 + r_1))_n = w(r_1 + r)_n = w(r_1)_n + w(r)_n$. Hence, it can be verified that $w(r_1)_n + \left(w(r_n)\right) = w(r_1)_n + (w(r_2 + r_3))$. Thus, so now, we have that, $(\mathrm{w}(\mathrm{a})_\mathrm{n} + \mathrm{w}(\mathrm{b})_\mathrm{n}) + \mathrm{w}(\mathrm{c})_\mathrm{n} = \mathrm{w}(\mathrm{a})_\mathrm{n} + (\mathrm{w}(\mathrm{b})_\mathrm{n} + \mathrm{w}(\mathrm{c})_\mathrm{n})$, demonstrating the desired property.

III. Property of the Neutral Element of Multiplication.

$$w(nk + 1)_n = 1$$

Proof: Suppose $w(a)_n = 1$. So, by the property of the NMAR, we have that, $w(a)_n = w(a - nk)_n = 1$. So, let $a = 1$ implies that, $w(a - nk)_n = w(1)_n - w(nk)_n = w(1)_n = 1$. That's the trivial solution. However, if $a \neq 1,$ we have that, $w(a - nk)_n = w(a)_n - w(nk)_n = 1.$

Hence, $w(nk)_n = 1 + w(a)$ and as $w(nk)_n = 0$, implies that $w(a)_n$ is 0 or a multiple of n. Hence, $a = nk$. Therefore, it is proved that the neutral element of the sum arithmetic is $w(nk + 1)_n = 1$.

Subsequently we will have all remainders of the form $w(nk + r)_n$ since, $r \neq nk$. That is, there will always be a remainder, as long as r is not a multiple of n. That is, the set of possible remainders, represented by r_n, will be:

$$r_n = \{\, nk + 1, nk + 2 \ \ldots + \left(nk + (n - 1)\right)\}$$

IV. Product Property of Non-modular Arithmetic

$$w(a)_n * w(b)_n = w(a * b)$$

Like $w(a - nk_1)_n = a'$ and $w(b - nk_2)_n = b'$. Then, the product property of the remainder, $w(a)_n * w(b)_n = w(a')_n * w(b')_n = r_1 * r_2 = w(r_1 * r_2)_n$. Recall that, in the Non-Modular arithmetic of Remainder, $w(r)_n = r$. For this reason, $r_1 * r_2 = w(r_1 * r_2)_n$. Now let $w(a * b)_n = w\big((a - nk_1) * (b - nk_2)\big)_n$. So, applying the property of sum of remainders, it is easy to see that, as $w(\ (a - nk_1)\ +\ (b - nk_2)\ )_n = w(\ a * b\ -\ ank_2\ -\ bnk_1\ -\ n^2k_1k_2\ )_n = w(a' * b')_n$. Hence, $w\big((a - nk_1) * (b - nk_2)\big)_n = w(a' * b')_n = w(r_1 * r_2)_n = r$. Therefore, in this way, it is proved that, $w(a)_n * w(b)_n = w(a * b)$.

V. Power Property of Non-modular Arithmetic.

$$w(a)_n^m = w(a)_n * \dots * w(a)_n = w(a * \dots * a) = w(a)^{m}{}_{n}$$

Let $w(a)_n = r$. Hence, $w(a)_n^m = r^m \therefore w(a)_n = r * r * r \dots r$. So, we have $w(a)_n = r * r * r \dots r = w(a)_n * w(a)_n * w(a)_n \dots w(a)_n$, *so we have* $w(a)_n = r$. And, according to the transitive property of arithmetic, it says that: if $a = b\ e\ b = c\ \to\ a = c$. In this way, it is proved that $w(a)_n^m = r * r * r \dots\ r = w(a)_n * w(a)_n \dots w(a)_n$. So, $w(a)_n^m = w(a)_n * w(a)_n \dots w(a)_n$ Now, notice that, $w(a)_n * w(a)_n \dots w(a)_n = w(a * a) * w(a) \dots w(a) = w(a^2)_n * w(a)_n \dots w(a)_n$ and that, when generalizing the property of the product of remainders, term a term, we will have, $w(a)_n * w(a)_n \dots w(a)_n = w(a * a * a \dots a)_n = w(a^m)^n$. Therefore, it is shown that $w(a^m)_n = w(a)_n * \dots * w(a)_n = w(a * \dots * a) = w(a)_n^m$.

VI. Commutative Property of Multiplication.

$$w(a)_n * w(b)_n = w(b)_n * w(a)_n$$

This property, commutative property, is immediate. Suppose that $w(a)_n = r_1\ and\ w(b)_n = r_2$. So, $w(a)_n * w(b)_n = r_1 * r_2 = w(r_1 * r_2)_n$. Likewise, notice that $w(b)_n * w(a)_n = w(b * a)_n = w(r_2 * r_1)_n$. Therefore, we have that, $a * b = b * a$, follows that, $w(a * b)_n = w(b * a)_n \therefore w(a)_n * w(b)_n = w(b)_n * w(a)_n$. Therefore, by the product property of NMAR, we have $w(a)_n * w(b)_n = w(b)_n * w(a)_n$.

VII. Inverse Element of Multiplication.

Suppose that, there is a solution for $w(ax)_n = 1,$ Therefore, by the property of the existence of the Non-Modular Arithmetic of Remainder, we have that: $w(ax)_n = w(ax - nk)_n = 1$. So, applying the Property of the Sum of Remainders, we have: $ax - nk = 1$. When applying the Property of the Remainder to Base n on both sides of the equality, we have that: $w(ax)_n - w(nk)_n = 1 \therefore w(ax)_n = 1$, that is, if $ax < n$ *implies that* $ax = 1$. So, for the expression $ax = 1$ to be true it is necessary that $a = x$. Which is a trivial solution to the problem, since $w(1)_n = 1\ and, if\ n \neq 1$.

Now, when applying again the Existence Remainder's Property in the equation $ax - nk = 1$ with the base a, we have then: $ax - nk = 1\ \to w(ax)_a - w(nk)_a = 1$. Therefore, $w(nk)_a = -1$. So, for the expression $\boldsymbol{w(nk)_n = -1}$ $\boldsymbol{nk \neq at, t} \in \mathbb{Z}$. Hence we can conclude that: se $\boldsymbol{a \not\equiv nk}$ and $\boldsymbol{n \not\equiv ta}$. Therefore, $\boldsymbol{gdc(a,n) = 1}$. Therefore, we can conclude that:

$\boldsymbol{Theorem\ 4. w(ax)_n = 1\ \ if\ and\ only\ if\ gdc(a,n) = 1.}$

Therefore, once theorem 4 is defined, it is easy to demonstrate that the expression $\boldsymbol{w(ax)_n = ax - nk = 1}$ exists, if and only if, $\boldsymbol{w(ax)_n = 1}$ exists. If, $\boldsymbol{gdc(a,n) = 1}$ *then*, $\boldsymbol{w(ax)_n = ax - nk = 1}$. Like $\boldsymbol{-k}$ can be rewritten as $\boldsymbol{y}$. So, $\boldsymbol{ax - nk = ax + ny = 1}$ So here's the next corollary,

$\boldsymbol{Corollary\ 4.1\ If\ \ gdc(a,n) = 1, then\ ax + ny = 1\ has\ solution.}$

Since the expression $\boldsymbol{ax + ny = 1}$ is a linear Diophantine equation, because in accordance with Burton (2007), we have:

The linear Diophantine Equation $\boldsymbol{ax + by = c}$ ***has a solution if and only if*** $\boldsymbol{d|c}$, ***where,*** $\boldsymbol{d = gdc(a,b)}$.

Where it results, made the due substitutions of integer variables for Non-Modular Arithmetic, that the existence of the neutral element $\boldsymbol{w(ax)_n = 1}$ is guaranteed, and implies that the linear Diophantine equation, in the form $\boldsymbol{ax + ny = 1}$ has solution. Since, $\boldsymbol{w(ax)_n = ax + nk = 1}$. So, we can conclude that the existence of the neutral element implies a direct proof of the Bézout Relation. For, by the Bézout Relation, we have that, $\boldsymbol{am + bn = 1}$ if and only if $\boldsymbol{gdc(a,b) = 1}$. This formulation of the Bézout Relation is analogous to the formulation of the neutral element, where $\boldsymbol{w(ax)_n = ax - nk = 1}$, if and only if, , $\boldsymbol{gdc(a,n) = 1}$.

CONSEQUENCES OF THE EXISTENCE OF THE NEUTRAL ELEMENT OF MULTIPLICATION

Suppose you have a Diophantine Equation of type $\boldsymbol{ax + by = 1}$, so the neutral element $\boldsymbol{w(ax)_b = 1}$ exists. So, by multiplying the equation by $\boldsymbol{c}$ on both sides, we have that, $\boldsymbol{acx + bcy = c}$. So when doing $\boldsymbol{ac = m}$ *and* $\boldsymbol{bc = n}$, we have, $\boldsymbol{mc + ny = c}$, *where* $\boldsymbol{c = gdc(m,n)}$.

Therefore, if there is any Diophantine Equation, in general, such that the remainder is different from $\boldsymbol{1}$. There will be a $\boldsymbol{c}$ such that $\boldsymbol{m}$ and $\boldsymbol{n}$ are multiples of **c**. In other words, the remainder when there is a Diophantine Equation, of type, $\boldsymbol{mx + ny = c}$, which is the same as the operator $\boldsymbol{w(mx)_y = r}$. It will have a solution, if and only if, $\boldsymbol{w(mx)_y = c}$.

Proof: Let $\boldsymbol{w(mx)_y = c}$, then, there is $\boldsymbol{mx + ny = c}$ So, for this equation to have a solution, we have that the expression $\boldsymbol{mx + ny = c}$, when divided by $\boldsymbol{n}$, results in, $\boldsymbol{ax + by = 1}$. Therefore, if $\boldsymbol{gdc(a,b) = 1}$, then $\boldsymbol{w(ax)_b = 1}$ has a solution. Hence, $\boldsymbol{w(mx)_y = w(cax)_y = w(c)_y * w(ax)_y = c}$. Likewise, it can be verified that, for the equation $\boldsymbol{mx + ny = c}$, has a solution, the necessary and not sufficient condition is that **m** and **n** are multiples of $\boldsymbol{c}$. That is, $\boldsymbol{m = ac}$ *and* $\boldsymbol{n = bc}$ *for* $\boldsymbol{a}$ *and* $\boldsymbol{b} \in \mathbb{Z}$. Therefore, we have a test for the existence of Diophantine Equations, as follows in the next corollary.

Corollary 4.2 If the $\boldsymbol{gdc(m,n,c) = c}$ ***a Diophantine equation*** $\boldsymbol{mx + ny = c}$. ***So, this equation admits a solution.***

Conditions of Remainder Existence $(\boldsymbol{ax})_{\boldsymbol{n}}$.

For $\boldsymbol{w(ax)_n = r}$ to have remainder, there must be $\boldsymbol{r \neq 0}$. If $\boldsymbol{r = 0}$, the division is exact and has no remainder. Hence, $\boldsymbol{ax - nk = r \;\rightarrow ax \neq nk}$ so that $\boldsymbol{r \neq 0}$. Hence, by the Product's Property of remainder in base $\boldsymbol{n}$, we have, $\boldsymbol{w(a)_n * w(b)_n = r}$ implies that $\boldsymbol{a \neq nk\; e\; b \neq nk}$. And, how $\boldsymbol{w(a)_n * w(x)_n = w(ax)_n}$, hence $\boldsymbol{ax \neq nk}$. Where, $\boldsymbol{k}$ can take any value, as long as $\boldsymbol{k} \in \mathbb{Z}$. Let $\boldsymbol{k = a \;\rightarrow ax \neq na}$, so, $\boldsymbol{ax - na = r}$. And, $\boldsymbol{w(ax)_n - w(na)_n = w(ax)_n = r}$ since $\boldsymbol{ax \neq nk}$, so $\boldsymbol{w(ax)_n = r}\; exists$. Likewise, it can be demonstrated for $\boldsymbol{k = x}$, and it stays as an exercise. Therefore, the theorem below can be stated.

Theorem 5. If $w(ax)_n = r$ exists. So the base n does not a ad the product ax. Then, n does not divide x.

Although Theorem 5 shows the Conditions of Existence of Remainder, we can ask ourselves what happens when $\boldsymbol{ab < n}$. Well, let's make the product $\boldsymbol{ab = a'}$, then, $\boldsymbol{w(a')_n = r}$, because by the Conditions of Existence of the Remainder, $\boldsymbol{r}$ exists, as long as $\boldsymbol{a' < r}$. Hence, the remainder $\boldsymbol{r = ab}$. Therefore, $\boldsymbol{w(ax)_n = r}$ exists. And Theorem 5 guarantees its existence completely.

By the Property of the Product of the Remainder, we have $\boldsymbol{w(ax)_n = ax}$, when $\boldsymbol{ax < r}$. Hence, by doing $\boldsymbol{r = 1 \;\rightarrow ax = 1 \;\therefore a = x}$. That is $\boldsymbol{w(1)_n = 1}$. And, when $\boldsymbol{w(ax)_n = 1}$, it follows that $\boldsymbol{ax = n + 1}$, because $\boldsymbol{w(ax)_n = w(n + 1)_n = 1}$. Therefore, for $\boldsymbol{w(ax)_n = 1}$, $\boldsymbol{ax = nk + 1}$, and whatever the value of **k**, the $\boldsymbol{gdc(ax, n) = 1}$. Since, $\boldsymbol{gdc(nk + 1, n) = 1}$. Whence we reach the following conclusion about existence.

Corollary 5.1 If $w(ax)_n = 1$ exists. Then, $gdc(ax, n) = 1$.

What has to be very clear, at this point, is that the remainder of the product ax of base $\boldsymbol{n}$, $\boldsymbol{w(ax)_n = 1}$ exists, since, $\boldsymbol{ax - nk = 1}$ are satisfied, and that according to the theorem 4 $\boldsymbol{w(ax)_n = 1}$ if and only if $\boldsymbol{gdc(a, n)_n = 1}$. Therefore, this result has an immediate consequence, since we can reach the conclusion demonstrated by Theorem 5.

And, for $\boldsymbol{w(ax)_n = 1}$ to exist, the values of $\boldsymbol{ax}$ can only be the family of values represented by the infinite sequence of terms, such that, $\boldsymbol{s = \{1, n + 1, \ldots, 2n + 1 \ldots, kn + 1\}}$. In which we have the most general test, $\boldsymbol{ax = kn + 1}$. Se $\boldsymbol{k = 0}$, it implies that $\boldsymbol{ax = 1\; and\; x = a = 1}$. And, without the loss of generality, another, possibility would be the general form, $\boldsymbol{ax = nk + 1}$ and as $\boldsymbol{gdc(nk + 1, nk) = 1}$, it is shown that $\boldsymbol{gdc(ax, n) = 1}$. Which is a more general way to obtain the multiplicative inverse for the product n of n elements, which can be generalized to the nth product, is an exercise, since this the $\boldsymbol{gdc(a * b \ldots, n)_n = 1}$.

A Special Property of the Remainder Product.

At this point, the existence of an inverse multiplicative element of remainders, called $\boldsymbol{a^{-1}}$. will be addressed. Although it is not defined in the set of natural numbers, it has applications that will be important for the proof of several important theorems that will emerge.

Definition of the Inverse of Element of Multiplication of the Remainder a^{-1}.

For $\forall \boldsymbol{a} \in \mathbb{N}, exists\; \boldsymbol{a^{-1}} \in \mathbb{Q},\; such\; that\; \boldsymbol{w(a)_n * w(a^{-1})_n = 1}$

It is worth remembering that, by the property of the remainder product, we have:

$$\boldsymbol{w(a)_n * w(a)_n * w(a^{-1})_n = w(a * a^{-1})_n = w(1)_n = 1.}$$

Proof of Fermat's Little Theorem by the W operator.

According to Fermat's Theorem, we have: Let $\boldsymbol{a^p}$ where $\boldsymbol{p}$ is prime, then, $\boldsymbol{a^p \equiv a\ (mod\ p)}$. That is, written, according to the language of the $\boldsymbol{w}$, we have: let $\boldsymbol{a^p}$ where the base $\boldsymbol{n = p}$. So, $\boldsymbol{w(a^p)_p = w(a)_p}$ admits solution.

Proof of Fermat's Little Theorem.

By defining the existence of the remainder, $\boldsymbol{w(a^p)_p = a}$ if and seed if $\boldsymbol{a \neq kp}$. So if $\boldsymbol{w(a^p)_p = a \to a^p - kp = a}$. Because, when applying the property of the rectum, we have $\boldsymbol{w(a^p)_a - w(kp)_a = w(a)_a \to w(kp)_a = 0}$ and as $\boldsymbol{p \neq 0,}$ then $\boldsymbol{k = 0}$ ou $\boldsymbol{k = a}$. Therefore, there must exist an $\boldsymbol{x \neq kp}$, such that $\boldsymbol{w(xa^p)_p = 1}$. Then, $\boldsymbol{xa^p - kp = 1}$ according to corollary 5.1 has a solution, since $\boldsymbol{gdc(xa^p, p) = 1}$. So, it is shown that $\boldsymbol{w(a^p)_p = a}$ exists for all $\boldsymbol{a \neq kp}$.

An important fact about the existence of the Neutral Element is that we can choose the values of $\boldsymbol{x}$, such that $\boldsymbol{x \neq \{p\}}$. That is, if the Neutral Element is of the type $\boldsymbol{x = p + (k + 1),}$ then there is an $\boldsymbol{x}$, such that $\boldsymbol{w(xa^p)_p = 1}$. For, the $\boldsymbol{gdc(x \neq kp, p) = 1}$. Which leads us to the conclusion that, for $\boldsymbol{w(a^p)_p = a}$, it is enough that there is a number $\boldsymbol{x \neq kp}$. Therefore, the following theorem is proved in relation to the property of the remainder.

$\boldsymbol{Theorem\ 6. If\ gdc(a^p, p) = 1. Then, w(a^p)_p = w(a)_p}$.

Remember that, $\boldsymbol{w(a^p)_p = a \to a^p \equiv a\ (mod\ p)}$.

Hence, let $\boldsymbol{a^p}$ and $\boldsymbol{x}$, such that, $\boldsymbol{gdc(xa^p, p) = 1}$. Then, in the same way, we can conclude that $\boldsymbol{gdc(ax, p) = 1}$. For, $\boldsymbol{p}$ being prime does not divide the product $\boldsymbol{ax}$.

Direct proof of Fermat's Little Theorem.

Assuming that $\boldsymbol{w(a^p)_p = w(a)_p}$ exists. Then, $\boldsymbol{a^p - kp = a \to a^p - a = kp}$ or $\boldsymbol{a(a^p - 1) = kp}$.

And, applying the property of the remainder, with the base p, we have, $\boldsymbol{w(a(a^{p-1} - 1)_p = w(np)_p}$ $\therefore$ $\boldsymbol{w(a)_p w(a^{p-1} - 1)_p = w(np)_p = 0}$. And, how the value of $\boldsymbol{(a)_p \neq 0}$ implies that, $\boldsymbol{w(a^{p-1} - 1)_p = 0}$ $\therefore$ $\boldsymbol{w(a^{p-1})_n = 1}$. At this moment, as the equation $\boldsymbol{w(a^{p-1})_p = 1}$ exists. Because, $\boldsymbol{gdc(a^{p-1}, p) = 1}$. So, $\boldsymbol{w(a^p)_p = a}$ is true. And in the same way, as $\boldsymbol{gdc(a^{p-1}, p) = 1}$, implies that, $\boldsymbol{w(a^{p-1})_P = 1}$. Since $\boldsymbol{w(a^{p-1})_P = w(a^{-1})_p w(a^p) = 1}$, we can multiply both sides of the equation by

$\boldsymbol{w(a)_p}$. And , $\boldsymbol{w(a)_p w(a^{-1})_p w(a^p) = w(a)_p}$. So, $\boldsymbol{w(aa^{-1})_p = 1}$, because $\boldsymbol{w(a^p)_p = w(a)_p}$. Therefore, Fermat's Little Theorem is demonstrated by the Algebraic Arithmetic of the Remainder, so we can state the following theorem.

$\boldsymbol{Theorem\ 7. If\ p\ is\ a\ prime\ number\ and\ p \neq a. Then\ w(a^p)_p = w(a)_p}$.

One of the immediate consequences of Theorem 7 is about the condition of existence of the theorem. For, as $\boldsymbol{w(a)_p w(a^{p-1} - 1)_p = w(np)_p}$ Therefore, as $\boldsymbol{w(a^{p-1} - 1)_p = 0}$, that is, $\boldsymbol{a^{p-1} - 1 = pk}$.

$\boldsymbol{Corollary\ 7.1\ If\ p\ \ is\ a\ prime\ number\ and. Then, a^{p-1} - 1 = pk}$.

Property of the Sum of the Remainder with Different Bases

The sum of the operation of the remainder with the same dividend $\boldsymbol{a}$ and bases $\boldsymbol{m}$ *and* $\boldsymbol{n}$, *such that* $\boldsymbol{m \neq n}$ is equal to the sum of the general value, where $\boldsymbol{a_0}$ is the particular case that satisfies the individual operations of different bases. Hence, $\boldsymbol{a = a_0 + mnk}$.

$\boldsymbol{Theorem\ 8. If\ \ w(n,m)1.\ Then,\ \ w(a)_n + w(a)_m = w(a_0 + nmk)_n + w(a_0 + nmk)_m}$

Proof: Let $\boldsymbol{w(a)_n = r_1}$ *and* $\boldsymbol{w(a)_m = r_2}$, hence, $\boldsymbol{w(a)_n + w(a)_m = r_1 + r_2 \therefore r_1 + r_2 = r}$. So let's check the values of $\boldsymbol{w(a)_n = r_1}$. That is, $\boldsymbol{w(a)_n = r_1 \to a = nk_1 + r_1}$ and likewise, $\boldsymbol{w(a)_m = r_2 \to a = mk_2 + r_2}$, as $\boldsymbol{a = a \to nk_1 + r_1 = mk_2 + r_2}$. Therefore, by regrouping the equation $\boldsymbol{nk_1 + r_1 = mk_2 + r_2}$ we obtain a Diophantine equation such like that $\boldsymbol{nk_1 - mk_2 = r_2 - r_1 = r}$.

And, if $\boldsymbol{gdc(m,n) = 1}$, implies that the equation $\boldsymbol{nk' - mk'' = 1}$ has a solution. Therefore, the equation $\boldsymbol{nrk_1 - mrk_2 = r}$ has a solution as well. Where $\boldsymbol{rk' = k_1}$ *and* $\boldsymbol{ek'' = k_2}$. Therefore, the initial value of $\boldsymbol{a_0 = nk_1 + r_1 = mk_2 + r_2}$ is determined. And, when obtaining the particular solution $\boldsymbol{a_0}$ there is a subsequence of values that satisfies the following equation $\boldsymbol{w(a)_n + w(a)_m = r_1 + r_2}$. And for that, you can take all the generic values of $\boldsymbol{a}$, such that $\boldsymbol{a = a_0 + mnk}$.

Let $\boldsymbol{w(a)_n = r_1}$ **and** $\boldsymbol{w(a)_m = r_2}$ satisfy $\boldsymbol{w(a)_n + w(a)_m = r_1 + r_2}$. There is only one solution for this system, and that solution is to do $\boldsymbol{a = a}$, which implies that $\boldsymbol{a_0 - nk_1 = a_0 - mk_2}$ or that $\boldsymbol{nk_1 = mk_2}$. However, as $\boldsymbol{m}$ ***and*** $\boldsymbol{n}$ are not only different, as $\boldsymbol{gdc(n,m) = 1}$.

So, the only form of $\boldsymbol{nk_1 = mk_2}$ *is equating* $\boldsymbol{k_1 = mk}$ ***and*** $\boldsymbol{k_2 = nk}$, **that is ,** $\boldsymbol{mnk = mnk}$. Thus, we can obtain the general form of the equality of the sum of remainder with different bases where $\boldsymbol{w(a_0 + mnk)_n = r_1}$ and $\boldsymbol{w(a_0 + mnk)_m = r_2}$. Hence it is proven that, if $\boldsymbol{w(nx)_m = 1}$, or the $\boldsymbol{gdc(n,m) = 1}$. Then, $\boldsymbol{w(a)_n + w(a)_m = w(a_0 + nmk)_n + w(a_0 + nmk)_m = r_1 + r_2}$. So this result was exactly the theorem we wanted to prove. Note that, the **Theorem 8** has the same application as the **Chinese Remainder Theorem**.

The generalization of **Theorem 8** about the Sum of Remainders with Different Bases can be generalized, taking the permutation of all sums two by two. Therefore, it can be stated like this.

$\boldsymbol{If\ the\ set\ n_1,,, n_m \in \mathbb{Z},\ and\ \ \ gdc(n_1, n_2, \dots n_m) = 1.\ Then,\ the\ equation\ (a)n_1 + w(a)_{n2} + w(a)_{n3} + \cdots + w(a)n_m = r_1 + r_2 + \cdots + r_m\ admits\ solution}$.

Proof of the Catalan Conjecture

According to **corollary 7.1** the algebraic equation $\boldsymbol{a^{p-1}-1=pk}$ admits a solution since the exponents are predecessors of any prime number. Hence, $\boldsymbol{a^{p-1}-1=pk}$ can be regrouped to $\boldsymbol{a^{p-1}-pk=1}$ Therefore, there is only a solution for even exponents, if the exponent $\boldsymbol{n=p-1}$, where $\boldsymbol{p}$ is a prime number.

Therefore, for the expression $\boldsymbol{a^{p-1}-pk=1}$ to be in the form of the Catalan conjecture, it is necessary that $\boldsymbol{pk=b^n}$**.** However, rewriting this expression as $\boldsymbol{pk=b^p \to b=\sqrt[p]{pk}}$ implies that $\boldsymbol{k=p^{n-1}}$**.** So we have that $\boldsymbol{a^{p-1}-p^p=1}$ is the only solution.

And since, $\boldsymbol{p-1}$ is the predecessor of E, como $\boldsymbol{p}$. The only solution to the Catalan equation in the form $\boldsymbol{p-1}$ is true, as long as **m** and **n** are consecutive primes. And, the only natural prime number that has the property of having an ancestor is the number $\mathbf{3}$**.** Therefore, the only consecutive primes that exist are $\mathbf{2}$ and $\mathbf{3}$. So the only solution to the Catalan equation is: $\boldsymbol{a^m-p^n=1}$**.** So, making $\boldsymbol{p=3}$ we have, $\boldsymbol{a^{p-1}-p^p=1}$, $\boldsymbol{a^{2-1}-2^3=1}$, $\boldsymbol{a^1-2^3=1}$, and finally $\boldsymbol{a=9}$ **.**

However, when making $\boldsymbol{\alpha=\sqrt{9}\to\alpha=\pm 3}$, which substituting in the equation, since, $\boldsymbol{a=\alpha^2}$ we have: $\boldsymbol{\alpha^{2(p-1)}-p^p=1}$. Which admits the only solution since , $\boldsymbol{a=\pm 3}$**.** So Catalan's Conjecture is proved.

Function to Find All Numbers of $\mathbf{p}^{\lambda}$ Divisible by $\boldsymbol{p}$.

Let $\boldsymbol{w(p^\lambda)_n=0}$ then, the base $\boldsymbol{n=p}$, can be made since there is no remainder. Therefore, we have that,, $\boldsymbol{w(p^\lambda-nk)=0}$, implying that, $\boldsymbol{p^\lambda=nk}$, and as $\boldsymbol{n=p}$, there is if $\boldsymbol{p^\lambda=pk}$, then

$$\boldsymbol{k=\frac{p^\lambda}{p}=p^{\lambda-1}}.$$

Therefore, the function that enumerates all the numbers that are divisors of $\boldsymbol{p^\lambda}$ with respect to $\boldsymbol{p}$ is $\boldsymbol{k=p^{\lambda-1}}$.

Because, all divisors of $\boldsymbol{p^\lambda}$ by $\boldsymbol{p}$ can be listed in a sequence $\boldsymbol{S_n}$ such that $\boldsymbol{S_n=\{p,2p,\dots\, p*p^{\lambda-1}\}}$**,** which in turn, when making a subsequence $\boldsymbol{S_m}$ such that $\boldsymbol{S_m=S_n/p}$, so we have that,

$$\boldsymbol{S_m=\{1,2,\dots,\,p^{\lambda-1}\}}.$$

And, this subsequence, which has the total amount of terms that can be divided by $\boldsymbol{p}$ and whose value, when enumerated, is equal to $\boldsymbol{p^{\lambda-1}}$, provided that $\boldsymbol{p^\lambda\cap S_m=0}$.

Therefore, by doing $\boldsymbol{k=\delta(p^\lambda)}$, we then have a function that enumerates all the values of $\boldsymbol{p^\lambda}$ that satisfy the desired property between p and $\boldsymbol{p\ and\ p^\lambda}$**.** Therefore, we can state the following property of divisors of $\boldsymbol{p^\lambda}$ with respect to $\boldsymbol{p}$**.**

THEOREM 9. If the base $\boldsymbol{n}$ is a prime number $\boldsymbol{p}$. Then, the function that enumerates all the values of a power of $\boldsymbol{p}$, such that, $\boldsymbol{gdc(p^\lambda,q)\neq 1}$ can be defined by $\boldsymbol{\delta(p^\lambda)=p^{\lambda-1}\ onde\ \lambda\in\mathbb{N}}$.

Function that enumerates all values of $\boldsymbol{p^k}$, with respect to a given $\boldsymbol{q} \in \mathbb{N}$, $\mathbf{0} < \boldsymbol{q} < \boldsymbol{p^\lambda}$, provided that $\boldsymbol{gdc(p^\lambda, q) = 1}$ And if the function $\boldsymbol{\delta(p^\lambda) = p^{\lambda-1}}$ enumerates all divisors of $\boldsymbol{p^k}$ with respect to $\boldsymbol{p}$, then all numbers **q,** $0 < \boldsymbol{q} < \boldsymbol{p^\lambda}$ whose $\boldsymbol{gdc(p^\lambda, q)_n = 1}$ can be expressed as the difference between $\boldsymbol{p^\lambda - p^{\lambda-1}}$. Therefore, by making $\boldsymbol{\overline{\delta}(p^\lambda) = p^\lambda - p^{\lambda-1}}$ we can represent a function that enumerates all the values of $\boldsymbol{p^\lambda}$ with respect to a given $\boldsymbol{q}$, $\mathbf{0} < \boldsymbol{q} < \boldsymbol{p^\lambda}$, such that $\boldsymbol{gdc(p^\lambda, q) = 1}$ and regrouping the terms in this expression $\boldsymbol{\overline{\delta}(p^\lambda) = p * p^{\lambda-1} - p^{\lambda-1} = p^{\lambda-1}(p - 1)}$. Therefore, the given expression $\boldsymbol{\overline{\delta}(p^\lambda) = p^{\lambda-1}(p-1)}$ is the function that enumerates all terms $\boldsymbol{q, q} \supset \left]\mathbf{0}, \boldsymbol{p^\lambda}\right[$ such that $\boldsymbol{gdc(p^\lambda,\ q) = 1}$.

Theorem10. If $\boldsymbol{p, q\ and\ \lambda} \in \mathbb{N}$, and $\boldsymbol{p}$ prime. So, the function $\boldsymbol{\delta(p^\lambda) = p^{\lambda-1}(p-1)}$ enumerates all natural numbers such that $\boldsymbol{gdc(p^\lambda, q) = 1}$.

Sum of Equal Bases with Different Kernel.

Theorem 11. If $\mathbf{w(a)_n = w(b)_n}$ exists. Then, $\mathbf{n|a - b}$.

Proof of the Theorem 11.

Let $\boldsymbol{w(a) = r}$ *and* $\boldsymbol{w(b)_n = r}$. We have that, $\boldsymbol{w(a)_n - w(b)_n = 0}$. And, by the property of the sum of the remainder, we have that, $\boldsymbol{w(a)_n - w(b)_n = w(a-b)_n = 0}$, and this implies that, $\boldsymbol{a - b = nk}$ *for a* $\boldsymbol{nk \neq 0}$. *Because*, $\boldsymbol{a \neq b}$. Then, $\boldsymbol{a - b = nk}$. Now, it only remains for us to prove that $\boldsymbol{n|a - b}$.

Therefore, when applying the property of the remainder with base n on $\boldsymbol{a - b = nk}$ we have: $\boldsymbol{w(a-b)_n = w(nk)_n}$. So, $\boldsymbol{w(a)_n = w(b)_n}$, and $\boldsymbol{a \neq b}$ we have $\boldsymbol{a = nk' + r}$ *and* $\boldsymbol{b = nk'' - r}$. Therefore, $\boldsymbol{a - b = nk' - r - nk'' + r}$. Hence , $\boldsymbol{a - b = n(k' - k'')}$ and doing $\boldsymbol{k' - k'' = k}$ we have that, $\boldsymbol{a - b = nk}$. So, $\boldsymbol{n|a - b}$. And, **Theorem 11** is proved.

Important information about the Property of the Sum of Different Kernel in relation to the same base is verified in proposition 11.1.

Corollary 11.1 If $\boldsymbol{w(a)_n = w(b)_n}$. *Then*, $\boldsymbol{w(a)_n - w(b)_n = nk, nk \neq 0}$

In fact, the need for $\boldsymbol{n \neq 0}$, is already guaranteed by the Axiom of the Existence of the Remainder. What can be deduced about $\boldsymbol{k \neq 0}$ is the simple consequence of $\boldsymbol{k' \neq k''}$, since, $\boldsymbol{k = k' - k''}$. And, obviously, this is what guarantees $\boldsymbol{a \neq b}$.

The important thing is to be clear about the following proposition

$$If\ \boldsymbol{w(a)_n = w(b)_n}.\ Then, \boldsymbol{a - b = nk}, where\ \boldsymbol{k} \in \mathbb{Z}.$$

A Relation of the Sum of Different Kernel and Congruence

The property of the sum of equal bases with a different kernel directly implies the notion of congruence. Because, just to make an analysis of Modular Arithmetic in relation to Non-Modular Arithmetic, just check that, $\boldsymbol{a} \equiv \boldsymbol{b} \bmod \boldsymbol{n}, implies\ that, \boldsymbol{w}(\boldsymbol{a})_{\boldsymbol{n}} = \boldsymbol{w}(\boldsymbol{b})_{\boldsymbol{n}}$.

According to Rosen (2010), there is a notation to indicate that two whole numbers have the same remainder when they are divided by the positive whole number m. That is,

DEFINITION: if $\boldsymbol{a}$ and $\boldsymbol{b}$ are integers and $\boldsymbol{m}$ (which in this work will be replaced by **n**) is a positive integer, then $\boldsymbol{a}$ is congruent to $\boldsymbol{b}$ modulo **m** if m divides $\mathbf{a-b}$.

This implies that if $\boldsymbol{a} \equiv \boldsymbol{b} \bmod \boldsymbol{n}$, it means to say that both $a\ and\ b$ are divisible by n leaving the same remainder $\boldsymbol{r}$, that is, $\boldsymbol{n}|\boldsymbol{a}-\boldsymbol{b}$. And if $\boldsymbol{n}|\boldsymbol{a}-\boldsymbol{b}$, then $\boldsymbol{w}(\boldsymbol{a})_{\boldsymbol{n}} = \boldsymbol{w}(\boldsymbol{b})_{\boldsymbol{n}}$. Despite being different languages, modular arithmetic and non-modular arithmetic express the same result, although using different arguments.

So it is clear that if $\boldsymbol{n}|\boldsymbol{a}-\boldsymbol{b}$, then $\boldsymbol{w}(\boldsymbol{a})_{\boldsymbol{n}} - \boldsymbol{w}(\boldsymbol{b})_{\boldsymbol{n}} = \boldsymbol{0}$. So we have the return of theorem 11. Which can be stated like this,

$$\boldsymbol{w}(\boldsymbol{a})_{\boldsymbol{n}} - \boldsymbol{w}(\boldsymbol{b})_{\boldsymbol{n}} = \boldsymbol{0} \iff \boldsymbol{n}|\boldsymbol{a}-\boldsymbol{b}.$$

The proof of the return of **Theorem 11**, as it is trivial, is up to the reader.

Final Considerations

Finally, it is expected that this new language of Algebraic Arithmetic of Remainders can be used as an analytical and complementary tool to Modular Mathematics, for all those who can see in it a way to express themselves algebraically, in this branch of Pure Mathematics. And, I hope that, the reader may appreciate the properties that were made with great effort and dedication to have another form of language that could be viable to demonstrate the arithmetic properties coherently and with all possible mathematical rigors.

It is also worth noting that the study of Non-Modular Arithmetic of the Remainder does not remove the cyclical character of its operations, but it has applications in various areas of Pure and Applied Mathematics. From Commutative Groups, applications in Groups of Permutations and in Non-Modular Analytic Geometry with a new approach to Non-Modular Vector Space that will be applied. As well as a new interpretation of the character of Function Operations used in Crystallography and Symmetries, which it will be addressed in the next articles.

References

L MOL R. S. **Introdução à história da matemática**. Belo Horizonte: CAEDE-UFMG, 2013. 138 p. earning, 2016.

HEFEZ A. **Elementos de Aritmética**. Testos Universitários, SBM. 2013

SCHEINERMAN E. R**. Matemática discreta: uma introdução**. São Paulo: Cengage, 2017.

BURTON. D. M. **Elementary Number Theory**. Sixth Edition, McGrawHill, 2007.

ROSEN K. H. **Discrete Mathematics and its Applications.** Sext Federal Rural University of Amazônia a edição, McGrawHill, 2010.