IMPACTO CIENTÍFICO EDITORA

MODULAR CONGRUENCES: THE APPLICABILITY OF NUMBER THEORY IN SUPPORTING PROBLEM SOLVING AND COMPUTATIONAL IMPLEMENTATION OF THE CHINESE REMAINDER THEOREM

CONGRUÊNCIAS MODULARES: A APLICABILIDADE DA TEORIA DOS NÚMEROS NO SUPORTE À RESOLUÇÃO DE PROBLEMAS E IMPLEMENTAÇÃO COMPUTACIONAL DO TEOREMA CHINÊS DOS RESTOS

CONGRUENCIAS MODULARES: LA APLICABILIDAD DE LA TEORÍA DE NÚMEROS PARA APOYAR LA RESOLUCIÓN DE PROBLEMAS Y LA IMPLEMENTACIÓN COMPUTACIONAL DEL TEOREMA DEL RESTO CHINO

10.56238/edimpacto2024.007-001

William Rodrigues da Silva[1], Walter Martins Rodrigues[2], José Eduardo Colle[3], Francisco José de Souza Silva[4]

ABSTRACT

This paper presents a comprehensive study on modular congruences and the Chinese Remainder Theorem (CRT), considering its historical importance and practical applications in solving mathematical and computational problems. The paper aims to investigate and demonstrate how modular congruence, based on Number Theory, can serve as an effective tool to support problem solving, presenting its computational implementation and applications in everyday situations. To this end, a pedagogical intervention on "Modular Congruence in High School" is carried out in a state school in Fortaleza-CE, using qualitative methodology and action research, in which the exposition has pedagogical and legal support. Thus, the analysis is carefully based on the National Common Curricular

[1] Specializing in Information Technologies and Systems
Federal University of ABC - UFABC
E-mail: rodrigues.william@ufabc.edu.br
Lattes: https://lattes.cnpq.br/2655746793690223
Orcid: https://orcid.org/0009-0005-2818-466X
[2] Post-Doctorate
University of São Paulo - IME - USP
Email: walterm@ufersa.edu.br
Lattes: http://lattes.cnpq.br/9658022121769752
Orcid: https://orcid.org/0000-0003-1486-8858
[3] Master of Science in Mathematics
Federal University of ABC - UFABC
Email: jecolle@gmail.com
Lattes: http://lattes.cnpq.br/4605460790587476
Orcid: https://orcid.org/0009-0009-8883-3536
[4] Master of Science in Mathematics
Federal University of the Semi-Arid - UFERSA
Email: souzasilvafranciscojose@gmail.com
Lattes: http://lattes.cnpq.br/3265950374549215
Orcid: https://orcid.org/0009-0002-0400-962X

Base (BNCC, 2017), in addition to the development of computational implementations of the CRT in C language. Thus, it is observed that the theorem demonstrated versatility in several applications, from RSA encryption to barcode verification systems, with efficient computational implementation of complexity O(n log m). The research also revealed significant pedagogical benefits in contextualizing mathematics through practical examples. This allows us to conclude that TCR and its computational implementation constitute valuable tools in both theoretical and practical terms, promoting the development of logical reasoning and offering efficient solutions to contemporary problems in areas such as digital security and data validation.

Keywords: Modular congruences. Chinese Remainder Theorem. Mathematics teaching. Computational mathematics.

RESUMO

Este trabalho apresenta um estudo abrangente sobre congruências modulares e o Teorema Chinês dos Restos (TCR), considerando sua importância histórica e aplicações práticas na resolução de problemas matemáticos e computacionais. O trabalho tem como objetivo investigar e demonstrar como a congruência modular, fundamentada na Teoria dos Números, pode servir como ferramenta eficaz no suporte à resolução de problemas, apresentando sua implementação computacional e aplicações em situações cotidianas. Para tanto, procede-se à intervenção pedagógica sobre "Congruência Modular no Ensino Médio" em uma escola estadual de Fortaleza-CE, utilizando metodologia qualitativa e pesquisa-ação, em que a exposição tem sustentação pedagógica e legal. Assim, a análise baseia-se criteriosamente na Base Nacional Comum Curricular (BNCC, 2017), além do desenvolvimento de implementações computacionais do TCR em linguagem C. Desse modo, observa-se que o teorema demonstrou versatilidade em diversas aplicações, desde criptografia RSA até sistemas de verificação de códigos de barras, com implementação computacional eficiente de complexidade O(n log m). A pesquisa também revelou benefícios pedagógicos significativos na contextualização da matemática através de exemplos práticos. Isso permite concluir que o TCR e sua implementação computacional constituem ferramentas valiosas tanto no âmbito teórico quanto prático, promovendo o desenvolvimento do raciocínio lógico e oferecendo soluções eficientes para problemas contemporâneos em áreas como segurança digital e validação de dados.

Palavras-chave: Congruências modulares. Teorema Chinês dos Restos. Ensino de matemática. Matemática computacional.

RESUMEN

Este artículo presenta un estudio exhaustivo sobre las congruencias modulares y el Teorema del Resto Chino (TRC), considerando su importancia histórica y sus aplicaciones prácticas en la resolución de problemas matemáticos y computacionales. El artículo busca investigar y demostrar cómo la congruencia modular, basada en la Teoría de Números, puede servir como una herramienta eficaz para la resolución de problemas, presentando su implementación computacional y aplicaciones en situaciones cotidianas. Para ello, se lleva a cabo una intervención pedagógica sobre "Congruencia Modular en la Educación Secundaria" en una escuela pública de Fortaleza-CE, utilizando una metodología cualitativa e investigación-acción, cuya exposición cuenta con respaldo pedagógico y legal. Así, el análisis se basa cuidadosamente en la Base Curricular Común Nacional (BNCC, 2017), además del desarrollo de implementaciones computacionales del TRC en lenguaje

C. Así, se observa que el teorema demostró versatilidad en diversas aplicaciones, desde el cifrado RSA hasta los sistemas de verificación de códigos de barras, con una implementación computacional eficiente de complejidad O(n log m). La investigación también reveló importantes beneficios pedagógicos al contextualizar las matemáticas mediante ejemplos prácticos. Esto nos permite concluir que el TCR y su implementación computacional constituyen herramientas valiosas tanto en términos teóricos como prácticos, promoviendo el desarrollo del razonamiento lógico y ofreciendo soluciones eficientes a problemas contemporáneos en áreas como la seguridad digital y la validación de datos.

Palabras clave: Congruencias modulares. Teorema del residuo chino. Enseñanza de las matemáticas. Matemáticas computacionales.

INTRODUCTION

Number Theory developed from practical counting and measurement needs throughout history. This area of mathematics has gained recognition through the contributions of several mathematicians and their practical applications.

The present work presents, in fact, a historical overview of Number Theory, addressing its main theoretical foundations, with emphasis on modular congruences. These are the basis of the Chinese Remnants Theorem and fundamental for solving mathematical problems. In this context, we seek to investigate the applicability of modular congruences and the Chinese Theorem of Remnants in the teaching of mathematics at the high school level.

As Boyer (1996, p. 104) points out, "the evolution of Number Theory has followed the practical needs of societies throughout history". Therefore, the research arises from the observation of the students' difficulty in understanding abstract concepts of number theory and the need to establish more meaningful connections between mathematical content and its everyday applications. As a complement to the central foundation of this research, it is added, therefore, the aspect of the subject contributing to the simplification and assimilation of the student about multiple concepts.

To consider this effect on teaching, experiences developed with high school students in a Full-Time School in Fortaleza, which occupies a prominent position in the educational indicators of the State Education Network of Ceará, were conducted and presented.

With this intervention, it was sought to enrich, among other elements of the National Common Curricular Base (BNCC), precisely the proposed content, seeking to highlight the relevance of understanding the applicability of number theory. This becomes pertinent, mainly, by highlighting the modular congruences in the current school environment in a post-pandemic context, in which educational institutions articulate the recovery of learning.

The central purpose of this study is, therefore, to explore the most relevant applications of modular arithmetic in contemporary identification and coding systems, following the specific objectives, namely:

1. Develop an efficient computational implementation of the Chinese Remnants Theorem in C language, aiming at practical applications in encryption and data validation systems;
2. To quantitatively analyze the impact of the application of modular congruences in high school through structured pedagogical interventions in a school in Fortaleza-CE;

3. Demonstrate the historical evolution and theoretical foundations of modular arithmetic, establishing connections with modern identification systems (barcodes, CPF) and cryptography;
4. Develop and validate a set of pedagogical strategies for the teaching of modular arithmetic, focusing on practical applications and measurement of results through comparative evaluations;
5. Document and analyze at least three cases of successful application of the Chinese Remnants Theorem in contemporary computational problems;

Thus, the research is justified by the effort to clarify the importance of the applications of modular arithmetic and the Chinese remainder theorem for society, in addition to highlighting the presence of mathematics in everyday situations. Above all, the advancement of studies in this field may, opportunely, arouse interest in improving pedagogical practices in the teaching of arithmetic in basic education, favoring an environment conducive to mathematical learning. It aims, consequently, to contribute and strengthen investigations in the computational area, expanding the impact of the applications of this theory in technological and scientific solutions.

THEORETICAL FRAMEWORK

HISTORICAL EVOLUTION OF MODULAR CONGRUENCES

Over the centuries, several contributions have been left by various researchers to enrich mathematical knowledge. Therefore, it is worth mentioning the term "mathematical knowledge", since this science encompasses multiple fields of study and different methodologies to reach similar conclusions, allowing its pluralization as an area of knowledge that has fascinated scholars since antiquity. Naturally, the discoveries and refinements occurred as new perspectives were adopted on this discipline, a process that continues to evolve in contemporary times and will continue in the ages to come.

Number theory, in turn, whose arithmetic is a fundamental component, represents the segment of mathematics dedicated to the study of numerical structure and the possible operations between its elements. Therefore, it is present in the daily life of the entire society, manifesting itself in activities such as counting, monetary calculations, measurements, and analysis of relationships between quantities. Arithmetic is among the most primitive branches of mathematics, as elementary operations have been performed since the dawn of civilization, although more sophisticated studies, classified as higher arithmetic, emerged only in the eighteenth and nineteenth centuries.

The progress of number theory is fundamentally linked to the practical imperatives of human development. Mathematical conceptions arose spontaneously during efforts to solve everyday issues, with each new obstacle catalyzing the emergence of innovative mathematical methodologies and instruments.

At the end of the sixth century, for example, the Hindus made an essential contribution, as highlighted by Costa and Santos (2008, p. 11): "After the creation of zero, the system of positioning the base ten is created, using the place of units, tens, hundreds and so on, thus getting rid of the problems generated by its absence, such as, for example, distinguish the number 15 from the 105."

The elaboration of a symbolic representation of emptiness represents a remarkable achievement of the human intellect, particularly in the context of the early Christian era. Caraca (2003, p. 6) points out: "One thing that not everyone notices is that this numbering is a real marvel that allows not only to write the numbers very simply, but also to carry out the operations."

After all, the evolution of numbering systems was motivated by the daily demands of civilization. Consequently, several counting mechanisms were conceived, especially the abacus. Regarding this device, Costa (1996, p.175-178) ponders: "Very practical, it freed man from the effort of accumulations, but it required knowledge of the combinations resulting from the position of each account. It is not, therefore, a calculating instrument, but only indicates the numbers added and subtracted."

Furthermore, the construction of integers derived from the primordial notion of natural numbers, originally elaborated to solve counting questions. Although negative numbers have occasionally emerged since ancient times, they have faced considerable skepticism in the mathematical community. Only with the flourishing of European trade, in the late Middle Ages, did the concrete demand for the incorporation of relative integers and their operations into the mathematical framework manifest itself.

In what follows the history of number theory, although the concept of integer precedes the systematization of natural numbers, contemplating their use in commercial transactions and other everyday applications, their formal legitimation was a prolonged process, as indicated by Hefez (2016).

In ancient China, the development of number theory had a significant moment with the mathematical text "Sun Zi Suanjing" (Sun Zi's Manual of Arithmetic). In this seminal work, mathematician Sun Zi presented problems that would lay the foundation for what would become the Chinese Remnants Theorem. Particularly the problem presented in

volume 3, question 26, which addresses the determination of numbers through their remains when divided by different divisors.

On the other hand, in the thirteenth century, the mathematician Qin Jiushao (1202-1261) took a significant step forward in developing a general approach to solving these types of problems, thus laying the theoretical foundations of what we know today as the Chinese Remainder Theorem. This fundamental contribution of Jiushao allowed him to transcend particular cases, providing a systematic method to solve an entire class of similar problems (DING, 1996, p. 16).

Arithmetic has therefore been built with the help of numerous mathematical theorists, particularly since Euclid, with his work *The Elements* (approximately 300 BC), until it reached its apex in the seventeenth century through the investigations conducted by Pierre de Fermat, which provided great advances for the field.

At first, in the Hellenistic period, Euclid of Alexandria presented in his masterful work *The Elements* (about three centuries before the Christian era) a formulation that resembled what would come to be known as the fundamental theorem of arithmetic. Although he offered a proof for such a proposition, it was only in the nineteenth century that Carl Friedrich Gauss was able to establish it with mathematical rigor, providing it with the appropriate mathematical notation and elevating it to the condition of a theorem, a formalization that remains valid and widely used in contemporary mathematics (Hefez, 2016, p. III).

Later, in discussions about modular arithmetic, it is essential to mention the contributions of Pierre de Fermat, a French jurist who cultivated mathematics, as the authors Boyer and Merzbach (2012, p. 244) point out: "Fermat was by no means a professional mathematician", considering that later mathematicians dedicated themselves to the study and formal demonstration of his propositions.

A significant illustration, presented by Mol (2013, p. 98) about Fermat's Little Theorem, states that if *p* is prime and *a* is a number not divisible by p, then it is divisible by $a^{p-1} - 1p$, although Fermat himself did not provide a formal proof when he proposed it. The proof of this theorem was first published by Leonhard Euler, approximately a century later.

The discoveries on modular arithmetic clarified by Fermat attracted the attention of other mathematicians, particularly in the eighteenth century, with Euler, and in the nineteenth century, with Lagrange and Legendre, who also devoted themselves to the study of the elucidations proposed by Gauss. In the eighteenth and nineteenth centuries, mathematics was enriched by the research of Leonhard Euler, Joseph Louis Lagrange, Adrien Marie Legendre, John Wilson, and Carl Friedrich Gauss. It is significant to mention

that, from the nineteenth century, after Gauss's contributions, arithmetic became Number Theory (Hefez, 2016).

History relates that Gauss demonstrated, from his childhood, an incredible aptitude that distinguished him from the other students in his class. He was the pioneer in the application of reasoning related to arithmetic progressions when, challenged by his teacher to calculate the sum of all integers from 1 to 100, he identified that adding 1 + 100 obtained 101, 2 + 99 also resulted in 101, 3 + 97 also totaled 101. From this observation, he deduced that he could multiply 101 by half of 100, that is, 50, which is the total of pairs added together to obtain the sum of all the numbers between 1 and 100, arriving at the result 50 to 50, a procedure that we now know as the formula for the sum of the terms of an arithmetic progression, $n(n + 1)/2$ (OLIVERO, 2007, p. 110).

As an observer of numerical correlations, Gauss noticed that expressions such as "(a) provide the same remainder as (b) when divided by (m)" were regularly used (Sa, 2007) and this finding instigated him to develop the reasoning and foundations of modular arithmetic. How is such a phenomenon justified? By verifying that distinct numbers when divided by the same divisor generated identical remains, he then established that such numbers are congruent, that is, "equivalent", in the context of divisibility by that divisor.

It is noteworthy that the terminology "congruence", in this specific context, was pioneered by Gauss in his treatise *Disquisitiones Arithmeticae* (Arithmetic Investigations) published in 1801. This work is considered the inaugural foundation of modern number theory. "In it, [Gauss] gathered the contributions of his predecessors and revitalized the field, developing the theories of quadratic congruences, forms, and residues" (Mol, 2013, p. 125).

For this reason, and by virtue of his remarkable contributions to the study of number theory, Gauss received the nickname of the father of modular arithmetic. It was through his work that a specific mathematical notation was established to formalize the issues pertaining to modular congruence and other arithmetic relations. Years later, Gauss demonstrated that Fermat's Little Theorem represents a particular case of congruence, since "if *a* is a prime number and *p* is any integer, then *p* divides (, which can be expressed using congruence notation as $a^p - a$)"$a^p \equiv a \ mod \ p$".

In the subsequent section, the fundamental concepts of the evolution of number theory will be explored in detail. It is worth emphasizing that such notions emerge in line with contemporary needs, manifesting themselves naturally during the problem-solving process. It is emphasized that each emerging need inevitably gives rise to a response oriented to the resolution of the question presented.

ASPECTS OF NUMBER THEORY FOR PROBLEM SOLVING

Having observed the relevance and development of number theory with regard to modular congruences, in the previous chapter, the essential mathematical foundations will now be explored, covering topics such as divisibility and its attributes, Euclidean Division, the universe of Prime Numbers and fundamental theorems such as Fermat's Little Theorem.

In addition, Linear Congruences, their systems and applications, as well as Linear Diophantine Equations will be investigated. Our journey will span through Wilson's, Fermat's, and Euler's Theorems, culminating in the fascinating Chinese Remnants Theorem and its computational implementation. This sequence of knowledge constitutes a fundamental basis for understanding and solving the mathematical challenges that motivate this work.

The BNCC (BRASIL, 2017) proposes five thematic units that correlate with each other, the one that refers to numbers, as it is directly linked to the Elementary Theory of Numbers, aims to develop numerical thinking, which implies the knowledge of ways to quantify attributes of objects and to judge and interpret arguments based on quantities.

> [...] For this construction, it is important to propose, through significant situations, successive expansions of the numerical fields. In the study of these numerical fields, records, uses, meanings and operations should be emphasized. (BRASIL, 2017, p. 268)

It is worth mentioning that, in addition to the technical richness of these concepts, there is an even more significant benefit: the development of logical reasoning and analytical capacity. This process not only facilitates the assimilation of specific content, but also cultivates cognitive skills that transcend mathematics. This systematic approach to thinking is clearly manifested in the exceptional performance of students who participate in mathematical olympiads, who often demonstrate academic excellence in various areas of knowledge. Such correlation is not mere chance, but rather a direct result of the development of robust analytical skills and the effective mastery of fundamental mathematical concepts.

The incorporation of the study of Linear Congruences, their systems and the Linear Diophantine Equations, together with Wilson's, Fermat's and Euler's Theorems, further enrich this theoretical basis. These topics not only complement the understanding of number theory, but also offer powerful tools for solving complex problems and practical applications in modern mathematics.

Fundamentals of Modular Divisibility and Congruence

The theory of divisibility can be understood through the following fundamental concepts:

1. **Base Definition:**

   For $a, b \in \mathbb{Z}, a \neq 0$, *we say that* $a \mid b$ *if* $\exists k \in \mathbb{Z}$ *such that* $b = ak$

2. **Essential Properties:**

   - Reflective: $a \mid a$
   - Transitive: If $a \mid b$ and $b \mid c$, $então\ a \mid c$
   - Linearity: If $a \mid b\ e\ a \mid c$, $então\ a \mid (mb + nc)$, $\forall m, n \in \mathbb{Z}$

3. **Key features:**

   - $1 \mid a\ e\ a \mid 0, \forall a \in \mathbb{Z}$
   - *If* $a \mid b\ com\ b \neq 0$, $então\ |a| \leq |b|$
   - *If* $b \mid 1\ então\ b = \pm 1$

This fundamental structure of divisibility naturally leads to a broader and more powerful concept: modular congruence. When we analyze the remnants of divisions by a fixed number, we observe patterns that allow us to group numbers with similar behaviors, thus leading to the concept of congruence.

Modular Congruence is a natural extension of divisibility theory, establishing a mathematical structure that relates numbers that, when divided by the same value (modulus), produce identical remainders. This relationship, formalized by Gauss, provides a powerful tool for analyzing numerical patterns and solving complex problems.

The formal structure of modular congruence is established when two numbers, when divided by a third (called module), produce identical remainders. Mathematically, it is expressed as *ab (mod m ≡)*, where *m*, *a*, *b* ∈ ℤ, indicating that *a* and *b* are congruent modulo *m*. The theory is based on crucial properties:

1. Equivalence Ratio:
   - Reflexivity: *the ≡ a (mod m)*
   - Symmetry: *If a ≡ b (mod m), then b ≡ a (mod m)*
   - Transitivity: *If a ≡ b (mod m) and b ≡ c (mod m), then the ≡ c (mod m)*

2. Operative Properties:

- Addition: *If a ≡ b (mod m) and c ≡ d (mod m), then a + c ≡ b + d (mod m)*
- Multiplication: *If the ≡ b mod (m) and c ≡ d (mod m), then ac ≡ comics (mod m)*
- Potentiation: *If a ≡ b (mod m), then $a^n \equiv b^n$ (mod m)*

This mathematical framework lays essential foundations for several fields of applied mathematics, including cryptography, code theory, and data verification systems, demonstrating its relevance both theoretical and practical in contemporary mathematics.

The intersection between divisibility and modular congruence establishes a mathematical paradigm of significant practical relevance. As Sant'Anna (2013) points out, traditional teaching often reduces these concepts to mnemonic rules, neglecting the development of analytical thinking. This approach limits the understanding of the mathematical structures that underlie several contemporary verification and validation systems.

The theoretical-mathematical framework of modular congruence, based on number theory, establishes an algebraic structure that relates numerical elements that, when divided by the same module, produce identical remains. This equivalence relation, initially formalized by Gauss in his treatise *Disquisitiones Arithmeticae*, constitutes a mathematical system that structures several practical applications today.

The rigorous mathematical formulation of this concept can be expressed as an equivalence relation in $\mathbb{Z}$, where two numbers *a* and *b* are considered congruent modulo *m* (denoted by *ab mod m* ≡) if, and only if, *m* divides the difference (*a* - *b*). This fundamental definition generates a partition of the set of integers into equivalence classes, providing an algebraic structure rich in properties and applications.

This theoretical framework of modular congruence, characterized by the relationship between numbers that share the same remainder when divided by a common module, transcends its formal definition to offer substantial practical applications, including:

1. Verification Systems:
   - Barcodes;
   - *International Standard Book Number* (ISBN);
   - Individual Taxpayer Registration (CPF);
   - Validation of digital documents;

2. Divisibility Criteria: According to Muniz Neto (2022), the approach through modular congruence offers a deeper and more structured perspective. For a modulus *m*, an expression is established in terms of the digits *an, an₋₁, an₋₂, ..., a₁ ao*, determining a congruent polynomial *modulo m*.

This analytical approach allows:

- Development of logical-deductive thinking;
- Understanding of fundamental properties;
- Ability to generalize to new criteria;

The application of these properties significantly simplifies complex calculations, particularly in the arithmetic of the remainders. For example, to find the remainder of the division of numbers high to large powers, such as 2545 by 11, the properties of congruence are used in conjunction with Fermat's Little Theorem, substantially reducing computational complexity.

This methodology not only facilitates the practical application of the concepts, but also promotes the development of structured mathematical reasoning, establishing meaningful connections between theory and contemporary applications, particularly in security and data verification systems.

This unified perspective on modular divisibility and congruence demonstrates how fundamental mathematical concepts underpin essential technologies of the digital age, emphasizing their practical and pedagogical relevance in today's educational context.

Euclidean division

Euclidean division is a fundamental concept of arithmetic that states:

Definition: Given two integers a (dividend) and $b \neq 0$ (divisor), there are single integers q (quotient) and r (remainder) such that:

$$a = bq + r, \; com \; 0 \leq r < |b|$$

Demonstration: The evidence can be reduced to the case $a \geq 0 \, e \, b > 0$ through the following transformations:

1. *For* $b < 0$ *: Setting* $b_1 = -b \, e \, q_1 = -q$
2.

$$a = bq + r \Rightarrow a = b_1 q_1 + r_1$$

3. *For* $a < 0 \, e \, b > 0$*: Setting* $a_1 = -a, \, q_1 = -q - 1 \, e \, r_1 = b - r$

$a = bq + r \Rightarrow a_1 = b_1 + r_1$

4. *For* $a \geq 0 \, e \, b > 0$*: By iterative construction*

Initially: $q_1 = 0, \, r_1 = a$

Iteration: $q_{k+1} = q_k + 1, \, r_{k+1} = r_k - b \;\; até \;\; r_1 < b$

This division is essential for:

- Euclidean algorithm of the MDC;
- Modular arithmetic;
- Computing (module operation);

Euclidean division, in addition to its fundamental importance in basic arithmetic, provides the foundation for one of the most important concepts in number theory: the Greatest Common Divide (CDM). The algorithm for finding the CDM, as we will see below, is based directly on the process of successive divisions that we have just studied.

Maximum Common Diffuser (CDM)

Definition 1: $Dados \; a, \, b \in \mathbb{Z}, \, ambos \;$ *No* $\; nulos, \, d \in \mathbb{Z}^* \; é \; o \; MDC \; de \; a \; e \; b \; se$:

1. $d \mid a \; e \; d \mid b$
2. $Para \; todo \; e \in \mathbb{Z} \; tal \; que \; e \mid a \;\; e \;\; e \mid b, \, tem - se \; e \mid d$

Fundamental Property: $Se \; a = bq + r$, *then* $mdc(a, b) = mdc(b, r)$

Bezout's definition: Data $a, \, b \in \mathbb{Z}$, not both null, exist $m, \, n \in \mathbb{Z}$ such that:

$mdc(a, b) = am + bm$

To calculate $mdc(680, 150)$:

$$680 = 150 \cdot 4 + 80$$
$$150 = 80 \cdot 1 + 70$$
$$80 = 70 \cdot 1 + 70$$
$$70 = 10 \cdot 7 + 0$$

Therefore, $mdc(680, 150) = 10$.

Euclid's algorithm provides an efficient method for calculating the CDM through successive divisions until zero remainder is obtained, with the last non-zero divisor being

the desired CDM. This method, as described by Hefez (*apud* FRANCO, 2016 pp.16-19), has remained essentially the same since its presentation in *The Elements*, having received only improvements in its implementation.

Bezout's theorem complements this algorithm by establishing that the MDC can be expressed as a linear combination of the original numbers, thus providing a fundamental bridge between divisibility and linear Diophantine equations. As exemplified earlier:

In Bezout: For $a = 41\ e\ b = 12$:

$$\begin{aligned} 41 &= 12\cdot 3 + 5 && \Rightarrow 5 = 41 - 12\cdot 3 \\ 12 &= 5\cdot 2 + 2 && \Rightarrow 2 = 12 - 5\cdot 2 \\ 5 &= 2\cdot 2 + 1 && \Rightarrow 1 = 5 - 2\cdot 2 \end{aligned}$$

Substituting recursively, we get the MDC as a linear combination of $a\ e\ b$.

Prime Numbers

Definition 2: A natural number greater than 1 is called prime if it has only two positive divisors: 1 and itself. Otherwise, it is called a compound. (MUNIZ NETO, 2022, p. 29):

For $a, p, q \in \mathbb{Z}, com\ p, q\ primos\ e\ q \neq 0$:

- *If* $p \mid q$, *then* $p = q$.
- *If* $p \nmid a$, *then mdc(p, a) = 1.*

Proposition 1: *Let n, a, b, p ,* $\in \mathbb{Z}$*with p prime. If p | ab, so p | A or P | b.*

Fundamental Theorem of Arithmetic: Every natural number greater than 1 is either prime or can be written in a unique way (except in the order of the factors) as a product of prime numbers.

Infinity of Primes: There are infinite prime numbers.

Proof: By absurdity, suppose that there are finite primes $p_1, \cdots, p_r$. Consider $n = p_1 \cdots p_r + 1$. By the Fundamental Theorem of Arithmetic, *n* has a prime factor *p* that divides $p_1 \cdots p_r$. Therefore, *p | 1,* absurd.

If *n > 1* is not divisible by any prime *p* such that $p^2 \leq n$, then *n* is prime.

To check if 353 is prime, simply test divisibility by prime *p* up to $\sqrt{353} \approx 19$:

$$353 = 2 \cdot 176 + 1$$
$$353 = 3 \cdot 117 + 2$$
$$\vdots$$
$$353 = 17 \cdot 20 + 13$$

Since it is not divisible by any of them, 353 is prime.

Sieve of Eratosthenes and Prime Numbers

Definition 3: A natural number is prime when it has exactly two positive divisors: 1 and itself.

Prime numbers, which have been studied for more than 2000 years, are fundamental in number theory and have significant practical applications. The Sieve of Eratosthenes emerged as an efficient method for identifying prime numbers, especially those of greater magnitude.

Sieve of Eratosthenes: Given $x \geq 2$, to ensure that *x* is prime, just show that no prime number $p \leq \sqrt{x}$ divides *x*.

Important properties:

1. 2 is the only pair prime.
2. 0 and 1 are not primes.
3. To test the primality of *n*, simply check divisors up to $\sqrt{n}$.

Sieve of Eratosthenes up to 100

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Source: Prepared by the authors.

To find all prime numbers up to *n*:

1. List all numbers from 1 to *n*;
2. Eliminate multiples of 2 (except 2);
3. Eliminate multiples of 3 (except 3);
4. Consider the process for each prime $p \leq \sqrt{n}$;

Fermat's Little Theorem

Pierre de Fermat (1601-1665) stood out in the history of mathematics for being known as the "Prince of Amateurs". Graduated in Law from the University of Toulouse, in France, he built a solid legal career, serving initially as a lawyer and later as an advisor in the local parliament. His passion for mathematics, cultivated in his spare time, resulted in extraordinary contributions that placed him among the greatest mathematicians of his time (BOYER, 2003).

Fermat's Little Theorem emerges as one of his most significant discoveries, revolutionizing number theory. This fundamental theorem states that: given a prime number *p*, *p* divides $a^p - a$, for all *belonging* to the set of integers ($\mathbb{Z}$). This proposition has become the cornerstone of contemporary Primal Tests, inspiring numerous variations and generalizations.

The proof of the theorem follows an elegant forked structure. For the specific case, in which *p* = 2, the proof is direct and evident. For odd primes, the method of mathematical induction over a is used, starting with the base case *a* = 0. The proof is completed through the application of Newton's Binomial, establishing the universal validity of the theorem for every prime number *p* and any element *a* of the set of real numbers.

Corollary: if *p* is a prime number and *a* is a natural number not divisible by *p*, then *p* divides $a^{p-1} - 1$.

This derivative result is not a particular case, but a powerful tool with extensive practical applications in several fields of mathematics, including divisibility criteria, potentiation in modular congruences and, above all, in advanced modern cryptography.

The historical and practical relevance of Fermat's Little Theorem transcends its time, laying relevant foundations for later mathematical developments and contemporary technological applications. Its elegant simplicity masks a conceptual depth that continues to influence modern mathematics and its practical applications.

Linear Diophantine Equations

Linear Diophantine Equations (EDL) are a sophisticated mathematical application of the concept of divisibility. To illustrate its practical application, consider a problem: a military corporation acquired vehicles, totaling 152 tires, distributed between motorcycles (2 tires each) and automobiles (4 tires each). The goal is to determine all possible combinations of vehicles.

Formally, an EDL is defined as $ax + by = c$, where *a*, *b*, c, ∈, $\mathbb{Z}$ and *x*, *y* are unknowns in $\mathbb{Z}$. This mathematical structure pays homage to Diophantus of Alexandria (third century AD), a pioneer in number theory.

Key aspects:

1. Condition of Existence:
   - *An EDL has solutions if and only if mdc (a, b) | c*
   - ***Demonstration:*** *If* $ax_0 + by_0 = c$*, then stops* $d = mdc(a, b) : a = dm, b = dn\ (m, n \in \mathbb{Z})$

$$c = dmx_0 + dny_0 = d(mx_0 + ny_0)$$

2. For a particular solution:

$r(x_0, y_0) : x = x_0 + (b/d)\,t\ y = y_0 - (a/d)\,t$ *where t* ∈ $\mathbb{Z}$ *and d = mdc(a, b)*

3. Resolution Methods:

   For simple cases (3x + 6y = 18):

   - By inspection: (4.1), (-6.6), (10.-2)
   - Direct condition check *mdc*(3,6) = 3 | 18

   For complex cases (172x + 20y = 1000):

   - Euclid's algorithm for *mdc*:

$$172 = 20 \cdot 8 + 12$$
$$20 = 12 \cdot 1 + 8$$
$$12 = 8 \cdot 1 + 4$$
$$8 = 4 \cdot 2 + 0$$

Therefore, the *mdc* (172, 20) = 4 and since 4|1000, it follows that the given equation has a solution.

- Retroactive linear combination:

$$4 = 12 - 8 \cdot 1$$
$$4 = 12 - (20 - 12 \cdot 1) \cdot 1$$
$$4 = 12 - 20 \cdot 1 + 12 \cdot 1$$
$$4 = 2 \cdot 12 - 20 \cdot 1$$
$$4 = 2 \cdot (172 - 20 \cdot 8) - 20 \cdot 1$$
$$4 = 172 \cdot 2 - 20 \cdot 16 - 20 \cdot 1$$
$$4 = 172 \cdot 2 - 20 \cdot 16 - 20 \cdot 1 \Rightarrow 4 = 172 \cdot 2 - 20 \cdot 17$$

Then we have the equation: $4 = 172 \cdot 2 - 20 \cdot 17$.

- Particular solution:

Since you want a solution for the combination that results in 1000, multiply both sides of this equality by 1000/4 = 250 and you get:

1000 72 · 500 + 20(−4250)

Therefore, the ordered set (500, negative 4250) represents a specific solution to the established equation. The complete set of solutions can be expressed through the algebraic expressions: *x* = 500 + 5t y = -4250 - 43t, where *t* goes through all the integers arriving at the general formula: $x = 500 + 5t \; y = -4250 - 43t \; (t \in \mathbb{Z})$

4. Advanced Properties:

- The set of solutions forms a two-dimensional arithmetic progression;
- The distance between consecutive solutions is determined by the coefficients normalized by the *mdc*;
- The uniqueness of the solution occurs if and only if |a| = |b| = 1;

This rigorous mathematical formulation of the EDL provides a robust approach to solving problems that require integer solutions, with applications in discrete optimization, number theory, and practical counting and distribution problems.

While the Diophantine Equations provide us with tools for working with linear equations in the domain of integers, Wilson's Theorem presents us with a different but complementary perspective on the properties of prime numbers, expanding the understanding of the fundamental structures of number theory.

2.2.8 Wilson's theorem

Wilson's Theorem is an expressive mathematical tool that establishes a deep connection between prime numbers and modular congruences (MUNIZ NETO, 2022, pp. 129-130). This theorem presents a necessary and sufficient condition for primality: a natural number *p* is prime if, and only if, (*pmod p).* − 1)! ≡ −1 (

In the context of linear congruences, an extension naturally emerges through systems of congruences. The Chinese Remnant Theorem (RCT) investigates the existence and uniqueness of solutions for these systems, establishing precise conditions for their resolvability.

The proof of Wilson's Theorem is based on a bijector function f: {1, 2, ..., p − 1} → {1, 2, ..., p − 1}, which maps each element to its modular inverse. The proof reveals that for a prime number p, only 1 and $p - 1$ are their own inverse modulo p, while the other elements form distinct pairs (a, a^{-1}) whose product is congruent to 1 modulo p.

The relationship between Wilson's Theorem and the RCT manifests itself on three fundamental levels:

1. Structural: Wilson's Theorem demonstrates the existence of a unique multiplicative structure in prime finite fields, an essential property for the RCT;
2. Operational: The modular inverses, fundamental for the proof of Wilson's Theorem, are crucial for the construction of solutions in the TCR, particularly in the combination phase of partial solutions;
3. Computational: The verification of primality via Wilson's Theorem guarantees the coprimality of the modules in the TCR, a necessary condition for its applicability;

The connection with the TCR is manifested mainly in the characterization of the modular inverses, a crucial element for the resolution of congruence systems. As Muniz Neto (2022, p. 129) points out, this relationship provides an elegant criterion for verifying primality and deepens the understanding of the properties of modular inverses.

The theorem demonstrates that in a modulo p prime system, every non-null element has exactly one multiplicative inverse, an essential property for the applicability of TCR. This characteristic underlies the resolution of linear congruence systems and their applications in number theory and cryptography.

Practical example:

For $p = 7$:
$6! = 720 \equiv -1 \pmod 7$
Check: $720 = 102 \times 7 + 6$
$6 \equiv -1 \pmod 7$

Confirms that 7 is prime.

The elegance and power of Wilson's Theorem in checking primality paves the way for one of the most versatile tools in number theory: the Chinese Remainder Theorem. While Wilson's theorem provides us with an accurate criterion for identifying prime numbers through congruences, TCR allows us to solve entire systems of simultaneous congruences. This progression is natural: once we understand how to work with congruences with respect to a single prime module (as in Wilson's theorem), the next logical step is to explore how to handle multiple modules simultaneously.

The transition between these theorems is not only sequential, but fundamentally connected. Wilson's Theorem assures us of the existence of specific structures in prime finite fields and this guarantee becomes crucial to understand why and how the RCT works. In fact, the primality check and the understanding of modular inverses that Wilson's Theorem provides us with are often used in the practical application of the RCT, especially when we need to ensure the coprimality of the modules - an essential condition for the applicability of the RCT.

THE CHINESE REMAINS THEOREM

The Chinese Remnants Theorem is associated with certain systems of linear congruences in this sense, according to Eves:

> The most important of the ancient Chinese mathematical texts is the K'ui-ch'ang Suanshu, or Nine Chapters on the Art of Mathematics, which dates to the Han period (206 BC, -221 AD) but most likely contains much older material. It is a synthesis of ancient Chinese mathematical knowledge. In its 9 chapters, the one of relevance to the present work is found in chapter 8 that talks about System of Linear Equations. (EVES, 2011, p.242)

A Linear Congruence System, therefore, is when we have several congruence equations, in which we wish to obtain a solution that simultaneously satisfies these equations. Thus, it is necessary to analyze whether the criteria to identify whether or not a Linear Congruence System admits a solution. One strategy is to divide into cases, they are: 1st case, one of the congruences does not admit a solution, so the system does not admit a solution; 2nd case, congruences admit solution, but the system does not admit solution; 3rd case, congruences admit solution and the system also admits solution.

According to Bezerra (2018, p.149), the Chinese Remnants Theorem can be stated as follows: consider the integers two by two primes to each other, then the Linear Congruence System:$m_1, m_2, \ldots, m_k$

$$\begin{cases} x \equiv b_1 \mod m_1 \\ x \equiv b_2 \mod m_2 \\ \ldots \quad \ldots \quad \ldots \\ x \equiv b_k \mod m_k \end{cases}$$

admits a solution, which is single modulo m = $..m_1.m_2.\ldots m_k$

Historical and Motivating Aspects

The Chinese Remnants Theorem (RCT) is a fundamental result of Number Theory that provides a systematic method for solving linear congruence systems, as seen. This

theorem has important applications both in theoretical mathematics and in practical areas of modern computing, such as cryptography. As we can see in its computational implementation in C language, the algorithm allows to determine unique solutions for congruence systems through an elegant process that involves the manipulation of remnants and divisibility. TCR is particularly relevant when dealing with modular congruences and their applications, as it offers a systematic method to solve problems involving multiple congruences simultaneously.

MATHEMATICAL FORMULATION

In contemporary mathematics, the Chinese Remainder Theorem is formulated with algebraic precision by the following statement: Consider a set of positive integers *m1*, *m2*, . . . , *mr* that are relatively prime to each other two by two. For this set, a system of linear congruences of the form:

$$\begin{aligned} x &\equiv a_1 \left(mod\ m_1 \right) \\ x &\equiv a_2 \left(mod\ m_2 \right) \\ &\vdots \\ x &\equiv a_r \left(mod\ m_r \right) \end{aligned}$$

allows for a single solution modulo *M*, where *M* is defined as the product *m1 m2* . . . *mr* (ROSEN, 2011, p.162).

Formal definition: The Chinese Remains Theorem states that, given the coprime natural numbers $n_1, n_2, \ldots, n_k$ two by two (i.e. = 1 for $i \neq j$), the $mdc\left(n_i, n_j \right)$ congruence system:

$$\begin{aligned} x &\equiv a_1 \left(mod\ n_1 \right) \\ x &\equiv a_2 \left(mod\ n_2 \right) \quad (I) \\ &\vdots \\ x &\equiv a_k \left(mod\ n_k \right) \end{aligned}$$

Has unique module $N = n_1 n_2 \ldots n_k.$ solution

Theorem Proof:

Be $N = n_1 n_2 \ldots n_k$ and $N_i = \frac{N}{n_i}$ for each $i = 1, 2, \ldots, k.$

1. Since the n_i are cousins two by two, we have that . $mdc\left(N_i, n_i \right) = 1$

2. For each i, there is a number y_i such that: . $N_i y_i \equiv 1 \left(mod\ n_i \right)$
3. A system solution is given by: . $x = a_1 N_1 y_1 + a_2 N_2 y_2 + \ldots + a_k N_k y_k$
4. To prove that this is the solution, note that:
   $j \neq i: N_j \equiv 0 \left(mod\ n_i \right)$ $Logo: x \equiv a_i N_i y_i \equiv a_i \left(mod\ n_i \right)$.
5. The uniqueness stems from the fact that if x_1 and x_2 there are two $x_1 \equiv x_2 \left(mod\ n_i \right)$ solutions: for all i. As they $x_1 \equiv x_2\ (mod\ N)$ n_i are cousins, .

Demonstration*:* To verify that the number is written as follows:

$$x = y_1 a_1 + y_2 a_2 + \ldots + y_r a_r,$$

is the solution of the congruence system (I) if we take:

$$y_1 \equiv 1 \left(mod\ m_1 \right) e\ y_1 \equiv 0 \left(mod\ m_i \right),\ i \neq 1$$
$$y_2 \equiv 1 \left(mod\ m_2 \right) e\ y_2 \equiv 0 \left(mod\ m_i \right),\ i \neq 2$$
$$\vdots$$
$$y_r \equiv 1 \left(mod\ m_r \right) e\ y_1 \equiv 0 \left(mod\ m_i \right),\ i \neq r.$$

Then we shall see that such $y_i's$ exist. First, note that:

$$y_2,\ y_3,\ \ldots,\ y_r \equiv 0 \left(mod\ m_1 \right)$$

And so, by the properties of congruence, we have:

$$y_2 a_2 + y_3 a_3 + \ldots + y_r a_r \equiv 0 \left(mod\ m_1 \right) e\ y_1 \equiv 1 \left(mod\ m_1 \right)$$

Since:

$$y_i \cdot a_i \equiv 0 \left(mod\ m_1 \right),\ i \neq 1$$

Since $y_1 \equiv 1 \left(mod\ m_1 \right)$ this implies that $y_1 \cdot a_1 \equiv a_1 \left(mod\ m_1 \right)$ using the congruence property, we have:

$$x = y_1 a_1 + y_2 a_2 + \ldots + y_r a_r \equiv a_1 \left(mod\ m_1 \right)$$

Which shows that x it satisfies the first congruence of the system (I). Proceeding in the same way, we see that it x satisfies the other congruences of the given system.

To find the values of the numbers $y_i's$, let's make the $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$ product. Since $mdc\left(m_1, \frac{m}{m_1}\right) = 1$ the , by the identity of Bezout, $s_1, t_1 \in \mathbb{Z}$ there are such that:

$$1 = s_1 \cdot m_1 + t_1 \cdot \left(\frac{m}{m_1}\right)$$

It follows that:

$$1 - t_1 \cdot \left(\frac{m}{m_1}\right) = s_1 \cdot m_1$$

And then:

$$t_1 \cdot \left(\frac{m}{m_1}\right) \equiv 1 \left(mod\ m_1\right)$$

How $m_2, \ldots, m_r\ são\ divisores\ de \left(\frac{m}{m_1}\right) = m_2 \cdot m_3 \cdot \ldots \cdot m_r$ then:

$$\frac{m}{m_1} \equiv 0\left(mod\ m_2\right), \frac{m}{m_1} \equiv 0\left(mod\ m_3\right), \ldots, \frac{m}{m_1} \equiv 0\left(mod\ m_r\right)$$

Therefore, we can take $y_1 = t_1\left(\frac{m}{m_1}\right)$. The same reasoning employed guarantees the

$$y_i = t \cdot \left(\frac{M}{m_i}\right)$$

existence of all $y_i's$ that will be equal to . Note that *M* = *m*.

$$x = y_1 a_1 + y_2 a_2 + \ldots + y_r a_r = t_1\left(\frac{M}{m_1}\right) a_1 + t_2\left(\frac{M}{m_2}\right) a_2 + \ldots + t_r\left(\frac{M}{m_r}\right) a_r$$

Soon:

It is a solution to the given congruence system.

To prove the uniqueness modulo *M*, suppose that there is another number $c \in \mathbb{Z}$, which is also the solution of the given system. By the property of congruence we have that, for all *i = 1, 2, ..., r*;

$$x \equiv c \left(mod\ m_1 \right)$$

As *m1, m2, ..., m_r*, are divisors of *M = m1m2... m_r* e are prime to each other, two by two, then, by the definition of congruence *m1 | X – C, M2 | x – c, ..., e m_r | X – C.* , by the property of primes among themselves, it follows that *M = m1m2... m_r | x – c* and therefore

$$x \equiv c\ (mod\ M)$$

as we wanted to demonstrate.

THE C LANGUAGE AS A TOOL

According to Schildt (1996), the C language was born intrinsically linked to the development of the UNIX operating system, being created by Dennis Ritchie in Bell laboratories. As the author explains, "C is the result of the evolution of two previous languages: the B language (created by Ken Thompson) and the BCPL (created by Martin Richards)" (SCHILDT, 1996, p.3).

The history of the C language is deeply connected with ANSI (*American National Standards Institute*) standardization. As Schildt (1996) points out, the establishment of this standard was crucial to ensure the portability and compatibility of codes between different platforms. This aspect is particularly relevant for implementations of complex mathematical algorithms such as the Chinese Remainder Theorem.

"C is a general-purpose programming language that offers economy of expression, flow control and modern data structures, and a rich set of operators" (SCHILDT, 1996, p.4). These characteristics make C an appropriate choice for the implementation of the Chinese Remainder Theorem algorithm, especially due to:

1. Efficiency in memory manipulation;
2. Precise control over mathematical operations;
4. Ability to manage dynamic data structures;
5. Optimized performance for complex calculations.

The C language, as Schildt (1996) points out, combines high-level programming capability with functionality traditionally associated with *assembly* programming, making it particularly suitable for mathematical implementations that require computational efficiency.

The algorithmic implementation of the Chinese Remnants Theorem can be performed through a modular approach in C language, structured in specific functions that perform the fundamental steps of the theorem. Thus, the Chinese Remnants Theorem can be implemented computationally through an algorithm structured in C language. The choice of this language, according to Schildt (1996), is justified by its efficiency in the treatment of mathematical operations and memory management.

We will continue with an approach to the practical applicability of the Chinese remainder theorem, particularly a computational implementation in C language. This theorem not only presents an intrinsic elegance in its mathematical formulation, but is also a key player in several technological and scientific areas. In RSA cryptography, it is vital for the efficiency of private key calculations, allowing operations with large numbers in a more agile and secure way. In addition, it is present in high-performance computing, facilitating the management of large numbers in computer systems and in the encoding of passwords and verification systems, ensuring security and data integrity.

In number theory, its solutions to calendar and optimization problems further exemplify its usefulness. This versatility makes the Chinese remainder theorem a foundation not only for its theoretical beauty, but also for its practical relevance in modern computing and cryptography contexts.

Proceeding to the methodology, the research was implemented in a full-time school in Fortaleza, focusing on the teaching of Mathematics, in particular, on modular congruence and its applications in everyday life. The methodology adopted a collaborative learning approach, with groups of students working together to build knowledge.

METHODOLOGY

OBJECTIVE

The objective of this research is to describe in detail how the study was conducted, encompassing the pedagogical intervention and the computational implementation of the concepts addressed. In pedagogical terms, the research was applied in a full-time school in Fortaleza, focusing on the teaching of Mathematics, especially on the theme of modular congruence. A collaborative learning approach was used, in which students were organized into heterogeneous groups to facilitate the exchange of knowledge and encourage joint problem solving. The methodology involved practical activities that used everyday examples

– such as checking CPF digits, barcodes and simple encryption situations – to make the concepts more concrete and relevant.

At the same time, the study explored the computational implementation of the Chinese Remnants Theorem using the C language, chosen for its efficiency in memory management, precise control in arithmetic operations, and ability to structure complex algorithms in an optimized way. The implementation involved the validation of necessary conditions (such as the coprimality of the modules and the existence of modular inverses) and the execution of specific functions to solve linear congruence systems. This computational approach not only reinforced the practical application of mathematical concepts, but also formed a direct bridge between theory and practice, demonstrating the usefulness of the theorem in contexts such as cryptography and data processing.

In summary, the study aimed to analyze the impact of collaborative pedagogical intervention on student performance and prove the technical feasibility of applying the Chinese Remnants Theorem through an algorithmic implementation in C, contributing to the improvement of teaching and the demonstration of practical applications in everyday situations.

PEDAGOGICAL INTERVENTION

In this study, the students were organized into heterogeneous groups. This strategy aimed to encourage the exchange of knowledge and promote joint problem solving. Practical activities focused on modular congruence were proposed. Students faced challenges in identifying numerical patterns, applying cryptographic concepts, analyzing calendars, and interpreting business cycles. Practical examples of everyday life, such as the verification of CPF digits and bar codes, were also used to consolidate the content. The teacher played the role of mediator. He proposed questions, stimulated reflection and facilitated discussions among students. Data collection included:

1. The application of diagnostic questionnaires before and after the intervention;
2. The observation of the students' interaction during the resolution of the activities;
3. The analysis of mistakes and successes to identify learning patterns;
4. The systematic recording of students' perceptions about the adopted methodology;

The expected results were:

1. Improved understanding of modular congruence and its applications;
2. The development of logical reasoning and the ability to solve problems collectively;

3. Increased student engagement by recognizing the relevance of content to everyday situations;

COMPUTATIONAL IMPLEMENTATION

The algorithm is based on the resolution of linear congruence systems:

Algorithm Structure

Code in C

```
#include <stdio.h>
#include <stdlib.h>

// Global variable of the product of the modules
int M;

int mdc(int numero1, int numeros2) {
while (numbers2 != 0) {
temporary int = numbers2;
numbers2 = number1 % numbers2;
number1 = temporary;
    }
return numero1;
}

int inverseModular(int a, int m) {
if (mdc(a, m) != 1) {
return -1;
    }
int newT = 0, newR = m;
int oldT = 1, oldR = a;
while (newR != 0) {
int quotient = oldR / newR;
int temp = newR;
newR = oldR - quotient * newR;
oldR = temporary;
temporary 27 = newT;
newT = oldT - quotient * newT;
oldT = temporary;
    }
if (oldT < 0) {
old T += m;
    }
return oldT;
}

int ChineseTheoremOfRemainder(int *remainders, int *modulos, int
numeroDeCongruencias) {
M = 1;
for (int i = 0; i < numberofCongruences; i++) {
M *= modules[i];
    }
int solution = 0;
for (int i = 0; i < numberofCongruences; i++) {
int Mi = M / modulos[i];
int yi = inverseModular(Mi, modulos[i]);
solution += remains[i] * Mi * yi;
    }
return solution %M;
```

```
49 }
50
51 int main() {
52 int numberOfCongruences = 1;
53 char text[] = "ENTER THE NUMBER OF CONGRUENCES IN THE SYSTEM OR
'ZERO' TO EXIT: ";
54 int width = 70;
55 while (CongruenceNumber!= 0) {
56 printf("%*s", width, text);
57 scanf("%d", &numeroDeCongruencias);
58 if (numberofCongruences == 0) {
59 break;
60         }
61 int *remainder = (int *) malloc(numberofCongruences * sizeof(int));
62 int *modules = (int *) malloc(numberofCongruences * sizeof(int));
63 printf("\nEnter the remainders and moduli for each congruence:\n\n");
64 for (int i = 0; i < numberofCongruences; i++) {
65 printf("Congruence %d\n", i + 1);
66 printf("Rest: ");
67 scanf("%d", &remains[i]);
68 printf("Module: ");
69 scanf("%d", &modulos[i]);
70 printf("\n");
71         }
72 int coprimos = 1;
73 for (int i = 0; i < numberofCongruences; i++) {
74 for (int j = i + 1; j < numberofCongruences; j++) {
75 if (mdc(modulos[i], modulos[j]) != 1) {
76 cousins = 0;
77 break;
78                 }
79             }
80 if (!coprimos) {
81 break;
82             }
83         }
84 int solution = ChineseTheoremOfRemainder(remainders, moduli,
numberOfCongruences);
85 if (!coprimos) {
86 printf("The system is not in the condition of the Chinese Remainder
Theorem.\n");
87 } else {
88 printf("The solution of the congruence system is: %d mod %d\n", solution, M);
89 printf("We have a solution of type x = %dk + %d\n", M, solution);
90         }
91 free(remains);
92 free(modules);
93     }
94 system("pause");
95 return 0;
```

Author: William Rodrigues da Silva

The Chinese Remnants Theorem can be implemented computationally through a structured algorithm in C language, as shown above. The choice of this language is justified by its efficiency in memory management, precise control in arithmetic operations and ability to structure complex algorithms in an optimized way.

Implementation steps may include calculating the modular inverse using Euclid's extended algorithm and a main function that calls helper functions. This computational approach reinforces the practical application of mathematical concepts and forms a direct bridge between theory and practice.

ANALYSIS OF THE RESULTS

PEDAGOGICAL INTERVENTION

The main objective of the proposed pedagogical intervention was to promote a more significant learning of modular congruence, combining theory and practice in a collaborative context and good applicability in the real world. As a result, a significant improvement in the understanding of concepts related to modular congruence was observed through the experience of contextualized problem-situations and the active mediation of the teacher.

With the formation of heterogeneous groups, the development of logical reasoning and the ability to solve problems cooperatively was also evidenced, favoring the collective construction of knowledge and the appreciation of the diversity of knowledge among students.

In addition, the use of practical examples from everyday life – such as the analysis of barcodes, check digits and time cycles – provided greater student engagement, as they realize the applicability of mathematical content in real situations.

Finally, based on the collection instruments (questionnaires, observations and reflective records), evidence of progress in learning, greater active participation in activities and a more positive attitude towards Mathematics on the part of students were identified.

COMPUTATIONAL IMPLEMENTATION

The algorithm implemented for the Chinese Remnants Theorem (TCR) was analyzed in terms of computational complexity, considering the main steps of its operation. The main step of the algorithm involves combining the partial solutions to obtain the single solution of the congruence system.

Considering all the steps, the temporal complexity of the algorithm is dominated by the combination of the partial solutions and the calculation of the modular inverses. Therefore, the polynomial complexity, which in general of the algorithm is:

$$O(k \cdot \log m)$$

where k is the number of congruences and m is the largest modulus.

The computational implementation of the algorithm in C language was tested with different datasets, including congruence systems with up to 5 equations. The experimental results confirmed that the temporal complexity follows the predicted theoretical behavior, making the algorithm efficient for practical applications in encryption and data validation.

Analysis of the complexity of the TCR algorithm has demonstrated that its implementation is efficient and scalable, making it a valuable tool for solving problems in cryptography, data validation, and other computational applications. The complexity of $O(k \cdot \log m)$ ensures that the algorithm can handle large congruence systems efficiently, with limited system requirements.

In short, the implementation of the Chinese Theorem of Remnants in C language, although functional, was tested with relatively small data sets (up to 5 congruences). Stress tests or comparative *benchmarks* with other languages or methods were not explored, which limits the evaluation of efficiency in more demanding contexts, such as real cryptography or validation of large databases. However, based on the theory and knowledge of the C language, the algorithm is expected to be efficient and scalable, with stable performance even with a high number of congruences.

DISCUSSION OF THE RESULTS

Although the study of Linear Congruence Systems is not worked on in the classroom in Basic Education, all the theory necessary for its understanding is widely discussed in the final years of Elementary School, which is important to be brought to the classroom beforehand. To consolidate the theoretical content on modular congruence, practical activities focused on the identification of check digits in CPFs and bar codes were implemented, as well as on the analysis of calendars, seeking practical examples of everyday life. In addition to the pedagogical activities, the study explored the computational implementation of the Chinese Theorem of Remnants (TCR), using the C language.

The Chinese Remainder Theorem describes the solutions of certain types of linear congruence systems that can describe numerous interesting problems, piquing a high school student's interest in solving them. In this way, it is possible to mobilize students in works involving reasoning and strategies related to the Chinese Remainder Theorem in solving mathematical problems involving congruences, as well as the identification of this theorem with certain patterns of specific problems.

Since, according to Ausbel (1980, p 623), **Meaningful Learning** is a process in which new information is connected to previous knowledge in a non-arbitrary and substantive way, it promotes the construction of a deeper and more lasting meaning, so that

the student not only memorizes, but understands and applies mathematical concepts in relevant contexts, personalizing learning.

In general, it can be seen that the students, at the end of the work, were able to use the Chinese Remainder Theorem as a tool for solving problems involving division with remainders, including making us hypothesize the study of the Chinese Remainder Theorem. Therefore, they were able to realize that Arithmetic, through Congruence, can greatly help in the solution of exercises involving division and remainders, being important in solving problems such as in Mathematical Olympiads and even in some selection processes of competitions or universities.

CPF CHECK DIGIT

Several numbers in our daily lives involve codes, called identification codes, which usually have control digits whose purpose is to validate an extensive sequence. This is the case of the CPF. The CPF (Cadastro de Pessoas Físicas) in Brazil has 11 digits, the last two being the check digits (DV), which guarantee the authenticity of the number. These digits are calculated using congruence modulo 11.

Taking into account the CPF, the idea, initially, was to talk to the students to see if they know the word algorithm and what they understand about it. In case of doubts, one would work, in terms of illustrating ideas, the algorithms of the four basic operations to explain. Then, it would be important to talk to the students if it was easy or difficult and explain that these algorithms are so used in our lives, that we often don't even realize that there are so many steps to be executed.

Of the 11 digits that make up the CPF, three are called check digits. The 9th digit corresponds to the identification of the state to which the CPF belongs. The 10th digit (called a10) is calculated from the first 9 digits and the 11th digit from the 10 before it.

Table to identify the CPF by State

9th digit	State
0	Rio Grande do Sul
1	Federal District, Goiás, Mato Grosso do Sul and Tocantins
2	Acre, Amapá, Amazonas, Pará, Rondônia and Roraima
3	Brazil, Brazil, Brazil
4	Alagoas, Paraiba, Pernambuco and Rio Grande do Norte
5	Bahia and Sergipe
6	Minas Gerais
7	Espírito Santo and Rio de Janeiro
8	São Paulo
9	Paraná and Santa Catarina

Source <http://scpc.tpc.inf.br/scpc/help/estadocpf.htm> accessed 10 March 2005

To get the first DV (a10):

1. The first nine digits are multiplied by the numbers 1 to 9, from left to right.
2. The products obtained are added.
3. The result of this sum, modulo 11, determines the value of a10.

For the second DV (a11):

1. The process is repeated, now with the first ten digits (includes a10) multiplied from 0 to 9.
2. The sum of the products, modulo 11, determines the value of a11.

In the example given (CPF: 002007571), the calculations result in the check digits 5 and 6, forming the complete CPF: 002.007.571-56.

CONCLUSION

In this work, modular congruence was explored as an application of Euclidean Division and divisibility, and its support in problem solving. Thus, we explore modular congruence as an application of Euclidean division and divisibility and the support in problem solving. There was also the intention to show the student that, in a way, the original essence of the content was sought, presenting it as a concrete and significant instrument for the teaching-learning process. This is because, on the one hand, we had the relevance of the subject and, on the other hand, the failure of many students, especially in the high school environment, especially in external activities and evaluations applied within the scope of the dissertation "Modular congruences: the applicability of Number Theory in

supporting problem solving". There was the intention of showing the student the essence of the content from its origin as a real instrument for teaching-learning.

The study investigated the applicability of modular congruences and the Chinese Remnants Theorem in the teaching of Mathematics at the high school level, as well as its computational implementation in C language. as well as for the resolution of practical problems. The literature review allowed us to identify the presence of modular arithmetic in contemporary identification and coding systems, such as barcodes and CPF, reinforcing the need to address these topics in teaching.

Analysis of the Chinese Remnants Theorem has demonstrated its versatility and importance in several fields, including Modern Cryptography (as the basis for RSA) and real-world applications. The literature review allowed us to identify the presence of modular arithmetic in contemporary identification and coding systems, such as barcodes and CPF, reinforcing the need to address these topics in teaching. It is concluded that it is necessary to apply innovative pedagogical intervention projects in schools. The study contributed to a better understanding of TCR and its applications, hoping to have sparked interest in future research.

REFERENCES

1. Ausubel, D. P., Novak, J. D., & Hanesian, H. (1980). *Educational psychology* (2nd ed.). Rio de Janeiro: Interamericana.

2. Bezerra, M. N. C., et al. (2018). *Number theory: An introductory course*. [S.l.]: Editora Universitária AEDI da UFPA-EditAedi.

3. Brazil. Ministry of Education. (2017). *National Common Curricular Base*. [S.l.]: MEC/CONSED/UNDIME.

4. Boyer, C. B. (1996). *História da matemática* (2nd ed.). São Paulo: Edgard Blücher.

5. Carvalho, A. L., Rodrigues, D. V. M., & Araujo, L. H. R. (2015). Applications of modular arithmetic in cryptography. *Caderno de Exatas*. Retrieved March 4, 2025, from https://periodicos.set.edu.br/index.php/cadernoexatas/article/view/2157

6. Ding, C., Pei, D., & Salomaa, A. (1996). *Chinese Remainder Theorem: Applications in computing, coding, cryptography*. *World Scientific, 1*(1), 16. Singapore: World Scientific.

7. Esquinca, J. C. P. [n.d.]. Arithmetic: Bar codes and other applications of congruences. Retrieved March 4, 2025, from https://posgraduacao.ufms.br/portal/trabalho-arquivos/download/1131

8. Eves, H. (2004). *Introduction to the history of mathematics*. São Paulo: Unicamp.

9. Hefez, A. (2011). *Elementos de aritmética* (2nd ed.). Rio de Janeiro: SBM.

10. Lopes, J. V., & Ávila, J. A. J. [n.d.]. Limitation of any prime factor of an odd perfect number. Retrieved March 8, 2025, from https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=39&id2=50131

11. Mol, R. S. (2013). *Introduction to the history of mathematics*. Belo Horizonte: CAEDUFMG.

12. Muniz Neto, A. C. (2022). *Topics in elementary mathematics: Number theory* (3rd ed., Vol. 5). Rio de Janeiro: SBM.

13. Oliveira, M. C. (2013). *Arithmetic: Cryptography and other applications of congruences* [Master's dissertation, Federal University of Mato Grosso do Sul]. Repositorio UFMS. Retrieved March 8, 2025, from https://repositorio.ufms.br/bitstream/123456789/2160/1/MAYKON%20COSTA%20DE%20OLIVEIRA.pdf

14. Pantano Filho, R., Oliveira, K. C., & Parente, L. K. (Eds.). (2025). *Themes in education, mathematics and natural science*. *FoxTablet, 1*(1), 147–168. Salto: FoxTablet.

15. Picado, J. [n.d.]. The algebra of identification systems: From modular arithmetic to dihedral groups. Retrieved March 8, 2025, from http://www.mat.uc.pt/~picado/SistIdent/isbn2.pdf

16. Sá, I. P. [n.d.]. Arithmetic modular and some of its applications. Retrieved March 10, 2025, from https://www.academia.edu/36388352/ARITM%C3%89TICA_MODULAR_E_ALGUMAS_DE_SUAS_APLICA%C3%87%C3%95ES

17. Sant'Anna, I. K. [n.d.]. Modular arithmetic as a tool for the final grades of elementary school. Retrieved March 10, 2025, from https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=137&id2=43601

18. Schildt, H. (1996). *C completo e total* (3rd ed.). São Paulo: Makron Books.

19. Silva, F. J. S. [n.d.]. Modular congruences: The applicability of number theory in support of problem solving. Retrieved March 15, 2025, from https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=7163&id2=171056198