IMPACTO CIENTÍFICO EDITORA

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

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

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
Especializando em Tecnologias e Sistemas de Informação
Universidade Federal do ABC - UFABC
E-mail: rodrigues.william@ufabc.edu.br
Lattes: https://lattes.cnpq.br/2655746793690223
Orcid: https://orcid.org/0009-0005-2818-466X

Walter Martins Rodrigues
Pós-Doutorado
Universidade de São Paulo - IME - USP
E-mail: walterm@ufersa.edu.br
Lattes: http://lattes.cnpq.br/9658022121769752
Orcid: https://orcid.org/0000-0003-1486-8858

José Eduardo Colle
Mestre em Matemática
Universidade Federal do ABC - UFABC
E-mail: jecolle@gmail.com
Lattes: http://lattes.cnpq.br/4605460790587476
Orcid: https://orcid.org/0009-0009-8883-3536

Francisco José de Souza Silva
Mestre em Matemática
Universidade Federal do Semiárido - UFERSA
E-mail: souzasilvafranciscojose@gmail.com
Lattes: http://lattes.cnpq.br/3265950374549215
Orcid: https://orcid.org/0009-0002-0400-962X

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.

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 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.

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.

1 INTRODUÇÃO

A Teoria dos Números desenvolveu-se a partir de necessidades práticas de contagem e medição ao longo da história. Esta área da Matemática ganhou reconhecimento através das contribuições de diversos matemáticos e suas aplicações práticas.

O presente trabalho apresenta, com efeito, um panorama histórico da Teoria dos Números, abordando seus fundamentos teóricos principais, com ênfase nas congruências modulares. Essas são a base do Teorema Chinês dos Restos e fundamentais para a resolução de problemas matemáticos. Nesse contexto, busca-se investigar a aplicabilidade das congruências modulares e do Teorema Chinês dos Restos no ensino da matemática no nível médio.

Conforme aponta Boyer (1996, p. 104), "a evolução da Teoria dos Números acompanhou as necessidades práticas das sociedades ao longo da história". Logo, a pesquisa surge da observação da dificuldade dos estudantes em compreender conceitos abstratos da teoria dos números e da necessidade de estabelecer conexões mais significativas entre o conteúdo matemático e suas aplicações cotidianas. Como complemento à fundamentação central desta pesquisa, adiciona-se, portanto, o aspecto da matéria contribuir para a simplificação e assimilação do estudante sobre múltiplos conceitos.

Para se considerar tal efeito no ensino, foram conduzidas e apresentadas experiências desenvolvidas com discentes do Ensino Médio em uma Escola de Tempo Integral de Fortaleza, que ocupa posição destacada nos indicadores educacionais da Rede Estadual de Ensino do Ceará.

Com esta intervenção, buscou-se enriquecer, entre outros elementos da Base Nacional Comum Curricular (BNCC), precisamente o conteúdo proposto, procurando evidenciar a relevância de compreender a aplicabilidade da teoria dos números. Isso se torna pertinente, principalmente, ao destacar as congruências modulares no ambiente escolar atual em um contexto pós-pandêmico, em que as instituições de ensino articulam a recuperação do aprendizado.

O propósito central deste estudo é, por conseguinte, explorar as aplicações mais relevantes da aritmética modular em sistemas de identificação e codificação contemporâneos, seguindo os objetivos específicos, a saber:

1. Desenvolver uma implementação computacional eficiente do Teorema Chinês dos Restos em linguagem C, visando aplicações práticas em sistemas de criptografia e validação de dados;
2. Analisar quantitativamente o impacto da aplicação de congruências modulares no ensino médio através de intervenções pedagógicas estruturadas em uma escola de Fortaleza-CE;
3. Demonstrar a evolução histórica e os fundamentos teóricos da aritmética modular, estabelecendo conexões com sistemas modernos de identificação (códigos de barras, CPF) e criptografia;

4. Elaborar e validar um conjunto de estratégias pedagógicas para o ensino de aritmética modular, com foco em aplicações práticas e mensuração de resultados através de avaliações comparativas;
5. Documentar e analisar pelo menos três casos de aplicação bem-sucedida do Teorema Chinês dos Restos em problemas computacionais contemporâneos;

Sendo assim, a pesquisa justifica-se pelo esforço de esclarecer a importância das aplicações da aritmética modular e do teorema chinês dos restos para a sociedade, além de destacar a presença da matemática em situações cotidianas. Sobretudo, o avanço de estudos nesse campo pode, oportunamente, despertar o interesse em aprimorar as práticas pedagógicas no ensino da aritmética na educação básica, favorecendo um ambiente propício ao aprendizado matemático. Visa-se, consequentemente, contribuir e fortalecer investigações na área computacional, ampliando o impacto das aplicações dessa teoria em soluções tecnológicas e científicas.

2 REFERENCIAL TEÓRICO

2.1 EVOLUÇÃO HISTÓRICA DAS CONGRUÊNCIAS MODULARES

Ao longo dos séculos, várias contribuições foram deixadas por diversos pesquisadores para o enriquecer dos saberes matemáticos. Por isso, vale ressaltar o termo "saberes matemáticos", uma vez que esta ciência abrange múltiplos campos de estudo e diversas metodologias para alcançar conclusões semelhantes, permitindo sua pluralização enquanto área do conhecimento que fascina os estudiosos desde a antiguidade. Naturalmente, as descobertas e refinamentos ocorreram conforme novas perspectivas foram adotadas sobre esta disciplina, processo que continua em evolução na contemporaneidade e seguirá nas épocas vindouras.

A teoria dos números, por sua vez, cuja aritmética constitui componente fundamental, representa o segmento da matemática dedicado ao estudo da estrutura numérica e das operações possíveis entre seus elementos. Por isso, está presente no cotidiano de toda a sociedade, manifestando-se em atividades como contagens, cálculos monetários, mensurações e análises de relações entre grandezas. A aritmética está entre os ramos mais primitivos da matemática, visto que as operações elementares são executadas desde os primórdios da civilização, embora estudos mais sofisticados, classificados como aritmética superior, tenham emergido apenas nos séculos XVIII e XIX.

O progresso da teoria dos números encontra-se fundamentalmente vinculado aos imperativos práticos do desenvolvimento humano. As concepções matemáticas surgiram espontaneamente durante os esforços para solucionar questões cotidianas, com cada novo obstáculo catalisando o surgimento de metodologias e instrumentos matemáticos inovadores.

No ocaso do século VI, por exemplo, os hindus realizaram uma contribuição essencial, conforme destacam Costa e Santos (2008, p. 11): “Após a criação do zero, cria-se o sistema de posicionamento da base dez, utilizando a casa das unidades, dezenas, centenas e ademais subsequentes, livrando-se, dessa forma, dos problemas gerados pela ausência deste, como, por exemplo, distinguir o número 15 do 105."

A elaboração de uma representação simbólica do vazio representa uma conquista notável do intelecto humano, particularmente no contexto do início da era cristã. Caraca (2003, p. 6) ressalta: “Uma coisa que nem toda a gente repara é que essa numeração constitui uma autêntica maravilha que permite, não só escrever muito simplesmente os números, como também efetuar as operações."

Afinal, a evolução dos sistemas de numeração foi motivada pelas exigências diárias da civilização. Consequentemente, diversos mecanismos de contagem foram concebidos, destacando-se o ábaco. Acerca desse dispositivo, Costa (1996, p.175-178) pondera: “Muito prático, desobrigou o homem do esforço de acumulações, porém, exigiu o conhecimento das combinações resultantes da posição de cada conta. Não é, pois, um instrumento de cálculo, mas, apenas, indica os números adicionados e subtraídos."

Ademais, a construção dos números inteiros derivou da noção primordial dos números naturais, originalmente elaborados para solucionar questões de contagem. Embora os números negativos tenham emergido ocasionalmente desde tempos remotos, enfrentaram considerável ceticismo na comunidade matemática. Somente com o florescimento do comércio europeu, no período final da Idade Média, manifestou-se a demanda concreta pela incorporação dos inteiros relativos e suas operações ao arcabouço matemático.

No que se segue à história da teoria dos números, ainda que o conceito de número inteiro preceda a sistematização dos números naturais, contemplando sua utilização em transações comerciais e outras aplicações cotidianas, sua legitimação formal foi um processo prolongado, como indica Hefez (2016).

Já, na China antiga, o desenvolvimento da teoria dos números teve um momento significativo com o texto matemático "Sun Zi Suanjing" (Manual de Aritmética de Sun Zi). Nesta obra seminal, o matemático Sun Zi apresentou problemas que estabeleceriam as bases para o que viria a se tornar o Teorema Chinês dos Restos. Particularmente o problema apresentado no volume 3, questão 26, que aborda a determinação de números através de seus restos quando divididos por diferentes divisores.

Por outro lado, no século XIII, o matemático Qin Jiushao (1202-1261) deu um passo significativo ao desenvolver uma abordagem geral para a resolução destes tipos de problemas, estabelecendo assim as bases teóricas do que conhecemos hoje como Teorema Chinês dos Restos. Esta contribuição fundamental de Jiushao permitiu transcender os casos particulares, fornecendo um método sistemático para resolver uma classe inteira de problemas similares (DING, 1996, p. 16).

A Aritmética tem sido, portanto, edificada com o auxílio de numerosos teóricos matemáticos, particularmente, desde Euclides, com sua obra *Os Elementos* (aproximadamente 300 a.C.), até atingir seu ápice no século XVII através das investigações conduzidas por Pierre de Fermat, que proporcionaram grandes avanços para o campo.

De início, no período helenístico, Euclides de Alexandria apresentou em sua magistral obra *Os Elementos* (cerca de três séculos antes da era cristã) uma formulação que se assemelhava ao que viria a ser conhecido como teorema fundamental da aritmética. Embora tenha oferecido uma demonstração para tal proposição, foi apenas no século XIX que Carl Friedrich Gauss conseguiu estabelecê-lo com rigor matemático, fornecendo-lhe a notação matemática adequada e elevando-o à condição de teorema, formalização esta que permanece válida e amplamente utilizada na matemática contemporânea (Hefez, 2016, p. III).

Posteriormente, em discussões sobre aritmética modular, é imprescindível mencionar as contribuições de Pierre de Fermat, jurista francês que cultivava a matemática, conforme os autores Boyer e Merzbach (2012, p. 244) pontuam: "Fermat não era de modo algum um matemático profissional", considerando que matemáticos posteriores se dedicaram ao estudo e demonstração formal de suas proposições.

Uma ilustração significativa, apresentada por Mol (2013, p. 98) acerca do Pequeno Teorema de Fermat, estabelece que, se p é primo e a é um número não divisível por p, então $a^{p-1} - 1$ é divisível por p, embora o próprio Fermat não tenha fornecido uma demonstração formal quando o propôs. A comprovação deste teorema foi publicada inicialmente por Leonhard Euler, aproximadamente um século depois.

As descobertas sobre aritmética modular esclarecidas por Fermat atraíram a atenção de outros matemáticos, em particular nos séculos XVIII, com Euler, e XIX, com Lagrange e Legendre, que também se dedicaram ao estudo das elucidações propostas por Gauss. Nos séculos XVIII e XIX, a matemática foi enriquecida pelas pesquisas de Leonhard Euler, Joseph Louis Lagrange, Adrien Marie Legendre, John Wilson e Carl Friedrich Gauss. É significativo mencionar que, a partir do século XIX, após as contribuições de Gauss, a aritmética tornou-se em Teoria dos Números (Hefez, 2016).

A história relata que Gauss demonstrava, desde sua infância, incrível aptidão que o distinguia dos outros estudantes de sua classe. Foi ele o pioneiro na aplicação de um raciocínio relacionado às progressões aritméticas quando, desafiado por seu professor a calcular a soma de todos os números inteiros de 1 a 100, identificou que ao somar 1 + 100 obtinha 101, 2 + 99 também resultava em 101, 3 + 97 também totaliza 101. A partir desta observação, deduziu que poderia multiplicar 101 pela metade de 100, ou seja, 50, que é o total de pares somados para obter a soma de todos os números compreendidos entre 1 e 100, chegando ao resultado 50 a 50, procedimento que hoje conhecemos

como a fórmula da soma dos termos de uma progressão aritmética, $n(n + 1)/2$ (OLIVERO, 2007, p. 110).

Com característica de observador das correlações numéricas, Gauss notou que regularmente utilizavam-se expressões como "(a) fornece o mesmo resto que (b) quando divididos por (m)" (Sa, 2007) e esta constatação o instigou a desenvolver o raciocínio e os fundamentos da aritmética modular. Como tal fenômeno se justifica? Ao verificar que números distintos quando divididos por um mesmo divisor geravam restos idênticos, ele então estabeleceu que tais números são congruentes, isto é, "equivalentes", no contexto da divisibilidade por aquele divisor.

Destaca-se que a terminologia "congruência", neste contexto específico, foi introduzida pioneiramente por Gauss em seu tratado *Disquisitiones Arithmeticae* (Investigações Aritméticas) publicado em 1801. Esta obra é considerada o fundamento inaugural da teoria dos números moderna. "Nela, [Gauss] reuniu as contribuições de seus antecessores e revitalizou o campo, desenvolvendo as teorias de congruências quadráticas, formas e resíduos" (Mol, 2013, p. 125).

Por essa razão, e em virtude de suas notáveis contribuições ao estudo da teoria dos números, Gauss recebeu a alcunha de pai da aritmética modular. Foi através de seu trabalho que se estabeleceu uma notação matemática específica para formalizar as questões pertinentes à congruência modular e outras relações aritméticas. Anos mais tarde, Gauss demonstrou que o Pequeno Teorema de Fermat representa um caso particular de congruência, uma vez que "se a é um número primo e p é um número inteiro qualquer, então p divide $(a^p - a)$", podendo ser expressa utilizando a notação de congruência como $a^p \equiv a \ mod \ p$".

Na seção subsequente, serão explorados detalhadamente os conceitos fundamentais da evolução da teoria dos números. Convém enfatizar que tais noções emergem em consonância com as necessidades contemporâneas, manifestando-se naturalmente durante o processo de resolução de problemas. Ressalta-se que cada necessidade emergente inevitavelmente suscita uma resposta orientada à resolução da questão apresentada.

2.2 ASPECTOS DA TEORIA DOS NÚMEROS PARA RESOLUÇÃO DE PROBLEMAS

Tendo observado a relevância e o desenvolvimento da teoria dos números no tocante às congruências modulares, no capítulo precedente, serão explorados agora os fundamentos matemáticos essenciais, abrangendo temas como divisibilidade e seus atributos, a Divisão Euclidiana, o universo dos Números Primos e teoremas fundamentais como o Pequeno Teorema de Fermat.

Ademais, serão investigados as Congruências Lineares, seus sistemas e aplicações, bem como Equações Diofantinas Lineares. Nossa jornada se estenderá pelos Teoremas de Wilson, Fermat e Euler, culminando com o fascinante Teorema Chinês dos Restos e sua implementação computacional. Esta

sequência de conhecimentos constitui uma base fundamental para a compreensão e resolução dos desafios matemáticos que motivam este trabalho.

A BNCC (BRASIL, 2017) propõe cinco unidades temáticas que se correlacionam entre si, a que se refere a números, por estar ligada diretamente à Teoria Elementar dos Números, tem como finalidade desenvolver o pensamento numérico, que implica o conhecimento de maneiras de quantificar atributos de objetos e de julgar e interpretar argumentos baseados em quantidades.

> [...] Para essa construção, é importante propor, por meio de situações significativas, sucessivas ampliações dos campos numéricos. No estudo desses campos numéricos, devem ser enfatizados registros, usos, significados e operações. (BRASIL, 2017, p. 268)

Vale ressaltar que, além da riqueza técnica destes conceitos, existe um benefício ainda mais significativo: o desenvolvimento do raciocínio lógico e da capacidade analítica. Este processo não apenas facilita a assimilação do conteúdo específico, mas também cultiva habilidades cognitivas que transcendem a matemática. Esta abordagem sistemática do pensamento se manifesta claramente no desempenho excepcional de estudantes que participam de olimpíadas matemáticas, os quais frequentemente demonstram excelência acadêmica em diversas áreas do conhecimento. Tal correlação não é mera casualidade, mas sim resultado direto do desenvolvimento de habilidades analíticas robustas e do domínio efetivo de conceitos matemáticos fundamentais.

A incorporação do estudo de Congruências Lineares, seus sistemas e as Equações Diofantinas Lineares, juntamente com os Teoremas de Wilson, Fermat e Euler, enriquecem ainda mais esta base teórica. Estes tópicos não apenas complementam o entendimento da teoria dos números, mas também oferecem ferramentas poderosas para a resolução de problemas complexos e aplicações práticas na matemática moderna.

2.2.1 Fundamentos de Divisibilidade e Congruência Modular

A teoria da divisibilidade pode ser compreendida através dos seguintes conceitos fundamentais:

1. **Definição Base:**

   Para $a, b \in \mathbb{Z}, a \neq 0$, *dizemos que* $a \mid b$ *se* $\exists\, k \in \mathbb{Z}$ *tal que* $b = ak$

2. **Propriedades Essenciais:**
   - Reflexiva: $a \mid a$
   - Transitiva: Se $a \mid b$ e $b \mid c$, *então* $a \mid c$
   - Linearidade: Se $a \mid b$ *e* $a \mid c$, *então* $a \mid (mb + nc)$, $\forall m, n \in \mathbb{Z}$

3. **Características Fundamentais:**
   - $1 \mid a$ *e* $a \mid 0$, $\forall a \in \mathbb{Z}$

- $Se \quad a \mid b \; com \; b \neq 0, \; então \; |a| \leq |b|$
- $Se \quad b \mid 1 \; então \; b = \pm 1$

Esta estrutura fundamental da divisibilidade naturalmente conduz a um conceito mais amplo e poderoso: a congruência modular. Quando analisamos os restos das divisões por um número fixo, observamos padrões que nos permitem agrupar números com comportamentos similares, levando assim ao conceito de congruência.

A Congruência Modular constitui uma extensão natural da teoria da divisibilidade, estabelecendo uma estrutura matemática que relaciona números que, quando divididos por um mesmo valor (módulo), produzem restos idênticos. Esta relação, formalizada por Gauss, proporciona uma ferramenta poderosa para análise de padrões numéricos e resolução de problemas complexos.

A estrutura formal da congruência modular estabelece-se quando dois números, ao serem divididos por um terceiro (denominado módulo), produzem idênticos restos. Matematicamente, expressa-se como $a \equiv b \; (mod \; m)$, onde $m, a, b \in \mathbb{Z}$, indicando que a e b são congruentes módulo m. A teoria fundamenta-se em propriedades cruciais:

1. Relação de Equivalência:
   - Reflexividade: $a \equiv a \; (mod \; m)$
   - Simetria: *Se* $a \equiv b \; (mod \; m)$, *então* $b \equiv a \; (mod \; m)$
   - Transitividade: *Se* $a \equiv b \; (mod \; m)$ *e* $b \equiv c \; (mod \; m)$, *então* $a \equiv c \; (mod \; m)$

2. Propriedades Operatórias:
   - Adição: *Se* $a \equiv b \; (mod \; m)$ *e* $c \equiv d \; (mod \; m)$, *então* $a + c \equiv b + d \; (mod \; m)$
   - Multiplicação: *Se* $a \equiv b \; mod(m)$ *e* $c \equiv d \; (mod \; m)$, *então* $ac \equiv bd \; (mod \; m)$
   - Potenciação: *Se* $a \equiv b \; (mod \; m)$, *então* $a^n \equiv b^n \; (mod \; m)$

Esta estrutura matemática estabelece fundamentos essenciais para diversos campos da matemática aplicada, incluindo criptografia, teoria dos códigos e sistemas de verificação de dados, demonstrando sua relevância tanto teórica quanto prática na matemática contemporânea.

A intersecção entre divisibilidade e congruência modular estabelece um paradigma matemático de significativa relevância prática. Como destaca Sant'Anna (2013), o ensino tradicional frequentemente reduz estes conceitos a regras mnemônicas, negligenciando o desenvolvimento do pensamento analítico. Esta abordagem limita a compreensão das estruturas matemáticas que fundamentam diversos sistemas de verificação e validação contemporâneos.

O arcabouço teórico-matemático da congruência modular, fundamentado na teoria dos números, estabelece uma estrutura algébrica que relaciona elementos numéricos que, quando divididos

por um mesmo módulo, produzem restos idênticos. Esta relação de equivalência, formalizada inicialmente por Gauss em seu tratado *Disquisitiones Arithmeticae*, constitui um sistema matemático que estrutura diversas aplicações práticas na atualidade.

A formulação matemática rigorosa deste conceito pode ser expressa como uma relação de equivalência em $\mathbb{Z}$, onde dois números a e b são considerados congruentes módulo m (denotado por $a \equiv b \ mod \ m$) se, e somente se, m divide a diferença (a - b). Esta definição fundamental gera uma partição do conjunto dos números inteiros em classes de equivalência, proporcionando uma estrutura algébrica rica em propriedades e aplicações.

Esse arcabouço teórico da congruência modular, caracterizado pela relação entre números que compartilham o mesmo resto quando divididos por um módulo comum, transcende sua definição formal para oferecer aplicações práticas substanciais, incluindo:

1. Sistemas de Verificação:
   - Códigos de barras;
   - *International Standard Book Number* (ISBN);
   - Cadastro de Pessoas Físicas (CPF);
   - Validação de documentos digitais;

2. Critérios de Divisibilidade: De acordo com Muniz Neto (2022), a abordagem através da congruência modular oferece uma perspectiva mais profunda e estruturada. Para um módulo m, estabelece-se uma expressão em termos dos dígitos $a_n, a_{n-1}, a_{n-2}, ..., {}^{a}{}_{1}, a_o$, determinando um polinômio congruente módulo m.

   Esta abordagem analítica permite:
   - Desenvolvimento do pensamento lógico-dedutivo;
   - Compreensão das propriedades fundamentais;
   - Capacidade de generalização para novos critérios;

A aplicação destas propriedades simplifica significativamente cálculos complexos, particularmente na aritmética dos restos. Por exemplo, para determinar o resto da divisão de números elevados a grandes potências, como 2545 por 11, utilizam-se as propriedades de congruência em conjunto com o Pequeno Teorema de Fermat, reduzindo substancialmente a complexidade computacional.

Esta metodologia não apenas facilita a aplicação prática dos conceitos, mas também promove o desenvolvimento do raciocínio matemático estruturado, estabelecendo conexões significativas entre teoria e aplicações contemporâneas, particularmente em sistemas de segurança e verificação de dados.

Esta perspectiva unificada sobre divisibilidade e congruência modular demonstra como conceitos matemáticos fundamentais sustentam tecnologias essenciais da era digital, enfatizando sua relevância prática e pedagógica no contexto educacional atual.

2.2.2 Divisão Euclidiana

A divisão euclidiana é um conceito fundamental da aritmética que estabelece:

Definição: Dados dois inteiros a (dividendo) e $b \neq 0$ (divisor), existem únicos inteiros q (quociente) e r (resto) tais que:

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

Demonstração: A prova pode ser reduzida ao caso $a \geq 0 \; e \; b > 0$ através das seguintes transformações:

1. *Para* $b < 0$ *: Definindo* $b_1 = -b \; e \; q_1 = -q$
2. $$a = bq + r \Rightarrow a = b_1 q_1 + r_1$$
3. *Para* $a < 0 \; e \; b > 0$*: Definindo* $a_1 = -a, \; q_1 = -q - 1 \; e \; r_1 = b - r$

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

4. *Para* $a \geq 0 \; e \; b > 0$*: Por construção iterativa*

Inicialmente: $q_1 = 0, \; r_1 = a$

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

Esta divisão é fundamental para:

- Algoritmo euclidiano do MDC;
- Aritmética modular;
- Computação (operação módulo);

A divisão euclidiana, além de sua importância fundamental na aritmética básica, fornece o alicerce para um dos conceitos mais importantes da teoria dos números: o Máximo Divisor Comum (MDC). O algoritmo para encontrar o MDC, como veremos a seguir, baseia-se diretamente no processo de divisões sucessivas que acabamos de estudar.

2.2.3 Máximo Divisor Comum (MDC)

Definição 1: *Dados* $a, \; b \in \mathbb{Z}$, *ambos não 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* $e \mid d$

Propriedade Fundamental: *Se* $a = bq + r$, *então* $mdc(a, b) = mdc(b, r)$

Definição de Bezout: Dados $a, b \in \mathbb{Z}$, não ambos nulos, existem $m, n \in \mathbb{Z}$ tais que:

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

Para calcular $mdc(680, 150)$:

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

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

O algoritmo de Euclides fornece um método eficiente para calcular o MDC através de divisões sucessivas até obter resto zero, sendo o último divisor não nulo o MDC procurado. Este método, conforme descrito por Hefez (*apud* FRANCO, 2016 pp.16-19), mantém-se essencialmente o mesmo desde sua apresentação em *Os Elementos*, de Euclides, tendo recebido apenas aperfeiçoamentos em sua implementação.

O Teorema de Bezout complementa este algoritmo ao estabelecer que o MDC pode ser expresso como combinação linear dos números originais, fornecendo assim uma ponte fundamental entre a divisibilidade e as equações diofantinas lineares. Como exemplificado anteriormente:

Em Bezout: Para $a = 41$ *e* $b = 12$:

$$41 = 12 \cdot 3 + 5 \quad \Rightarrow 5 = 41 - 12 \cdot 3$$
$$12 = 5 \cdot 2 + 2 \quad \Rightarrow 2 = 12 - 5 \cdot 2$$
$$5 = 2 \cdot 2 + 1 \quad \Rightarrow 1 = 5 - 2 \cdot 2$$

Substituindo recursivamente, obtemos o MDC como combinação linear de a *e* b.

2.2.4 Números Primos

Definição 2: Um número natural maior que 1 é chamado primo se possui apenas dois divisores positivos: 1 e ele mesmo. Caso contrário, é denominado composto. (MUNIZ NETO, 2022, p. 29):

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

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

Proposição 1: *Sejam n, a, b, p ∈ ℤ, com p primo. Se p | ab, então p | a ou p | b.*

Teorema Fundamental da Aritmética: Todo número natural maior que 1 ou é primo ou pode ser escrito de modo único (a menos da ordem dos fatores) como produto de números primos.

Infinitude dos Primos: Existem infinitos números primos.

Demonstração: Por absurdo, suponha que existam finitos primos $p_1, \cdots, p_r$. Considere $n = p_1 \cdots p_r + 1$. Pelo Teorema Fundamental da Aritmética, n possui um fator primo p que divide $p_1 \cdots p_r$. Logo, $p \mid 1$, absurdo.

Se $n > 1$ não é divisível por nenhum primo p tal que $p^2 \leq n$, então n é primo.

Para verificar se 353 é primo, basta testar divisibilidade por primos p até $\sqrt{353} \approx 19$:

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

Como não é divisível por nenhum deles, 353 é primo.

2.2.5 Crivo de Eratóstenes e os Números Primos

Definição 3: Um número natural é primo quando possui exatamente dois divisores positivos: 1 e ele próprio.

Os números primos, estudados há mais de 2000 anos, são fundamentais na Teoria dos Números e têm aplicações prática significativas. O Crivo de Erastóstenes surgiu como um método eficiente para identificar números primos, especialmente os de maior magnitude.

Crivo de Eratóstenes: Dado $x \geq 2$, para garantir que x é primo, basta mostrar que nenhum número primo $p \leq \sqrt{x}$ divide x.

Propriedades importantes:

1. 2 é o único primo par.
2. 0 e 1 não são primos.
3. Para testar a primalidade de n, basta verificar divisores até $\sqrt{n}$.

Crivo de Eratóstenes até 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

Fonte: Elaborado pelos autores.

Para encontrar todos os números primos até n:

1. Liste todos os números de 1 a n;
2. Elimine os múltiplos de 2 (exceto 2);
3. Elimine os múltiplos de 3 (exceto 3);
4. Considere o processo para cada primo $p \leq \sqrt{n}$;

2.2.6 O Pequeno Teorema de Fermat

Pierre de Fermat (1601-1665) destacou-se na história da matemática por ser conhecido como "Príncipe dos Amadores". Graduado em Direito pela Universidade de Toulouse, na França, construiu uma carreira jurídica sólida, servindo inicialmente como advogado e posteriormente como conselheiro no parlamento local. Sua paixão pela matemática, cultivada nas horas vagas, resultou em contribuições extraordinárias que o colocaram entre os maiores matemáticos de sua época (BOYER, 2003).

O Pequeno Teorema de Fermat emerge como uma de suas descobertas mais significativas, revolucionando a teoria dos números. Este teorema fundamental estabelece que: dado um número primo p, p divide $a^p - a$, para todo a pertencente ao conjunto dos números inteiros ($\mathbb{Z}$). Esta proposição tornou-se a pedra fundamental dos Testes de Primalidade contemporâneos, inspirando numerosas variações e generalizações.

A demonstração do teorema segue uma elegante estrutura bifurcada. Para o caso específico, em que $p = 2$, a prova é direta e evidente. Para números primos ímpares, emprega-se o método de indução matemática sobre a, iniciando com o caso base $a = 0$. A prova se completa através da aplicação do Binômio de Newton, estabelecendo a validade universal do teorema para todo número primo p e qualquer elemento a do conjunto dos números reais.

Corolário: se p é um número primo e a é um número natural não divisível por p, então p divide $a^{p-1} - 1$.

Este resultado derivado não é um caso particular, mas uma ferramenta poderosa com aplicações práticas extensivas em diversos campos da matemática, incluindo critérios de divisibilidade, potenciação em congruências modulares e, sobretudo, na criptografia moderna avançada.

A relevância histórica e prática do Pequeno Teorema de Fermat transcende seu tempo, estabelecendo fundamentos relevantes para desenvolvimentos matemáticos posteriores e aplicações tecnológicas contemporâneas. Sua simplicidade elegante mascara uma profundidade conceitual que continua influenciando a matemática moderna e suas aplicações práticas.

2.2.7 Equações Diofantinas Lineares

As Equações Diofantinas Lineares (EDL) constituem uma aplicação matemática sofisticada do conceito de divisibilidade. Para ilustrar sua aplicação prática, considere-se um problema: uma corporação militar adquiriu veículos, totalizando 152 pneus, distribuídos entre motocicletas (2 pneus cada) e automóveis (4 pneus cada). O objetivo é determinar todas as combinações possíveis de veículos.

Formalmente, uma EDL é definida como $ax + by = c$, onde a, b, c $\in \mathbb{Z}$ e x, y são incógnitas em $\mathbb{Z}$. Esta estrutura matemática homenageia Diofante de Alexandria (século III d.C.), pioneiro na teoria dos números.

Aspectos fundamentais:

1. Condição de Existência:
   - *Uma EDL possui soluções se e somente se mdc (a, b) | c*
   - ***Demonstração:*** *Se* $ax_0 + by_0 = c$, *então para* $d = mdc(a, b) : a = dm,\ b = dn\ (m, n \in \mathbb{Z})$

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

2. Para uma solução particular:

$$r(x_0, y_0) : x = x_0 + (b/d)\,t\ y = y_0 - (a/d)\,t \text{ onde } t \in \mathbb{Z} \text{ e } d = mdc(a, b)$$

3. Métodos de Resolução:

   Para casos simples (3x + 6y = 18):

   - Por inspeção: (4,1), (-6,6), (10,-2)
   - Verificação direta da condição *mdc*(3,6) = 3 | 18

   Para casos complexos (172*x* + 20*y* = 1000):

   - Algoritmo de Euclides para *mdc*:

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

Portanto, o *mdc* (172, 20) = 4 e como 4 |1000, segue-se que a equação dada tem solução.

- Combinação linear retroativa:

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

Logo temos a equação: $4 = 172 \cdot 2 - 20 \cdot 17$.

- Solução particular:

Como se quer uma solução para a combinação que resulta 1000, multiplique-se ambos os membros desta igualdade por 1000/4 = 250 e obtém-se:

$$1000 \quad 72 \cdot 500 + 20(-4250)$$

Logo, o conjunto ordenado (500, -4250) representa uma solução específica para a equação estabelecida. O conjunto completo de soluções pode ser expresso através das expressões algébricas: $x = 500 + 5t$ $y = -4250 - 43t$, em que t percorre todos os números inteiros chegando à fórmula geral: $x = 500 + 5t$ $y = -4250 - 43t$ ($t \in \mathbb{Z}$)

4. Propriedades Avançadas:
   - O conjunto de soluções forma uma progressão aritmética bidimensional;
   - A distância entre soluções consecutivas é determinada pelos coeficientes normalizados pelo *mdc*;
   - A unicidade da solução ocorre se e somente se $|a| = |b| = 1$;

Esta formulação matemática rigorosa das EDL proporciona uma abordagem robusta para resolver problemas que exigem soluções inteiras, com aplicações em otimização discreta, teoria dos números e problemas práticos de contagem e distribuição.

Enquanto as Equações Diofantinas nos fornecem ferramentas para trabalhar com equações lineares no domínio dos inteiros, o Teorema de Wilson nos apresenta uma perspectiva diferente, mas

complementar sobre as propriedades dos números primos, expandindo a compreensão das estruturas fundamentais da teoria dos números.

2.2.8 Teorema de Wilson

O Teorema de Wilson constitui uma ferramenta matemática expressiva que estabelece uma conexão profunda entre números primos e congruências modulares (MUNIZ NETO, 2022, pp. 129-130). Este teorema apresenta uma condição necessária e suficiente para a primalidade: um número natural p é primo se, e somente se, $(p-1)! \equiv -1 \ (mod\ p)$.

No contexto das congruências lineares, emerge naturalmente uma extensão através de sistemas de congruências. O Teorema Chinês dos Restos (TCR) investiga a existência e unicidade de soluções para estes sistemas, estabelecendo condições precisas para sua resolubilidade.

A demonstração do Teorema de Wilson fundamenta-se em uma função bijetora f: $\{1, 2, ..., p-1\} \rightarrow \{1, 2, ..., p-1\}$, que mapeia cada elemento a seu inverso modular. A prova revela que para um número primo p, apenas 1 e $p-1$ são seus próprios inversos módulo p, enquanto os demais elementos formam pares distintos (a, a^{-1}) cujo produto é congruente a 1 módulo p.

A relação entre o Teorema de Wilson e o TCR manifesta-se em três níveis fundamentais:

1. Estrutural: O Teorema de Wilson demonstra a existência de uma estrutura multiplicativa única em campos finitos primos, propriedade essencial para o TCR;
2. Operacional: Os inversos modulares, fundamentais para a demonstração do Teorema de Wilson, são cruciais para a construção das soluções no TCR, particularmente na fase de combinação das soluções parciais;
3. Computacional: A verificação da primalidade via Teorema de Wilson garante a coprimalidade dos módulos no TCR, condição necessária para sua aplicabilidade;

A conexão com o TCR manifesta-se principalmente na caracterização dos inversos modulares, elemento crucial para a resolução de sistemas de congruências. Como destaca Muniz Neto (2022, p. 129), esta relação fornece um critério elegante para verificação de primalidade e aprofunda a compreensão das propriedades dos inversos modulares.

O teorema demonstra que em um sistema módulo p primo, todo elemento não nulo possui exatamente um inverso multiplicativo, propriedade essencial para a aplicabilidade do TCR. Esta característica fundamenta a resolução de sistemas de congruências lineares e suas aplicações em teoria dos números e criptografia.

Exemplo prático:

Para $p = 7$:
$6! = 720 \equiv -1 \ (mod\ 7)$

Verificação: $720 = 102 \times 7 + 6$
$6 \equiv -1 \ (mod\ 7)$

Confirma que 7 é primo.

A elegância e poder do Teorema de Wilson na verificação de primalidade abre caminho para uma das ferramentas mais versáteis da teoria dos números: o Teorema Chinês dos Restos. Enquanto o Teorema de Wilson nos fornece um critério preciso para identificar números primos através de congruências, o TCR nos permite solucionar sistemas inteiros de congruências simultâneas. Esta progressão é natural: após compreendermos como trabalhar com congruências em relação a um único módulo primo (como no Teorema de Wilson), o próximo passo lógico é explorar como lidar com múltiplos módulos simultaneamente.

A transição entre estes teoremas não é apenas sequencial, mas fundamentalmente conectada. O Teorema de Wilson nos garante a existência de estruturas específicas em campos finitos primos e esta garantia torna-se crucial para entender por que e como o TCR funciona. De fato, a verificação de primalidade e a compreensão dos inversos modulares que o Teorema de Wilson nos proporciona são frequentemente utilizadas na aplicação prática do TCR, especialmente quando precisamos garantir a coprimalidade dos módulos - uma condição essencial para a aplicabilidade do TCR.

2.4 O TEOREMA CHINÊS DOS RESTOS

O Teorema Chinês dos restos está associado a certos sistemas de congruências lineares, nesse sentido, de acordo com Eves:

> O mais importante dos textos de Matemática chineses antigos é o K'ui-ch'ang Suanshu, ou Nove Capítulos sobre a Arte da Matemática, que data o período Han (206 a.C., -221d.C.) mas que muito provavelmente contém material bem mais antigo. É uma síntese do conhecimento matemático chinês antigo. Em seus 9 capítulos, o de relevância para o presente trabalho encontra-se no capítulo 8 que fala sobre Sistema de equações Lineares. (EVES, 2011, p.242)

Um Sistema de Congruências Lineares, por conseguinte, é quando temos várias equações de congruências, na qual desejamos obter uma solução que satisfaça simultaneamente estas equações. Assim, deve-se analisar se os critérios para identificar se um Sistema de Congruências Lineares admite ou não solução. Uma estratégia é dividir em casos, são eles: 1º caso, uma das congruências não admite solução, logo o sistema não admite solução; 2º caso, as congruências admitem solução, mas o sistema não admite solução; 3º caso, as congruências admitem solução e o sistema também admite solução.

De acordo com Bezerra (2018, p.149), pode-se enunciar o Teorema Chinês dos Restos da seguinte forma: considere os inteiros $m_1, m_2, \ldots, m_k$ dois a dois primos entre si, então o Sistema de congruências lineares:

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

admite uma solução, que é única módulo $m = m_1 . m_2 . \dots . m_k$.

2.4.1 Aspectos Históricos e Motivadores

O Teorema Chinês dos Restos (TCR) é um resultado fundamental da Teoria dos Números que fornece um método sistemático para resolver sistemas de congruências lineares, como visto. Este teorema tem importantes aplicações tanto na matemática teórica quanto em áreas práticas da computação moderna, como criptografia. Como poderemos observar em sua implementação computacional em linguagem C, o algoritmo permite determinar soluções únicas para sistemas de congruências através de um elegante processo que envolve a manipulação de restos e a divisibilidade. O TCR é particularmente relevante quando tratamos de congruências modulares e suas aplicações, pois oferece um método sistemático para resolver problemas que envolvem múltiplas congruências simultaneamente.

2.5 FORMULAÇÃO MATEMÁTICA

Na matemática contemporânea, o Teorema Chinês dos Restos é formulado com precisão algébrica através do seguinte enunciado: Considere um conjunto de inteiros positivos $m_1, m_2, \dots, m_r$ que são relativamente primos entre si dois a dois. Para este conjunto, um sistema de congruências lineares da forma:

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

admite uma única solução módulo M, onde M é definido como o produto $m_1 m_2 \dots m_r$ (ROSEN, 2011, p.162).

Definição formal: O Teorema Chinês dos Restos estabelece que, dados os números naturais $n_1, n_2, \dots, n_k$ coprimos dois a dois (ou seja $mdc(n_i, n_j) = 1$ para $i \neq j$), o sistema de congruências:

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

Tem solução única módulo $N = n_1 n_2 \ldots n_k$.

Demonstração do Teorema:

Seja e $N = n_1 n_2 \ldots n_k$ para $N_i = \frac{N}{n_i}$ cada $i = 1, 2, \ldots, k$.

1. Como os n_i são coprimos dois a dois, temos que . $mdc\left(N_i, n_i \right) = 1$
2. Para cada i, existe um número y_i tal que: . $N_i y_i \equiv 1 \left(mod\ n_i \right)$
3. Uma solução do sistema é dada por: . $x = a_1 N_1 y_1 + a_2 N_2 y_2 + \ldots + a_k N_k y_k$
4. Para provar que esta é a solução, observe que: Para $j \neq i: N_j \equiv 0 \left(mod\ n_i \right)$ $Logo: x \equiv a_i N_i y_i \equiv a_i \left(mod\ n_i \right)$.
5. A unicidade decorre do fato de que se x_1 e x_2 são duas soluções: para todo i. Como os n_i são coprimos, $x_1 \equiv x_2 \left(mod\ n_i \right)$ $x_1 \equiv x_2 \left(mod\ N \right)$.

Demonstração: Para verificar que o número é escrito da forma:

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

é solução do sistema de congruência (I) se tomarmos:

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

Depois, veremos que tais $y_i's$ existem. Primeiramente, note que:

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

E assim, pelas propriedades de congruência, temos:

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

Uma vez que:

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

Como $y_1 \equiv 1 \left(mod\ m_1 \right)$ isso implica que, $y_1 \cdot a_1 \equiv a_1 \left(mod\ m_1 \right)$ usando a propriedade de congruência, temos:

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

Que mostra que x satisfaz a primeira congruência do sistema (I). Procedendo da mesma forma, vemos que x satisfaz as demais congruências do sistema dado.

Para encontrar os valores dos números $y_i's$, façamos o produto $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$. Uma vez que o $mdc\left(m_1, \frac{m}{m_1} \right) = 1$, pela identidade de Bezout, $s_1,\ t_1 \in \mathbb{Z}$ existem tais que:

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

Segue que:

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

E logo:

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

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

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

Portanto, podemos tomar $y_1 = t_1 \left(\frac{m}{m_1} \right)$. Os mesmos raciocínios empregados garantem a

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

existência de $y_i's$ todos os que serão iguais a . Note que $M = m$.

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

Logo:

É uma solução para o sistema de congruências dado.

Para provar a unicidade módulo M, suponha que existe outro número $c \in \mathbb{Z}$, que também seja solução do sistema dado. Pela propriedade de congruência temos que, para todo $i = 1, 2, ..., r$;

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

Como $m_1, m_2, ..., m_r$, são divisores de $M = m_1m_2...m_r$ e são primos entre si, dois a dois, então, pela definição de congruência $m_1 \mid x - c$, $m_2 \mid x - c$, ..., e $m_r \mid x - c$. , pela propriedade de primos entre si, segue que $M = m_1m_2...m_r \mid x - c$ e, portanto

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

como queríamos demonstrar.

2.6 A LINGUAGEM C COMO FERRAMENTA

Segundo Schildt (1996), a linguagem C nasceu intrinsecamente ligada ao desenvolvimento do sistema operacional UNIX, sendo criada por Dennis Ritchie nos laboratórios Bell. Como explica o autor, "C é o resultado da evolução de duas linguagens anteriores: a linguagem B (criada por Ken Thompson) e a BCPL (criada por Martin Richards)" (SCHILDT, 1996, p.3).

A história da linguagem C está profundamente conectada com a padronização ANSI (*American National Standards Institute*). Como destaca Schildt (1996), o estabelecimento desse padrão foi crucial para garantir a portabilidade e compatibilidade dos códigos entre diferentes plataformas. Esse aspecto é particularmente relevante para implementações de algoritmos matemáticos complexos como o Teorema Chinês dos Restos.

"C é uma linguagem de programação de propósito geral que oferece economia de expressão, controle de fluxo e estruturas de dados modernos e um rico conjunto de operadores" (SCHILDT, 1996, p.4). Estas características fazem de C uma escolha apropriada para a implementação do algoritmo do Teorema Chinês dos Restos, especialmente devido a:

1. Eficiência na manipulação de memória;
2. Controle preciso sobre operações matemáticas;
4. Capacidade de gerenciamento de estruturas de dados dinâmicas;

5. Performance otimizada para cálculos complexos.

A linguagem C, como ressalta Schildt (1996), combina a capacidade de programação de alto nível com a funcionalidade tradicionalmente associada à programação em *assembly*, tornando-a particularmente adequada para implementações matemáticas que exigem eficiência computacional.

A implementação algorítmica do Teorema Chinês dos Restos pode ser realizada através de uma abordagem modular em linguagem C, estruturada em funções específicas que executam as etapas fundamentais do teorema. Assim, o Teorema Chinês dos Restos pode ser implementado computacionalmente através de um algoritmo estruturado em linguagem C. A escolha dessa linguagem, conforme Schildt (1996), justifica-se pela sua eficiência no tratamento de operações matemáticas e gerenciamento de memória.

Seguiremos com abordagem às aplicabilidades práticas do teorema chinês dos restos, particularmente uma implementação computacional em linguagem C. Esse teorema não só apresenta uma elegância intrínseca na sua formulação matemática, mas é também peça-chave em diversas áreas tecnológicas e científicas. Na criptografia RSA, ele é vital para a eficiência dos cálculos de chave privada, permitindo operações com grandes números de maneira mais ágil e segura. Além disso, está presente na computação de alto desempenho, facilitando o manejo de grandes números em sistemas computacionais e na codificação de senhas e sistemas de verificação, garantindo segurança e integridade de dados.

Na teoria dos números, suas soluções para problemas de calendário e otimização exemplificam ainda mais sua utilidade. Essa versatilidade torna o teorema chinês dos restos um fundamento não apenas pela sua beleza teórica, mas também pela sua relevância prática em contextos modernos de computação e criptografia.

Prosseguindo para a metodologia, a pesquisa foi implementada em uma escola de tempo integral em Fortaleza, concentrando-se no ensino de Matemática, em particular, na congruência modular e suas aplicações no cotidiano. A metodologia adotou uma abordagem de aprendizagem colaborativa, com grupos de alunos trabalhando juntos na construção do conhecimento.

3 METODOLOGIA

3.1 OBJETIVO

O objetivo desta pesquisa é descrever de maneira detalhada como o estudo foi conduzido, englobando a intervenção pedagógica e a implementação computacional dos conceitos abordados. Em termos pedagógicos, a pesquisa foi aplicada em uma escola de tempo integral em Fortaleza, focando no ensino de Matemática, especialmente na temática da congruência modular. Utilizou-se uma abordagem de aprendizagem colaborativa, na qual os alunos foram organizados em grupos

heterogêneos para facilitar a troca de conhecimentos e estimular a resolução conjunta de problemas. A metodologia envolveu atividades práticas que utilizaram exemplos do cotidiano – como a verificação de dígitos do CPF, códigos de barras e situações de criptografia simples – para tornar os conceitos mais concretos e relevantes.

Paralelamente, o estudo explorou a implementação computacional do Teorema Chinês dos Restos utilizando a linguagem C, escolhida por sua eficiência no gerenciamento de memória, controle preciso nas operações aritméticas e capacidade de estruturar algoritmos complexos de forma otimizada. A implementação envolveu a validação de condições necessárias (como a coprimalidade dos módulos e a existência de inversos modulares) e a execução de funções específicas para resolver sistemas de congruências lineares. Essa abordagem computacional não apenas reforçou a aplicação prática dos conceitos matemáticos, mas também formou uma ponte direta entre teoria e prática, demonstrando a utilidade do teorema em contextos como a criptografia e o processamento de dados.

Em resumo, o estudo teve como propósito analisar o impacto da intervenção pedagógica colaborativa no desempenho dos alunos e comprovar a viabilidade técnica da aplicação do Teorema Chinês dos Restos por meio de uma implementação algorítmica em C, contribuindo para o aprimoramento do ensino e a demonstração de aplicações práticas em situações cotidianas.

3.2 INTERVENÇÃO PEDAGÓGICA

Nesse estudo, os alunos foram organizados em grupos heterogêneos. Essa estratégia visou incentivar a troca de conhecimentos e promover a resolução conjunta de problemas. Foram propostas atividades práticas focadas na congruência modular. Os estudantes enfrentaram desafios para identificar padrões numéricos, aplicar conceitos criptográficos, analisar calendários e interpretar ciclos econômicos. Exemplos práticos do cotidiano, como a verificação de dígitos do CPF e códigos de barras, também foram utilizados para consolidar o conteúdo. O professor desempenhou o papel de mediador. Ele propôs questões, estimulou a reflexão e facilitou discussões entre os alunos. A coleta de dados incluiu:

1. A aplicação de questionários diagnósticos antes e após a intervenção;
2. A observação da interação dos alunos durante a resolução das atividades;
3. A análise dos erros e acertos para identificar padrões de aprendizagem;
4. O registro sistemático das percepções dos alunos acerca da metodologia adotada;

Os resultados esperados foram:

1. A melhoria na compreensão da congruência modular e suas aplicações;
2. O desenvolvimento do raciocínio lógico e da capacidade de resolver problemas coletivamente;

3. O aumento do engajamento dos alunos ao reconhecer a relevância do conteúdo para situações cotidianas;

3.3 IMPLEMENTAÇÃO COMPUTACIONAL

O algoritmo fundamenta-se na resolução de sistemas de congruências lineares:

3.3.1 Estrutura do Algoritmo

3.3.1.1 Código em C

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

// Variável global do produto dos módulos
int M;

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

int inversoModular(int a, int m) {
    if (mdc(a, m) != 1) {
        return -1;
    }
    int novoT = 0, novoR = m;
    int antigoT = 1, antigoR = a;
    while (novoR != 0) {
        int quociente = antigoR / novoR;
        int temporaria = novoR;
        novoR = antigoR - quociente * novoR;
        antigoR = temporaria;
        temporaria = novoT;
        novoT = antigoT - quociente * novoT;
        antigoT = temporaria;
    }
    if (antigoT < 0) {
        antigoT += m;
    }
    return antigoT;
}

int teoremaChinesDoResto(int *restos, int *modulos, int numeroDeCongruencias) {
    M = 1;
    for (int i = 0; i < numeroDeCongruencias; i++) {
        M *= modulos[i];
    }
    int solucao = 0;
    for (int i = 0; i < numeroDeCongruencias; i++) {
        int Mi = M / modulos[i];
        int yi = inversoModular(Mi, modulos[i]);
        solucao += restos[i] * Mi * yi;
    }
    return solucao % M;
}
```

```
50
51 int main() {
52     int numeroDeCongruencias = 1;
53     char texto[] = "DIGITE O NUMERO DE CONGRUENCIAS NO SISTEMA OU 'ZERO'
PARA SAIR: ";
54     int largura = 70;
55     while (numeroDeCongruencias != 0) {
56         printf("%*s", largura, texto);
57         scanf("%d", &numeroDeCongruencias);
58         if (numeroDeCongruencias == 0) {
59             break;
60         }
61         int *restos = (int *) malloc(numeroDeCongruencias * sizeof(int));
62         int *modulos = (int *) malloc(numeroDeCongruencias * sizeof(int));
63         printf("\nDigite os restos e modulos para cada congruencia:\n\n");
64         for (int i = 0; i < numeroDeCongruencias; i++) {
65             printf("Congruencia %d\n", i + 1);
66             printf("Resto: ");
67             scanf("%d", &restos[i]);
68             printf("Modulo: ");
69             scanf("%d", &modulos[i]);
70             printf("\n");
71         }
72         int coprimos = 1;
73         for (int i = 0; i < numeroDeCongruencias; i++) {
74             for (int j = i + 1; j < numeroDeCongruencias; j++) {
75                 if (mdc(modulos[i], modulos[j]) != 1) {
76                     coprimos = 0;
77                     break;
78                 }
79             }
80             if (!coprimos) {
81                 break;
82             }
83         }
84     int solucao = teoremaChinesDoResto(restos, modulos, numeroDeCongruencias);
85         if (!coprimos) {
86     printf("O sistema nao esta na condicao do Teorema Chines dos Restos.\n");
87         } else {
88     printf("A solucao do sistema de congruencia e: %d mod %d\n", solucao, M);
89     printf("Temos uma solucao do tipo x = %dk + %d\n", M, solucao);
90         }
91         free(restos);
92         free(modulos);
93     }
94     system("pause");
95     return 0;
```

Autor: William Rodrigues da Silva

O Teorema Chinês dos Restos pode ser implementado computacionalmente através de um algoritmo estruturado em linguagem C, como mostrado acima. A escolha dessa linguagem justifica-se por sua eficiência no gerenciamento de memória, controle preciso nas operações aritméticas e capacidade de estruturar algoritmos complexos de forma otimizada.

Os passos da implementação podem incluir o cálculo do inverso modular usando o algoritmo estendido de Euclides e uma função principal que chama funções auxiliares. Essa abordagem

computacional reforça a aplicação prática dos conceitos matemáticos e forma uma ponte direta entre teoria e prática.

4 ANÁLISE DOS RESULTADOS

4.1 INTERVENÇÃO PEDAGÓGICA

A intervenção pedagógica proposta teve como objetivo principal promover uma aprendizagem mais significativa da congruência modular, aliando teoria e prática em um contexto colaborativo e de boa aplicabilidade no mundo real. Observou-se, como resultado, uma melhoria expressiva na compreensão dos conceitos relacionados à congruência modular por meio da vivência de situações-problema contextualizadas e da mediação ativa do professor.

Com a formação de grupos heterogêneos, evidenciou-se também o desenvolvimento do raciocínio lógico e da capacidade de resolver problemas de forma cooperativa, favorecendo a construção coletiva do conhecimento e a valorização da diversidade de saberes entre os alunos.

Além disso, a utilização de exemplos práticos do cotidiano – como a análise de códigos de barras, dígitos verificadores e ciclos temporais – proporcionou um maior engajamento dos estudantes, à medida que percebem a aplicabilidade dos conteúdos matemáticos em situações reais.

Por fim, com base nos instrumentos de coleta (questionários, observações e registros reflexivos), foram identificadas evidências de avanço na aprendizagem, maior participação ativa nas atividades e uma atitude mais positiva em relação à Matemática por parte dos alunos.

4.2 IMPLEMENTAÇÃO COMPUTACIONAL

O algoritmo implementado para o Teorema Chinês dos Restos (TCR) foi analisado em termos de complexidade computacional, considerando as etapas principais de seu funcionamento. A etapa principal do algoritmo envolve a combinação das soluções parciais para obter a solução única do sistema de congruências.

Considerando todas as etapas, a complexidade temporal do algoritmo é dominada pela combinação das soluções parciais e pelo cálculo dos inversos modulares. Portanto, a complexidade polinomial, que em geral do algoritmo é:

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

onde k é o número de congruências e m é o maior módulo.

A implementação computacional do algoritmo em linguagem C foi testada com diferentes conjuntos de dados, incluindo sistemas de congruências com até 5 equações. Os resultados

experimentais confirmaram que a complexidade temporal segue o comportamento teórico previsto, tornando o algoritmo eficiente para aplicações práticas em criptografia e validação de dados.

A análise da complexidade do algoritmo TCR demonstrou que sua implementação é eficiente e escalável, tornando-o uma ferramenta valiosa para resolver problemas em criptografia, validação de dados e outras aplicações computacionais. A complexidade de $O(k \cdot \log m)$ assegura que o algoritmo possa lidar com sistemas de congruências de grande porte de forma eficiente, com exigência limitada do sistema.

Em suma, a implementação do Teorema Chinês dos Restos em linguagem C, apesar de funcional, foi testada com conjuntos de dados relativamente pequenos (até 5 congruências). Não foram explorados testes de estresse ou *benchmarks* comparativos com outras linguagens ou métodos, o que limita a avaliação da eficiência em contextos mais exigentes, como criptografia real ou validação de grandes bases de dados. Porém, com base na teoria e conhecimentos da linguagem C, espera-se que o algoritmo seja eficiente e escalável, com desempenho estável mesmo com um número alto de congruências.

5 DISCUSSÃO DOS RESULTADOS

Apesar do estudo de Sistema de Congruência Lineares não ser trabalhado em sala de aula no Ensino Básico, toda a teoria necessária para sua compreensão é amplamente discutida nos anos finais do Ensino Fundamental, o que é importante ser trazido à sala de antemão. Para consolidar o conteúdo teórico sobre congruência modular, foram implementadas atividades práticas focadas na identificação de dígitos verificadores em CPFs e códigos de barras, bem como na análise de calendários, buscando exemplos práticos do cotidiano. Além das atividades pedagógicas, o estudo explorou a implementação computacional do Teorema Chinês dos Restos (TCR), utilizando a linguagem C.

O Teorema Chinês do Resto descreve as soluções de certos tipos de sistemas de congruências lineares que podem descrever inúmeros problemas interessantes, despertando o interesse de um aluno de ensino médio para resolvê-los. Desta forma, pode-se conseguir a mobilização dos alunos em trabalhos envolvendo raciocínios e estratégias ligadas ao Teorema Chinês do Resto na resolução de problemas matemáticos envolvendo congruências, bem como a identificação desse teorema com certos padrões de problemas específicos.

Uma vez que, de acordo com Ausbel (1980, p 623), a **Aprendizagem Significativa** é um processo no qual as novas informações são conectadas aos conhecimentos prévios de forma não arbitrária e substantiva, ela promove a construção de um significado mais profundo e duradouro, de modo que o aluno não apenas memoriza, mas compreende e aplica os conceitos matemáticos em contextos relevantes, personalizando o aprendizado.

De modo geral, pode-se constatar que os alunos, ao final do trabalho, conseguiram utilizar o Teorema Chinês do Resto como uma ferramenta para a resolução de problemas envolvendo divisão com restos, inclusive fazendo com que possamos ter como hipótese o estudo do Teorema Chinês do Restos. Por conseguinte, puderam perceber que a Aritmética, através da Congruência, pode muito auxiliar na solução de exercícios envolvendo divisão e restos, sendo importante em resolução de problemas como em Olimpíadas de Matemática e, até mesmo, em alguns processos seletivos de concursos ou universidades.

5.1 DÍGITO VERIFICADOR DO CPF

Diversos números do nosso dia a dia envolvem códigos, chamados códigos de identificação, que geralmente apresentam algarismos de controle cuja finalidade é validar uma sequência extensa. Esse é o caso do CPF. O CPF (Cadastro de Pessoas Físicas) no Brasil possui 11 dígitos, sendo os dois últimos os dígitos verificadores (DV), que garantem a autenticidade do número. Esses dígitos são calculados usando congruência módulo 11.

Levando em consideração o CPF, a ideia, inicialmente, foi conversar com os alunos para ver se eles conhecem a palavra algoritmo e o que entendem dela. Em caso de dúvidas, trabalhar-se-ia, em termos de ilustração das ideias, os algoritmos das quatro operações básicas para explicar. Em seguida, seria importante conversar com os alunos se foi fácil ou difícil e explicar que esses algoritmos são tão utilizados em nossa vida, que muitas vezes nem percebemos que tem tantos passos para serem executados.

Dos 11 dígitos que compõem o CPF, três são chamados de dígitos verificadores. O 9º dígito corresponde à identificação do estado a que pertence o CPF. O 10º dígito (chamado a10) é calculado a partir dos 9 primeiros e o 11º, a partir dos 10 anteriores a ele.

Tabela para identificar o CPF por Estado

9º dígito	Estado
0	Rio Grande do Sul
1	Distrito Federal, Goiás, Mato Grosso do Sul e Tocantins
2	Acre, Amapá, Amazonas, Pará, Rondônia e Roraima
3	Ceará, Maranhão, Piauí
4	Alagoas, Paraíba, Pernambuco e Rio Grande do Norte
5	Bahia e Sergipe
6	Minas Gerais
7	Espírito Santo e Rio de Janeiro
8	São Paulo
9	Paraná e Santa Catarina

Fonte <http://scpc.tpc.inf.br/scpc/help/estadocpf.htm> acesso 10 mar 2025

Para obter o primeiro DV (a10):

1. Multiplicam-se os nove primeiros dígitos pelos números de 1 a 9, da esquerda para a direita.
2. Soma-se os produtos obtidos.
3. O resultado dessa soma, módulo 11, determina o valor de a10.

Para o segundo DV (a11):

1. Repete-se o processo, agora com os dez primeiros dígitos (inclui a10) multiplicados de 0 a 9.
2. A soma dos produtos, módulo 11, determina o valor de a11.

No exemplo dado (CPF: 002007571), os cálculos resultam nos dígitos verificadores 5 e 6, formando o CPF completo: 002.007.571-56.

6 CONCLUSÃO

Neste trabalho, explorou-se a congruência modular como aplicação da Divisão Euclidiana e divisibilidade, e seu suporte na resolução de problemas. Assim, exploramos a congruência modular como aplicação da divisão Euclidiana e divisibilidade e o suporte na resolução de problemas. Houve também a intenção de mostrar ao aluno que, de certa forma, buscou-se resgatar a essência original do conteúdo, apresentando-o como um instrumento concreto e significativo para o processo de ensino-aprendizagem. Isto porque de um lado tínhamos a relevância do assunto e, por outro, o insucesso de muitos alunos, principalmente no ambiente de ensino médio, sobretudo em atividades e avaliações externas aplicadas no âmbito da dissertação “Congruências modulares: a aplicabilidade da Teoria dos Números no suporte à resolução de problemas”. Houve a intenção de mostrar ao aluno a essência do conteúdo desde sua origem como instrumento real para o ensino-aprendizagem.

O estudo investigou a aplicabilidade das congruências modulares e do Teorema Chinês dos Restos no ensino da Matemática no nível médio, bem como sua implementação computacional em linguagem C. Por meio de uma abordagem que combinou a análise teórica, a intervenção pedagógica e a implementação computacional, foi possível evidenciar a relevância e o potencial desses conceitos para a formação dos estudantes, bem como para a resolução de problemas práticos. A revisão da literatura permitiu identificar a presença da aritmética modular em sistemas de identificação e codificação contemporâneos, como códigos de barras e CPF, reforçando a necessidade de abordar esses temas no ensino.

A análise do Teorema Chinês dos Restos demonstrou sua versatilidade e importância em diversos campos, incluindo a Criptografia Moderna (como base para o RSA) e aplicações do mundo real. A revisão da literatura permitiu identificar a presença da aritmética modular em sistemas de identificação e codificação contemporâneos, como códigos de barras e CPF, reforçando a necessidade

de abordar esses temas no ensino. Conclui-se que se faz necessária a aplicação de projetos de intervenções pedagógicas inovadoras nas escolas. O estudo contribuiu para uma melhor compreensão do TCR e suas aplicações, esperando ter despertado interesse em pesquisas futuras.

REFERÊNCIAS

AUSUBEL, D. P.; NOVAK, J. D.; HANESIAN, H. Psicologia educacional. 2. ed. Rio de Janeiro: Interamericana, 1980.

BEZERRA, M. N. C. et al. Teoria dos números: um curso introdutório. [S.l.]: Editora Universitária AEDI da UFPA-EditAedi, 2018.

BRASIL. Ministério da Educação. Base Nacional Comum Curricular. [S.l.]: MEC/CONSED/UNDIME, 2017.

BOYER, C. B. História da matemática. 2. ed. São Paulo: Edgard Blücher, 1996.

CARVALHO, A. L.; RODRIGUES, D. V. M.; ARAUJO, L. H. R. Aplicações da aritmética modular na criptografia. Caderno de Exatas, [S.l.], 2015. Disponível em: https://periodicos.set.edu.br/index.php/cadernoexatas/article/view/2157. Acesso em: 4 mar. 2025.

DING, C.; PEI, D.; SALOMAA, A. Chinese Remainder Theorem: applications in computing, coding, cryptography. Singapore: World Scientific, v. 1, n. 1, p. 16, 1996.

ESQUINCA, J. C. P. Aritmética: códigos de barras e outras aplicações de congruências. [S.l.]: [s.n.], [s.d.]. Disponível em: https://posgraduacao.ufms.br/portal/trabalho-arquivos/download/1131. Acesso em: 4 mar. 2025.

EVES, H. Introdução à história da matemática. São Paulo: Unicamp, 2004.

HEFEZ, A. Elementos de aritmética. 2. ed. Rio de Janeiro: SBM, 2011.

LOPES, J. V.; ÁVILA, J. A. J. Limitação de qualquer fator primo de um número perfeito ímpar. [S.l.]: [s.n.], [s.d.]. Disponível em: https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=39&id2=50131. Acesso em: 8 mar. 2025.

MOL, R. S. Introdução à história da matemática. Belo Horizonte: CAEDUFMG, 2013.

MUNIZ NETO, A. C. Tópicos de matemática elementar: teoria dos números. 3. ed. Rio de Janeiro: SBM, 2022. v. 5.

OLIVEIRA, M. C. Aritmética: criptografia e outras aplicações de congruências. 2013. Dissertação (Mestrado em Matemática) – Universidade Federal de Mato Grosso do Sul, Campo Grande, 2013. Disponível em: https://repositorio.ufms.br/bitstream/123456789/2160/1/MAYKON%20COSTA%20DE%20OLIVEIRA.pdf. Acesso em: 8 mar. 2025.

PANTANO FILHO, R.; OLIVEIRA, K. C.; PARENTE, L. K. (orgs.). Temas em educação, matemática e ciência da natureza. Salto: FoxTablet, v. 1, n. 1, p. 147-168, 2025.

PICADO, J. A álgebra dos sistemas de identificação: da aritmética modular aos grupos diedrais. [S.l.]: [s.n.], [s.d.]. Disponível em: http://www.mat.uc.pt/~picado/SistIdent/isbn2.pdf. Acesso em: 8 mar. 2025.

SÁ, I. P. Aritmética modular e algumas de suas aplicações. [S.l.]: [s.n.], [s.d.]. Disponível em: https://www.academia.edu/36388352/ARITM%C3%89TICA_MODULAR_E_ALGUMAS_DE_SUAS_APLICA%C3%87%C3%95ES. Acesso em: 10 mar. 2025.

SANT'ANNA, I. K. A aritmética modular como ferramenta para as séries finais do ensino fundamental. [S.l.]: [s.n.], [s.d.]. Disponível em: https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=137&id2=43601. Acesso em: 10 mar. 2025.

SCHILDT, H. C completo e total. 3. ed. São Paulo: Makron Books, 1996.

SILVA, F. J. S. Congruências modulares: a aplicabilidade da teoria dos números no suporte à resolução de problemas. [S.l.]: [s.n.], [s.d.]. Disponível em: https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=7163&id2=171056198. Acesso em: 15 mar. 2025.