UNIVERSIDADE FEDERAL DO NORTE DO TOCANTINS
CENTRO DE CIÊNCIAS INTEGRADAS
CURSO DE LICENCIATURA EM MATEMÁTICA

MARCELLA SOUSA MAIA

O TEOREMA CHINÊS DO RESAO E SEU PAPEL NA TEORIA DOS NÚMEROS

Araguaína / TO

2023

MARCELLA SOUSA MAIA

O TEOREMA CHINÊS DO RESTO E SEU PAPEL NA TEORIA DOS NÚMEROS

Monografia apresentada ao curso de Licenciatura em Matemática da Universidade Federal do Norte do Tocantins – Centro de Ciências Integradas, como requisito parcial para obtenção do título de Licenciada em Matemática.

Orientadora: Profª. Drª. Renata Alves da Silva.

Araguaína / TO

2023

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

S725t Sousa Maia, Marcella.
O TEOREMA CHINÊS DO RESTO E SEU PAPEL NA TEORIA DOS NÚMEROS. / Marcella Sousa Maia. – Araguaína, TO, 2023.
38 f.

Monografia Graduação - Universidade Federal do Tocantins – Câmpus Universitário de Araguaína - Curso de Matemática, 2023.
Orientadora : Renata Alves da Silva

1. Divisibilidade. 2. Números Primos. 3. Congruência. 4. Teorema Chinês do Resto. I. Título

CDD 510

Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

MARCELLA SOUSA MAIA

O TEOREMA CHINÊS DO RESTO E SEU PAPEL NA TEORIA DOS NÚMEROS

Monografia apresentada ao curso de Licenciatura em Matemática da Universidade Federal do Norte do Tocantins – Centro de Ciências Integradas, como requisito parcial para obtenção do título de Licenciada em Matemática.

Orientadora: Profª. Drª. Renata Alves da Silva.

Data de aprovação: 19 / 12 / 2023

Banca Examinadora

gov.br Documento assinado digitalmente
RENATA ALVES DA SILVA
Data: 26/12/2023 16:50:11-0300
Verifique em https://validar.iti.gov.br

_____

Profª. Drª. Renata Alves da Silva, UFNT – Orientadora

gov.br Documento assinado digitalmente
ALVARO JULIO YUCRA HANCCO
Data: 20/12/2023 09:37:01-0300
Verifique em https://validar.iti.gov.br

_____

Prof. Dr. Alvaro Julio Yucra Hancco, UFNT – Examinador

gov.br Documento assinado digitalmente
JOSE CARLOS DE OLIVEIRA JUNIOR
Data: 26/12/2023 17:35:51-0300
Verifique em https://validar.iti.gov.br

_____

Prof. Dr. José Carlos de Oliveira Junior, UFNT– Examinador

Araguaína - TO

2023

“Que todos os nossos esforços estejam sempre focados no desafio à impossibilidade. Todas as grandes conquistas humanas vieram daquilo que parecia impossível.” (Charles Chaplin)

Dedico este trabalho aos meus pais, Rosimar Sousa Lima Maia, e Francisco Márcio Maia, aos meus sobrinhos, Davy Luiz Sousa Ribeiro e Hiago Sousa Ribeiro, e à minha irmã Rafaella Sousa Maia.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus por ter me auxiliado a superar todos os obstáculos encontrados ao longo deste percurso. À minha família, em especial à minha mãe Rosimar, meu pai Márcio, e minha irmã Rafaella, que sempre me apoiaram e incentivaram. À minha avó Maria Valdelice, que ao longo destes anos me deu apoio para que eu conseguisse me manter aqui, e ao meu avô Geraldo Felipe, que sempre que possível se fez presente. Aos meus sobrinhos Davy Luiz e Hiago, os quais têm respeito e admiração pela pessoa que venho me tornando. Ao meu namorado Daniel, por sempre me incentivar e acreditar na minha capacidade, e ao meu cunhado Reinaldo, por inúmeras vezes ter se disponibilizado a me ajudar no que fosse preciso.

Agradeço à Universidade Federal do Norte do Tocantins, Campus Araguaína, e aos professores por todos os ensinamentos que me permitiram apresentar um bom desempenho em todo o meu processo de formação profissional. Em especial, à Professora Drª Renata Alves da Silva por ter me orientado na realização deste trabalho.

Aos colegas e amigos que fiz ao longo dessa jornada, Raielly, Sinara, Pedro Darc, Matheus Amorim, Kemile, Rafael e Welder, que de alguma maneira contribuíram para minha formação acadêmica. Em especial, à minha amiga Adrielly, que em todos os momentos esteve ao meu lado, desde cada cálculo não compreendido até cada lista finalizada, superando juntas todas as dificuldades.

RESUMO

O presente trabalho tem como foco principal a resolução de sistemas de congruências lineares envolvendo números primos entre si. Ao abordar a problemática, o estudo se aprofunda em uma análise histórica detalhada do Teorema Chinês do Resto, uma poderosa ferramenta matemática com raízes históricas profundas na China antiga. Assim, exploramos sua formulação e propriedades, enfatizando a sua aplicação na teoria dos números, exemplos práticos são apresentados para ilustrar como o Teorema Chinês do Resto pode ser usado para resolver problemas de congruência modular. O estudo contribui para uma compreensão abrangente do significado deste teorema na teoria matemática e suas implicações práticas.

Palavras-chave: Divisibilidade, Números Primos, Congruência, Teorema Chinês do Resto.

ABSTRACT

The main focus of this work is the resolution of linear congruency systems involving prime numbers. In addressing the issue, the study delves into a detailed historical analysis of the Chinese Remainder Theorem, a powerful mathematical tool with deep historical roots in ancient China. Thus we explore its formulation and properties, emphasizing its application in number theory, practical examples are presented to illustrate how the Chinese Remainder Theorem can be used to solve modular congruence problems. The study contributes to a comprehensive understanding of the meaning of this theorem in mathematical theory and its practical implications.

Keywords: Divisibility, Prime Numbers, Congruence, Chinese Remainder Theorem.

SUMÁRIO

1 INTRODUÇÃO 11
2 CONTEXTO HISTÓRICO 13
3 ARITMÉTICA DOS INTEIROS 16
3.1 Divisibilidade 16
3.2 Divisão Euclidiana 17
3.3 Máximo Divisor Comum 19
3.4 Algoritmo de Euclides 20
3.5 Números Primos 23
3.6 Equações Diofantinas Lineares 26
3.7 Congruência Linear 28
4 TEOREMA CHINÊS DO RESTO 32
4.1 Sistema de Congruência Linear 32
5 CONSIDERAÇÕES FINAIS 38
REFERÊNCIAS BIBLIOGRÁFICAS 39

1 INTRODUÇÃO

Possivelmente o Teorema Chinês do Resto teve seus primeiros aparecimentos em alguma aplicação prática e veio evoluindo ao longo da história, de maneira semelhante a vários problemas famosos na Matemática.

É relatado que na antiguidade os generais chineses frequentemente utilizavam métodos criativos para contar suas tropas após uma batalha e descobrir o número de soldados que haviam perdido. Um desses métodos envolvia organizar as tropas sobreviventes em formações específicas e, em seguida, contar quantas formações completas poderiam ser criadas. Esse método era uma maneira eficaz de estimar o número de tropas restante. Assim, se um general tivesse um certo número de soldados e quisesse determinar quantos deles sobreviveram a uma batalha, ele poderia ordenar que eles se alinhassem em fileiras com um certo número de soldados não alocados para formação completa, isso indicaria o número aproximado de tropas perdidas.

Como exemplo, considere que um general chinês dispunha de 1700 tropas ao início da batalha. Ao final da batalha ele deseja saber o número de tropas que havia perdido. Desta forma ele ordenava que suas tropas se alinhassem em fileiras, primeiro que se dispusessem de 5 em 5, assim sobraram 3 soldados, em seguida que se alinhassem de 6 em 6, assim sobraram 4 soldados, e por último que se alinhassem de 7 em 7, e dessa maneira sobraram 5 soldados. Diante disso, a questão que ficava era: quantas tropas lhe restaram afinal?

Embora não exista evidência definitiva que confirme, é provável que problemas semelhantes tenham ocorrido na China antiga ou em outras civilizações.

A resolução desse tipo de problema prático se tornou possível graças ao desenvolvimento do Teorema Chinês do Resto. Esse teorema é um resultado fundamental na teoria dos números e tem suas raízes na antiga China. Foi desenvolvido para resolver problemas relacionados a sistema de congruências lineares. Ele fornece uma maneira sistemática de encontrar uma solução única para esses sistemas quando os módulos envolvidos são primos entre si.

Acredita-se que o teorema tenha sido desenvolvido por matemáticos chineses em diferentes momentos ao longo da história, mas a atribuição mais comum é de Sun Zi Suanjing durante os primeiros séculos entre 280 d.C a 483 d.C. Sun escreveu um livro chamado “Manual de aritmética do Sol”, que inclui três seções, e exatamente na terceira e última encontram-se 36 problemas aritméticos sendo utilizado pela primeira vez o teorema a partir do vigésimo sexto

problema. Essa seção é considerada uma das primeiras apresentações registradas do Teorema Chinês do Resto.

O Teorema é frequentemente associado à história chinesa do transporte de mercadorias, onde a ideia era dividir grandes quantidades de itens em pacotes menores para facilitar o transporte. Assim, através do teorema era permitido calcular quantos pacotes de diferentes tamanhos seriam necessários para transportar a mercadoria total de maneira eficiente.

A formulação do Teorema Chinês do Resto foi se desenvolvendo no decorrer dos séculos por matemáticos ocidentais como Carl Friedrich Gauss, que contribuiu para a teoria dos números e desenvolveu métodos mais abstratos de demonstração.

Uma frase muito dita por ele é: “A matemática é a rainha das ciências: a aritmética é a rainha da matemática” (Gauss, 1777-1885).

Em sua obra Disquisitiones arithmeticae (Investigações aritméticas), Gauss introduz a noção de congruência e, ao fazê-lo, agregou a teoria dos números. Iniciando seu prefácio com o seguinte enunciado: “As investigações contidas neste volume pertencem à parte da Matemática que trata dos números inteiros, por vezes, frações, mas nunca de irracionais” (Gauss, 1801, p.7 apud Picado, 2021,p.5).

O principal objetivo deste trabalho consiste em determinar soluções para sistemas de congruências lineares, sob condições específicas relacionadas aos números primos. As questões norteadoras do nosso estudo sãos: Como encontrar soluções de um sistema de congruências lineares? Quais as condições suficientes para descrever tais soluções?

A escolha do tema justifica-se pelo fato do Teorema Chinês do Resto ser um assunto relevante dentro da teoria dos números, sobretudo na resolução de problemas de congruências lineares e de estudar restos da divisão entre inteiros. Este trabalho se torna também uma forma de introduzir e detalhar a teoria de divisibilidade dos números inteiros, trazendo sempre que possível exemplos diversos.

Nos dias de hoje, o Teorema é frequentemente introduzido em cursos avançados de matemática, especialmente em disciplinas relacionadas à teoria dos números, álgebra abstrata e criptografia.

Desta forma, este trabalho está dividido em mais dois capítulos. No Capítulo 3, abordaremos sobre os conceitos preliminares do teorema, que são: Divisibilidade, Divisão Euclidiana, Máximo Divisor Comum, Algoritmo de Euclides, Equações Diofantinas Lineares, Números Primos e Congruência Linear. No Capítulo 4 finalizamos com a apresentação e a demonstração do Teorema Chinês do resto e alguns exemplos práticos.

2 CONTEXTO HISTÓRICO

No século III, um dos problemas mais antigos relacionados a restos foi identificado em um manuscrito chinês intitulado "Sun-Tsu Suanjing" (Manual de Aritmética do Mestre Sun), cuja autoria permanece desconhecida. Este problema histórico resultou na formulação da ferramenta conhecida como o Teorema Chinês do Resto, projetada para solucionar questões que envolvem restos, como exemplificado a seguir. A primeira documentação conhecida desse teorema é encontrada nesse manuscrito chinês, que data de algum período entre 287 e 473 d.C. (COUTINHO, 1997).

O Teorema Chinês do Resto foi localizado no Capítulo 3, específico no problema numerado como 26 dentro do manuscrito previamente mencionado, Bonfim (2021) cita Nascimento (2016).

> Existe um número desconhecido de objetos, se nós contarmos de 3 em 3, teremos resto 2, se contarmos de 5 em 5, teremos resto 3, se contarmos de 7 em 7, teremos resto 2. Descubra o número de objetos, (NASCIMENTO, 2016, *apud* BOMFIM, 2021, p.11).

Logo em seguida são fornecidos pelo matemático o método e a resolução do problema citado:

> Resposta: 23.
> Método: Se contarmos de 3 em 3 e tivermos resto 2, consideramos 140. Se contarmos de 5 em 5 e tivermos resto 3, consideramos 63. Se contarmos de 7 em 7 e tivermos resto 2, consideramos 30. Adicionando-os, obtemos 233 e subtraindo 210 chegamos a resposta. Se contarmos de 3 em 3 e tivermos resto 1, consideramos 70. Se contarmos de 5 em 5 e tivermos resto 1, consideramos 21. Se contarmos de 7 em 7 e tivermos resto 1, consideramos 15. Quando (um número) excede 106, o resultado é obtido subtraindo por 105, (NASCIMENTO, 2016, *apud* BOMFIM, 2021, p.11).

É importante notar que, historicamente, a atribuição da sua descoberta é incerta, e sua origem não pode ser definitivamente rastreada até um único matemático ou período. Este Teorema como muitos outros, pode ter uma história complexa de desenvolvimento ao longo dos séculos. No entanto, é importante destacar que o Teorema Chinês do Resto é uma parte fundamental da teoria dos números e tem aplicações amplas em Matemática e Ciência da Computação, independentemente de sua autoria histórica específica. Sua utilidade e importância transcendem a atribuição de créditos individuais e são reconhecidas por matemáticos e cientistas em todo o mundo.

Deste modo, apresentamos um dos textos mais importantes para a matemática chinesa

antiga, um deles

> é o K'uich'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, 1995, p.242).

O Teorema Chinês dos Restos e o conceito de congruências são apresentados no livro de Gauss, "Disquisitiones Arithmeticae", publicado em 1801. Nessa obra seminal, Gauss introduziu a noção de congruência, desenvolveu a teoria dos resíduos quadráticos e apresentou a demonstração da Lei da Reciprocidade quadrática, entre outras contribuições importantes. Logo no primeiro capítulo, Gauss abordou o conceito de congruência, introduzindo a notação $a \equiv b \, mod \, m$, que se tornou uma técnica poderosa.

Em suas palavras:

"Sejam a e b inteiros quaisquer, e seja $m > 1$ um inteiro positivo fixo. Diz-se que a é congruente a b módulo m, se, e somente se, m divide a diferença $a - b$."

Gauss foi pioneiro no uso dessa notação, que se tornou fundamental para expressar a congruência de forma concisa e eficaz.

No contexto do livro, Gauss utiliza o Teorema Chinês dos Restos para abordar um problema relacionado a calendários, especificamente, a tarefa de "encontrar os anos que têm um certo número de períodos em relação ao ciclo solar e lunar, juntamente com a indicação romana". Gauss introduz um método para resolver esse problema, que já havia sido empregado por Euler, embora fosse, na verdade, um método antigo que já havia sido mencionado várias vezes.

Outro matemático de destaque na Teoria dos Números é Diofanto de Alexandria, nascido entre 201 e 214 e falecido entre 284 e 298. Conforme BOYER & MERZBACH (2012), há poucas informações disponíveis sobre a vida de Diofanto, e os únicos detalhes pessoais conhecidos sobre sua carreira estão registrado na formulação de um problema epigrama[1]:

> Deus lhe concedeu ser um menino pela sexta parte de sua vida, e somando uma duodécima parte a isto cobriu-lhe as faces de penugem. Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! Infeliz, criança tardia; depois de chegar à metade da vida de seu pai, o destino frio o levou. Depois de consolar sua dor com a ciência dos números por quatro anos, ele terminou sua vida, (BOYER; MERZBACH, 2012, p.133).

As contribuições de Diofanto à Teoria dos Números são notáveis e têm grande

[1] Epigrama: Pequena composição poética que termina num pensamento engenhoso ou satírico.

relevância para o estudo de números inteiros, envolvendo conceitos de divisibilidade, números primos e congruência, todos relacionados ao tema central deste trabalho.

A abordagem dos antigos gregos também desempenhou um papel fundamental na Teoria dos Números, abrangendo o cálculo do máximo divisor comum de dois números, o conceito de números primos e a demonstração de que há uma infinitude de números primos.

Além de todos os conceitos e de todas as aplicações mencionadas acima, a poderosa ferramenta congruência pode ser usada para estudar mdc (máximo divisor comum) e critérios de divisibilidade entre inteiros, relacionando-os com números primos. Sobre isso, por volta de 300 a.C., em Alexandria, Euclides de Alexandria (330−275 a.C.) desempenhou um papel importante ao organizar os conhecimentos sobre números deixados por Tales e Pitágoras. Euclides compilou uma coleção de 13 livros conhecidos como "Os Elementos". Embora se acredite que Euclides não tenha demonstrado todos esses livros pessoalmente, eles reuniam demonstrações de seus alunos. Os livros VII, VIII e IX focalizam a Teoria dos Números, relacionando os números à construção geométrica, conforme concebido pelos gregos, que consideravam os números como inteiros e positivos.

De acordo com Boyer & Merzbach (2012, p.95), o livro VII de Euclides define conceitos fundamentais como divisibilidade, números primos e números perfeitos. Além disso, apresenta o famoso "algoritmo de Euclides", utilizado para determinar o máximo divisor comum de dois números. O livro VIII inicia com proposições sobre números em proporção contínua (progressão geométrica) e, em seguida, aborda propriedades simples de quadrados e cubo.

3 ARITMÉTICA DOS INTEIROS

Neste capítulo, exploraremos conceitos e resultados relevantes da Aritmética dos Inteiros para o desenvolvimento deste trabalho. Estes incluem tópicos essenciais, como divisibilidade, divisão euclidiana, máximo divisor comum, algoritmo de Euclides, equações diofantinas lineares, números primos e congruência linear. Para embasar nossos estudos, utilizaremos como referência o livro de Domingues e Iezzi (2003).

3.1 Divisibilidade

A divisibilidade é um conceito matemático que descreve condições para as quais um número inteiro é ou não divisível por outro inteiro, isto é, quando o resto da divisão é zero.

Definição 3.1: $a \in Z$ é divisível por outro número inteiro b se existe um número inteiro c tal que $a = b \cdot c$. Nesse caso, b é chamado de divisor de a, e a é chamado de múltiplo de b. Denotamos por $a|b$ quando a é divisor de b e quando a não é divisor de b, escreveremos $a \nmid b$.

A relação entre elementos do conjunto dos números inteiros, definida como a | b, que acabamos de introduzir, possui as seguintes propriedades:

Propriedade 3.2: Sejam $a, b, c \in Z$, temos que:
(i) Se $a \neq 0$, a relação de divisibilidade $a|a$ é sempre verdadeira. (*reflexiva)*
(ii) Se $a|b$ e $b|c$, então $a|c$. *(transitiva)*
(iii) Se $a, b \geq 0, a|b$, e $b|a$, então $a = b$. *(assimétrica)*
Demonstração:
i. De fato $a|a$ pois $a = a \cdot 1$.
ii. Se $a|b$ e $b|c$, existem k e m inteiros tais que $b = a \cdot k, e\ c = b \cdot m$. Temos que $c = a \cdot k \cdot m$, logo $a|c$.
iii. Se $a, b \geq 0, a|b$, e $b|a$, existem m e n inteiros, tais que $b = a \cdot m$ e $a = b \cdot n$. Se $a = 0$ então $b = 0$. Suponhamos que $a, b > 0$. Se $b = a \cdot m$, então $b = b \cdot n \cdot m$, segue que $m \cdot n = 1$, ou seja, $m = 1$ e $n = 1$. Como m e n são positivos, a igualdade só vale para $m = n = 1$. Portanto $a = b$.

■

Exemplo 3.3: Vale que $5|20$. De fato, 20 é divisível por 5, pois $20 = 5 \cdot 4$. Neste caso, 5 é um divisor de 20, e 20 é um múltiplo de 5.

Exemplo 3.4: Tomemos *2*, *6* e *12*. Se $2|6$, $6|12$ então $2|12$. *6* é divisível por *2*, porque $6 = 2 \cdot 3$. *12* é divisível por *6*, porque $12 = 6 \cdot 2$, e *12* também é divisível por *2*, porque $12 = 6 \cdot 2$.

Exemplo 3.5: $4 \nmid 7$. De fato, veja que $4 \cdot 1 = 4$ e $4 \cdot 2 = 8$, e *7* está entre *4* e *8*. Como não existe um inteiro c entre *1* e *2*, temos que *4* não divide *7*.

Lema 3.6: Se $a|b$ e $a|c$ então $a|(bx + cy)$, quaisquer que sejam os inteiros x e y.

Demonstração: Se $a|b$ e $a|c$, existem dois inteiros k_1 e k_2 tais que, $b = k_1 \cdot a$ e $c = k_2 \cdot a$. Para $a|(bx + cy)$, x e y quaisquer inteiros, temos $bx + cy = (k_1 \cdot a) \cdot x + (k_2 \cdot a) \cdot y$. Distribuindo os coeficientes, temos $bx + cy = k_1 \cdot a \cdot x + k_2 \cdot a \cdot y$. Agrupando os termos comuns, obtemos $bx + cy = a \cdot (k_1 \cdot x + k_2 \cdot y)$. Logo $a|(bx + cy)$.

■

3.2 Divisão Euclidiana

A Divisão Euclidiana é um procedimento matemático usado para dividir dois números inteiros e expressar o quociente e o resto dessa divisão em termos de números inteiros.

Segundo Hefez (2002)

> A Aritmética de Euclides tem início no livro VII dos Elementos, onde é usada sistematicamente sem menção explícita e sem demonstração, a divisão com resto que denominamos de Divisão Euclidiana, (HEFEZ, 2002, p.65).

Teorema 3.7: Dados os inteiros a e b com $b \neq 0$, existem inteiros q e r tais que

$$a = b \cdot q + r \text{ e } 0 \leq r < |b|.$$

Demonstração: (Existência) Consideremos o conjunto S limitado inferiormente,

$$S = \{x = a - b \cdot y, y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Vamos mostrar que o conjunto S é não vazio. De fato, como $b \neq 0$, pela Propriedade Arquimediana [HEFEZ (2002, p.31)], existe $n \in \mathbb{Z}$, tal que

$$n \cdot (-b) > (-a)$$

$$a - b \cdot n > 0.$$

Ou seja, existe $n \in \mathbb{Z}$ tal que $a - b \cdot n \in S$. Como S é limitado inferiormente por *0*, pelo Princípio da Boa Ordenação [IEZZI (2002, p.30)], existe um menor elemento $r = a - b \cdot y$, onde $y \in \mathbb{Z}$ e $r \geq 0$. Resta mostrar que $r < |b|$. Suponha por contradição que $r \geq |b|$. Isso nos diz que existe $s \in \mathbb{N} \cup \{0\}$ tal que

$$r = |b| + s, 0 \leq s < r,$$
$$s = r - |b| \ = \ a - b \cdot y - |b|$$
$$s = a - b \cdot (y \ \pm \ 1).$$

Portanto, $s \ \in \ S$. Mas isso é um absurdo, porque $s < r$ e r é o menor elemento de S. Logo $r < |b|$.

(Unicidade): Suponha que existam $q', r' \in Z$, onde $a = b \cdot q' + r' = b \cdot q + r$, com $0 \leq r' < |b|$ e $0 \leq r < |b|$. Assim, temos que

$$-|b| < (-r) \leq r' - r \leq r' < |b|$$
$$-|b| < r' - r < |b|.$$

Logo,

$$\text{I) } 0 \leq |r' - r| < |b|$$
$$\text{II) } b \cdot q' + r' = b \cdot q + r$$
$$b \cdot q' - b \cdot q = r - r'.$$

Por outro lado,

$$\text{III) } b \cdot (q' - q) = r - r'$$
$$|b| \cdot \ |q' - q| = |r - r'| < |b|.$$

Isso vale se $q = q'$. Por III), $0 = r - r'$. Portanto, $r = r'$.

■

Exemplo 3.8: [HEFEZ (2002, p.59)] Encontre *q* e *r* na divisão Euclidiana quando:

a) $D \ = 25, d \ = 7$
b) $D \ = \ 25, d \ = \ -7.$

Solução: Vamos calcular o resto da divisão utilizando a fórmula: $r = D - \ q \cdot d$, onde q é obtido como o maior inteiro que multiplicado por $d > 0$, fica menor ou igual a D. Quando $d < 0$, fazemos considerando $-d$ e tomamos $-q$.

a) Para $D = 25$ e $d = 7$: Usando a divisão Euclidiana, temos $25 = 7 \cdot 3 + 4$, $q = 3$. Assim $r = 25 - 3 \cdot 7 = 25 - 21 = 4$.
b) Para $D = 25$ e $d = -7$: Temos $25 = (-3) \cdot (-7) + 4$, $q = (-3)$. Assim $r \ = 25 - (-3 \cdot (-7)) = 25 - 21 = 4$.

Exemplo 3.9: [HEFEZ (2002, p.39)] Se o resto na divisão euclidiana de um inteiro m por *8* é *5*, qual é o resto da divisão de m por *4*?

Solução: Sabemos que o resto na divisão de m por *8* é igual a *5*, e isso significa que

$$m \ = 8n \ + 5 \text{ onde } n \ \in \ Z.$$

Agora vamos escrever

$$5 = 4 \cdot 1 + 1$$

Para encontrar o resto da divisão de m por 4, substituímos na expressão anterior. Então

$$m = 8 \cdot n + 4 \cdot 1 + 1 = 4 \cdot (2 \cdot n + 1) + 1 = 4k + 1. \text{ Com } k = 2n + 1.$$

Como o resto é único pelo Teorema 3.7, temos que a resposta é 1.

3.3 Máximo Divisor Comum

O Máximo divisor comum (mdc) é um conceito matemático fundamental que descreve o maior número que pode dividir dois números inteiros deixando o resto igual a 0. É frequentemente representado pelos símbolos $mdc(a, b)$ ou (a, b) para dois números inteiros a e b.

Definição 3.10: Sejam a e b dois números inteiros. Um elemento $d \in Z$ se diz máximo divisor comum de a e b se cumpre as seguintes condições:

i) $d \geq 0$

ii) $d|a$ e $d|b$

iii) Se d' é um inteiro tal que $d'|a$ e $d'|b$, então $d'|d$ (ou seja, todo divisor comum a a e b também é divisor de d).

Proposição 3.11 (Identidade de Bezout): Para quaisquer inteiros a e b, existem inteiros x_0 e y_0 tais que $d = a \cdot y_0 + b \cdot y_0$, onde d é o máximo divisor comum de a e b.

Demonstração: Veja em IEZZI (2003, p. 40).

■

Lema 3.12: Se $a|b$, então $mdc(a, b) = |a|$.

Demonstração: Veja em IEZZI (2003, p. 41).

■

Lema 3.13: Se $a = b \cdot q + r$, então $d = mdc(a, b)$ se, e somente se, $d = mdc(b, r)$.

Demonstração: Veja em IEZZI (2003, p. 41).

■

Definição 3.14: Dois inteiros a e b dizem-se primos entre si se $mdc(a, b) = 1$.

Proposição 3.15: Para que os inteiros a e b sejam primos entre si, é necessário e suficiente que se possam encontrar $x_0, y_0 \in Z$ tais que $a \cdot x_0 + b \cdot y_0 = 1$.

Demonstração: Veja em IEZZI (2003, p. 43).

■

Exemplo 3.16: [IEZZI (2003, p.45)] Se a e b são inteiros primos entre si, demonstre que $mdc(2a + b, a + 2b) = 1$ ou 3.

Solução: Começamos assumindo que a e b são inteiros primos entre si, ou seja, $mdc(a, b) = 1$. Seja d o mdc de $2 \cdot a + b$ e $a + 2 \cdot b$, então $d \cdot k = a + 2 \cdot b$ e $d \cdot m = 2 \cdot a + b$. Multiplicamos por 2 a primeira igualdade e, em seguida, subtraímos pela segunda, obtendo como resultado $d \cdot n = 3 \cdot b$ para algum n. De forma análoga, temos $d \cdot g = 3 \cdot a$ para algum g. Há duas alternativas, $mdc(d, 3) = 1$ ou 3. Se $mdc(d, 3) = 1$, podemos usar a Proposição 3 do Iezzi (2003, p.43) e, como $mdc(d, 3) = 1$ e $d|3 \cdot b$, temos que $d|b$. Da mesma forma, $d|a$. Assim, $d|mdc(a, b) = 1$. Logo, $d = 1$. Por fim, se $mdc(d, 3) = 3$, escrevemos $d = 3j$ e obtemos $3a = 3jg$ e $3b = 3jn$, o que implica em $a = jg$ e $b = jn$. Isso nos diz que o número $j|a$ e $j|b$. Pela definição de mdc, segue que $j|mdc(a, b)$, isto é, $j|1$, mostrando que $j = 1$ e concluindo que $d = 3j = 3$.

Exemplo 3.17: Vamos determinar o mdc de 12 e 18: Os divisores de 12 são $1, 2, 3, 4, 6$ e 12. Os divisores de 18 são $1, 2, 3, 6, 9$ e 18. O maior divisor comum é 6, portanto, $mdc(12, 18) = 6$.

Proposição 3.18: Sejam $a, m \cdot n \in \mathbb{Z}$, tais que $(m, n) = 1$. Então:

$$(a, m \cdot n) = 1 \Leftrightarrow (a, m) = 1 = (a, n).$$

Demonstração: Veja PRAZERES (2014, p.19).

■

Proposição 3.19: Sejam a e b inteiros primos entre si. Se $a|c$ e $b|c$, então $ab|c$.

Demonstração: Veja IEZZI (2003, p. 44).

■

3.4 Algoritmo de Euclides

O Algoritmo de Euclides é um método eficaz para encontrar o maior divisor comum de dois números inteiros. Esse algoritmo foi nomeado em homenagem ao matemático grego Euclides (330 − 275 a.C.).

Segundo BURTON (2016),

> O máximo divisor comum de dois inteiros pode ser encontrado ao listarmos todos os seus divisores positivos e escolhermos o maior comum aos dois, mas isto é embaraçoso para números maiores. Um processo mais eficiente, envolvendo aplicações repetidas do Algoritmo da Divisão, é dado no sétimo livro Os elementos. Embora haja evidências históricas de que este método é anterior a Euclides, hoje ele é apresentado como o Algoritmo de Euclides, (BURTON, 2016, p.25).

Ele pode ser enunciado da seguinte forma: Primeiro aplica-se a divisão euclidiana de a por b, depois para b e o primeiro resto parcial, e assim por diante. Ou seja:

$$a = b \cdot q_1 + r_1 \qquad (0 \leq r_1 < |b|)$$
$$b = r_1 \cdot q_2 + r_2 \qquad (r_2 < r_1)$$
$$r_1 = r_2 \cdot q_3 + r_3 \qquad (r_3 < r_2) \quad .$$

É claro que, se acontecer de r_1 ser nulo então $b = mdc(a, b)$, devido ao **Lema 3.12** e o processo termina na primeira etapa. Se $r_1 \neq 0$, passa-se à segunda e procedemos da mesma maneira com relação a r_2. Se $r_2 = 0$, então $r_1 = mdc(b, r_1)$, devido ao **Lema 3.12**; mas devido ao **Lema 3.13** $mdc(b, r_1) = mdc(a, b)$. E assim por diante.

Ocorre que, como $b > r_1 > r_2 > \ldots \geq 0$, então para algum índice n teremos com certeza $r_{n+1} = 0$. De fato, se todos os elementos de $\{r_1, r_2, r_3, \ldots\}$ fossem não nulos, então esse conjunto que é limitado inferiormente, não teria mínimo, o que é um absurdo pelo Princípio da Boa Ordenação. Assim, para o índice n referido:

$$r_{n-2} = r_{n-1} \cdot q_n + r_n$$
$$r_{n-1} = r_n \cdot q_{n+1}.$$

Portanto, em virtude dos lemas apresentados acima:

$$r_n = mdc(r_{n-1}, r_n) = mdc(r_{n-2}, r_{n-1}) = \ldots = mdc(b, r_1) = mdc(a, b).$$

Diante disso pode-se proceder da seguinte maneira: Sejam $a, b \in Z, b \neq 0$, pela Divisão Euclidiana, temos

$$a = b \cdot q_1 + r_1.$$

Quocientes →		q_1	
Divisores →	a	b	
Restos →	r_1		

Logo depois: $b = r_1 \cdot q_2 + r_2$,

Quocientes →		q_1	q_2	
Divisores →	a	b	r_1	
Restos →	r_1	r_2		

Desenvolvendo:

Quocientes →		q_1	q_2	q_3	…	q_{n-1}	q_n	q_{n+1}
Divisores →	a	b	r_1	r_2	…	r_{n-1}	r_{n-1}	$r_n = mdc(a,b)$
Restos →	r_1	r_2	r_3	r_4	…	r_n	0	

Exemplo 3.20: Calcule o mdc entre 70 e 375.

Utilizaremos o método acima para resolução:

$$375 = 70 \cdot 5 + 25$$

Quocientes →		5	
Divisores →	375	70	
Restos →	25		

$$70 = 25 \cdot 2 + 20$$

Quocientes →		5	2	
Divisores →	375	70	25	
Restos →	25	20		

$$25 = 20 \cdot 1 + 5$$

Quocientes →		5	2	1	
Divisores →	375	70	25	20	
Restos →	25	20	5	0	

$20 = 5 \cdot 4 + 0$

Quocientes →		5	2	1	4
Divisores →	375	70	25	20	5
Restos →	25	20	5	0	

Logo, o $mdc(70,375) = 5$.

Exemplo 3.21: Vamos calcular o mdc de 48 e 18 usando o Algoritmo de Euclides.
Inicialmente, $a = 48$ e $b = 18$. Divisão:

$$48 = 18 \cdot 2 + 12.$$

Agora, $a = 18$ e $b = 12$.
Divisão: $18 = 12 \cdot 1 + 6$.
Continuamos, $a = 12$ e $b = 6$.
Divisão:

$$12 = 6 \cdot 2 + 0.$$

O último valor não nulo de r é 6. Portanto o $mdc(48,18) = 6$.

3.5 Números Primos

Os números primos desempenham um papel fundamental na teoria dos números. Eles possuem diversas propriedades e resultados interessantes, dos quais se destaca a decomposição em fatores primos, conhecida como o Teorema Fundamental da Aritmética.

Definição 3.22: Um número inteiro positivo p é chamado número primo se as seguintes condições se verificam:
i) $p \neq 1$
ii) Os únicos divisores de p são os divisores triviais $1, p$.

Um número inteiro $a \neq 1$ é chamado número composto se tem outros divisores, além dos triviais.

Lema 3.23 (Lema de Euclides): Sejam $a, b, p \in Z$. Se p é primo e $p|a \cdot b$ então $p|a$ ou $p|b$.
Demonstração: Veja em IEZZI (2003, p. 45).

■

Exemplo 3.24: Sejam $a = 15$, $b = 6$, $p = 5$, logo $a \cdot b = 90$. Como $5|90$, p divide a ou b. No caso, $p|a$.

Lema 3.25: Seja $a \neq 0, \pm 1$ um inteiro. Então, o conjunto

$$L = \{x \in Z \mid x > 1 \text{ e } x \text{ é } divisor\ de\ a\}$$

possui um mínimo e esse mínimo é um número primo.
Demonstração: Veja em IEZZI (2003, p. 45).

■

Exemplo 3.26: Os números 2 e 3 são primos, pois os únicos divisores positivos de 2 são 1 e 2 e os únicos divisores positivos de 3 são 1 e 3. Assim, o número 2 e o número 3 são números primos.

Exemplo 3.27: Veja alguns inteiros positivos que também são primos, $2, 3, 5, 7, 11, 13$ e 17. O 2 é o único número par que é primo, pois qualquer outro par que não seja o 2 pode ser dividido por 1, por 2 e por ele mesmo e, portanto, não é primo.

Proposição 3.28: Dados dois números primos p e q e um número inteiro r qualquer:
i) $p|q$ então $p = q$
ii) Se $p \nmid r$ então $mdc(p, r) = 1$.
Demonstração: i) Realmente, como $p|q$, e sendo q primo, temos $p = 1$ ou $p = q$. Contudo, p é primo, ou seja, $p > 1$, portanto, $p = q$.
ii) Certamente, se $mdc(p, r) = k$, temos $k|p$ e $k|r$. Já que p é primo, então $k = p$ ou $k = 1$. No entanto $k \neq p$, visto que $p \nmid r$, desse modo, $k = 1$.

■

O resultado seguinte é um dos teoremas mais famosos quando se fala sobre números primos. Ele afirma, em outras palavras, que os números primos geram todos os demais números inteiros positivos maiores do que 1.

Teorema 3.29 (Teorema Fundamental da Aritmética): Qualquer número inteiro maior do que 1 pode ser expresso de maneira única (a menos de ordem) como o produto de fatores primos.

Demonstração: Se n é um número primo, a afirmação é evidente e não requer demonstração. Suponhamos, então, que n seja composto. Vamos considerar p_1 como o menor dos divisores positivos de $n(p_1 > 1)$. O número p_1 deve ser primo, pois se não fosse existiria um p tal que $1 < p < p_1$ e $p|n$, o que contradiz a escolha de p_1. Portanto, $n = p_1 \cdot n_1$. Se n_1 for primo, a demonstração está concluída. Caso contrário, podemos tomar p_2 como o menor fator de n_1. Comparada ao argumento anterior, p_2 deve ser primo, e podemos escrever $n = p_1 \cdot p_2 \cdot n_2$. Repetindo este procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, \ldots, n_r$. Como todos eles são maiores do que *1*, este processo deve terminar. Os primos na sequência $p_1, p_2, \ldots, p_k$ não são necessariamente distintos, então n terá a seguinte forma geral:

$$n = p_1^m \cdot p_2^m \cdot \ldots \cdot {p_k}^m.$$

Para provar a unicidade, usaremos indução sobre n. Para $n = 2$, a afirmação é verdadeira. Consideremos que a afirmação seja válida para todos os inteiros maiores do que *1* e menores do que n. Vamos provar que ela é verdadeira para n. Se n é primo, não há nada a ser demonstrado. Suponhamos, portanto, que n seja composto e tenha duas formas distintas de fatoração:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_r.$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1 \cdot q_2 \cdot \ldots \cdot q_r$ pela Proposição 3 do IEZZI (2022, p.43). Sem perda de generalidade, podemos supor que $p_1|q_1$. Logo,

$$n/p_1 = p_2 \cdot p_3 \cdot \ldots \cdot p_s = q_2 \cdot q_3 \cdot \ldots \cdot q_r .$$

Particularmente $1 < n/p_1 < n$, a hipótese de indução diz que as duas fatorações são idênticas, ou seja, $s = r$ e, a menos da ordem, as fatorações $p_1 \cdot p_2 \cdot \ldots \cdot p_s$ *e* $q_1 \cdot q_2 \cdot \ldots \cdot q_r$ são iguais.

■

Exemplo 3.30: Vamos encontrar a decomposição em fatores primos do inteiro positivo $n = 3450$.

Solução: A decomposição pode ser dada da seguinte forma: Primeiro dividimos *3450* até encontrarmos o menor resultado maior do que *1*.

3450 | *2*

$$1725 \mid 3$$
$$575 \mid 5$$
$$115 \mid 5$$
$$23 \mid 23$$
$$1$$

Logo, $3250 = 2 \cdot 3 \cdot 5^2 \cdot 23$.

3.6 Equações Diofantinas Lineares

Diofanto de Alexandria foi um eminente matemático grego do século III a.C, cuja vida foi dedicada à produção de diversos livros, sendo o mais notável intitulado Aritmética. Dentro desta obra, Diofanto apresenta uma breve introdução acerca de equações que envolvem mais de uma variável e buscam soluções inteiras, denominando-as de Equações Diofantinas.

> Diofanto viveu presumivelmente no século III em Alexandria, já sob o domínio de Roma. Foi praticamente o único matemático de renome na Grécia antiga que se dedicou predominantemente à teoria dos números. Interessou-se por uma grande variedade de equações para as quais procurava soluções racionais e eventualmente inteiras, (HEFEZ, 2002, p.101).

Apresentaremos equações diofantinas lineares somente com duas incógnitas, do tipo:

$$ax + by = c.$$

Assumimos que todo par de inteiros x_0, y_0 em que $ax_0 + by_0 = c$, chama - se uma solução inteira da equação.

Definição 3.31: A equação $ax + by = c$, onde $a, b, c, x\ e\ y \in Z$ é chamada de equação diofantina linear.

Exemplo 3.32: São equações diofantinas lineares:

i) $2x + 3y = 7$.

ii) $7x + 4y = 26$.

iii) $5x - 3y = 13$.

Teorema 3.33: Dada a equação $ax + by = c$, ela admite solução se, e somente se, $mdc(a, b)|c$.

Demonstração: Se x_0, y_0 é uma solução da equação, então vale,

$$ax_0 + by_0 = c.$$

Como $mdc(a,b)|a$ e $mdc(a,b)|b$, então $mdc(a,b)|ax_0 + by_0 = c$. Consideremos que $mdc(a,b)|c$, então existe um inteiro g tal que $c = g \cdot (a,b)$. Pela Identidade de Bezout, t_0 *e* s_0 tais que $t_0 \cdot a + s_0 \cdot b = (a,b)$, segue que $c = g \cdot (a,b) = (g \cdot t_0) \cdot a + (g \cdot s_0) \cdot b$. Com isso os inteiros $x_0 = g \cdot t_0$ e $y_0 = g \cdot s_0$ são uma solução da equação dada.

■

Teorema 3.34: Sejam x_0, y_0 uma solução particular da equação diofantina $ax + by = c$. Então essa equação admite infinitas soluções, caracterizadas pelos elementos do conjunto

$$S = \{(x_0 + (b/d) \cdot t, y_0 - (a/d) \cdot t) \mid t \in Z\},$$

em que $d = mdc(a,b)$.

Demonstração: Veja em IEZZI (2003, p.51)

■

Exemplo 3.35: Resolva a equação diofantina: $375x + 70y = 20$.

Solução: Primeiro vamos calcular $(375,70)$.

	5	2	1	4
375	70	25	20	5
25	20	5	0	

Dado que $(375,70) = 5$ e $5|20$, a equação admite solução. Existem $x_0, y_0 \in Z$ tais que, pela Identidade de Bezout, $375x_0 + 70y_0 = 5$

$$375 = 70 \cdot 5 + 25$$
$$70 = 25 \cdot 2 + 20$$
$$25 = 20 \cdot 1 + 5$$
$$20 = 5 \cdot 4 + 0.$$

Segue que

$$\begin{aligned} 5 = 25 - 20 \cdot 1 &= 25 - [70 - 25 \cdot 2] \cdot 1 \\ &= 25 \cdot 1 - 70 + 25 \cdot 2 \\ &= 25(1+2) - 70 \cdot 1 \\ &= 25 \cdot 3 - 70 \cdot 1 \\ &= [375 - 70 \cdot 5] \cdot 3 - 70 \cdot 1 \\ &= 375 \cdot 3 - 70 \cdot 15 - 70 \cdot 1 \\ &= 375 \cdot 3 + 70(-15 - 1) \\ &= 375 \cdot 3 + 70 \cdot (-16) . \end{aligned}$$

Logo, $5 = 375 \cdot 3 + 70 \cdot (-16)$. Multiplicamos toda a equação por 4, obtendo

$$375 \cdot 12 + 70 \cdot (-64) = 20.$$

Uma solução da equação diofantina é dada por $x = 12$ e $y = -64$. Assim a solução geral é dada por: $x = 75 \cdot g$ e $y = 14 \cdot g$.

Exemplo 3.36: Veja se a equação $27x + 6y = 4$ possui solução.
Solução: Verifiquemos o $mdc(27,6)$.

	4	2	
27	6	3	
3	0		

A equação não admite solução, pois $(27,6) = 3$ e $3 \nmid 4$.

3.7 Congruência Linear

Na Matemática, o termo congruência é amplamente reconhecido e frequentemente utilizado quando se trata da comparação de duas figuras geométricas.

De acordo com BARBOSA (2006, p.26), podemos afirmar que dois triângulos são considerados congruentes quando é possível estabelecer uma correspondência biunívoca entre seus vértices, de modo que os lados e ângulos correspondentes sejam equivalentes.

No entanto, foi somente em 1801 que Carl F. Gauss (1777-1855) aplicou a noção de congruência aos números inteiros, conforme apresentado em seu livro "Disquisitiones Arithmeticae" (Estudos de Aritmética).

A congruência linear é uma relação de equivalência entre números inteiros que está relacionada à divisibilidade. Sua definição precisa segue abaixo.

Definição 3.37. Sejam a, b números inteiros quaisquer e m um inteiro estritamente positivo. Diz-se que a é congruente a b módulo m se $m|(a - b)$, isto é, se $a - b = m \cdot q$ para um conveniente inteiro q. Para indicar que a é congruente a b, módulo m, usa-se a notação

$$a \equiv b(mod\ m).$$

Se a e b não são congruentes módulo m escrevemos:

$$a \not\equiv b\ (mod\ m).$$

Exemplo 3.38: Se $a = 17$ e $b = 7$, e estamos considerando a congruência módulo 5, então podemos dizer que $17 \equiv 7\ (mod\ 5)$ porque $(17 - 7) = 10$, sendo um múltiplo de 5.

Exemplo 3.39: Se $a = 7$ e $b = 11$, e estamos considerando a congruência módulo *5*, vamos verificar se eles são congruentes módulo *5*:
$(7 - 11 = (-4))$, não sendo um múltiplo de *5*, ou seja, $7 \not\equiv 11 \ (mod\ 5)$.

Proposição 3.40: i) Para quaisquer inteiros $a,n > 0$, temos $a \equiv a \ (mod\ n)$, pois $(a - a) = 0$, sendo sempre um múltiplo de n $(0 = 0 \cdot n)$. (*reflexiva)*
ii) Se $a \equiv b \ (mod\ n)$, então $b \equiv a \ (mod\ n)$. *(simétrica)*
iii) Sendo $a \equiv b \ (mod\ n)$ e $b \equiv c \ (mod\ n)$, então $a \equiv c \ (mod\ n)$. *(transitiva)*
Demonstração: Veja em IEZZI (2003, p. 54)

■

Proposição 3.41. Se $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$, então:
i) $a + c \equiv b + d \ (mod\ n)$
ii) $a - c \equiv b - d \ (mod\ n)$
iii) $a \cdot c \equiv b \cdot d \ (mod\ n)$.
Demonstração: *i):* $a + c \equiv b + d \ (mod\ n)$. Partimos das congruências iniciais:

$$a \equiv b \ (mod\ n) \text{ e } c \equiv d \ (mod\ n).$$

Isso significa que $a - b$ é um múltiplo inteiro de n e $c - d$ é um múltiplo de n. Ou seja, $a - b = k \cdot n$ para algum inteiro k, $c - d = l \cdot n$ para algum inteiro l. Agora, somamos as duas equações:

$$(a - b) + (c - d) = k \cdot n + l \cdot n.$$

Isso nos dá:

$$(a + c) - (b + d) = n \cdot (k + l).$$

Uma vez que k e l são inteiros, sua soma $(k + l)$ também é um inteiro. Portanto, $(a + c) - (b + d)$ é um múltiplo de n, o que implica que $a + c \equiv b + d \ (mod\ n)$.

ii): $a - c \equiv b - d \ (mod\ n)$. Iniciamos em $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$. Denota que, $a - b$ é um múltiplo de n e $c - d$ é um múltiplo de n. Isto é, $a - b = k \cdot n$ para algum inteiro $k, c - d = l \cdot n$ para algum inteiro l. Subtraímos as equações:

$$(a - b) - (c - d) = k \cdot n - l \cdot n.$$

Temos,

$$(a - c) - (b - d) = n \cdot (k - l).$$

Sendo k e l inteiros, sua diferença $(k - l)$ também é um número inteiro. Assim, $(a - c) - (b - d)$ é um múltiplo de n, o que implica que $a - c \equiv b - d \ (mod\ n)$.

iii): $ac \equiv bd\ (mod\ n)$. Para provar essa congruência, precisamos mostrar que a diferença entre $a \cdot c$ e $b \cdot d$ é um múltiplo de n. Começamos notando que $a \cdot c \equiv b \cdot d\ (mod\ n)$ significa que $a \cdot c - b \cdot d$ é um múltiplo de n. Podemos escrever $a \cdot c - b \cdot d$ como $(a \cdot c - b \cdot d) = k \cdot n$, onde k é um número inteiro. Agora, vamos agrupar os termos $a \cdot c - b \cdot d$ como $(a - b) \cdot c + b \cdot (c - d) = k \cdot n$, vamos olhar para os termos entre parênteses. Como k é um número inteiro, podemos escrever k como $k' + 1$, onde k' é outro número inteiro. Substituindo na equação novamente, temos $(a - b) \cdot c + b \cdot (c - d) = (k' + 1) \cdot n$.
Agora, vamos simplificar ainda mais. Podemos distribuir o termo c na primeira parcela e o termo b na segunda parcela. Isso nos dá $a \cdot c - b \cdot c + b \cdot c - b \cdot d = (k' + 1) \cdot n$. Podemos cancelar os termos $-b \cdot c$ e $b \cdot c$, pois eles se anulam. Isso nos deixa com $a \cdot c - b \cdot d = (k' + 1) \cdot n$. Vemos que $(a \cdot c) - (b \cdot d)$ é realmente um múltiplo de n, pois é igual a $(k' + 1) \cdot n$. Logo, $a \cdot c \equiv b \cdot d\ (mod\ n)$.

■

Teorema 3.42: A congruência linear $ax \equiv b\ (mod\ m)$, onde $a, b,$ e $n \in \mathbb{Z}$, com $m > 1$, possui solução se, e somente se, $d|b$, onde $d = mdc(a, m)$.

Demonstração: Vamos supor que a congruência tem uma solução, ou seja, existe um número inteiro x que satisfaz $ax \equiv b\ (mod\ m)$. Isso significa que $ax - b$ é divisível por m. Podemos escrever isso como $ax - b = k \cdot m$, onde k é um número inteiro. Agora, vamos calcular o $mdc(a, m)$. Se d é o $mdc(a, m)$, então d divide tanto a quanto m. Portanto, d também divide $a \cdot x$ e $k \cdot m$. Isso implica que d divide $(ax - b + km)$. Mas $(ax - b + km)$ é igual a zero, pois $ax \equiv b\ (mod\ m)$. Logo, d divide b. Se $d|b$, então a congruência tem uma solução. Agora vamos mostrar a recíproca. Suponha que d divide b. Isso significa que existe um número inteiro k tal que $b = d \cdot k$. Pela Identidade de Bezout, existem x e y tais que $d = a \cdot x + m \cdot y$. Multiplicando por k obtemos $b = d \cdot k = a(x \cdot k) + m(y \cdot k)$, isto é, $a(x \cdot k) - b = m(y \cdot k)$, um múltiplo de m. Logo, $x \cdot k$ é uma solução da congruência $ax \equiv b\ (mod\ m)$. Portanto, a congruência tem uma solução.

■

Exemplo 3.43: Considere que tenhamos a congruência linear $8x \equiv 16\ (mod\ 4)$. Queremos encontrar a solução e verificar se a proposição se mantém.
Primeiro, calculamos o mdc de $a = 8$ e $n = 4$:

$$d = (8,4) = 4.$$

Assim,

$$d|16.$$

Certificamos se *8* divide *16*:

$$16 = 8 \cdot 2 + 0.$$

Agora, dividimos ambos os lados por *8* para simplificar a equação:

$$8x \div 8 \equiv 16 \div 8.$$

Isso nos dá a nova congruência:

$$x \equiv 2 \,(mod\ 4),$$

vamos verificar se essa solução está correta substituindo-a na congruência original. Temos:

$$8 \cdot 2 \equiv 16 \,(mod\ 4),$$

obtemos:

$$16 \equiv 16 \,(mod\ 4).$$

A congruência é verdadeira, logo, a solução $x \equiv 2\,(mod\ 4)$ é correta e a proposição se mantém.

4 TEOREMA CHINÊS DO RESTO

Conforme Castro et. al (2016), o Teorema Chinês do Resto provavelmente teve suas origens em aplicações práticas ao longo da história, como indicam relatos sobre os generais chineses na antiguidade.

Estes líderes militares utilizavam métodos criativos para calcular suas perdas após uma batalha. Uma estratégia comum envolvia organizar as tropas sobreviventes em formações específicas e contar quantas formações completas poderiam ser formadas. Esse método eficiente permitia estimar o número de tropas remanescentes.

Por exemplo, se um general quisesse determinar quantos soldados sobreviveram a uma batalha, poderia ordenar que se alinhassem em fileiras com um número específico de soldados não alocados para formação completa. Um caso hipotético envolve um general chinês com 1700 tropas no início da batalha. Ao final, ele comandava que se alinhassem de 5 em 5, resultando em 3 soldados não alocados; depois de 6 em 6, gerando 4 soldados não utilizados; e por último de 7 em 7, deixando 5 soldados sem formação completa. A pergunta final era: quantas tropas restaram afinal?

Embora não exista evidência definitiva que confirme, é provável que problemas semelhantes tenham ocorrido na China antiga ou em outras civilizações.

4.1 Sistema de Congruência Linear

Um sistema de congruência é um conjunto de congruências da forma:

$$\begin{aligned} x &\equiv a_1 \,(mod\, m_1) \\ x &\equiv a_2 \,(mod\, m_2) \\ &\vdots \\ x &\equiv a_k \,(mod\, m_k) \end{aligned}$$

onde:

$x \in \mathbb{Z}$ é a incógnita que estamos tentando encontrar, $a_1, a_2, \ldots, a_k$, são números inteiros dados, $m_1, m_2, \ldots, m_k$, são os módulos específicos usados nas congruências.

A solução para esse sistema consiste em encontrar o valor de x que satisfaz todas as equações simultaneamente. Isso pode ser feito usando o Teorema Chinês do Resto, que fornece uma solução única em módulo se os módulos forem coprimos. Caso contrário, pode haver zero

ou várias soluções, dependendo da relação entre os módulos. Enunciamos abaixo tal resultado, que é o mais importante deste trabalho.

Teorema 4.2 (Teorema Chinês do Resto): Sejam $m_1, m_2, \ldots, m_r$ inteiros maiores que *1* e tais que $mdc(m_i, m_j) = 1, i \neq j$. Considerando $a_1, a_2, \ldots, a_r$ inteiros arbitrários, então o sistema de congruências lineares dado por (i):

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

admite solução $x \in \mathbb{Z}$. Além disso, duas soluções quaisquer são congruentes módulo o produto dos números $m_1, m_2, \ldots, m_r$, isto é, módulo $M = m_1 m_2 \ldots m_r$.

Demonstração: Vamos verificar que o número escrito da forma

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

é solução do sistema (i) se tomarmos

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

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

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

e, assim, pelas propriedades de congruência encontradas na **Proposição 3.40**, temos

$$y_2 a_2 + y_3 a_3 + \ldots + y_r a_r \equiv 0 \ (mod\ m_1) \text{ e } \ y_1 \equiv 1 \ (mod\ m_1)$$

uma vez que

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

Como $y_1 \equiv 1 \ (mod\ m_1)$, isso implica que $y_1 \cdot a_1 \equiv a_1 \ (mod\ m_1)$. Usando a propriedade de congruência dada na **Proposição 3.41**, temos

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

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. Resta-nos encontrar os valores dos números $y_i's$. Para isso, façamos o produto $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$. Uma vez que

$mdc\left(m_1, \frac{m}{m_1}\right) = 1$, veja a **Proposição 3.18**, onde $\frac{m}{m_1} = m_2 \ldots m_r$, pela **Proposição 3.11**, existem $s_1, t_1 \in \mathbb{Z}$ tais que $1 = s_1 \cdot m_1 + t_1 \cdot \left(\frac{m}{m_1}\right)$. Segue que

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

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

Agora, como $m_2, \ldots, m_r$ são divisores de $m \div m_1 = m_2 \cdot m_3 \cdot \ldots \cdot m_r$, então

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

Diante desses fatos, basta escolhermos $y_1 = t_1 \frac{m}{m_1}$. Para determinarmos y_2, procedemos da mesma forma, fazendo

$$\frac{m}{m_2} = m_1 \cdot m_3 \cdot \ldots \cdot m_r.$$

Então, novamente, $mdc\left(m_2, \frac{m}{m_2}\right) = 1$ e, assim, existem s_2, t_2 inteiros tais que $s_2 \cdot m_2 + t_2(m \div m_2) = 1$. Daí,

$$1 - t_2 \cdot \left(\frac{m}{m_2}\right) = s_2 \cdot m_2, \text{ e logo}$$

$$t_2 \cdot \left(\frac{m}{m_2}\right) \equiv 1 \ (mod\ m_2).$$

Como $m_1, m_2, \ldots, m_r$ são divisores de $\frac{m}{m_2} = m_1 \cdot m_3 \cdot \ldots \cdot m_r$, isso implica que

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

Portanto, podemos tomar $y_2 = t_2 \frac{m}{m_1}$. Os mesmos raciocínios empregados até aqui garantem a existência de todos os $y_i's$ que serão iguais a $y_i = t_i \frac{M}{m_i}$. Note que $M = m$. Logo,

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

é uma solução para o sistema de congruências dado. Vamos mostrar agora que essa solução é única módulo M. Com efeito, suponha que existe o número $c \in \mathbb{Z}$ também seja solução do sistema dado. Pela **Proposição 3.40** temos que, para todo $i = 1,2, \ldots, r$,

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

como $m_1, m_2, \ldots, m_r$ são divisores de $m_1 \cdot m_2 \cdot \ \ldots \cdot m_r$ e são primos entre si, dois a dois, e pela definição de Congruência $m_1 | x - c$, $m_2 | x - c$, ..., e $m_r | x - c$, segue da **Proposição 3.19**, segue que $M = m_1 m_2 \ldots m_r | x - c$ e, portanto, $x \equiv c \ (mod\ M)$, como queríamos mostrar.

■

Exemplo 4.3: Considere o seguinte sistema de congruência linear:

$$x \equiv 1\ (mod\ 2)$$
$$x \equiv 2\ (mod\ 3)$$
$$x \equiv 3 (mod\ 5)$$

O $mdc(2,3) = 1, mdc(3,5) = 1, mdc(2,5) = 1$, ou seja, são primos entre si. Logo, o sistema tem solução. Temos $m_1 = 2, m_2 = 3, m_3 = 5$ e $a_1 = 1, a_2 = 2, a_3 = 3$. Pelo Teorema Chinês do Resto, $m = m_1 \cdot m_2 \cdot m_3 = 2 \cdot 3 \cdot 5 = 30$, seguimos $m\ /\ m_1 = 30/2 = 15$, o

$$mdc\left(\frac{m}{m_1}, m_1\right) = mdc(15,2) = 1.$$

Se $\frac{m}{m_2} = 30/3 = 10$, então o

$$mdc\left(\frac{m}{m_2}, m_2\right) = mdc(10,3) = 1.$$

Se $\frac{m}{m_3} = 30/5 = 6$, então

$$mdc\left(\frac{m}{m_3}, m_3\right) = mdc(6,5) = 1.$$

$$15 - 1 = 14 = 2 \cdot 7 \qquad 15y \equiv 1\ (mod\ 2)$$
$$10 - 1 = 9 = 3 \cdot 3 \qquad 10y \equiv 1\ (mod\ 3)$$
$$6 - 1 = 5 = 5 \cdot 1 \qquad 6y \equiv 1\ (mod\ 5).$$

Veja que 1 é solução particular para as três congruências acima. Assim,

$$x = \left(\frac{m}{m_1}\right) \cdot 1 \cdot a_1 + \left(\frac{m}{m_2}\right) \cdot 1 \cdot a_2 + \left(\frac{m}{m_3}\right) \cdot 1 \cdot a_3$$

e, então,

$$x = 15 \cdot 1 \cdot 1 + 10 \cdot 1 \cdot 2 + 6 \cdot 1 \cdot 3 = 53.$$

Segue que

$$53 - 1 = 52 = 2 \cdot 26 \qquad 53 \equiv 1\ (mod\ 2)$$
$$53 - 2 = 51 = 3 \cdot 17 \qquad 53 \equiv 2\ (mod\ 3)$$
$$53 - 3 = 50 = 5 \cdot 10 \qquad 53 \equiv 3\ (mod\ 5).$$

Podemos fazer também:

$$z \equiv 53\ (mod\ m_1 \cdot m_2 \cdot m_3)$$
$$z \equiv 53\ (mod\ 30)$$
$$53 - 23 = 30 \qquad z \equiv 23\ (mod\ 30).$$

Portanto, $z \equiv 23\ (mod\ 30)$ é a menor solução positiva do sistema dado.

Exemplo 4.4: Vejamos o sistema de congruência linear:

$$x \equiv 1 \ (mod\ 10)$$
$$x \equiv 2 \ (mod\ 11)$$

Temos que, $m_1 = 10, m_2 = 11$, e $a_1 = 1, a_2 = 2$, e o $mdc(10,11) = 1$. Como solução particular, temos $x = \left(\frac{m}{m_1}\right) \cdot b_1 \cdot a_1 + \left(\frac{m}{m_2}\right) \cdot b_2 \cdot a_2$. Seguindo:

$$m = m_1 \cdot m_2$$
$$m = 10 \cdot 11 = 110$$
$$\frac{m}{m_1} = 110/10 = 11$$
$$\frac{m}{m_2} = 110/11 = 10$$

Usando o fato de $mdc\left(\frac{m}{m_1}, m_1\right) = 1$, temos

$$mdc(11,10) = 1 \Rightarrow \left(\frac{m}{m_1}\right) \cdot y \equiv 1 \ (mod\ m_1)$$
$$11y \equiv 1 \ (mod\ 10) \rightarrow y = 1 \text{ é solução}$$
$$10y \equiv 1 \ (mod\ 11) \rightarrow y = 10 \text{ é solução}$$

Então,

$$x = 11 \cdot 1 \cdot 1 + 10 \cdot 10 \cdot 2 = 211$$

é solução do sistema. Assim,

$$211 - 1 = 210 = 2 \cdot 10 \cdot 5 \qquad 211 \equiv 1 \ (mod\ 10)$$
$$211 - 2 = 209 = 11 \cdot 19 \qquad 211 \equiv 2 \ (mod\ 11)$$

Agora, usando a solução geral do sistema: $x \equiv b \ (mod\ m_1 \cdot m_2)$, temos

$$x \equiv 211 \ (mod\ 110)$$

Logo,

$$211 \equiv 101 \ (mod\ 110) \Rightarrow z \equiv 101 \ (mod\ 110)$$
$$101 - 1 = 100 = 10 \cdot 10 \qquad 101 \equiv 1 \ (mod\ 10)$$
$$101 - 2 = 99 = 9 \cdot 11 \qquad 101 \equiv 2 \ (mod\ 11).$$

Exemplo 4.5: Considere o seguinte sistema de congruência linear, envolvendo a quantidade de tropas que um general chinês perdia durante o fim de uma guerra:

$$x \equiv 3 \ (mod\ 5)$$
$$x \equiv 4 \ (mod\ 6)$$
$$x \equiv 5 \ (mod\ 7)$$

Temos $m_1 = 5, m_2 = 6, m_3 = 7$ e $a_1 = 3, a_2 = 4, a_3 = 5$. Pelo Teorema Chinês do Resto, $m = m_1 \cdot m_2 \cdot m_3 = 5 \cdot 6 \cdot 7 = 210$, seguimos $m \ / \ m_1 = 210/5 = 42$, o

$$mdc\left(\frac{m}{m_1}, m_1\right) = mdc(42,5) = 1.$$

Se $\frac{m}{m_2} = 210/6 = 35$, então o

$$mdc\left(\frac{m}{m_2}, m_2\right) = mdc(35,6) = 1.$$

Se $\frac{m}{m_3} = 210/7 = 30$, então

$$mdc\left(\frac{m}{m_3}, m_3\right) = mdc(30,7) = 1.$$

$$42 - 1 = 41 = 41 \cdot 1 \qquad 41y \equiv 1 \ (mod\ 5)$$

$$35 - 1 = 34 = 17 \cdot 2 \qquad 34y \equiv 1 \ (mod\ 6)$$

$$30 - 1 = 29 = 29 \cdot 1 \qquad 29y \equiv 1 \ (mod\ 7).$$

Veja que 1 é solução particular para as três congruências acima. Assim,

$$x = \left(\frac{m}{m_1}\right) \cdot 1 \cdot a_1 + \left(\frac{m}{m_2}\right) \cdot 1 \cdot a_2 + \left(\frac{m}{m_3}\right) \cdot 1 \cdot a_3$$

e, então,

$$x = 42 \cdot 1 \cdot 3 + 35 \cdot 1 \cdot 4 + 30 \cdot 1 \cdot 5 = 416.$$

Segue que

$$416 - 1 = 415 = 5 \cdot 83 \qquad 416 \equiv 1 \ (mod\ 5)$$

$$416 - 2 = 414 = 2 \cdot 207 \qquad 416 \equiv 2 \ (mod\ 6)$$

$$416 - 3 = 413 = 7 \cdot 59 \qquad 416 \equiv 3 \ (mod\ 7).$$

Podemos fazer também:

$$z \equiv 416 \ (mod\ m_1 \cdot m_2 \cdot m_3)$$

$$z \equiv 416 \ (mod\ 210)$$

$$416 - 206 = 210 \qquad z \equiv 206 \ (mod\ 210).$$

Portanto, $z \equiv 206 \ (mod\ 210)$ é a menor solução positiva do sistema dado.

5 CONSIDERAÇÕES FINAIS

Ao final desta pesquisa concluímos que o Teorema Chinês do Resto é uma poderosa ferramenta matemática com diversas aplicações práticas. Ele permite resolver sistemas de congruências de maneira eficiente, encontrando soluções únicas que satisfazem a todas as equações simultaneamente. Além disso, o teorema desempenha um papel importante em campos como a criptografia e a computação, onde é utilizado para otimizar cálculos e garantir a segurança dos dados. Ao explorar esse tema, pudemos compreender sua importância e complexidade, abrindo portas para futuras pesquisas e avanços na área da teoria dos números.

Consideramos que este trabalho pode servir como material de apoio para professores e estudantes como recursos adicionais e complementares para solução de problemas desta natureza.

Como dito, existem diversas outras aplicações deste teorema, uma delas é na partilha de senhas que se destaca como uma abordagem inovadora para lidar com a segurança de informações confidenciais. A divisão de segredos, baseada no Teorema, oferece uma camada adicional de proteção ao distribuir partes da senha entre diferentes entidades, tornando a recuperação do segredo original uma tarefa desafiadora, mesmo em situações de comprometimento parcial. É o que se mostra no trabalho apresentado por Prazeres (2014) que estuda o campo do Teorema Chinês do Resto e Partilhar de Senhas.

No trabalho apresentado por Tanaka (2021), visa mostrar o contexto da implementação computacional, a eficiência do Teorema em lidar com aritmética modular o torna um recurso valioso. Sua capacidade de acelerar cálculos em sistemas com restrições modulares, como na redução de grandes números, contribui para a otimização de algoritmos e operações matemáticas em computação de alto desempenho.

Ao longo deste trabalho, exploramos os fundamentos e as aplicações deste teorema, compreendendo sua importância e relevância para a matemática. Espero que este estudo tenha contribuído para uma melhor compreensão desse assunto e despertado interesse em pesquisas futuras.

REFERÊNCIAS BIBLIOGRÁFICAS

Bárbara de Almeida S. **CARL FRIEDRICH GAUSS**. 2016. Disponível em: <https://www3.unicentro.br/petfisica/2016/07/12/karl-friedrich-gauss-1777-1855/> Acesso em: 23, Novembro, 2023

BARBOSA, J. L. M. **Geometria euclidiana plana. coleção do professor de matemática.** Rio de Janeiro: SBM, 2006.

BOMFIM, Luciane Sousa. **Subsunçores para Resolução de Problemas de Divisão de Numeros Inteiros: o Caso do Teorema Chinês do Resto**. 2021, Dissertação (Mestrado em Matemática em Rede Nacional-PROFMAT) – Universidade Estadual de Maringá, Centro de Ciências Exatas, Departamento de Matemática, Maringá-PR, 2021.

BOYER, C. B.; MERZBACH, U. C. **História da matemática**. [S.l.]: Editora Blucher, 2012.

BURTON, D. **Teoria elementar dos números**. [S.l.]: Grupo Gen-LTC, 2016.

CASTRO, Alessandra; PAIVA, Ariane; SOUZA, Charles; RUIVO, José. **Teorema Chinês do Resto**. 2016. 8 f. TCC (Graduação) - Curso de Matemática, Unicamp, 2016.

COUTINHO, Severino Collier. **Números inteiros e criptografia RSA.** IMPA, 1997.

DOMINGUES, H. H., IEZZI, Gelson. **Álgebra Moderna.** 4ª ed. São Paulo: Atual, 2003.

EPIGRAMA. In: DICIO, Dicionário Online de Português, Porto: 7Graus, 2023. Disponível em: <https://www.dicio.com.br/epigrama/>. Acesso em 30, Novembro, 2023.

EVES, H. W. **Introdução à história da matemática.** [S.l.]: Editora Unicamp, 1995.

HEFEZ, ABRAMO. **Curso de Álgebra, volume 1 (3ª edição).** Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2002.

PICADO, Francisco Manuel Albuquerque. **Formas Quadráticas e Testes de Primalidade em "Disquisitiones Arithmeticae"**. 2021. Dissertação (Mestrado em Matemática) – Universidade de Lisboa, Faculdade de Ciências, Departamento de Matemática, Campo Grande, 2021.

PRAZERES, Sidmar Bezerra dos. **O Teorema Chinês dos Restos e a Partilhar das Senhas**. 2014. 71 f. Dissertação (Mestrado) - Curso de Matemática, Universidade Federal Rural de Pernambuco, Recife-Pe, 2014.

TANAKA, Diandra Chisa. **Teorema Chines dos Restos: Uma Proposta de Abordagem Teorica com Implementações Computacional**. 2021. 59 f. Dissertação (Mestrado) - Curso de Profmat, Universidade Federal do Oeste da Bahia, Barreiras, 2021.