Universidade Federal de Uberlândia
Faculdade de Matemática
Programa de Mestrado Profissional em Matemática em Rede Nacional

APLICAÇÕES DA TEORIA DOS NÚMEROS NA EDUCAÇÃO BÁSICA COM ENFOQUE EM DIVISIBILIDADE E NA ARITMÉTICA DOS RESTOS

Renato Rodrigues

Uberlândia-MG
2024

Renato Rodrigues

APLICAÇÕES DA TEORIA DOS NÚMEROS NA EDUCAÇÃO BÁSICA COM ENFOQUE EM DIVISIBILIDADE E NA ARITMÉTICA DOS RESTOS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para a obtenção de título de **MESTRE EM MATEMÁTICA**.

Área de concentração: Matemática
Linha de pesquisa: Teoria dos Números

Orientador(a): Rafael Antônio Rossato

Uberlândia-MG
2024

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

R696 Rodrigues, Renato, 1989-
2024 Aplicações da Teoria dos Números na Educação Básica com Enfoque em Divisibilidade e na Aritmética dos Restos [recurso eletrônico] / Renato Rodrigues. - 2024.

Orientador: Rafael Antônio Rossato.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2024.588
Inclui bibliografia.

1. Matemática. I. Rossato, Rafael Antônio,1986-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:

Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática em Rede Nacional
Av. João Naves de Ávila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3230-9452 - www.famat.ufu.br - profmat@famat.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Mestrado Profissional em Matemática em Rede Nacional - PPGMPMAT UFU				
Defesa de:	Dissertação de Mestrado Profissional, 03, PPGMPMAT				
Data:	Vinte de agosto de dois mil e vinte e quatro	Hora de início:	14:15	Hora de encerramento:	16:15
Matrícula do Discente:	12212PFT013				
Nome do Discente:	Renato Rodrigues				
Título do Trabalho:	Aplicações da Teoria dos Números na Educação Básica com Enfoque em Divisibilidade e na Aritmética dos Restos				
Área de concentração:	Ciências e Humanidades para a Educação Básica				
Linha de pesquisa:	Formação de Professores de Matemática da Educação Básica				
Projeto de Pesquisa de vinculação:	Não há				

Reuniu-se em webconferência pela plataforma *Google Meet* a Banca Examinadora, aprovada pelo Colegiado do Programa de Pós-graduação em Matemática - Mestrado Profissional em Matemática em Rede Nacional (PPGMPMAT), assim composta pelos professores doutores: Narciso da Hora Lisboa - UNIMONTES; Marcus Augusto Bronzi - IME/UFU e Rafael Antônio Rossato - IME/UFU, orientador do candidato.

Iniciando os trabalhos, o presidente da mesa, Prof. Dr. Rafael Antônio Rossato, apresentou a Comissão Examinadora e juntamente com o candidato agradeceram a presença de todos. Posteriormente, o presidente concedeu ao Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

Dando continuidade, o senhor presidente concedeu a palavra para os examinadores que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final considerando o candidato:

Aprovado

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Marcus Augusto Bronzi**, **Professor(a) do Magistério Superior**, em 20/08/2024, às 16:07, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Narciso da Hora Lisboa**, **Usuário Externo**, em 20/08/2024, às 16:07, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Rafael Antonio Rossato**, **Professor(a) do Magistério Superior**, em 20/08/2024, às 16:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5600983** e o código CRC **D3EF6E86**.

Referência: Processo nº 23117.051591/2024-57 SEI nº 5600983

RODRIGUES, R. *Aplicações da Teoria dos Números na Educação Básica com Enfoque em Divisibilidade e na Aritmética dos Restos*. **2024**. **73p**. **Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.**

Resumo

Este trabalho apresenta uma proposta na área da teoria dos números. Inicialmente, abordaremos os critérios de divisibilidade a partir de duas perspectivas: a representação decimal dos números naturais e a aritmética modular. Serão discutidos conceitos fundamentais da teoria dos números, como o algoritmo da divisão, a aritmética dos restos e a representação decimal dos números naturais.Em seguida, propomos um plano de trabalho direcionado a estudantes da educação básica, abrangendo tanto o Ensino Fundamental quanto o Ensino Médio. Acreditamos que essa abordagem promoverá uma compreensão profunda de conceitos da aritmética elementar, com um rigor matemático adequado, contribuindo significativamente para o desenvolvimento do raciocínio lógico e a compreensão de problemas e conceitos matemáticos entre os estudantes.

Palavras-chave: Teoria dos Números, Divisibilidade, Aritmética dos Restos, Educação Básica.

RODRIGUES, R. .***Applications of Number Theory in Basic Education with a Focus on Divisibility and Residue Arithmetic***. **2024**. **73p**. **M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.**

Abstract

This work presents a proposal in the field of number theory. Initially, we will explore divisibility criteria from two perspectives: the decimal representation of natural numbers and modular arithmetic. Fundamental concepts of number theory, such as the division algorithm, modular arithmetic, and the decimal representation of natural numbers, will be discussed.Following this, we propose a work plan aimed at students in basic education, covering both elementary and high school levels. We believe this approach will foster a deep understanding of elementary arithmetic concepts, with appropriate mathematical rigor, significantly contributing to the development of logical reasoning and the understanding of mathematical problems and concepts among students.

Keywords: Number Theory, Divisibility, Residue Arithmetic, Basic Education.

Sumário

Introdução

Os números naturais e inteiros surgiram na antiguidade para suprir as necessidades humanas de contagem. Posteriormente, com as organizações sociais das civilizações antigas, esses números se tornaram imprescindíveis na realização de operações mercantis. Os sistemas de numeração surgiram nesse contexto como meios de representar diversas quantidades utilizando o menor número de símbolos possível, de modo a possibilitar operações que satisfizessem as necessidades humanas ao longo do tempo.

A necessidade de representar números grandes trouxe o desenvolvimento de sistemas de numeração ao longo da história. Para essas representações, surgiu a necessidade do uso de bases, isto é, dada a unidade, a base se definiria por uma certa quantidade dessa unidade, sendo representada por um único símbolo.

O historiador Eves Howard [1] destaca que há evidências do uso de 2, 3 e 4 como bases primitivas por nativos de Queensland, da Terra do Fogo e algumas tribos da América do Sul. Ele aponta para evidências do uso do sistema quinário (base 5), que até hoje é usado em tribos na América do Sul onde contam com as mãos: "um, dois, três, quatro, mão (cinco), mão e um (seis)"e assim sucessivamente.

Segundo Eves [1], há ainda evidências pré-históricas do uso da base 12, possivelmente por ser o número aproximado de períodos entre aparições da lua ou por apresentar vários divisores inteiros. O sistema vigesimal teria sido usado por índios americanos e pelos maias.

Entre os sistemas antigos, o que mais se destaca é o sistema sexagesimal, usado pelos antigos babilônios e, ainda nos dias atuais, para representar medidas de tempo e de ângulos, em minutos e segundos.

O nosso sistema decimal, de base 10, segundo Abramo Hefez, é uma variante do sistema sexagesimal babilônico. Este foi desenvolvido na China e na Índia e espalhou-se pelo Oriente Médio, tendo grande aceitação no mundo árabe.

Segundo Hefez [5], embora Euclides não tenha criado muitos novos resultados, ele estabeleceu

um padrão de apresentação e rigor matemático jamais visto anteriormente, que ainda é seguido atualmente. Dos treze livros de Os Elementos, dez tratam de Geometria e três de aritmética. Neste trabalho, focaremos principalmente em conceitos como divisibilidade e divisão euclidiana, presentes no Livro VII de Euclides.

Neste estudo, abordaremos principalmente a divisibilidade e os critérios de divisibilidade no sistema decimal atual. Nos Capítulos 1, 2 e 3, discutiremos as operações com números naturais, a divisão nos números naturais e o sistema de numeração decimal. Em Capítulos posteriores (4 e 5), trataremos da aritmética dos restos e dos principais critérios de divisibilidade.

Além disso, apresentaremos uma sequência didática sobre divisibilidade. Segundo Zabala (1998, p. 18) [9], sequência didática é um conjunto de atividades ordenadas, estruturadas e articuladas visando alcançar objetivos educacionais, sendo que tanto professores quanto alunos devem conhecer seu início e fim.

Peretti e Tonin da Costa (2013, p. 6) [8] afirmam que a sequência didática consiste em atividades inter-relacionadas que visam ensinar o conteúdo de aprendizagem gradualmente, organizadas de acordo com os objetivos de aprendizagem definidos pelo professor, e que inclui atividades de avaliação que podem durar dias, semanas ou mesmo durante todo o ano.

Nesse sentido, abordaremos a divisibilidade no Capítulo 6, apresentando uma sequência didática que visa à compreensão dos critérios de divisibilidade e suas demonstrações.

CAPÍTULO 1

O Conjunto dos Números Naturais

Neste capítulo, apresentaremos o Conjunto dos Números Naturais, que é dado por:

$$\mathbb{N} = \{0, 1, 2, 3, \cdots\}.$$

Nesse contexto, definimos o conjunto $\mathbb{N}^* = \{1, 2, 3, \cdots\}$, que é equivalente a $\mathbb{N} - \{0\}$.

O conjunto dos números naturais surgiu das necessidades de resolver problemas de contagem do cotidiano, tendo uma construção bastante lenta, de acordo com Hefez (2022) [4]. Segundo o autor, no final do século XIX, os fundamentos da matemática foram questionados e intensamente repensados. Foi nesse período que a noção de número começou a ser baseada em conceitos da teoria dos conjuntos, considerados mais primitivos.

Apresentamos, a seguir, uma abordagem axiomática, admitindo, como ponto de partida, que o leitor esteja familiarizado com o conjunto dos números naturais aqui apresentado, além das operações de adição $(a, b) \to a + b$ e de multiplicação $(a, b) \to a \cdot b = ab$.

1.1 A Adição e a Multiplicação

Vamos assumir, no conjunto dos números naturais, como válidas as seguintes propriedades:

(i) A adição e a multiplicação são bem definidas:
Para $a, b, c, d \in \mathbb{N}$, se $a = c$ e $b = d$, então $a + b = c + d$ e $ab = cd$.

(ii) A adição e a multiplicação são comutativas:
Para $a, b \in \mathbb{N}$, então $a + b = b + a$ e $ab = ba$.

(iii) A adição e a multiplicação são associativas:

Para $a, b, c \in \mathbb{N}$, $(a+b)+c = a+(b+c)$ e $(ab)c = a(bc)$.

(iv) A adição e a multiplicação possuem elemento neutro:

Existem $0,\ 1 \in \mathbb{N}$ tal que para todo $a \in \mathbb{N}$, $a+0 = 0+a = a$ e $a \cdot 1 = 1 \cdot a = a$.

(v) Distributiva com relação à adição:

Para $a, b, c \in \mathbb{N}$, $a(b+c) = ab + ac$.

Observemos que a propriedade (i) permite adicionar um dado número natural a ambos os membros de uma igualdade, bem como multiplicar ambos os membros por um número natural, sem alterar a validade da equação inicial.

Vamos assumir em $\mathbb{N}$ as seguintes propriedades:

(vi) **Integridade**: Dados $a, b \in \mathbb{N}^*$, tem-se que $ab \in \mathbb{N}^*$. Equivalentemente, pela formulação contrapositiva

$$\forall a, b \in \mathbb{N}, \quad ab = 0 \implies a = 0 \text{ ou } b = 0.$$

(vii) **Propriedade da Tricotomia**: Das seguintes, uma e somente uma das propriedades é verificada:

1) $a = b$;

2) $\exists\, c \in \mathbb{N}^*,\ b = a + c$;

3) $\exists\, c \in \mathbb{N}^*,\ a = b + c$.

Sempre que a propriedade 2) é verificada, dizemos que $a < b$ (lê-se "a menor que b"), ou, equivalentemente, que $b > a$ (lê-se "b maior que a). Desse modo, pela propriedade da Tricotomia, exatamente uma das seguintes propriedades é verificada:

- $a = b$;
- $a < b$;
- $a > b$.

Das propriedades acima, decorrem as seguintes proposições.

Proposição 1.1

$a \cdot 0 = 0$, para todo $a \in \mathbb{N}$.

Demonstração. Suponhamos, por absurdo, que $a \cdot 0 \neq 0$. Notemos que:

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

Mas, por hipótese $a \cdot 0 \in \mathbb{N}^*$ e, assim, $a \cdot 0 > a \cdot 0$, o que é uma contradição. Logo, $a \cdot 0 = 0$. □

Proposição 1.2

A relação "menor do que" é transitiva, isto é, $\forall a, b, c \in \mathbb{N},\ a < b$ e $b < c \implies a < c$.

Demonstração. Dados $a < b$ e $b < c$, então existem $d, f \in \mathbb{N}^*$, tais que $b = a + d$ e $c = b + f$. Assim, aplicando a associatividade da adição, segue que

$$c = b + f = (a + d) + f = a + (d + f).$$

Como $d + f \in \mathbb{N}^*$, segue que $c > a$. □

Proposição 1.3

A adição é compatível e cancelativa com respeito à relação "menor do que", isto é, $\forall a, b, c \in \mathbb{N},\ a < b \iff a + c < b + c$.

Demonstração. ($\Rightarrow$) Suponhamos que $a < b$. Logo, existe $d \in \mathbb{N}^*$, tal que $b = a + d$. Somando c a ambos os lados desta equação, temos

$$b + c = (a + d) + c = (a + c) + d.$$

Como $d \in \mathbb{N}^*$, podemos concluir que $a + c < b + c$.

($\Leftarrow$) Reciprocamente, suponhamos que $a + c < b + c$. Pela propriedade da tricotomia, temos as seguintes possibilidades:

- $a = b$, implicando que $a + c = b + c$, o que contradiz a hipótese $a + c < b + c$;
- $a > b$, e portanto $a = b + k$ para algum $k \in \mathbb{N}^*$. Somando c a ambos os lados, obtemos $a + c = (b + k) + c = (b + c) + k$. Como $k \in \mathbb{N}^*$, isso implica que $a + c > b + c$, o que contradiz a hipótese $a + c < b + c$.

Dessa forma, a única possibilidade restante é $a < b$. □

Proposição 1.4

A multiplicação é compatível e cancelativa com respeito à relação "menor do que", isto é, $\forall a, b \in \mathbb{N}, \forall c \in \mathbb{N}^*,\ a < b \iff ac < bc$.

Demonstração. ($\Rightarrow$) Suponhamos que $a < b$. Logo, existe $d \in \mathbb{N}^*$, tal que $b = a + d$. Multiplicando ambos os lados da equação por c, e aplicando a distributividade em relação à adição, temos

$$bc = (a + d)c = ac + dc.$$

Como $dc \in \mathbb{N}^*$, podemos concluir que $ac < bc$.

($\Leftarrow$) Reciprocamente, suponhamos que $ac < bc$. Pela propriedade da tricotomia, temos as seguintes possibilidades:

- $a = b$, implicando que $ac = bc$, o que contradiz a hipótese $ac < bc$;
- $a > b$, e portanto $a = b + k$ para algum $k \in \mathbb{N}^*$. Multiplicando ambos os lados por c, obtemos $ac = (b + k)c = bc + kc$. Como $kc \in \mathbb{N}^*$, isso implica que $ac > bc$, o que contradiz a hipótese $ac < bc$.

Dessa forma, a única possibilidade restante é $a < b$. □

Proposição 1.5

A adição é compatível e cancelativa com respeito à igualdade, isto é, $\forall a, b, c \in \mathbb{N},\ a = b \iff a + c = b + c$.

Demonstração. A implicação $a = b \Rightarrow a + c = b + c$ é consequência direta do fato da adição ser bem definida.

Reciprocamente, suponhamos que $a + c = b + c$. Neste caso, temos as seguintes possibilidades:

- $a < b$, e pela Proposição 1.3, temos $a + c < b + c$, o que é uma contradição;
- $b < a$, pelo mesmo raciocínio acima, temos $b + c < a + c$, o que também é uma contradição.

Assim, a única alternativa válida é $a = b$. □

Proposição 1.6

A multiplicação é compatível e cancelativa com respeito à igualdade, isto é, $\forall a, b, c \in \mathbb{N},\ a = b \iff a \cdot c = b \cdot c$.

Demonstração. A implicação $a = b \Rightarrow ac = bc$ é consequência direta do fato da multiplicação ser bem definida.

Reciprocamente, suponhamos que $ac = bc$. Neste caso, temos as seguintes possibilidades:

- $a < b$, e pela Proposição 1.4, temos $ac < bc$, o que é contradição;
- $b < a$, pelo mesmo raciocínio acima, temos $bc < ac$, o que também é uma contradição.

Portanto, a única possibilidade é $a = b$. □

Observamos que as relações dadas por $<$ (menor que) e $>$ (maior que) não são relações de ordem, uma vez que não são reflexivas. Entretanto, a partir delas podemos obter as seguintes relações de ordem: $a \geq b$ (lê-se a maior ou igual a b) e $a \leq b$ (lê-se a menor ou igual a b). Observe que estas são, de fato, relações de ordem, uma vez que:

1) São reflexivas: $\forall a, a \geq a$ e $a \leq a$;
2) São anti-simétricas: $\forall a, b,\ a \leq b$ e $b \leq a \Rightarrow a = b$ (reciprocamente, $\forall a, b,\ a \geq b$ e $b \geq a \Rightarrow a = b$);
3) São transitivas: $\forall a, b, c,\ a \leq b$ e $b \leq c \Rightarrow a \leq c$ (reciprocamente, $\forall a, b, c,\ a \geq b$ e $b \geq c \Rightarrow a \geq c$).

1.2 Subtração

Dados dois números naturais a e b, sabemos que $a \leq b$ significa que existe um número natural c, tal que $b = a + c$. Desse modo, o número c é escrito como $c = b - a$.

O número c é, portanto, o resultado da subtração $b - a$. Logo, definimos

$$c = b - a \iff b = a + c.$$

Observemos que esta operação nem sempre é possível em $\mathbb{N}$. De fato, $b - a$ só existe se $b \geq a$.

Além disso, $a-a=0$, para todo $a\in\mathbb{N}$, e, por definição, $(b-a)+a=b$. Veremos também que a subtração não é associativa. Considere o exemplo abaixo.

Exemplo 1.1

$$7-5=2,\quad 2-1=1,\quad 5-1=4,\quad 7-4=3$$
$$(7-5)-1=2-1=1,\quad 7-(5-1)=7-4=3$$

Na Proposição abaixo mostramos que a multiplicação é distributiva com relação a subtração.

Proposição 1.7

Sejam $a,b,c\in\mathbb{N}$. Se $a\leq b$, então

$$c(b-a)=cb-ca.$$

Demonstração. Observemos que, se $a\leq b$, então $b-a$ está bem definido, e $cb-ca$ também está bem definido (pois $b\geq a \;\Rightarrow\; cb\geq ca$).

Suponhamos que $b-a=d$, então $b=a+d$ e $c(b-a)=cd$. Por outro lado,

$$cb-ca=c(a+d)-ca=ca+cd-ca=cd.$$

Logo

$$c(b-a)=cb-ca=cd,$$

o que conclui o resultado. □

1.3 Princípio de Indução Matemática

As propriedades apresentadas até aqui não são suficientes para caracterizar os números naturais, pois não são exclusivas deles. Por exemplo, tanto os números racionais quanto os reais não negativos possuem todas as propriedades mencionadas. No entanto, há uma propriedade exclusiva dos números naturais: o Axioma da Indução.

viii) **Axioma da Indução:** Seja S um subconjunto de $\mathbb{N}$, tal que:

1) $0\in S$.

2) S é fechado com respeito à operação de "somar 1" a seus elementos, ou seja, $\forall n \in S \Rightarrow n+1 \in S$.

Então, $S = \mathbb{N}$.

Se $A \subset \mathbb{N}$ e $a \in \mathbb{N}$, usaremos a seguinte notação

$$a + A = \{a + x \mid x \in A\}.$$

Podemos verificar que

$$a + \mathbb{N} = \{m \in \mathbb{N} \mid m \geq a\}.$$

Como consequência do Axioma da Indução, obtemos o Teorema da Indução Matemática, um importante instrumento para provar teoremas e resultados importantes em $\mathbb{N}$.

Teorema 1.1: Princípio da Indução Matemática

Seja $a \in \mathbb{N}$ e seja $p(n)$ uma sentença aberta em n. Suponhamos que

i) $p(a)$ é verdade; e

ii) $\forall n \geq a$, $p(n) \Rightarrow p(n+1)$ é verdade.

Então, $p(n)$ é verdade para todo $n \geq a$.

Demonstração. Seja $\mathcal{V} = \{n \in \mathbb{N} \mid p(n)\}$, ou seja, $\mathcal{V}$ é um conjunto de números naturais para os quais a sentença $p(n)$ é verdadeira. Consideremos o conjunto

$$S = \{m \in \mathbb{N} \mid a + m \in \mathcal{V}\},$$

que trivialmente satisfaz $a + S \subseteq \mathcal{V}$.

Pela hipótese i), temos que $a + 0 = a \in \mathcal{V}$, portanto $0 \in S$.

Além disso, se $m \in S$, então $a + m \in \mathcal{V}$. Pela hipótese ii), isso implica que $a + (m+1) \in \mathcal{V}$, logo $m + 1 \in S$. Assim, pelo Axioma da Indução, concluímos que $S = \mathbb{N}$. Portanto,

$$\{m \in \mathbb{N} \mid m \geq a\} = a + \mathbb{N} \subseteq \mathcal{V},$$

o que prova o resultado. □

1.4 Propriedade da Boa Ordem

Seja S um subconjunto de $\mathbb{N}$. Um número natural a é chamado de menor elemento de S se satisfaz as seguintes propriedades:

1. $a \in S$;

2. $\forall n \in S, a \leq n$.

A propriedade da tricotomia garante a unicidade do menor elemento. De fato, notemos que, se a e a' são ambos menores elementos de S, teremos $a \leq a'$ e $a' \leq a$, portanto, $a = a'$.

Além disso, o menor elemento de S, quando existente, é denotado por $\min S$.

Note que o conjunto $\mathbb{N}^*$ é limitado inferiormente por 1. Além disso, demonstramos abaixo que todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento. Esta propriedade diferencia este conjunto dos números inteiros, dos racionais e reais. Observemos, por exemplo, que o intervalo $[(0,1) \cap \mathbb{Q}]$ é limitado tanto em $\mathbb{Q}$, quanto em $\mathbb{R}$, no entanto, não apresenta menor elemento em nenhum dos dois conjuntos.

Teorema 1.2: Propriedade da Boa Ordem

Todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.

Demonstração. A prova será feita por contradição. Suponhamos que S seja um subconjunto não vazio de $\mathbb{N}$, que S não possua um menor elemento. Vamos mostrar que isso implica que S é vazio, o que contradiz a hipótese inicial.

Definimos o conjunto $I_n = \{k \in \mathbb{N} \mid k \leq n\}$ e a sentença $P(n) : I_n \subset T$, onde T é o complemento de S em relação a $\mathbb{N}$, isto é, $T = \mathbb{N} \setminus S$. Queremos mostrar que $T = \mathbb{N}$.

Primeiro, observemos que $0 \leq n$ para todo $n \in \mathbb{N}$. Portanto, $0 \in T$, pois, caso contrário, 0 estaria em S e seria um menor elemento de S, o que contradiz nossa suposição. Assim, $P(0)$ é verdadeiro.

Agora, suponhamos que $P(n)$ seja verdadeira para algum $n \in \mathbb{N}$. Isso significa que $I_n \subset T$. Queremos provar que $P(n+1)$ também é verdadeiro, ou seja, que $I_{n+1} \subset T$. Se $n+1 \in S$, então, como nenhum elemento de I_n está em S (por hipótese de indução), $n+1$ seria o menor elemento de S, o que contradiz nossa suposição de que S não possui um menor elemento. Portanto, $n+1 \notin S$ e, desta forma $n+1 \in T$. Logo,

$$I_{n+1} = I_n \cup \{n+1\} \subset T.$$

Portanto, $P(n+1)$ é verdadeira. Pelo Princípio da Indução Matemática, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$, o que implica que $\mathbb{N} \subset T$. Como $T \subset \mathbb{N}$ por definição, concluímos que $T = \mathbb{N}$.

Concluímos dessa forma que S é vazio, o que contradiz nossa hipótese inicial de que S é não vazio. Portanto, nossa suposição de que S não possui um menor elemento é falsa. Logo, S possui um menor elemento, como queríamos demonstrar. □

Corolário 1.1

Não existe nenhum número natural n, tal que $0 < n < 1$.

Demonstração. O enunciado acima é equivalente a dizer que $p(n) : n > 0 \Rightarrow n \geq 1$ é verdadeiro para todo $n \in \mathbb{N}$.

Como $0 > 0$ é falso, temos que $p(0) : 0 > 0 \Rightarrow 0 \geq 1$ é verdadeiro. Por outro lado, observemos que $p(n+1) : n+1 > 0 \Rightarrow n+1 \geq 1$ é verdadeiro para todo $n \in \mathbb{N}$. De fato, $n+1 \geq 1$ é verdadeiro para todo $n \in \mathbb{N}$, pois isso implica, pela lei do cancelamento, que $n \geq 0$, o que é sempre verdadeiro no conjunto dos naturais.

Assim, o resultado decorre do Princípio da Indução Matemática. □

Corolário 1.2

Dado um número natural n qualquer, não existe nenhum número natural m tal que $n < m < n+1$.

Demonstração. Suponha, por absurdo, que exista um número natural m com $n < m < n+1$. Logo, existiria um número $k \in \mathbb{N}^*$ tal que $n + k = m < n + 1$, o que, pela Proposição 1.3, implicaria que $0 < k < 1$, o que é uma contradição, tendo em vista o Corolário anterior.

□

Corolário 1.3

Sejam $a, b \in \mathbb{N}$. Se $a \cdot b = 1$, então $a = b = 1$.

Demonstração. Observe que $a \neq 0$ e $b \neq 0$, pois caso contrário $a \cdot b = 0$. Por outro lado, se $a \neq 1$ e $b \neq 1$, então, pelo Corolário anterior, segue-se que $a > 1$ e $b > 1$. Logo, $a \cdot b > b > 1$, o que é um absurdo. Portanto, $a = 1$ ou $b = 1$. Qualquer uma dessas possibilidades implica $a = b = 1$. □

A prova por indução pode ser aplicada na resolução de diversos problemas envolvendo números naturais, contribuindo também com o estudo de divisibilidade, abordado no próximo capítulo.

A seguir apresentamos uma variante do Teorema de Indução Matemática, muito útil para validar relações de recorrência.

Teorema 1.3: Princípio de Indução Matemática, 2ª Forma

Seja $p(n)$ uma sentença aberta, tal que

i) $p(a)$ é verdadeira, e

ii) $\forall n \geq a$, $p(a)$ e $p(a+1)$ e $\cdots$ e $p(n) \Rightarrow p(n+1)$.

Então, $p(n)$ é verdadeira para todo $n \geq a$.

Demonstração. A prova será feita por contradição. Definamos o conjunto:

$$V = \{n \in a + \mathbb{N};\ p(n)\}.$$

Queremos provar que o conjunto $W = (a+\mathbb{N}) \backslash V$ é vazio. Suponha, por contradição, que W não seja vazio. Pela Propriedade da Boa Ordem, W possui um menor elemento, digamos k. Como sabemos que $a \notin W$ (por i)), segue que $k = a + n$ para algum $n > a$. Portanto, $a, a+1, \ldots, k-1 \notin W$; ou seja, $a, a+1, \ldots, k-1 \in V$. Pela hipótese de indução (ii), temos que $k = k-1+1 \in V$, o que contradiz o fato de $k \in W$.

Assim, W deve ser vazio, e portanto, $p(n)$ é verdadeira para todo $n \geq a$. □

CAPÍTULO 2

Divisão nos Naturais

Neste Capítulo, iremos explorar a divisão dos números naturais. Apesar de nem sempre existir uma relação de divisibilidade entre dois números, há a possibilidade de efetuar uma divisão com resto pequeno, a qual é denominada divisão euclidiana. Esta operação é sempre possível, e é responsável por inúmeras propriedades envolvendo números naturais, as quais exploraremos ao longo deste Capítulo.

2.1 Divisibilidade

Diremos que $a \mid b$ (lê-se "a divide b") se existir um e somente um $c \in \mathbb{N}$, tal que $b = ac$. Este valor c é dado pelo quociente $\frac{b}{a}$. Caso não exista este valor c, dizemos que $a \nmid b$ (lê-se "a não divide b").

Exemplo 2.1

$$1 \mid 0, \quad 3 \mid 0, \quad 5 \mid 5, \quad 6 \mid 6, \quad 1 \mid 4, \quad 3 \mid 12.$$

Desse modo, em cada relação acima, temos

a) $0 = 1 \cdot 0$ isto é: $c = 0 = \frac{0}{1}$;

b) $0 = 3 \cdot 0$ isto é: $c = 0 = \frac{0}{3}$;

c) $5 = 5 \cdot 1$ isto é: $c = 1 = \frac{5}{5}$;

d) $6 = 2 \cdot 3$ isto é: $c = 3 = \frac{6}{2}$;

e) $4 = 1 \cdot 4$ isto é: $c = 4 = \frac{4}{1}$;

f) $12 = 3 \cdot 4$ isto é: $c = 4 = \dfrac{12}{3}$.

A seguir, apresentamos algumas propriedades de divisibilidade de números naturais.

Proposição 2.1

Sejam $a, b \in \mathbb{N}^*$ e $c \in \mathbb{N}$. Então

i) $1 \mid c$, $a \mid a$ e $a \mid 0$.

ii) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração. O item i) segue diretamente das igualdades $c = 1 \cdot c$, $a = a \cdot 1$ e $0 = a \cdot 0$.

Para mostrarmos o item ii), observemos que, da definição de divisibilidade, temos:

- $a \mid b \Rightarrow \exists\ d \in \mathbb{N}$, tal que $b = ad$;
- $b \mid c \Rightarrow \exists\ e \in \mathbb{N}$, tal que $c = be$.

Assim, $c = be = (ad)e = a(de)$, isto é, $a \mid c$. □

Proposição 2.2

Se $a, b, c, d \in \mathbb{N}$, com $a \neq 0$ e $c \neq 0$, então

$$a \mid b \text{ e } c \mid d \Rightarrow ac \mid bd.$$

Demonstração. Para mostrarmos a proposição, observemos que pela definição de divisibilidade,

- $a \mid b \Rightarrow \exists\ m \in \mathbb{N}$, tal que $b = am$;
- $c \mid d \Rightarrow \exists\ n \in \mathbb{N}$, tal que $d = cn$.

Assim, combinando essas expressões, temos

$$bd = (am)(cn) = a(cn)m = ac(nm).$$

Isto é, $ac \mid bd$. □

Proposição 2.3

Sejam $a, b, c \in \mathbb{N}$, com $a \neq 0$, tais que $a \mid (b + c)$. Então $a \mid b \Leftrightarrow a \mid c$.

Demonstração. Consideremos as duas implicações separadamente.

($\Rightarrow$) Suponhamos que $a \mid b$. Então existe $k \in \mathbb{N}$, tal que $b = ak$. Como $a \mid (b+c)$, existe $m \in \mathbb{N}$, tal que $b + c = am$. Substituindo $b = ak$ na expressão $b + c = am$, temos $ak + c = am$. Assim, $c = am - ak = a(m-k)$.

Portanto, existe um natural $n = m - k$ tal que $c = an$, logo $a \mid c$.

($\Leftarrow$) Suponhamos que $a \mid c$. Então existe $n \in \mathbb{N}$, tal que $c = an$. Como $a \mid (b+c)$, existe $m \in \mathbb{N}$, tal que $b + c = am$. Substituindo $c = an$ na expressão $b + c = am$, temos $b + an = am$. Assim, $b = am - an = a(m-n)$.

Portanto, existe um natural $k = m - n$ tal que $b = ak$, logo $a \mid b$.

Concluímos que $a \mid b \Leftrightarrow a \mid c$. □

Proposição 2.4

Sejam $a, b, c \in \mathbb{N}$, com $a \neq 0$ e $b \geq c$, tais que $a \mid (b-c)$. Então $a \mid b \Leftrightarrow a \mid c$.

Demonstração. Consideremos as duas implicações separadamente.

($\Rightarrow$) Suponhamos que $a \mid b$. Então existe $k \in \mathbb{N}$, tal que $b = ak$. Como $a \mid (b-c)$, existe $m \in \mathbb{N}$, tal que $b - c = am$. Substituindo $b = ak$ na expressão $b - c = am$, temos $ak - c = am$. Assim, $c = ak - am = a(k-m)$.

Portanto, existe um natural $n = k - m$ tal que $c = an$, logo $a \mid c$.

($\Leftarrow$) Suponhamos que $a \mid c$. Então existe $n \in \mathbb{N}$, tal que $c = an$. Como $a \mid (b-c)$, existe $m \in \mathbb{N}$ tal que $b - c = am$. Substituindo $c = an$ na expressão $b - c = am$, temos $b - an = am$. Assim, $b = am + an = a(m+n)$.

Portanto, existe um natural $k = m + n$ tal que $b = ak$, logo $a \mid b$.

Concluímos que $a \mid b \Leftrightarrow a \mid c$. □

Proposição 2.5

Se $a, b, c \in \mathbb{N}$, com $a \neq 0$, e $x, y \in \mathbb{N}$ são tais que $a \mid b$ e $a \mid c$, então $a \mid (xb + yc)$; e se $xb \geq yc$, então $a \mid (xb - yc)$.

Demonstração. Vamos usar a definição de divisibilidade para provar a proposição.

1. Como $a \mid b$ e $a \mid c$, existem $k, l \in \mathbb{N}$ tais que $b = ak$ e $c = al$. Então, podemos escrever $(xb + yc)$

como $x(ak)+y(al)=a(xk+yl)$. Como $xk+yl$ é um número natural, segue que $a \mid (xb+yc)$.

2. Agora, se $xb \geq yc$, então $xb-yc$ é não negativo. Da mesma forma que no caso anterior, podemos escrever $xb-yc$ como $x(ak)-y(al)=a(xk-yl)$. Como $xk-yl$ também é um número natural, concluímos que $a \mid (xb-yc)$.

O que prova o resultado. □

Proposição 2.6

Dados $a, b \in \mathbb{N}^*$, temos que $a \mid b \Rightarrow a \leq b$.

Demonstração. Como $a \mid b$, então, por definição, existe um natural $k \in \mathbb{N}^*$ tal que $b = ak$.

Como a e k são ambos números naturais não nulos ($a, k \geq 1$), podemos afirmar que:

$$b = ak \geq a \cdot 1 = a.$$

Portanto, temos que $b \geq a$, ou seja, $a \leq b$. □

Observação 2.1

a) Em particular, se $a \mid 1$, então $a \leq 1$ e, portanto, $a = 1$;

b) A recíproca da Proposição acima não é verdadeira. Observemos que, por exemplo, $5 > 2$ e, no entanto, 2 não divide 5.

Notemos que a relação de divisibilidade em $\mathbb{N}^*$ é uma relação de ordem, pois satisfazem as propriedades listadas abaixo.

1. é reflexiva: $\forall a \in \mathbb{N}, a \mid a$,
2. é transitiva: se $a \mid b$ e $b \mid c$, então $a \mid c$ (segue da Proposição 2.1 item ii),
3. é anti-simétrica: se $a \mid b$ e $b \mid a$, então $a = b$ (segue da Proposição 2.6).

Segue uma aplicação de divisibilidade:

Exemplo 2.2

Prove que $11^{n+2} + 12^{2n+1}$ é divisível por 133, para qualquer número natural n.

Demonstração. Utilizaremos a prova por indução. Queremos mostrar que $11^{n+2} + 12^{2n+1} = 133t$, $t \in \mathbb{N}$. Para $n = 0$, temos,

$$11^{0+2} + 12^{2\cdot 0+1} = 11^2 + 12^1 = 121 + 12 = 133 = 133 \cdot 1,$$

logo, é divisível por 133.

Suponhamos que a igualdade seja válida para algum $k \in \mathbb{N}$, isto é,

$$11^{k+2} + 12^{2k+1} = 133t, \quad t \in \mathbb{Z}.$$

Mostraremos que esta continua válida para $n = k + 1$. De fato, notemos que

$$\begin{aligned} 11^{(k+1)+2} + 12^{2(k+1)+1} &= 11^{(k+2)+1} + 12^{(2k+1)+2} \\ &= 11^{k+2} \cdot 11 + 12^{2k+1} \cdot 12^2 \\ &= 11^{k+2} \cdot 11 + 12^{2k+1} \cdot (11 + 133) \\ &= 11^{k+2} \cdot 11 + 12^{2k+1} \cdot 11 + 12^{2k+1} \cdot 133 \\ &= (11^{k+2} + 12^{2k+1}) \cdot 11 + 12^{2k+1} \cdot 133. \end{aligned}$$

Mas, por hipótese de indução

$$11^{k+2} + 12^{2k+1} = 133t,$$

e portanto,

$$11^{(k+1)+2} + 12^{2(k+1)+1} = 133t \cdot 11 + 12^{2k+1} \cdot 133 = (11t + 12^{2k+1}) \cdot 133.$$

Concluímos, pelo Princípio de Indução Finita, que $11^{n+2} + 12^{2n+1}$ é divisível por 133, para qualquer número natural n. □

As proposições a seguir são úteis para a resolução de alguns exercícios de divisibilidade.

Proposição 2.7

Sejam $a, b, n \in \mathbb{N}$, com $a > b > 0$. Então $a - b$ divide $a^n - b^n$.

Demonstração. A prova segue por indução sobre n. Para $n = 0$, segue que $a - b$ divide $a^0 - b^0 = 0$, logo a afirmação é verdadeira.

Suponhamos que a afirmação seja válida para $n = k > 0$, isto é: $a - b \mid a^k - b^k$. Queremos mostrar

que a afirmação continua válida para $n = k+1$. De fato, notemos que

$$a^{k+1} - b^{k+1} = aa^k - ba^k + ba^k - bb^k = (a-b)a^k + b(a^k - b^k).$$

Como $a-b \mid a-b$ e, por hipótese de indução, $a-b \mid a^k - b^k$ e, da Proposição 2.5, segue que $a-b \mid a^{k+1} - b^{k+1}$. Logo, segue pelo princípio de indução finita que $a-b$ divide $a^n - b^n$, para todo $n \in \mathbb{N}$

□

Proposição 2.8

Sejam $a, b, n \in \mathbb{N}$, com $a+b \neq 0$. Então $a+b$ divide $a^{2n+1} + b^{2n+1}$.

Demonstração. A prova segue por indução sobre n. Para $n = 0$, temos que $a+b$ divide $a^1 + b^1 = a+b$, o que é trivialmente verdadeiro.

Suponhamos que a afirmação seja válida para $n = k > 0$, isto é, $a+b$ divide $a^{2k+1} + b^{2k+1}$. Queremos mostrar que a afirmação continua válida para $n = k+1$. De fato, notemos que

$$\begin{aligned} a^{2(k+1)+1} + b^{2(k+1)+1} &= a^2a^{2k+1} - b^2a^{2k+1} + b^2a^{2k+1} + b^2b^{2k+1} \\ &= (a^2 - b^2)(a^{2k+1}) + b^2(a^{2k+1} + b^{2k+1}). \end{aligned}$$

Como $a+b$ divide $a^{2k+1} + b^{2k+1}$ (hipótese de indução), $a+b$ divide $a^2 - b^2 = (a-b)(a+b)$ e, da Proposição 2.5, concluímos que $a+b$ divide $a^{2(k+1)+1} + b^{2(k+1)+1}$.

Logo, pelo princípio de indução finita, concluímos que $a+b$ divide $a^{2n+1} + b^{2n+1}$ para todo $n \in \mathbb{N}$ com $a+b \neq 0$.

□

Proposição 2.9

Sejam $a, b, n \in \mathbb{N}$, com $a > b > 0$. Então $a+b$ divide $a^{2n} - b^{2n}$.

Demonstração. A prova segue por indução sobre n. Para $n = 0$, temos que $a+b$ divide $a^0 - b^0 = 0$, o que é trivialmente verdadeiro.

Suponhamos que a afirmação seja válida para $n = k > 0$, isto é, $a+b$ divide $a^{2k} - b^{2k}$. Queremos

mostrar que a afirmação continua válida para $n = k+1$. De fato, notemos que

$$a^{2(k+1)} - b^{2(k+1)} = a^2a^{2k} - b^2a^{2k} + b^2a^{2k} - b^2b^{2k} = (a^2 - b^2)(a^{2k}) + b^2(a^{2k} - b^{2k}).$$

Como $a+b$ divide $a^{2k}-b^{2k}$ (hipótese de indução), $a+b$ divide a^2-b^2 e, da Proposição 2.5, concluímos que $a+b$ divide $a^{2(k+1)} - b^{2(k+1)}$.

Logo, pelo princípio de indução finita, concluímos que $a+b$ divide $a^{2n} - b^{2n}$ para todo $n \in \mathbb{N}$ com $a > b > 0$. □

Vejamos no exemplo abaixo alguns exercícios resolvidos que utilizam as proposições anteriores.

Exemplo 2.3

Mostre que:

a) $9 \mid 10^n - 1$

b) $17 \mid 10^{2n+1} + 7^{2n+1}$

Resolução:

a) Sabemos, pela Proposição 2.7, que $a - b \mid a^n - b^n$. Assim:

$$9 = (10-1) \mid (10^n - 1^n) = 10^n - 1.$$

Portanto, $9 \mid 10^n - 1$.

b) Sabemos, pela Proposição 2.8, que $a + b \mid a^{2n+1} + b^{2n+1}$. Assim:

$$17 = (10+7) \mid (10^{2n+1} + 7^{2n+1}).$$

Portanto, $17 \mid 10^{2n+1} + 7^{2n+1}$.

2.2 Divisão Euclidiana

Euclides, em sua obra *Os Elementos*, utiliza o fato que sempre é possível realizar a divisão de b por a, com resto. Neste capítulo, apresentaremos e discutiremos o Teorema denominado Divisão Euclidiana, que é a base fundamental da Teoria dos Números.

2.3 Divisão Euclidiana

A seguir, apresentaremos o Teorema da Divisão Euclidiana:

Teorema 2.1: Divisão Euclidiana

Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais q e r, tais que

$$b = aq + r, \quad \text{com } 0 \leq r < a.$$

Demonstração. Sejam $b > a > 0$ e S o conjunto dos números naturais da forma:

$$S = \{b, b-a, b-2a, \ldots, b-na\}.$$

Pelo Teorema 1.2 (Propriedade da Boa Ordem), S tem um menor elemento, que denotamos por $r = b - qa$. Devemos provar que $0 \leq r < a$.

Notemos que, se $a \mid b$, então $r = 0$ e, portanto, $0 = r < a$. Consideremos então o caso em que $a \nmid b$. Suponhamos, por absurdo, que $r \geq a$. Neste caso, existe um número natural c, tal que $0 \leq c < r$ e $r = c + a$. Assim, temos:

$$r = c + a = b - qa.$$

Portanto,

$$c = b - (q+1)a.$$

Isso implica que $c \in S$ e $c < r$, o que contradiz o fato de r ser o menor elemento de S. Portanto, $r < a$, como desejado. Assim, provamos que existem q e r, tais que $b = a \cdot q + r$ com $0 \leq r < a$.

Agora, vamos provar a unicidade de q e r. Suponhamos que existam dois pares (q, r) e (q', r') que satisfaçam as condições do teorema. Isto é,

$$b = aq + r \quad \text{e} \quad b = aq' + r'.$$

Dessas duas igualdades, obtemos

$$aq + r = aq' + r' \implies aq - aq' = r' - r \implies a(q - q') = r' - r.$$

Por hipótese, r e r' satisfazem $0 \leq r, r' < a$. Supondo que r e r' sejam distintos, podemos considerar,

sem perda de generalidade, que $r' > r$. Então, temos

$$0 < r' - r < a.$$

Como $r' - r = a(q - q')$ e a é um número natural positivo, a diferença $r' - r$ deve ser pelo menos a se $q \neq q'$. Isto é um absurdo pois $r' - r < a$.

Portanto, pela propriedade da tricotomia, a única possibilidade é $r' = r$. Substituindo $r = r'$ na igualdade $a(q - q') = r' - r$, e pela propriedade da integridade, obtemos:

$$a(q - q') = 0 \implies q = q'.$$

Assim, concluímos que os números q e r são únicos, o que completa a demonstração. □

Nas condições do Teorema 2.1, os números q e r são, respectivamente, *quociente* e *resto* na divisão de b por a. Além disso, $r = 0$ se, e somente se, se $a \mid b$.

A demonstração do teorema acima, fornece um algoritmo para obtermos o quociente e o resto da divisão de b por a. Tal procedimento consiste em subtrair a de b repetidamente até obtermos um resto $r < a$. O quociente é dado pela quantidade de vezes que repetimos o processo. Observemos a utilização deste algoritmo no exemplo a seguir.

Exemplo 2.4: Divisão de 14 por 3

Vamos achar o quociente e o resto na divisão de 14 por 3.

Solução: Vamos utilizar o algoritmo apresentado acima:

$$\begin{aligned} 14 - 3 &= 11, \\ 11 - 3 &= 8, \\ 8 - 3 &= 5, \\ 5 - 3 &= 2 < 3. \end{aligned}$$

Logo, $r = 2$ e $q = 4$, pois repetimos o processo quatro vezes para obtermos $r < 3$.

No exemplo a seguir, apresentamos um resultado que será utilizado para o estudo do critério de divisibilidade por 3.

Exemplo 2.5

Vamos mostrar, por indução, que 10^n deixa sempre resto 1 na divisão por 3.

Solução: Em outras palavras, queremos provar que

$$10^n = 3q + 1,$$

para algum natural q. Considerando $n = 0$, temos $10^0 = 1 = 3 \cdot 0 + 1$. Portanto, a afirmação é verdadeira para $n = 0$.

Suponhamos que a afirmação seja verdadeira para um natural $n = k$, isto é, $10^k = 3q + 1$ para algum natural q. Queremos mostrar que a afirmação também é verdadeira para $n = k + 1$.

De fato, observemos que

$$10^{k+1} = 10 \cdot 10^k.$$

Pela hipótese de indução, sabemos que $10^k = 3q+1$. Substituindo isso na expressão acima, obtemos:

$$10^{k+1} = 10(3q + 1) = 10 \cdot 3q + 10 \cdot 1 = 30q + 10 = 3(10q + 3) + 1$$

Notemos que $10q + 3 \in \mathbb{N}$, implicando que a afirmação é verdadeira para $n = k + 1$.

Portanto, pelo princípio da indução finita, a afirmação é verdadeira para todo n natural.

Observemos que, como $10^n = 3q + 1$, então $10^n - 1 = 3q$. Ou seja, $3 \mid 10^n - 1$. Utilizaremos este fato na demonstração do critério de divisibilidade por 3.

CAPÍTULO 3

Sistema de Numeração Decimal

Neste capítulo, faremos um estudo sobre o nosso atual sistema de numeração decimal e a representação de números naturais. Este estudo se faz necessário para a compreensão dos critérios de divisibilidade e de outras propriedades da operação de divisão de dois números naturais. Hefez [4] destaca que o nosso atual sistema de numeração é uma variante do sistema sexagesimal babilônico, utilizado pelos babilônios por volta de 1700 anos antes de Cristo. O sistema de numeração decimal, desenvolvido na China e na Índia, se espalhou pelo Oriente Médio, tendo grande aceitação no mundo árabe.

3.1 Sistema de Numeração Decimal

O sistema decimal é composto pela sequência:

$$1, 2, 3, 4, 5, 6, 7, 8, 9,$$

com o acréscimo do símbolo "0" (zero), que representa a ausência de algarismo. Como é composto por dez algarismos, recebe o nome de sistema decimal.

Este sistema é chamado de posicional, pois, em sua representação, a posição do algarismo determina a sua ordem de grandeza. Na representação decimal, da direita para a esquerda, o primeiro algarismo tem peso 1, o segundo tem peso 10, o terceiro tem peso 100 e assim por diante, de modo que podemos representar um número qualquer em potências de base 10.

Por exemplo, o número 20423 pode ser representado do seguinte modo:

$$2 \cdot 10^4 + 0 \cdot 10^3 + 4 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$$

Cada terna de ordens da esquerda para a direita compõe uma classe, como podemos observar na tabela abaixo:

Classe	Ordem	Nome
Classe das Unidades	1ª ordem	unidades
	2ª ordem	dezenas
	3ª ordem	centenas
Classe do Milhar	4ª ordem	unidades de milhar
	5ª ordem	dezenas de milhar
	6ª ordem	centenas de milhar
Classe do Milhão	7ª ordem	unidades de milhão
	8ª ordem	dezenas de milhão
	9ª ordem	centenas de milhão

Tabela 3.1: Classificação das Ordens de Grandezas no Sistema Decimal.

Os sistemas de numeração posicionais como os babilônicos e binários (de base 2), o de base 10, entre outros, baseiam-se no seguinte resultado, que é uma aplicação da divisão euclidiana.

Teorema 3.1

Dados $a, b \in \mathbb{N}$, com $b > 1$, existem números naturais $a_0, a_1, \ldots, a_n$ menores do que b, univocamente determinados, tais que

$$a = a_0 + a_1 b + a_2 b^2 + \ldots + a_n b^n.$$

Demonstração. Vamos demonstrar o resultado usando o Teorema 1.2 (Princípio de Indução Matemática na 2ª forma) sobre a.

Se $a = 0$ ou $a = 1$, basta tomar $n = 0$ e $a_0 = a$.

Suponhamos que o resultado seja válido para todo natural menor que a. Mostraremos que isto implica na validade do resultado para a. De fato, pela divisão euclidiana, existem naturais q e r tais que

$$a = bq + r, \quad \text{com} \quad 0 \leq r < b.$$

Notemos que $q < a$, pois sendo $a = bq + r$, então $a \geq bq$. Como $b > 1$, portanto $b \cdot q > 1 \cdot q = q$. Assim, $a \geq bq > q \implies a > q$. Pela hipótese de indução, existem números naturais n' e $c_0, c_1, \ldots, c_{n'}$,

com $c_j < b$ para todo j, tais que

$$q = c_0 + c_1 b + c_2 b^2 + \ldots + c_{n'} b^{n'}.$$

Dadas as igualdades acima, temos

$$a = bq + r = b(c_0 + c_1 b + c_2 b^2 + \ldots + c_{n'} b^{n'}) + r,$$

de onde o segue resultado ao tomarmos $a_0 = r$, $n = n' + 1$, e $a_j = c_{j-1}$ para $j = 1, \ldots, n$. Das igualdades acima, segue também a unicidade do resultado. □

CAPÍTULO 4

Aritmética dos Restos

Neste capítulo, apresentamos uma breve introdução às congruências e às congruências lineares. Começamos com definições, exemplos e propriedades básicas. Ao final, utilizamos a teoria de equações diofantinas (que não são detalhadas neste trabalho) para demonstrar o Teorema do Resto Chinês. Nossa abordagem é fundamentada principalmente nas referências como [2], [3], e [7].

4.1 Congruências

Definição 4.1

Seja $n \in \mathbb{N}$ um número fixo. Dois números $a, b \in \mathbb{Z}$ chamam-se congruentes módulo n, se $a-b$ é múltiplo de n, isto é, $a \equiv b \pmod{n}$. Ou seja, em linguagem simbólica,

$$a \equiv b \pmod{n} \iff n \mid (a-b).$$

Abaixo, listamos alguns exemplos de congruências.

Exemplo 4.1

(a) Para $n = 7$, temos que

$$3 \equiv 10 \pmod{7}, \quad \text{já que } 7 \text{ divide } 3-10=-7.$$

(b) Para $n = 3$, temos que

$$4 \equiv 7 \pmod 3, \text{ já que 3 divide } 4 - 7 = -3.$$

Observação 4.1

Sejam $n > 0$, $a, b \in \mathbb{Z}$ escritos na forma

$$a = nq_1 + r_1 \quad \text{e} \quad b = nq_2 + r_2$$

com $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ e $0 \leq r_1, r_2 < n$. Então

$$a \equiv b \pmod n \iff r_1 = r_2.$$

Demonstração. ($\Leftarrow$) Se $r_1 = r_2$, temos

$$a - b = n(q_1 - q_2) + (r_1 - r_2) = n(q_1 - q_2),$$

ou seja, $n \mid (a - b)$. Isto significa $a \equiv b \pmod n$.

($\Rightarrow$) Se $a \equiv b \pmod n$, temos

$$n \mid (a - b) = n(q_1 - q_2) + (r_1 - r_2),$$

e daí,

$$n \mid (r_1 - r_2).$$

Mas de $0 \leq r_1 - r_2 < n$, concluímos então $r_1 - r_2 = 0$, ou seja, $r_1 = r_2$. □

Uma consequência imediata da observação anterior é que todo número $a \in \mathbb{Z}$ é congruente módulo n a exatamente um dos números do conjunto

$$\{0, 1, \ldots, n-1\},$$

onde $n \in \mathbb{N} \setminus \{0\}$. O conjunto $\{0, 1, \ldots, n-1\}$ é denominado *menores restos não-negativos módulo* n.

Definição 4.2

Seja $n > 0$. Um conjunto de n números $\{r_1, r_2, \ldots, r_n\}$ chama-se um sistema completo de resíduos (restos) módulo n se cada $a \in \mathbb{Z}$ é congruente a exatamente um dos números $r_1, r_2, \ldots, r_n$. Equivalentemente: Os $r_1, r_2, \ldots, r_n$ são congruentes módulo n, em alguma ordem, aos números $0, 1, 2, \ldots, n-1$.

Exemplo 4.2

Para $n = 5$ temos:

$$\{0, 1, 2, 3, 4\}$$

é o conjunto dos menores restos não-negativos módulo 5.

$$\{-28, -15, -6, 11, 15\}$$

é um sistema completo de resíduos módulo 5, pois:

$$-28 \equiv 2, \quad -15 \equiv 0, \quad -6 \equiv 4, \quad 11 \equiv 1, \quad 15 \equiv 0 \pmod 5.$$

Sejam $n \in \mathbb{N}$, $q_0, q_1, \ldots, q_{n-1} \in \mathbb{Z}$. Então,

$$\{nq_0, nq_1 + 1, \ldots, nq_{n-1} + (n-1)\}$$

é um sistema completo de resíduos módulo n. Além disso, todo sistema completo de restos módulo n é obtido desta forma.

Teorema 4.1: Propriedades fundamentais das congruências

Sejam $n \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$. Os seguintes ocorrem:

(a) $a \equiv a \pmod n$;

(b) Se $a \equiv b \pmod n$, então $b \equiv a \pmod n$;

(c) Se $a \equiv b \pmod n$ e $b \equiv c \pmod n$, então $a \equiv c \pmod n$;

(d) Se $a \equiv b \pmod n$ e $c \equiv d \pmod n$, então

$$a + c \equiv b + d \pmod n \quad \text{e} \quad ac \equiv bd \pmod n.$$

Demonstração. Provaremos apenas os itens (b) e (d). Começamos com o item (b). Por definição, $a \equiv b \pmod{n} \Leftrightarrow a - b = nq$ para algum $q \in \mathbb{Z}$. Ora, mas isso é o mesmo que $b - a = n(-q)$, ou seja, $b \equiv a \pmod{n}$, o que prova o item (b).

Agora, mostraremos o item (d). Por hipótese, existem $q_1, q_2 \in \mathbb{Z}$ tais que

$$a - b = q_1 n \text{ e } c - d = q_2 n. \tag{4.1}$$

Somando as igualdades em (4.1), obtemos

$$(a + c) - (b + d) = (q_1 + q_2)n.$$

Logo $a + c \equiv b + d \pmod{n}$.

Por outro lado, por (4.1), temos:

$$ac - bd = ac - cb + cb - bd = c(a - b) + b(c - d) = n(cq_1 + bq_2), \text{ i.e.,}$$

$ac \equiv bd \pmod{n}$.

□

Exemplo 4.3

Encontrar os últimos 1, 2, 3, 4, ... dígitos de $n = 1! + 2! + 3! + 4! + \ldots + 100!$:

1. **Último dígito de n:** Como $10 \mid k!$ para $k \geq 5$, o último dígito de n é o mesmo de $1! + 2! + 3! + 4! \equiv 33 \equiv 3 \pmod{10}$. Portanto, o último dígito de n é 3.

2. **Últimos dois dígitos de n:** Para encontrar os últimos dois dígitos de n, consideramos $1! + 2! + \ldots + 9!$, pois $100 \mid k!$ para $k \geq 10$.

$$1! + 2! + \ldots + 9! \equiv 33 \pmod{100}$$

Assim, os últimos dois dígitos de n são 33.

3. **Últimos três dígitos de n:** Para os últimos três dígitos de n, calculamos $1! + 2! + \ldots + 14!$:

$$1! + 2! + \ldots + 14! \equiv 313 \pmod{1000}$$

Portanto, os últimos três dígitos de n são 313.

Dessa forma, podemos continuar a calcular os últimos dígitos de n considerando progressivamente mais fatoriais até 100!. Cada etapa depende dos resultados anteriores e da aplicação dos conceitos de congruência modular para determinar os últimos dígitos correspondentes.

etc.

O Teorema 4.1 nos diz, em particular, que, dado $n \in \mathbb{N}$, $n > 0$ fixo, a seguinte relação:

$$x, x' \in \mathbb{Z} \iff x \equiv x' \pmod{n}$$

é uma relação de equivalência, para mais detalhes veja [2], isto é:

Definição 4.3

Uma relação R em um conjunto A é chamada de relação de equivalência se, e somente se, satisfaz as seguintes propriedades:

1. **Reflexividade**: Para todo $a \in A$, temos $a R a$;
2. **Simetria**: Para todos $a, b \in A$, se $a R b$, então $b R a$;
3. **Transitividade**: Para todos $a, b, c \in A$, se $a R b$ e $b R c$, então $a R c$.

Dessa forma, isso nos motiva a definir duas operações binárias em $\mathbb{Z}_n := \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, onde $\overline{a} := \{m \in \mathbb{Z} \mid m \equiv a \pmod{n}\}$, como segue.

Adição

A adição em $\mathbb{Z}_n$ é uma operação binária definida como uma função:

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$

onde para $\overline{a}, \overline{b} \in \mathbb{Z}_n$,

$$\overline{a} + \overline{b} = \overline{a + b}.$$

Multiplicação

A multiplicação em $\mathbb{Z}_n$ é uma operação binária definida como uma função:

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$

onde para $\overline{a}, \overline{b} \in \mathbb{Z}_n$,

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

No entanto, para essas operações fazerem sentido é necessário observar com mais cuidado o item (d) do Teorema 4.1, mais precisamente:

Seja $n \in \mathbb{N}$, $n > 1$. Se $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$ então:

1. $\overline{a+b} = \overline{a'+b'}$ (a classe da soma independe dos representantes das classes das parcelas);
2. $\overline{a \cdot b} = \overline{a' \cdot b'}$ (a classe do produto independe dos representantes das classes dos fatores).

Teorema 4.2

Seja n um número inteiro maior do que 1. Então

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \quad ; \quad \cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$

definidas respectivamente por

$$\overline{a} + \overline{b} = \overline{a+b}$$

e

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b},$$

definem duas operações (denominadas soma e produto) no conjunto $\mathbb{Z}_n$. Mais precisamente, essas duas operações gozam das seguintes propriedades: $\forall \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n$,

(i) $\overline{(x+y)} + \overline{z} = \overline{x} + \overline{(y+z)}$ (associatividade da soma);

(ii) existe $\overline{0} \in \mathbb{Z}_n$ tal que $\overline{x} + \overline{0} = \overline{0} + \overline{x} = \overline{x}$ (existência do elemento neutro);

(iii) existe $-\overline{x} \in \mathbb{Z}_n$ tal que $\overline{x} + (-\overline{x}) = (-\overline{x}) + \overline{x} = \overline{0}$ (existência do inverso aditivo de cada elemento $\overline{x} \in \mathbb{Z}_n$);

(iv) $\overline{x} + \overline{y} = \overline{y} + \overline{x}$ (comutatividade da soma);

(v) $\overline{(x \cdot y)} \cdot \overline{z} = \overline{x} \cdot \overline{(y \cdot z)}$ (associatividade do produto);

(vi) existe $\overline{1} \in \mathbb{Z}_n$ tal que $\overline{x} \cdot \overline{1} = \overline{1} \cdot \overline{x} = \overline{x}$ (existência da unidade);

(vii) $\overline{x} \cdot \overline{y} = \overline{y} \cdot \overline{x}$ (comutatividade do produto);

(viii) $\overline{x} \cdot (\overline{y} + \overline{z}) = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z}$ (distributividade do produto em relação à soma).

Além disso, se $n = p$ é um número primo e $0 \neq \overline{x} \in \mathbb{Z}_p$, então existe $\overline{y} \in \mathbb{Z}_p$ tal que $\overline{x} \cdot \overline{y} = \overline{y} \cdot \overline{x} = \overline{1}$ (isto é, os elementos não nulos de $\mathbb{Z}_p$ possuem inverso multiplicativo).

Demonstração. Vamos provar cada uma das propriedades listadas no teorema.

(i) **Associatividade da soma**: Para todos $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n$,

$$\overline{(x+y)} + \overline{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \overline{x} + \overline{(y+z)}.$$

Portanto, a soma é associativa.

(ii) **Existência do elemento neutro**: Existe $\overline{0} \in \mathbb{Z}_n$ tal que para todo $\overline{x} \in \mathbb{Z}_n$,

$$\overline{x} + \overline{0} = \overline{x+0} = \overline{x} \quad \text{e} \quad \overline{0} + \overline{x} = \overline{0+x} = \overline{x}.$$

Portanto, $\overline{0}$ é o elemento neutro para a soma.

(iii) **Existência do inverso aditivo**: Para cada $\overline{x} \in \mathbb{Z}_n$, existe $-\overline{x} \in \mathbb{Z}_n$ tal que

$$\overline{x} + (-\overline{x}) = \overline{x+(-x)} = \overline{0} \quad \text{e} \quad (-\overline{x}) + \overline{x} = \overline{(-x)+x} = \overline{0}.$$

Portanto, $-\overline{x}$ é o inverso aditivo de $\overline{x}$.

(iv) **Comutatividade da soma**: Para todos $\overline{x}, \overline{y} \in \mathbb{Z}_n$,

$$\overline{x} + \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} + \overline{x}.$$

Portanto, a soma é comutativa.

(v) **Associatividade do produto**: Para todos $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n$,

$$(\overline{x} \cdot \overline{y}) \cdot \overline{z} = \overline{(x \cdot y)} \cdot \overline{z} = \overline{(x \cdot y) \cdot z} = \overline{x \cdot (y \cdot z)} = \overline{x} \cdot \overline{(y \cdot z)}.$$

Portanto, o produto é associativo.

(vi) **Existência da unidade**: Existe $\overline{1} \in \mathbb{Z}_n$ tal que para todo $\overline{x} \in \mathbb{Z}_n$,

$$\overline{x} \cdot \overline{1} = \overline{x \cdot 1} = \overline{x} \quad \text{e} \quad \overline{1} \cdot \overline{x} = \overline{1 \cdot x} = \overline{x}.$$

Portanto, $\overline{1}$ é a unidade para o produto.

(vii) **Comutatividade do produto**: Para todos $\overline{x}, \overline{y} \in \mathbb{Z}_n$,

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y} = \overline{y \cdot x} = \overline{y} \cdot \overline{x}.$$

Portanto, o produto é comutativo.

(viii) **Distributividade do produto em relação à soma**: Para todos $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n$,

$$\overline{x} \cdot (\overline{y} + \overline{z}) = \overline{x} \cdot \overline{(y+z)} = \overline{x \cdot (y+z)} = \overline{(x \cdot y) + (x \cdot z)} = \overline{x \cdot y} + \overline{x \cdot z} = \overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z}.$$

Portanto, o produto é distributivo em relação à soma.

Existência do inverso multiplicativo em $\mathbb{Z}_p$: Para p primo, se $0 \neq \overline{x} \in \mathbb{Z}_p$, então $mdc(x, p) = 1$. Portanto, existe um $y \in \mathbb{Z}$ tal que

$$x \cdot y \equiv 1 \pmod{p},$$

ou seja, $\overline{x} \cdot \overline{y} = \overline{1}$. Assim, $\overline{x}$ possui um inverso multiplicativo em $\mathbb{Z}_p$. □

Portanto, as operações de adição e multiplicação em $\mathbb{Z}_n$ satisfazem todas as propriedades de um anel comutativo com unidade, para mais detalhes veja [2]. Além disso, para p primo, o anel $\mathbb{Z}_p$ é um corpo.

4.2 Congruências Lineares

Neste texto, adentramos no fascinante mundo das congruências lineares, uma parte fundamental da teoria dos números. Uma congruência linear assume a forma $ax \equiv b \pmod{n}$, onde a, b são inteiros e n é um número natural maior do que 1. Exploramos suas propriedades, condições para a existência de soluções e aplicamos o Teorema do Resto Chinês para resolver sistemas de congruências simultâneas. Este estudo revela resultados teóricos profundos e oferece aplicações práticas em

áreas como criptografia, teoria dos códigos e computação. Baseado nas notas de aula do Professor Rudolf R. Maier [7].

Definição 4.4

Dado $n \in \mathbb{N}$. Uma congruência linear é uma congruência da forma

$$ax \equiv b \pmod{n}$$

onde $a, b \in \mathbb{Z}$ são dados e as soluções $x \in \mathbb{Z}$ são procuradas.

Exemplo 4.4

A congruência linear

$$2x \equiv 5 \pmod{6}$$

não tem solução, enquanto

$$4x \equiv 2 \pmod{6}$$

possui duas soluções incongruentes $x \equiv 2$ e $x \equiv 5 \pmod{6}$. Ou seja, no conjunto de 6 números $\{0,1,2,3,4,5\}$ no sistema completo de resíduos módulo 6 tem -se dois números 2 e 5, como soluções.

Teorema 4.3

Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$.

(a) A congruência $ax \equiv b \pmod{n}$ admite uma solução, se e somente se, $d = mdc(a,n) \mid b$.

(b) Se $d \mid b$, então $ax \equiv b \pmod{n}$ possui exatamente d soluções incongruentes entre si módulo n. Se $x_0 \in \mathbb{Z}$ é uma solução particular, então d soluções incongruentes são obtidas por:

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + 2 \cdot \frac{n}{d}, \quad \ldots, \quad x_0 + (d-1) \cdot \frac{n}{d}.$$

Demonstração. (a) A congruência $ax \equiv b \pmod{n}$ equivale à equação Diofantina linear $ax + ny = b$, veja mais detalhes em [3], a qual é solúvel se e somente se $d = mdc(a,n) \mid b$.

(b) Seja $d \mid b$ e seja $x_0 \in \mathbb{Z}$ com $ax_0 \equiv b \pmod{n}$, isto é, $ax_0 + ny_0 = b$ para algum $y_0 \in \mathbb{Z}$. Como toda solução de $ax \equiv b \pmod{n}$ é da forma $x = x_0 + \frac{n}{d}t$ com $t \in \mathbb{Z}$, escrevendo $t = qd + k$ com

$q, k \in \mathbb{Z}$ e $0 \leq k \leq d-1$, vemos que

$$x = x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd+k) = x_0 + qn + k \cdot \frac{n}{d} \equiv x_0 + k \cdot \frac{n}{d} \pmod{n}.$$

Mostramos, portanto, que toda solução é congruente módulo n a um dos d números indicados. Mais ainda, de $x_0 + j \cdot \frac{n}{d} \equiv x_0 + k \cdot \frac{n}{d} \pmod{n}$ com $0 \leq j, k \leq d-1$ segue

$$j \cdot \frac{n}{d} \equiv k \cdot \frac{n}{d} \pmod{n}$$

e daí $j \cdot \frac{n}{d} = k \cdot \frac{n}{d} + \ell n$, com $\ell \in \mathbb{Z}$. Dividindo-se por $\frac{n}{d}$, segue

$$j = k + \ell d \equiv k \pmod{d}.$$

De $0 \leq |j-k| \leq d-1$ concluímos $\ell = 0$ e $j = k$. Isto mostra que as d soluções indicadas são incongruentes módulo n.

□

A seguir, listamos uma das consequências do Teorema 4.3. Sejam $n \in \mathbb{N}$ e $a, x, y \in \mathbb{Z}$ com $d = mdc(a, n)$. Então

$$ax \equiv ay \pmod{n} \implies x \equiv y \pmod{\frac{n}{d}}.$$

Isto quer dizer, um fator comum numa congruência módulo n pode ser cancelado, desde que se observe que a nova congruência só é válida módulo $\frac{n}{d}$.

4.3 Congruências Simultâneas e o Teorema do Resto Chinês

Para motivar o teorema do resto chinês, iniciamos com o seguinte problema: quais são os números naturais que deixam simultaneamente o resto 4 quando divididos por 5 e o resto 3 quando divididos por 4? A resposta é: são os números da forma $19 + 20k$, onde k é um número inteiro não negativo, $k = 0, 1, 2, 3, \ldots$.

Podemos expressar o problema da forma:

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{4}; \end{cases}$$

e a solução como

$$x \equiv 19 \pmod{20}.$$

Teorema 4.4

Sejam $n_1, n_2, \ldots, n_r \in \mathbb{N}$ tais que mdc$(n_i, n_j) = 1$ para $1 \leq i \neq j \leq r$, i.e., os $n_1, \ldots, n_r$ são relativamente primos, dois a dois. Sejam $a_1, a_2, \ldots, a_r \in \mathbb{Z}$. Então as congruências

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

possuem uma solução simultânea. Além disso, quaisquer duas soluções são congruentes módulo o produto $n_1 \cdot n_2 \cdot \ldots \cdot n_r$.

Demonstração. Coloquemos $N = n_1 n_2 \ldots n_r$ e para todo $k = 1, 2, \ldots, r$:

$$N_k = \prod_{\substack{1 \leq j \leq r \\ j \neq k}} n_j = n_1 n_2 \ldots n_{k-1} n_{k+1} \ldots n_r \quad (1 \leq k \leq r),$$

isto é,

$$N_1 = \frac{N}{n_1}, \quad N_2 = \frac{N}{n_2}, \quad \ldots, \quad N_r = \frac{N}{n_r}.$$

Para todo $k = 1, 2, \ldots, r$ temos mdc$(N_k, n_k) = 1$, pois os $n_1, \ldots, n_r$ são relativamente primos em pares. Isso implica que a congruência $N_k x \equiv 1 \pmod{n_k}$ possui uma solução. Seja $x_k \in \mathbb{Z}$ tal que $N_k x_k \equiv 1 \pmod{n_k}$ $(1 \leq k \leq r)$.

Afirmamos que $x = N_1 x_1 a_1 + N_2 x_2 a_2 + \ldots + N_r x_r a_r$ é uma solução simultânea das congruências. De fato, como n_k divide $N_1, N_2, \ldots, N_{k-1}, N_{k+1}, \ldots, N_r$ para todo $k = 1, 2, 3, \ldots, r$ segue-se que

$$x \equiv 0 + \ldots + 0 + N_k x_k a_k + 0 + \ldots + 0 \equiv 1 \cdot a_k = a_k \mod n_k.$$

Como $N \equiv 0 \pmod{n_1}, N \equiv 0 \pmod{n_2}, \ldots, N \equiv 0 \pmod{n_r}$, qualquer número que difira de x por um múltiplo de N é também solução simultânea das congruências. Reciprocamente, se x' $\in \mathbb{Z}$ é qualquer solução das congruências, então x' $\equiv a_k \equiv x \pmod{n_k}$ e assim $n_k \mid (x' - x)$ para todo

$k = 1, 2, \ldots, r$. Concluímos que $x' \equiv x \pmod{n_1 n_2 \ldots n_r}$, pois os $n_1, n_2, \ldots, n_r$ são relativamente primos em pares e, portanto, seu mínimo múltiplo comum é seu produto.

□

Exemplo 4.5

Resolva o sistema

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7. \end{cases}$$

Solução:

Escrevemos $N = 3 \cdot 5 \cdot 7 = 105$. Segue do Teorema do Resto Chinês, usando a mesma notação, que:

$$\begin{cases} N_1 = \dfrac{105}{3} = 35 \\ N_2 = \dfrac{105}{5} = 21 \\ N_3 = \dfrac{105}{7} = 15 \end{cases} ; \quad \begin{cases} N_1 x_1 \equiv 1 \pmod 3 \\ N_2 x_2 \equiv 1 \pmod 5 \\ N_3 x_3 \equiv 1 \pmod 7 \end{cases} ; \quad \begin{cases} 35 x_1 \equiv 1 \pmod 3 \\ 21 x_2 \equiv 1 \pmod 5 \\ 15 x_3 \equiv 1 \pmod 7. \end{cases}$$

Agora, como

$$35 \cdot 2 \equiv 1 \pmod 3,$$
$$21 \cdot 1 \equiv 1 \pmod 5,$$
$$15 \cdot 1 \equiv 1 \pmod 7,$$

então a solução do sistema é

$$x = a_1 \cdot N_1 \cdot x_1 + a_2 \cdot N_2 \cdot x_2 + a_3 \cdot N_3 \cdot x_3 = 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 157 \equiv 52 \pmod{105},$$

onde $a_1 = 1, a_2 = 2$ e $a_3 = 3$.

CAPÍTULO 5

Critérios de Divisibilidade

Neste capítulo, apresentaremos e demonstraremos os principais critérios de divisibilidade. Realizaremos as demonstrações em duas frentes: pela representação decimal dos números naturais e pela aritmética dos restos, proporcionando uma abordagem intuitiva para o leitor. Observemos que, se $a \mid b$ então $a \mid -b$, assim, faremos as demonstrações considerando o conjunto dos números inteiros. Desse modo, diremos que $a \mid b$ se existir um inteiro c tal que $b = ac$.

5.1 Divisibilidade por 2, 4, 8

Para demonstrarmos alguns dos critérios de divisibilidade, consideraremos a representação do número decimal $a = a_n a_{n-1} \ldots a_2 a_1 a_0$ (de algarismos $a_n, \ldots, a_0$), sendo:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

5.1.1 Divisibilidade por 2

Proposição 5.1: Critério de Divisibilidade por 2

Seja $a = a_n a_{n-1} \ldots a_2 a_1 a_0$. Então:

$$2 \mid a \text{ se, e somente se, } 2 \mid a_0.$$

Demonstração. (⇒) Suponhamos que $2 \mid a$, ou seja, $a = 2t$, $t \in \mathbb{Z}$. Notemos que:

$$a = a_n a_{n-1} \dots a_2 a_1 a_0 = a_n a_{n-1} \dots a_2 a_1 \cdot 10 + a_0 = \underbrace{(a_n a_{n-1} \dots a_2 a_1 \cdot 5)}_{l,\, l \in \mathbb{Z}} \cdot 2 + a_0 = 2l + a_0.$$

Segue que:

$$a_0 = a - 2l = 2t - 2l = 2(t-l) \Rightarrow 2 \mid a_0.$$

(⇐) Reciprocamente, suponhamos que $2 \mid a_0$. Podemos escrever $a_0 = 2m$, $m \in \mathbb{Z}$. Como $a = 2l + a_0$, temos:

$$a = 2l + a_0 = 2l + 2m = 2(l+m) \Rightarrow 2 \mid a.$$

□

Em outras palavras, a_0 deve ser par. Assim, obtemos o critério de divisibilidade por 2:

Critério de divisibilidade por 2: Um número inteiro é divisível por 2 se, e somente se, o seu algarismo das unidades é par.

5.1.2 Divisibilidade por 4

Proposição 5.2: Critério de Divisibilidade por 4

Seja $a = a_n a_{n-1} \dots a_2 a_1 a_0$. Então

$$4 \mid a \text{ se, e somente se, } 4 \mid (a_1 a_0).$$

Demonstração. (⇒) Suponhamos que $4 \mid a$, ou seja, $a = 4t$, $t \in \mathbb{Z}$. Observemos que:

$$a = a_n a_{n-1} \dots a_2 a_1 a_0 = a_n a_{n-1} \dots a_2 \cdot 100 + a_1 a_0 = \underbrace{(a_n a_{n-1} \dots a_2 \cdot 25)}_{l,\, l \in \mathbb{Z}} \cdot 4 + a_1 a_0 = 4l + a_1 a_0.$$

Segue que:

$$a_1 a_0 = a - 4l = 4t - 4l = 4(t-l) \Rightarrow 4 \mid a_1 a_0.$$

(⇐) Por outro lado, suponhamos que $4 \mid (a_1 a_0)$. Podemos escrever $a_1 a_0 = 4m$, $m \in \mathbb{Z}$. Como $a = 4l + a_1 a_0$, temos:

$$a = 4l + a_1 a_0 = 4l + 4m = 4(l+m) \Rightarrow 4 \mid a.$$

□

Desse modo, o número formado pelos dois últimos algarismos de a deve ser divisível por 4. Assim, obtemos o critério de divisibilidade por 4:

Critério de divisibilidade por 4: Um número inteiro é divisível por 4 se, e somente se, o número formado pelos seus dois últimos algarismos é divisível por 4.

5.1.3 Divisibilidade por 8

Proposição 5.3: Critério de Divisibilidade por 8

Seja $a = a_n a_{n-1} \dots a_2 a_1 a_0$. Então

$$8 \mid a \text{ se, e somente se, } 8 \mid (a_2 a_1 a_0).$$

Demonstração. ($\Rightarrow$) Suponhamos que $8 \mid a$, ou seja, $a = 8t$, $t \in \mathbb{Z}$. Obtemos:

$$a = a_n a_{n-1} \dots a_3 a_2 a_1 a_0 = a_n a_{n-1} \dots a_3 \cdot 1000 + a_2 a_1 a_0 = \underbrace{(a_n a_{n-1} \dots a_3 \cdot 125)}_{l,\, l \in \mathbb{Z}} \cdot 8 + a_2 a_1 a_0 = 8l + a_2 a_1 a_0.$$

Segue que:

$$a_2 a_1 a_0 = a - 8l = 8t - 8l = 8(t-l) \Rightarrow 8 \mid a_2 a_1 a_0.$$

($\Leftarrow$) Por outro lado, suponhamos que $8 \mid (a_2 a_1 a_0)$. Podemos escrever $a_2 a_1 a_0 = 8m$, $m \in \mathbb{Z}$. Como $a = 8l + a_2 a_1 a_0$, temos:

$$a = 8l + a_2 a_1 a_0 = 8l + 8m = 8(l+m) \Rightarrow 8 \mid a.$$

□

Portanto, o número formado pelos três últimos dígitos de a deve ser divisível por 8. Assim, obtemos o critério de divisibilidade por 8:

Critério de divisibilidade por 8: Um número inteiro é divisível por 8 se, e somente se, o número formado pelos seus três últimos algarismos é divisível por 8.

5.2 Critérios de Divisibilidade por 3 e por 9

Nesta seção, apresentaremos os critérios de divisibilidade por 3 e por 9. Estas duas demonstrações são bastante semelhantes, pois ambas se baseiam no fato de que $10^n - 1$ é divisível por 3 e por 9.

5.2.1 Critério de Divisibilidade por 3

Sabemos pelo Exemplo 2.5 que 10^n deixa resto 1 na divisão por 3, isto é, $3 \mid 10^n - 1$.

Proposição 5.4: Critério de Divisibilidade por 3

Seja $a = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$. Então

$$3 \mid a \Leftrightarrow 3 \mid a_m + a_{m-1} \ldots + a_2 + a_1 + a_0.$$

Demonstração. Para mostrarmos a divisibilidade por 3, seja $a = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$ e $S = a_m + a_{m-1} + \cdots + a_1 + a_0$ a soma dos algarismos de a. Queremos mostrar que 3 divide a, se e somente se, 3 divide S.

Afirmamos que: se 3 divide S, então 3 divide a. De fato:

($\Leftarrow$) Suponhamos que $3 \mid S$, isto é, $S = 3t$, $t \in \mathbb{Z}$. Notemos que:

$$\begin{aligned} a - S &= a - (a_m + a_{m-1} + \cdots + a_1 + a_0) \\ &= a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 10 + a_0 - (a_m + a_{m-1} + \cdots + a_1 + a_0) \\ &= a_m \cdot (10^m - 1) + a_{m-1} \left(10^{m-1} - 1\right) + \cdots + a_1 \cdot \left(10^1 - 1\right). \end{aligned}$$

Como 3 divide $(10^m - 1), \left(10^{m-1} - 1\right), \ldots, \left(10^1 - 1\right)$, segue que $a - S = 3q_1$, $q_1 \in \mathbb{Z}$, isto é:

$$a = 3q_1 + S$$

$$a = 3q_1 + 3t = 3(q_1 + t).$$

Logo 3 divide a.

Por fim, mostraremos que: se 3 divide a, então 3 divide S.

(⇒) Suponhamos que 3 divide a, ou seja $a = 3q_2$, $q_2 \in \mathbb{Z}$. Como $a = 3q_1 + S$, então:

$$S = a - 3q_1 = 3q_2 - 3q_1 = 3(q_2 - q_1).$$

Logo, 3 divide S. □

Daí temos o **critério de divisibilidade por** 3**:** um número inteiro qualquer é divisível por 3 se, e somente se, a soma dos seus algarismos também é divisível por 3.

5.2.2 Critério de Divisibilidade por 9

Pelo Exemplo 2.3 sabemos que 9 divide $10^n - 1$, para todo $n \in \mathbb{N}$. Utilizaremos este fato para a demonstração do critério de divisibilidade por 9, a seguir:

Proposição 5.5: Critério de Divisibilidade por 9

Seja $a = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$. Então:

$$9 \mid a \Leftrightarrow 9 \mid a_m + a_{m-1} \ldots + a_2 + a_1 + a_0.$$

Demonstração. Para mostrarmos a divisibilidade por 9, sejam $a = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$ e $S = a_m + a_{m-1} + \cdots + a_1 + a_0$ a soma dos algarismos de a. Queremos mostrar que 9 divide a, se e somente se, 9 divide S.

(⇐) Suponhamos que $9 \mid S$, isto é, $S = 9t$, $t \in \mathbb{Z}$. Observemos que

$$\begin{aligned} a - S &= a - (a_m + a_{m-1} + \cdots + a_1 + a_0) \\ &= a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 10 + a_0 - (a_m + a_{m-1} + \cdots + a_1 + a_0) \\ &= a_m \cdot (10^m - 1) + a_{m-1} \left(10^{m-1} - 1\right) + \cdots + a_1 \cdot \left(10^1 - 1\right). \end{aligned}$$

Como 9 divide $(10^m - 1), \left(10^{m-1} - 1\right), \ldots, \left(10^1 - 1\right)$, segue que $a - S = 9q_1$, $q_1 \in \mathbb{Z}$, isto é

$$\begin{aligned} a &= 9q_1 + S \\ a &= 9q_1 + 9t = 9(q_1 + t). \end{aligned}$$

Logo 9 divide a.

(⇒) Por outro lado, suponhamos que 9 divide a, ou seja $a = 9q_2$, $q_2 \in \mathbb{Z}$. Como $a = 9q_1 + S$, então

$$S = a - 9q_1 = 9q_2 - 9q_1 = 9(q_2 - q_1).$$

Logo, 9 divide S. □

Daí segue o **critério de divisibilidade por** 9**:** um número inteiro qualquer é divisível por 9 se, e somente se, a soma dos seus algarismos também é divisível por 9.

5.3 Divisibilidade por 5 e 10

Para demonstrarmos os critérios de divisibilidade por 5 e por 10, consideraremos novamente a representação do número decimal $a = a_n a_{n-1} \ldots a_2 a_1 a_0$ (de algarismos $a_n, \ldots, a_0$), sendo:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

5.3.1 Divisibilidade por 5

Proposição 5.6: Critério de Divisibilidade por 5

Seja $a = a_n a_{n-1} \ldots a_2 a_1 a_0$. Então

$5 \mid a$ se, e somente se, $5 \mid a_0$.

Demonstração. (⇒) Suponhamos que $5 \mid a$, ou seja, $a = 5t$, $t \in \mathbb{Z}$. Observemos que:

$$a = a_n a_{n-1} \ldots a_2 a_1 a_0 = a_n a_{n-1} \ldots a_2 a_1 \cdot 10 + a_0 = \underbrace{(a_n a_{n-1} \ldots a_2 a_1 \cdot 2)}_{l,\, l \in \mathbb{Z}} \cdot 5 + a_0 = 5l + a_0.$$

Segue que:

$$a_0 = a - 5l = 5t - 5l = 5(t - l) \Rightarrow 5 \mid a_0.$$

(⇐) Reciprocamente, suponhamos que $5 \mid a_0$. Podemos escrever $a_0 = 5m$, $m \in \mathbb{Z}$. Como $a = 5l + a_0$, obtemos

$$a = 5l + a_0 = 5l + 5m = 5(l + m) \Rightarrow 5 \mid a.$$

□

Em outras palavras, a_0 deve ser 0 ou 5. Obtemos o critério de divisibilidade por 5:

Critério de divisibilidade por 5: Um número inteiro é divisível por 5 se, e somente se, o seu algarismo das unidades é 0 ou 5.

5.3.2 Divisibilidade por 10

Proposição 5.7: Critério de Divisibilidade por 10

Seja $a = a_n a_{n-1} \dots a_2 a_1 a_0$. Então

$$10 \mid a \text{ se, e somente se, } 10 \mid a_0.$$

Demonstração. ($\Rightarrow$) Suponhamos que $10 \mid a$, ou seja, $a = 10t$, $t \in \mathbb{Z}$. Notemos que:

$$a = a_n a_{n-1} \dots a_2 a_1 a_0 = a_n a_{n-1} \dots a_2 a_1 \cdot 10 + a_0 = \underbrace{(a_n a_{n-1} \dots a_2 a_1 \cdot 1)}_{l,\, l \in \mathbb{Z}} \cdot 10 + a_0 = 10l + a_0.$$

Segue que:

$$a_0 = a - 10l = 10t - 10l = 10(t-l) \Rightarrow 10 \mid a_0.$$

($\Leftarrow$) Por outro lado, suponhamos que $10 \mid a_0$. Podemos expressar $a_0 = 10m$, $m \in \mathbb{Z}$. Como $a = 10l + a_0$, podemos escrever:

$$a = 10l + a_0 = 10l + 10m = 10(l+m) \Rightarrow 10 \mid a.$$

□

Em resumo, a_0 precisa ser 0. Chegamos assim ao critério de divisibilidade por 10:

Critério de divisibilidade por 10: Um número inteiro é divisível por 10 se, e somente se, o seu algarismo das unidades é 0.

5.4 Divisibilidade por 7

Proposição 5.8: Critério de Divisibilidade por 7

Seja $a = a_n a_{n-1} \dots a_2 a_1 a_0$. Então

$$7 \mid a \Leftrightarrow 7 \mid a_n a_{n-1} \dots a_3 a_2 a_1 + 5a_0.$$

Demonstração. ($\Rightarrow$) Suponhamos que $7 \mid a$, isto é,

$$10^n a_n + 10^{n-1} a_{n-1} + \dots + 10^2 a_2 + 10a_1 + a_0 = 7q,$$

com $q \in \mathbb{Z}$.

Adicionando $49a_0$ a ambos os membros da equação, temos

$$10^n a_n + 10^{n-1} a_{n-1} + \dots + 10^2 a_2 + 10a_1 + 50a_0 = 7q + 49a_0.$$

Consequentemente,

$$10\left(10^{n-1} a_n + 10^{n-2} a_{n-1} + \dots + 10a_2 + a_1 + 5a_0\right) = 7(q + 7a_0).$$

Como $10^{n-1} a_n + 10^{n-2} a_{n-1} + \dots + 10a_2 + a_1 + 5a_0 = a_n a_{n-1} \dots a_3 a_2 a_1 + 5a_0$ e $7 \nmid 10$, segue que

$$7 \mid a_n a_{n-1} \dots a_3 a_2 a_1 + 5a_0.$$

($\Leftarrow$) Suponhamos que $7 \mid a_n a_{n-1} \dots a_3 a_2 a_1 + 5a_0$, isto é,

$$a_n a_{n-1} \dots a_3 a_2 a_1 + 5a_0 = 7k,$$

com $k \in \mathbb{Z}$.

Podemos escrever

$$10\left(10^{n-1} a_n + 10^{n-2} a_{n-1} + \dots + 10a_2 + a_1\right) + 50a_0 = 70k.$$

Subtraindo $49a_0$ de ambos os membros, temos

$$10\left(10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + 10a_2 + a_1\right) + a_0 = 70k - 49a_0.$$

Consequentemente,

$$10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0 = 7(10k - 7a_0).$$

Como $10k - 7a_0 \in \mathbb{Z}$, segue que

$$7 \mid 10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0.$$

Portanto, $7 \mid a$. □

Assim, temos o **critério de divisibilidade por 7:** Um número é divisível por 7, se o quíntuplo do algarismo da sua unidade adicionado ao número formado pelos seus demais algarismos for divisível por 7.

5.5 Divisibilidade por 11

Proposição 5.9: Critério de Divisibilidade por 11

Seja $a = a_n a_{n-1} \ldots a_2 a_1 a_0$. Então

$$11 \mid a \Leftrightarrow 11 \mid a_n a_{n-1} \ldots a_3 a_2 a_1 - a_0.$$

Demonstração. (⇒) Suponhamos que $11 \mid a$, isto é,

$$10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0 = 11q,$$

com $q \in \mathbb{Z}$.

Subtraindo $11a_0$ de ambos os membros da equação, temos

$$10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10^2 a_2 + 10a_1 - 10a_0 = 11q - 11a_0.$$

Consequentemente,

$$10\left(10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + 10a_2 + a_1 - a_0\right) = 11(q - a_0).$$

Como

$$10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + 10a_2 + a_1 - a_0 = a_n a_{n-1} \ldots a_3 a_2 a_1 - a_0$$

e $11 \nmid 10$, segue que

$$11 \mid a_n a_{n-1} \ldots a_3 a_2 a_1 - a_0.$$

($\Leftarrow$) Suponhamos que $11 \mid a_n a_{n-1} \ldots a_3 a_2 a_1 - a_0$, isto é,

$$a_n a_{n-1} \ldots a_3 a_2 a_1 - a_0 = 11k,$$

com $k \in \mathbb{Z}$.

Podemos escrever

$$10\left(10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + 10a_2 + a_1\right) - 10a_0 = 110k.$$

Adicionando $11a_0$ a ambos os membros, temos

$$10\left(10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + 10a_2 + a_1\right) + a_0 = 110k + 11a_0.$$

Consequentemente,

$$10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0 = 11(10k + a_0).$$

Como $10k + a_0 \in \mathbb{Z}$, segue que

$$11 \mid 10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0.$$

Portanto, $11 \mid a$. □

Assim, temos o critério de divisibilidade por 11: Um número inteiro é divisível por 11, se o número formado pelos algarismos deste número excluindo o algarismo da unidade, menos esse

algarismo excluído, for divisível por 11.

5.6 Divisibilidade por 13

Proposição 5.10: Critério de Divisibilidade por 13

Seja $a = a_n a_{n-1} \dots a_2 a_1 a_0$. Então

$$13 \mid a \iff 13 \mid a_n a_{n-1} \dots a_3 a_2 a_1 + 4a_0.$$

Demonstração. ($\Rightarrow$) Seja $a = a_n a_{n-1} \dots a_2 a_1 a_0$ divisível por 13, isto é: $a_n a_{n-1} \dots a_2 a_1 a_0 = 13q$, com $q \in \mathbb{Z}$.

Podemos escrever:

$$10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0 = 13q$$

Somando $39a_0$ a ambos os membros:

$$10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + 40a_0 = 13q + 39a_0$$

Consequentemente:

$$10\left(10^{n-1} a_n + 10^{n-2} a_{n-1} + \ldots + 10a_2 + a_1 + 4a_0\right) = 13(q + 3a_0)$$

Como:

$$10^{n-1} a_n + 10^{n-2} a_{n-1} + \ldots + 10a_2 + a_1 + 4a_0 = a_n a_{n-1} \dots a_3 a_2 a_1 + 4a_0$$

e $13 \nmid 10$, segue que:

$$13 \mid a_n a_{n-1} \dots a_3 a_2 a_1 + 4a_0$$

($\Leftarrow$) Se $a_n a_{n-1} \dots a_3 a_2 a_1 + 4a_0$ for divisível por 13, ou seja, $a_n a_{n-1} \dots a_3 a_2 a_1 + 4a_0 = 13k$, com $k \in \mathbb{Z}$ então:

$$10\left(10^{n-1} a_n + 10^{n-2} a_{n-1} + \ldots + 10a_2 + a_1\right) + 40a_0 = 13k, \text{para algum } k \in \mathbb{Z}$$

Subtraindo $39a_0$ de ambos os membros, vemos que

$$10\left(10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + 10a_2 + a_1\right) + a_0 = 13k - 39a_0.$$

Consequentemente,

$$10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0 = 13(k - 3a_0).$$

Como $k - 3a_0 \in \mathbb{Z}$, segue que

$$13 \mid 10^n a_n + 10^{n-1}a_{n-1} + \ldots + 10^2 a_2 + 10a_1 + a_0.$$

Portanto, $13 \mid a$. □

Segue o critério de divisibilidade por 13: Um número inteiro é divisível por 13 se a soma do quádruplo do algarismo da sua unidade somado com o número formado pelos seus demais algarismos for divisível por 13.

5.7 Critérios de Divisibilidade por Congruências

Nesta seção, demonstraremos os critérios de divisibilidade utilizando congruências. Tal abordagem torna as demonstrações práticas e diretas, além de facilitar a verificação de critérios de divisibilidade considerados mais complexos. Apresentaremos, a seguir, alguns desses critérios de divisibilidade.

5.7.1 Divisibilidade por 2

Considere a representação polinomial:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

Para demonstrarmos esse critério, observemos que:

$$10^n \equiv 0^n \equiv 0 \pmod 2$$

Desse modo:

$$\begin{aligned} a &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv a_n \cdot 0 + a_{n-1} \cdot 0 + \ldots + a_2 \cdot 0 + a_1 \cdot 0 + a_0 \\ &\equiv 0 + 0 + \ldots + 0 + 0 + a_0 \\ &\equiv a_0 \pmod 2 \end{aligned}$$

Dado que $a \equiv a_0 \pmod 2$, pela definição de congruência, temos que $a \equiv 0 \pmod 2$ se e somente se $a_0 \equiv 0 \pmod 2$, o que nos dá o critério de divisibilidade por 2: Um número inteiro é divisível por 2 se o algarismo das unidades é par.

5.7.2 Divisibilidade por 3

Dada a expressão polinomial:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

Para mostrar este critério, observemos que:

$$10^n \equiv 1^n \equiv 1 \pmod 3$$

Assim:

$$\begin{aligned} a &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv a_n \cdot 1 + a_{n-1} \cdot 1 + \ldots + a_2 \cdot 1 + a_1 \cdot 1 + a_0 \\ &\equiv a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 \pmod 3 \end{aligned}$$

Portanto, $a \equiv 0 \pmod 3$ se e somente se a soma dos algarismos for divisível por 3. O critério de divisibilidade por 3 é: um número é divisível por 3 se a soma de seus dígitos é divisível por 3.

5.7.3 Divisibilidade por 4

Vamos considerar a forma polinomial:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

Para estabelecer este critério, notamos que:

$$\begin{aligned} 10^1 &\equiv 2 \pmod 4 \\ 10^2 &\equiv 2^2 \equiv 0 \pmod 4 \\ 10^3 &\equiv 2^3 \equiv 0 \pmod 4 \\ 10^n &\equiv 0 \pmod 4, \text{ se } n \geq 2 \end{aligned}$$

Assim:

$$\begin{aligned} a &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv 0 + 0 + \ldots + 0 + 10a_1 + a_0 \\ &\equiv 10a_1 + a_0 \pmod 4 \end{aligned}$$

Portanto, $a \equiv 0 \pmod 4$ se e somente se os dois últimos dígitos formarem um número divisível por 4. O critério de divisibilidade por 4 é: um número é divisível por 4 se os dois últimos algarismos formarem um número divisível por 4.

5.7.4 Divisibilidade por 5

Consideremos a representação polinomial:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

Para verificar este critério, observamos que:

$$10^n \equiv 0^n \equiv 0 \pmod 5$$

Portanto:

$$\begin{aligned} a &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv 0 + 0 + \ldots + 0 + 0 + a_0 \equiv a_0 \pmod 5 \end{aligned}$$

Portanto, $a \equiv a_0 \pmod 5$, o que implica que $a \equiv 0 \pmod 5$ se e somente se $a_0 \equiv 0 \pmod 5$. O critério de divisibilidade por 5 é: um número é divisível por 5 se o último dígito for 0 ou 5.

5.7.5 Divisibilidade por 8

Analisemos a forma polinomial:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

Para definir este critério, notamos que:

$$\begin{aligned} 10^1 &\equiv 2 \pmod 8 \\ 10^2 &\equiv 2^2 \equiv 4 \pmod 8 \\ 10^3 &\equiv 2^3 \equiv 0 \pmod 8 \\ 10^n &\equiv 0 \pmod 8, \text{ se } n \geq 3 \end{aligned}$$

Assim:

$$\begin{aligned} a &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv 0 + 0 + \ldots + 0 + 100a_2 + 10a_1 + a_0 \\ &\equiv 100a_2 + 10a_1 + a_0 \pmod 8 \end{aligned}$$

Portanto, $a \equiv 0 \pmod 8$ se e somente se os três últimos dígitos formarem um número divisível por 8. O critério de divisibilidade por 8 é: um número é divisível por 8 se os três últimos algarismos formarem um número divisível por 8.

5.7.6 Divisibilidade por 9

Analisemos a expressão polinomial:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

Para demonstrar este critério, observamos que:

$$10^n \equiv 1^n \equiv 1 \pmod 9$$

Portanto:

$$\begin{aligned} a &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 \pmod 9 \end{aligned}$$

Então, $a \equiv 0 \pmod 9$ se a soma dos algarismos for divisível por 9. O critério de divisibilidade por 9 é: um número é divisível por 9 se a soma de seus dígitos é divisível por 9.

5.7.7 Divisibilidade por 10

Consideremos a expressão polinomial:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

Para validar este critério, notamos que:

$$10^n \equiv 0^n \equiv 0 \pmod{10}$$

Portanto:

$$\begin{aligned} a &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv 0 + 0 + \ldots + 0 + 0 + a_0 \\ &\equiv a_0 \pmod{10} \end{aligned}$$

Portanto, $a \equiv a_0 \pmod{10}$, o que implica que $a \equiv 0 \pmod{10}$ se e somente se $a_0 \equiv 0 \pmod{10}$. O critério de divisibilidade por 10 é: um número é divisível por 10 se o algarismo das unidades é 0.

5.8 Um critério de Divisibilidade por 7, 11 e 13

Apresentaremos, a seguir, um critério de divisibilidade por 7, 11 e 13. Esses critérios foram também demonstrados por Hefez [6] e apresentam uma alternativa de critério de divisibilidade por congruência por 7, 11 e 13 para números grandes.

Observemos inicialmente que $7 \cdot 11 \cdot 13 = 1001$, portanto:

$$1000 \equiv -1 \pmod 7$$

$$1000 \equiv -1 \pmod{11}$$

$$1000 \equiv -1 \pmod{13}$$

Segue que, módulo 7, 11 e 13:

$$10^3 \equiv -1$$

$$10^6 \equiv (10^3)^2 \equiv (-1)^2 \equiv 1$$

$$10^9 \equiv (10^3)^3 \equiv (-1)^3 \equiv -1$$

$$10^{12} \equiv (10^3)^4 \equiv (-1)^4 \equiv 1$$

e assim por diante.

Assim, sendo $a = a_n a_{n-1} \dots a_2 a_1 a_0$, podemos escrever:

$$a = a_2 a_1 a_0 + a_5 a_4 a_3 \times 10^3 + a_8 a_7 a_6 \times 10^6 + \cdots$$

$$\equiv a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots \mod (7, 11, 13)$$

Concluímos que o resto da divisão de a por 7, 11 ou 13 é igual ao resto da divisão de $a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$ por 7, 11 ou 13, respectivamente.

Critério de divisibilidade por 7, 11 ou 13: O número $a_n \dots a_2 a_1 a_0$ é divisível por 7, 11 ou 13 se, e somente se, o número $a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \cdots$ é divisível por 7, 11 ou 13, respectivamente.

CAPÍTULO 6

Sequência Didática: Critérios de Divisibilidade

6.1 Introdução

Para início das atividades de demonstrações e validações dos critérios de divisibilidade, introduziremos a representação genérica de números decimais na base 10. Para as demonstrações, utilizaremos noções intuitivas, da representação de números na forma decimal, apresentando um cálculo básico para introduzir a ideia da demonstração. O professor pode, nesse contexto, aproveitar as sequências didáticas apresentadas para realizar as demonstrações dos critérios de divisibilidade.

Observemos que, quando escrevemos um número qualquer na base 10, os algarismos da esquerda para a direita possuem peso de acordo com sua posição. Da direita para a esquerda, o primeiro valor tem peso 1 (unidade), o segundo valor tem peso 10^1 (dezena), o terceiro tem peso 10^2 (centena) e assim por diante.

Consideremos os exemplos

$$a) \quad 234 = 2 \cdot 10^2 + 3 \cdot 10 + 4$$

$$b) \quad 1205 = 1 \cdot 10^3 + 2 \cdot 10^2 + 0 \cdot 10 + 5$$

Exercício: Escreva os valores abaixo em potências de base 10:

a) 7549;

b) 10423.

Vamos considerar a representação do número decimal $a = a_n a_{n-1} \ldots a_1 a_0$ (de algarismos $a_n, \ldots, a_0$), sendo:

$$a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0.$$

6.2 Atividade 1: Critérios de Divisibilidade por 2, 4 e 8

6.2.1 Critério de Divisibilidade por 2

Consideremos o exemplo:

Exemplo 1: Mostre que 2432 é divisível por 2.

Solução: Notemos que:

$$\begin{aligned} 2432 &= 2430 + 2 \\ &= 243 \cdot 10 + 2 \\ &= 243 \cdot 5 \cdot 2 + 2 \end{aligned}$$

Observemos que $2430 = 243 \cdot 5 \cdot 2 = 1215 \cdot 2$, é divisível por 2. Assim, como 2 divide 2, então 2 divide $(2430 + 2) = 2432$.

Exercício 1: Como no exemplo anterior, verifique se 2 divide:

a) 5358

b) 3425

Exercício 2: Considere o número $a = a_n a_{n-1} \ldots a_1 a_0$.

a) Verifique que: 2 divide $a - a_0 = a_n a_{n-1} \ldots a_1 \cdot 10$. (Dica: faça como nos exemplos anteriores)

b) Em qual condição 2 divide $a = a_n a_{n-1} \ldots a_1 \cdot 10 + a_0$?

c) Quando podemos garantir que um número $a = a_n a_{n-1} \ldots a_1 a_0$ é divisível por 2?

6.2.2 Critério de Divisibilidade por 4

Consideremos o exemplo:

Exemplo 2: Mostre que 2432 é divisível por 4.

Solução: Notemos que:

$$\begin{aligned} 2432 &= 2400 + 32 \\ &= 24 \cdot 100 + 32 \\ &= 24 \cdot 25 \cdot 4 + 32 \end{aligned}$$

Observemos que $2400 = 24 \cdot 25 \cdot 4 = 600 \cdot 4$, é divisível por 4. Assim, como 4 divide 32, então 4 divide $(2400 + 32) = 2432$.

Exercício 1: Como no exemplo anterior, verifique se 4 divide:

a) 7356

b) 4828

Exercício 2: Considere o número $a = a_n a_{n-1} \ldots a_1 a_0$.

a) Mostre que: 4 divide $a - a_1 a_0 = a_n a_{n-1} \ldots a_2 \cdot 100$. (Dica: faça como nos exemplos anteriores)

b) Em qual condição 4 divide $a = a_n a_{n-1} \ldots a_2 \cdot 100 + a_1 a_0$?

c) Quando podemos garantir que um número $a = a_n a_{n-1} \ldots a_1 a_0$ é divisível por 4?

6.2.3 Critério de Divisibilidade por 8

Vamos agora analisar um novo exemplo:

Exemplo 3: Verifique se 15128 é divisível por 8.

Solução: Note que:

$$\begin{aligned} 15128 &= 15000 + 128 \\ &= 15 \cdot 1000 + 128 \\ &= 15 \cdot 125 \cdot 8 + 128 \end{aligned}$$

Observe que $15000 = 15 \cdot 125 \cdot 8 = 1875 \cdot 8$, que é divisível por 8. Além disso, 128 também é divisível por 8. Portanto, 8 divide $(15000 + 128) = 15128$.

Exercício 1: Usando o método acima, verifique se 8 divide:

a) 245064

b) 234114

Exercício 2: Considere o número $a = a_n a_{n-1} \ldots a_1 a_0$.

a) Mostre que: 8 divide $a - a_2 a_1 a_0 = a_n a_{n-1} \ldots a_3 \cdot 1000$. (Dica: faça como nos exemplos anteriores)

b) Em qual condição 8 divide $a = a_n a_{n-1} \ldots a_3 \cdot 1000 + a_2 a_1 a_0$?

c) Quando podemos afirmar que um número $a = a_n a_{n-1} \ldots a_1 a_0$ é divisível por 8?

6.3 Critérios de Divisibilidade por 5 e por 10

6.3.1 Critério de Divisibilidade por 5

Observemos, inicialmente, que de 0 a 9, 5 divide apenas 0 e 5. Vamos utilizar este fato no seguinte exemplo:

Exemplo: Verifique se 5 divide 2345. Notemos que:

$$\begin{aligned} 2345 &= 2340 + 5 \\ &= 234 \cdot 10 + 5 \\ &= 234 \cdot 2 \cdot 5 + 5 \end{aligned}$$

Como 5 divide $2340 = 234 \cdot 2 \cdot 5 = 468 \cdot 5$ e 5 divide 5, concluímos que 5 divide $2345 = 2340 + 5$.

Exercício 1: Utilize o método acima para verificar se são divisíveis por 5:

a) 3460

b) 6543

Exercício 2: Considere o número $a = a_n a_{n-1} \ldots a_1 a_0$.

a) Mostre que 5 divide $a - a_0 = a_n a_{n-1} \dots a_1 \cdot 10$.

b) Quando podemos dizer que 5 divide $a = a_n a_{n-1} \dots a_1 \cdot 10 + a_0$? Justifique!

c) Utilize o exercício acima para enunciar o critério de divisibilidade por 5.

6.3.2 Critério de Divisibilidade por 10

Vamos observar inicialmente que, de 0 a 9, 10 divide apenas 0. Utilizaremos este fato no seguinte exemplo:

Exemplo: Verifique se 10 divide 3450. Notemos que:

$$\begin{aligned} 3450 &= 3450 + 0 \\ &= 345 \cdot 10 + 0 \end{aligned}$$

Como 10 divide $3450 = 345 \cdot 10$ e 10 divide 0, concluímos que 10 divide $3450 = 345 \cdot 10 + 0$.

Exercício 1: Utilize o método acima para verificar se são divisíveis por 10:

a) 6720

b) 1234

Exercício 2: Considere o número $a = a_n a_{n-1} \dots a_1 a_0$.

a) Mostre que 10 divide $a - a_0$.

b) Quando podemos dizer que 10 divide $a = a_n a_{n-1} \dots a_1 \cdot 10 + a_0$? Justifique!

c) Utilize o exercício acima para enunciar o critério de divisibilidade por 10.

6.4 Critérios de Divisibilidade por 3 e por 9

6.4.1 Critério de Divisibilidade por 3

Observemos inicialmente que:

$$10-1=9=3\cdot 3,$$

$$100-1=99=3\cdot 33,$$

$$1000-1=999=3\cdot 333.$$

É possível mostrar que:

$$10^n-1=\underbrace{9\ldots 9}_{\text{n noves}}=3\cdot\underbrace{3\ldots 3}_{\text{n três}}.$$

Vamos utilizar esta ideia para verificar se o número 231 é divisível por 3.

Exemplo 2: Verifique se 231 é divisível por 3.

Solução: Notemos que:

$$\begin{aligned}231&=2\cdot 100+3\cdot 10+1\\&=2\cdot(99+1)+3\cdot(9+1)+1\\&=2\cdot 99+2+3\cdot 9+3+1\\&=(2\cdot 99+3\cdot 9)+(2+3+1)\end{aligned}$$

Sabemos que 3 divide $2\cdot 99+3\cdot 9$, pois divide 99 e 9 (verifique!). Agora, basta perceber que 3 divide $2+3+1=6$. Assim, concluímos que 3 divide 231.

Exercício 1: Usando o raciocínio anterior, verifique se 3 divide os números:

a) 345

b) 451

Exercício 2: Considere o número $a=a_n\cdot 10^n+\ldots+a_2\cdot 10^2+a_1\cdot 10+a_0$.

a) Verifique que $a=a_n(10^n-1)+\cdots+a_2\cdot(10^2-1)+a_1\cdot(10-1)+(a_n+\ldots+a_2+a_1+a_0)$.

b) 3 divide $a_n(10^n-1)+\cdots+a_2\cdot(10^2-1)+a_1\cdot(10-1)$? Justifique!

c) Quando podemos ter certeza de que 3 divide a?

6.4.2 Critério de Divisibilidade por 9

Observemos inicialmente que:

$$10-1=9=9\cdot 1,$$

$$100-1=99=9\cdot 11,$$

$$1000-1=999=9\cdot 111.$$

É possível mostrar que:

$$10^n-1=\underbrace{9\ldots 9}_{\text{n noves}}=9\cdot\underbrace{1\ldots 1}_{\text{n uns}}.$$

Vamos utilizar esta ideia para verificar se o número 342 é divisível por 9.

Exemplo 2: Verifique se 342 é divisível por 9.

Solução: Notemos que:

$$\begin{aligned}342&=3\cdot 100+4\cdot 10+2\\&=3\cdot(99+1)+4\cdot(9+1)+2\\&=3\cdot 99+3+4\cdot 9+4+2\\&=(3\cdot 99+4\cdot 9)+(3+4+2)\end{aligned}$$

Sabemos que 9 divide $3\cdot 99+4\cdot 9$, pois divide 99 e 9 (verifique!). Agora, basta perceber que 9 divide $3+4+2=9$. Assim, concluímos que 9 divide 342.

Exercício 1: Usando o raciocínio anterior, verifique se 9 divide os números:

a) 567

b) 736

Exercício 2: Considere o número $a=a_n\cdot 10^n+\ldots+a_2\cdot 10^2+a_1\cdot 10+a_0$.

a) Verifique que $a=a_n(10^n-1)+\cdots+a_2\cdot(10^2-1)+a_1\cdot(10-1)+(a_n+\ldots+a_2+a_1+a_0)$.

b) 9 divide $a_n(10^n - 1) + \cdots + a_2 \cdot (10^2 - 1) + a_1 \cdot (10 - 1)$? Justifique!

c) Quando podemos ter certeza de que 9 divide a?

CAPÍTULO 7

Considerações Finais

Neste trabalho, buscamos demonstrar os principais critérios de divisibilidade, utilizando conceitos de divisibilidade, a notação decimal de um número natural e a aritmética modular. Discutimos sobre sistemas de numeração e apresentamos o sistema de numeração decimal, que foi utilizado nas demonstrações propostas.

Além disso, exploramos a aritmética dos restos e uma de suas mais importantes aplicações: o Teorema Chinês dos Restos. Utilizamos a aritmética modular nas demonstrações de divisibilidade, que se mostrou prática para a obtenção dos resultados desejados.

Propomos também uma sequência de atividades com o objetivo de induzir os estudantes a compreender as demonstrações dos principais critérios de divisibilidade, de modo que o professor possa apresentá-los aos alunos de forma que estes possam acompanhar, compreender e, eventualmente, reproduzir tais demonstrações. Essas demonstrações são abordadas após a verificação de casos particulares pelos estudantes, permitindo que, gradativamente, eles consigam formular a prova para o caso geral.

As atividades apresentadas buscam atrelar aos critérios de divisibilidade o rigor por trás desses importantes resultados, que são pouco abordados em sala de aula. Além disso, exploramos a utilização do sistema de numeração decimal para a compreensão desses critérios, ressaltando sua importância na demonstração e verificação de diversas operações matemáticas envolvendo números naturais e inteiros.

Referências Bibliográficas

[1] EVES, Howard Whitley. ***Introdução à história da matemática***. Unicamp, 2011 (citado na página 1).

[2] GONÇALVES, A. ***Introdução à Álgebra***. 6ª. Rio de Janeiro: IMPA, 2017 (citado nas páginas 26, 30, 33).

[3] HARDY, G. H. e WRIGHT, E. M. ***An Introduction to the Theory of Numbers***. Sixth. Oxford University Press, 2008 (citado nas páginas 26, 34).

[4] HEFEZ, Abramo. ***Aritmética***. 3ª ed. Vol. 1. SBM, 2022 (citado nas páginas 3, 23).

[5] HEFEZ, Abramo. ***Elementos de aritmética***. Sociedade Brasileira de Matemática, 2006 (citado na página 1).

[6] HEFEZ, Abramo. "**Iniciação à aritmética**". Em: ***Sociedade Brasileira de Matemática*** (2009) (citado na página 53).

[7] MAIER, Rudolf R. ***Teoria dos Números - Texto de Aula***. https://mat.unb.br/maierr/tnotas.pdf. Versão atualizada. 2005 (citado nas páginas 26, 34).

[8] PERETTI, Lisiane e TONIN DA COSTA, Gisele Maria. "**Sequência didática na matemática**". Em: ***Revista de Educação do IDEAU*** 8.17 (2013), pp. 1–14 (citado na página 2).

[9] ZABALA, Antoni. ***A Prática Educativa: como ensinar***. Porto Alegre: Artmed, 1998 (citado na página 2).